Seguridad para tod@s en la Sociedad de la Información

CSIRT-CV

con la colaboración de

S2 Grupo, Área de Seguridad

GENERALITAT VALENCIANA

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

S2 GRUPO

COLEGIO OFICIAL DE INGENIEROS EN INFORMÁTICA DE LA COMUNIDAD VALENCIANA

ADCV
Agenda Digital de la Comunitat Valenciana

Seguridad para todos en la Sociedad de la Información

Editado por Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana (COIICV)

CIF: V-97046189

Datos de contacto:

Av. Barón de Carcer 48, 3ºO. 46001 – Valencia

963622994 – secretaria@coiicv.org

www.coiicv.org

ISBN: 978-84-697-0351-9

Primera edición: Mayo 2014

ÍNDICE

PRESENTACIÓN

Juan Carlos Moragues Ferrer
CONSELLER DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un elemento clave en nuestra vida cotidiana. Acciones tales como enviar un correo electrónico, consultar información en Internet o conectarnos a una red social desde nuestro teléfono móvil son tan habituales que, seguramente, ninguno de nosotros puede imaginar ya su día a día sin ellas.

Estas tecnologías introducen enormes avances que hacen más cómoda y fácil nuestra actividad diaria, aunque también cuentan con ciertas características que actúan como barreras a la generalización de su uso en todos los ámbitos.

Sin embargo, el conocimiento de las prácticas más seguras para el uso de las TIC reduce el impacto de estos riesgos y contribuye a crear una sociedad capaz de aprovechar todo el potencial que ofrecen estas tecnologías para el desarrollo económico y social en el marco de la sociedad digital.

La Agenda Digital de la Comunitat Valenciana cuenta, entre sus prioridades estratégicas, con el objetivo de impulsar la seguridad y la confianza en la red mediante una intensa actividad de concienciación dirigida a fomentar el uso seguro de las TIC.

En este contexto se enmarcan iniciativas como el presente libro, Seguridad para tod@s en la Sociedad de la Información, que son un ejemplo del esfuerzo por desarrollar en la Comunitat una cultura sólida de la ciberseguridad entre la ciudadanía, las empresas y las Administraciones Públicas.

Este trabajo monográfico ha sido elaborado por el Centro de Seguridad TIC de la Comunitat Valenciana (CSIRT-CV) de la Generalitat, con la colaboración del Colegio Oficial de Ingenieros en Informática de la Comunitat Valenciana y la empresa S2 Grupo, líder nacional del sector de la seguridad de la información.

A lo largo de sus trece capítulos, el libro proporciona ejemplos de buenas prácticas, así como los conocimientos necesarios para el uso de los distintos medios tecnológicos. La finalidad es que los ciudadanos puedan llegar a identificar y sortear las principales amenazas presentes en Internet y que desarrollen capacidades que les permitan disfrutar de forma segura del amplio abanico de posibilidades que ofrecen las TIC.

Esperamos que estas páginas contribuyan a cultivar esa cultura de la ciberseguridad en la Comunitat Valenciana y que, entre todos, podamos crear un ciberespacio más seguro y confiable para nuestro futuro.

Valencia, mayo de 2014

Juan Pablo Peñarrubia Carrión
PRESIDENTE
Colegio Oficial de Ingenieros en Informática
de la Comunidad Valenciana (COIICV)

La informática es la materia prima de esta nueva era que se ha dado en llamar "Sociedad de la Información y el Conocimiento". Estamos asistiendo desde hace dos décadas a una penetración creciente y progresiva de la informática en todas las actividades individuales y en las organizaciones, tanto a nivel personal como social en general.

Desde el Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana (COIICV) hemos iniciado una línea de edición de monografías, para incrementar el conocimiento de temas específicos en el ámbito de la informática, tanto a nivel profesional como a nivel de divulgación en general, especialmente de materias de actualidad, como es el caso de la monografía "Seguridad para todos en la Sociedad de la Información".

Es bien sabido que toda tecnología lleva asociada la necesidad de gestionar su utilización segura. También la ingeniería informática está sujeta a esta regla, con la complejidad añadida de la velocidad de cambio e innovación continua que experimenta. En este contexto es igualmente importante abordar acciones proactivas no solo en el ámbito de la propia ingeniería informática construyendo soluciones sólidas desde el punto de vista profesional, sino también en el ámbito de la divulgación y formación para generar una cultura de la seguridad informática que resulta imprescindible en la sociedad actual.

La labor de divulgación debe formar parte de la contribución al interés general que las organizaciones profesionales debemos hacer a la sociedad, en este caso en el ámbito del aprovechamiento de la potencia, la productividad y las facilidades que ofrece la informática para mejorar nuestro día a día, pero de modo seguro. Este es en definitiva el objetivo final de esta monografía, en la que el lector encontrará una explicación sencilla y amena sobre el uso seguro de productos y servicios tan generalizados como la navegación por internet, el correo electrónico, las compras online, las redes sociales, los dispositivos fijos y móviles, los juegos, los menores en internet, etc.

A pesar de los enormes esfuerzos y avances de los profesionales de la ingeniería informática para mejorar la facilidad de uso de los dispositivos, aplicaciones y servicios informáticos, su ingente cantidad tanto a nivel personal como general, y sobre todo su gran velocidad de cambio hacen muy complejo para el ciudadano de a pie su adecuado conocimiento y su utilización segura. La seguridad tiene un factor común a todos los ámbitos y tecnologías: las personas. En todos los ámbitos la gestión de la seguridad tiene como elemento central la importancia de la creación entre las personas de un cierto sentido común de la seguridad, la creación de inercias de comportamientos seguros, en definitiva de una cultura de la seguridad. En este caso de la seguridad informática o como se está dando en llamar de la ciberseguridad.

Esperamos que esta colaboración de la Generalitat a través del Centro de Seguridad TIC de la Comunidad Valenciana (CSIRT-CV), la empresa S2 Grupo y el COIICV, editada con motivo del Día de Internet 2014, sea de interés para los ciudadanos y organizaciones y les ayude a mejorar el uso seguro de los productos y servicios informáticos.

Valencia, mayo de 2014

José Miguel Rosell Tejada
SOCIO DIRECTOR DE S2 Grupo

Con demasiada frecuencia, a la hora de hablar de seguridad de los sistemas de información, seguridad de la información o sencillamente de seguridad, todos nos ponemos en el lado más negativo posible: todo lo malo que nos puede pasar por usar un ordenador, un cajero automático o realizar una compra por Internet; como en cualquier aspecto de nuestra vida, las nuevas tecnologías aportan un sinfín de ventajas, y algún que otro inconveniente que por supuesto debemos conocer para poder evitarlo o minimizarlo. En este sentido, en el presente trabajo hemos tratado de ser positivos, no centrarnos exclusivamente en los problemas de seguridad existentes en diferentes ámbitos tecnológicos, sino aportar además soluciones a estos problemas o cuanto menos directrices que nos permitan mitigar el riesgo asociado y, al mismo tiempo, poder seguir trabajando de forma cómoda y aprovechando las indiscutibles ventajas de la tecnología.

Con este enfoque positivo en mente, sin duda el poder transmitir a los ciudadanos la importancia de la seguridad en el uso cotidiano de nuevas tecnologías es a la vez un reto y una obligación. Un reto, porque los que trabajamos en nuestro día a día con sistemas de información, grandes problemas de seguridad y complejos entornos de vigilancia, con miles o millones de datos a procesar, muchas veces no nos damos cuenta de que los problemas que afectan al usuario de a pie son casi siempre más sencillos –pero no por ello menos importantes- y nos cuesta mucho olvidar nuestra complejidad y nuestras ininteligibles siglas (en definitiva, nuestro día a día) para acercarnos a ellos desde un punto de vista claro y conciso, que no asuste y que consiga, en definitiva, ayudar al usuario a la hora de realizar una compra por Internet, de navegar o de gestionar su correo electrónico. Justamente de eso se trata: de ser útiles.

Como decía, aparte del reto que supone para las personas técnicas olvidarse de la complejidad de su trabajo para lograr ser realmente útiles a los ciudadanos, es también para nosotros una obligación hacerlo. Una obligación porque inculcar el conocimiento, la precaución y el sentido común en el ámbito de la seguridad a colectivos que no tienen por qué poseer grandes conocimientos técnicos, es sembrar las semillas de lo que se viene a denominar la cultura de seguridad: el conseguir que todo el mundo, en cualquier ámbito, incorpore como rutina una visión de seguridad que en muchos casos se echa de menos en nuestros días. Y esa cultura de seguridad es desde luego obligatoria en cualquier sociedad moderna, e incluso en España viene marcada como una de las líneas principales de trabajo de la Estrategia Española de Ciberseguridad, recientemente publicada.

Poder aportar nuestro granito de arena a esta gigantesca tarea es sin duda reconfortante; confiamos en que el trabajo que desde S2 Grupo, junto al equipo de CSIRT-cv y con el apoyo del Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana, hemos realizado, sirva para que todos aprendamos a utilizar las nuevas tecnologías de forma segura y con sentido común, a que obtengamos el máximo rendimiento de ellas y, sobre todo, a que no tengamos problemas graves de seguridad en nuestro día a día tecnológico. Con ese objetivo hemos realizado esta publicación, que esperamos sea de utilidad para todos.

Valencia, mayo de 2014

2

SEGURIDAD GLOBAL

1 Introducción

El incremento exponencial del uso de las nuevas tecnologías en nuestras vidas, y la cada vez mayor dependencia de los sistemas de información que todos tenemos, motivan que la **Seguridad de la Información** tenga un papel básico en nuestro día a día. En la actualidad, nadie cuestiona la importancia de la **disponibilidad** de los sistemas de información, ni de la **integridad** y **confidencialidad** de los datos que éstos gestionan. No tenemos más que pensar en las actividades que a diario desarrollamos conectados a la red, desde consultas o movimientos bancarios, hasta la compartición de información por múltiples canales (páginas web, P2P, telefonía...) o incluso relaciones personales y profesionales -nuestras y de los nuestros- en redes sociales como Facebook, Tuenti o LinkedIn. Por supuesto, al igual que en nuestro entorno "real" nos preocupa la seguridad, debe ***preocuparnos***[1] en el entorno virtual que, cada vez con mayor frecuencia, todos utilizamos.

Al hablar de seguridad, son tres los pilares sobre los que se basa ésta:

- **Disponibilidad:** debemos tener garantías de que la información va a estar disponible en el momento en que se necesita.

- **Integridad:** debemos tener garantías de que la información es exacta, y de que está protegida frente a alteraciones o pérdidas.

- **Confidencialidad:** debemos tener garantías de que sólo las personas autorizadas disponen de acceso a la información.

Obviamente, garantizar la seguridad de la información es un aspecto crítico para todos nosotros y para las organizaciones que nos prestan servicios (empresas, administraciones públicas, etc.), sin importar su tamaño o su sector de actividad; esta importancia de la seguridad es especialmente relevante en aquellos entornos en los que se manejan datos especialmente protegidos por leyes como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD): información económica, de salud, etc. Así, la seguridad de la información no es sólo un tema técnico, sino también un tema legal, con aspectos perfectamente regulados y que, más allá de decisiones, concienciaciones o preferencias particulares, todos estamos obligados a cumplir.

2 La importancia de la seguridad

Sin duda, todos estamos de acuerdo en que la seguridad es muy importante en nuestras vidas.Ya en 1943, ***Abraham Maslow***[2] en su obra "Una teoría sobre la motivación humana" ("A Theory of Human Motivation"), formula una teoría sobre la jerarquía de las necesidades humanas y defiende que conforme se satisfacen

1 Accesible en http://www.csirtcv.gva.es/es/paginas/uso-indebido-de-datos-en-la-red.html
2 Accesible en http://es.wikipedia.org/wiki/Abraham_Maslow

las necesidades más básicas, los seres humanos desarrollan necesidades y deseos más elevados. Así, según Maslow, en la jerarquía propuesta, las necesidades más altas ocupan nuestra atención sólo cuando se han satisfecho las necesidades inferiores de la pirámide. La seguridad aparecía en el segundo escalón, justo por encima de las necesidades básicas para sobrevivir; la lectura es sencilla: lo que necesitamos, una vez sobrevivimos, es tranquilidad.

Abandonemos por un instante nuestra vida "digital" y pensemos en la vida "real" de todos nosotros, sin darnos cuenta, le estamos dando un papel fundamental a la seguridad; nadie cruza una calle sin mirar, evitamos pasear a determinadas horas por determinadas zonas, no dejamos a nuestros hijos solos en la calle... Ésto, que a todos nos parece obvio, debemos trasladarlo al mundo digital, donde las cosas a veces no son tan directas. Si no se nos ocurriría aceptar medicinas de un desconocido en plena calle... ¿por qué las vamos a aceptar de ese mismo desconocido pero a través del correo electrónico? Si no dejamos a nuestros hijos abandonados a su suerte, ¿por qué les dejamos conectarse libremente a Internet mientras nosotros descansamos? Debemos contemplar Internet como un entorno con peligros y virtudes similares al mundo real, donde podemos encontrar excelentes amigos, debates o puntos de encuentro, pero también asesinos, violadores o ladrones. Seguridad debe ser sinónimo de tranquilidad, y para nosotros utilizar las nuevas tecnologías debe suponer un avance, no una amenaza a nuestra seguridad ni a la de los que nos rodean.

3 Falsos mitos de la seguridad

Al hablar de seguridad para el usuario o para el ciudadano -no estamos hablando ahora de seguridad en grandes compañías, con complejos sistemas tecnológicos, análisis de riesgos, revisiones anuales...etc- siempre surgen falsos mitos que debemos romper, ya que la seguridad a título individual suele ser menospreciada frente a la seguridad de las grandes corporaciones. Obviamente, para un atacante tendrá mucho más interés la información financiera de un banco o caja de ahorros online, que nuestras fotos del fin de semana con los amigos, y por tanto esa entidad financiera deberá adoptar unas medidas de seguridad mucho más duras que las nuestras. Pero es falso que nuestras fotos no le interesen a nadie, y ese es uno de los ***grandes mitos a romper***[3] como los que os mostramos a continuación:

Mi sistema no es interesante para nadie

FALSO. Está claro que un sistema particular no es tan atractivo para una mafia organizada que los sistemas bancarios o de control energético de un país. Esto es obvio, pero también es cierto que en un sistema particular encontramos un objetivo de ataques no dirigidos, es decir, aquellos que no persiguen un objetivo concreto, sino que basan su efectividad en lograr múltiples objetivos para luego utilizarlos a su favor. Un ejemplo: las redes zombie están formadas por miles de máquinas de usuarios conectados a líneas domésticas que, sin saberlo, atacan a terceros o son la base de estafas online. Además, nuestro sistema es el que

3 Accesible en http://www.securityartwork.es/2011/08/29/%C2%BFciberque-%C2%BFciberataque-eso-no-me-puede-pasar-a-mi/

utilizamos para acceder a nuestras cuentas bancarias, por poner sólo un ejemplo más. Parece claro que los ordenadores domésticos son un objetivo para atacantes, y si a eso le añadimos que las medidas de seguridad que utilizamos en nuestros hogares son muy inferiores a las que usan las grandes corporaciones, resultará más fácil para una mafia organizada lograr tomar el control de nuestro equipo que hacerlo de los sistemas de una gran multinacional.

Como tengo antivirus/actualizaciones/cortafuegos... estoy a salvo

FALSO. Las medidas de protección -muchas de las cuales veremos en este curso- son necesarias pero no garantizan la inmunidad frente a cualquier amenaza, de la misma forma que llevar abrochado el cinturón de seguridad, disponer de un vehículo con airbag o respetar las normas de circulación, no garantiza que no podamos tener un accidente. A pesar de todas las salvaguardas técnicas que utilicemos, no debemos confiarnos jamás.

Eso sólo pasa en las películas...

FALSO. Los delitos relacionados con nuevas tecnologías son cada día más habituales (y si no estamos convencidos podemos preguntar a las unidades especializadas del Cuerpo Nacional de Policía o de la Guardia Civil). Dejemos de pensar en protagonistas de ***películas***[4] de hackers con final feliz, y pensemos en mafias organizadas, en criminales... o en el vecino de al lado que quiere aprovechar nuestra conexión a Internet. A diario, millones de ataques son realizados desde cualquier lugar del mundo, y es simplemente una cuestión de tiempo que uno de los objetivos de estos ataques seamos nosotros.

Uso Linux, estoy a salvo

FALSO. Unix o Linux son sistemas operativos más alejados del estándar de entorno doméstico que Windows, y no se ven tan afectados por el malware más habitual de estos entornos (virus, troyanos,etc.). No obstante, existen multitud de vulnerabilidades en Linux que un atacante, ya sea un programa o una persona, puede aprovechar en beneficio propio, con un problema añadido: generalmente, el usuario medio no conoce en profundidad el entorno, menos amigable que Windows, con lo que puede no ser consciente de los riesgos a los que está expuesto.

4 Protección

A vista de lo expuesto con anterioridad, parece claro que en el uso de las nuevas tecnologías, particularmente de Internet, debemos adoptar medidas de protección que garanticen la integridad, confidencialidad y disponibilidad de nuestros datos, de la misma forma que nos protegemos cuando paseamos por la ciudad o conducimos un vehículo. Ojo, no se trata de tener en nuestros hogares un sistema de seguridad militar -al igual que no caminamos con ocho escoltas a nuestro alrededor-, sino simplemente de disponer de unas medidas mínimas que nos garanticen tranquilidad, y también de usar el sentido común en el uso de las nuevas tecnologías.

4 Accesible en http://www.securityartwork.es/2010/11/08/las-pifias-de-%E2%80%9Chollywood%E2%80%9D/

Actualmente, existen a nuestra disposición múltiples medidas de seguridad que, como hemos dicho, no nos convertirán en infalibles, pero nos ayudarán a dormir más tranquilos en lo que a nuestra seguridad digital respecta. Vamos a repasar aquí las que consideramos más importantes para el ***usuario de a pie***[5], aquel que no tiene por qué ser un experto en tecnología ni en seguridad pero, como todo el mundo, desea una tranquilidad relativa en el uso de las nuevas tecnologías. En diferentes capítulos de este curso se profundiza en estos aspectos, pero los presentamos aquí a modo de resumen:

Sistemas actualizados: parches

Mantener el sistema actualizado es crítico para garantizar su seguridad. Instalar regularmente los parches que los diferentes fabricantes o proveedores de sistemas (Windows, Linux, Solaris...) proporcionan es una buena práctica que no debemos descuidar, ya que a diario surgen programas (virus, gusanos...) que aprovechan las ***vulnerabilidades***[6] que estos parches corrigen, y que pueden comprometer la seguridad de nuestros equipos.

Descargas de software no confiables

Debemos tener mucha precaución a la hora de ejecutar programas o tratar archivos (PPT, PDF...) que no provengan de fuentes confiables. La descarga de programas en sistemas P2P, aparte de los problemas legales que nos pueden acarrear, puede ser una fuente de problemas técnicos, como virus o troyanos, para nuestros sistemas, por lo que se recomienda utilizar únicamente software y archivos procedentes de fuentes de confianza.

Cortafuegos

Habilitar el cortafuegos personal en nuestros equipos es otra de las formas más importantes para evitar problemas; todos los entornos operativos, como Windows o Linux, incorporan, de una u otra manera, cortafuegos "de serie" en el sistema, cortafuegos que evitan en muchos casos el acceso desde Internet a nuestros equipos por parte de programas o atacantes y que, bien utilizados, nos permiten estar protegidos frente a algunas de las amenazas más comunes en la red.

Privacidad

Es cada vez más habitual el uso de redes sociales (Facebook, Tuenti,Twitter...), chats, foros, páginas de intercambio de imágenes... sistemas que, en definitiva, nos facilitan el intercambio de información personal con amigos o conocidos. No obstante, debemos tener especial cuidado con qué información publicamos en estos foros, ya que poner a disposición de desconocidos ciertos datos de nuestra vida personal (lugares que frecuentamos, horas de entrada y salida al trabajo o al estudio, direcciones...) puede poner en peligro no sólo nuestra información o nuestros equipos, sino también nuestra propia integridad física. Si un atacante conoce dónde vivimos, a qué horas entramos y salimos de casa, a qué lugares acudimos de forma habitual... tiene una información muy valiosa de cara a cometer delitos contra nuestros bienes o nuestra propia persona.

---

5 Accesible en http://www.securityartwork.es/2011/02/23/el-eslabon-mas-debil/
6 Accesible en http://www.csirtcv.gva.es/es/paginas/alertas.html

Banca online

Hoy en día, casi todos nosotros utilizamos la red para realizar las transacciones bancarias que hasta hace unos años sólo podíamos ejecutar presencialmente en una sucursal. Esto ha motivado que atacantes, tanto individuales como organizados en mafias, tengan en la banca online una fuente de ingresos muy interesante para ellos y con un nivel de riesgo muy bajo; el beneficio que pueden obtener de un ***phishing***[7] sin arriesgarse a ser capturados, es ***mucho mayor***[8] que el que puede proporcionar un atraco. Así, debemos extremar las precauciones a la hora de utilizar la banca online y estar especialmente atentos a páginas no cifradas -o cifradas con certificados que no sean del propio banco-, así como a correos que podamos recibir indicándonos que facilitemos nuestros datos de acceso. Ninguna entidad le pedirá sus datos a través de internet, por lo que estos correos debemos por supuesto ignorarlos y borrarlos cuanto antes.

Correo electrónico

El correo electrónico, en especial los webmails más habituales (Hotmail, Gmail...), es sin duda uno de los elementos más utilizados por todos nosotros a diario, pero también una de las mayores fuentes de problemas con la que nos encontramos. Por correo electrónico nos llega desde spam (correo no deseado, generalmente con publicidad) hasta ataques de phishing o incluso virus. A pesar de que todos los proveedores de correo suelen incorporar salvaguardas para evitar que estos e-mails lleguen a nuestro buzón, es imposible que al final no se nos cuele alguno, por lo que ***debemos evitar***[9] caer en las trampas de estos correos (nadie regala dinero en Internet, ni Viagra, ni nada parecido). A ésto hay que añadir que el correo, salvo que se utilice firma digital -lamentablemente, no muy habitual todavía-, es una fuente no confiable, y es muy fácil suplantar la entidad del emisor de forma transparente a quien recibe el correo. Así, es trivial para un atacante enviarnos un virus, un troyano, o un spam, simulando ser un amigo o conocido, sencillamente falsificando la dirección de correo origen del e-mail.

WiFi

Seguramente todos nosotros tenemos una red WiFi en nuestras casas, red que en caso de no estar correctamente protegida puede ser también una fuente de problemas. Por un lado, si alguien consigue utilizar de forma no autorizada nuestra red, seguramente habrá dado un paso muy importante hacia el acceso a nuestra información, y podrá antes o después, tomar el control de nuestro equipo y ver la información que tenemos en él. Pero, casi peor todavía, puede utilizar nuestra red para atacar a un tercero, y a todos los efectos el ataque será originado desde nuestra dirección IP y por tanto a quién primero buscarán como culpable del mismo será a nosotros. Así, debemos utilizar un cifrado robusto en la WiFi de casa (WPA2 es lo recomendable), cambiar la contraseña periódicamente, no publicar el SSID, y todas las medidas que veremos en el capítulo correspondiente del presente curso. Aunque aplicando estas salvaguardas no se garantiza la inmunidad, si un atacante encuentra dificultades para entrar en nuestra red seguramente nos dejará en paz e irá a buscar otra WiFi menos protegida.

---

7 Accesible en http://es.wikipedia.org/wiki/Phishing
8 Accesible en http://www.securityartwork.es/2011/02/01/mercado-negro-del-cibercrimen/
9 Accesible en https://www.facebook.com/note.php?note_id=146070748776981

3

MALWARE

1 Introducción al malware

Se conoce como **malware (del inglés malicious software, también llamado badware, software malicioso o software malintencionado)** todo aquel software que realiza cualquier acción malintencionada (desde capturar contraseñas a mostrar publicidad) sin el consentimiento del usuario. Los objetivos del malware actualmente son muy variados, pero entre ellos destacamos siempre la obtención de información sensible, el daño a la máquina donde se encuentra instalado el software o la ejecución de estafas online, por poner unos ejemplos.

La evolución del malware ha sufrido un cambio a lo largo de los últimos años en los que ha pasado de ser software creado a título individual o por un pequeño grupo de piratas informáticos con fines reivindicativos, egocéntricos o de simple satisfacción personal, a ser producido por mafias organizadas (ciberdelincuencia) cuyo único fin es el lucro económico. Debido a estos nuevos fines, en estos años se han generado diversos tipos de malware nuevo para lograr el objetivo de estas mafias: ganar dinero. Estos nuevos tipos de malware cada día están más perfeccionados y son más abundantes en la red, razón por la cual existen más programas nocivos y cada vez más peligrosos.

El problema para combatir este tipo de ciberdelincuencia reside en que las personas u organizaciones que lo desarrollan operan desde países que no contemplan en sus leyes acciones penales contra estos delitos por lo que éstos no pueden ser juzgados y quedan finalmente impunes. Aquí disponen de una serie de enlaces a ***Vídeos***[10] de distinto tipos de infecciones.

A continuación, dentro de este capítulo, exponemos los principales tipos de malware existentes en la actualidad, así como una serie de consejos importantes para no convertirnos en víctimas de estos programas maliciosos.

2 Tipos de malware

Dentro de los distintos tipos de malware que existen en la actualidad queremos destacar en este punto los más comunes, para poder entender cómo funcionan y así tomar las medidas preventivas que nos permitan evitar que un software malicioso pueda infectar nuestra máquina.

10 Accesible en http://www.eset-la.com/centro-amenazas/videos-educativos

2.1 Virus

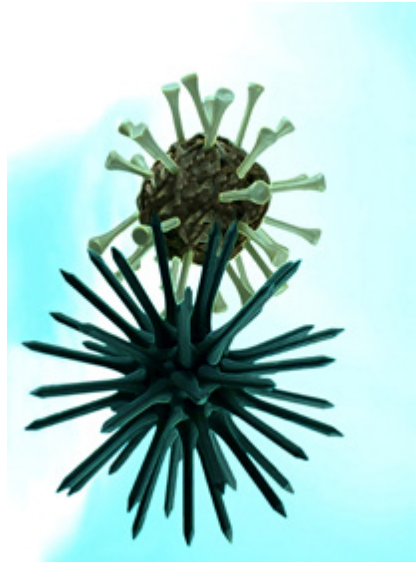


Ilustración 1 · Virus

Los virus informáticos es el tipo de malware más conocido. Se trata de programas que se reproducen infectando a otros ficheros e intentando que esos ficheros sean accedidos en otro entorno para que éste también sea infectado. Los virus pueden ser desde cómicos o bromistas hasta programas destructivos.

Pese a que existen un gran número de tipos de virus, principalmente se pueden clasificar en tres grandes familias:

- Aquellos que se encargan de dañar el arranque de una máquina impidiendo que ésta pueda iniciarse correctamente. Su objetivo es puramente destructivo.

- Aquellos que residen en la memoria de la máquina y son capaces de funcionar en segundo plano sin que el usuario conozca la existencia de dicho virus.

- Por último, y no por ello menos peligrosos, existen los virus de macros o script, que suelen aprovechar la capacidad de ejecutar diferentes lenguajes de programación de algunos de los visores de documentos más utilizados: XLS (Excel), DOC (Word), PPS (PowerPoint), PDF (Acrobat Reader), etc, para infectar el equipo.

En la actualidad, la principal fuente de peligro se produce cuando los virus están encubiertos en ficheros facilitados por personas conocidas, ya sea por correo electrónico, pendrives o cualquier otro medio de transmisión de datos entre usuarios. Por ejemplo, un compañero puede enviarnos un correo electrónico con un documento malicioso, sin ninguna mala intención -ya que desconoce que el documento está contaminado-, y al abrirlo en nuestro equipo nos contaminaremos nosotros y repetiremos el proceso, sin saberlo, de enviar el documento contaminado a otras personas, infectando al resto de usuarios de la red. El envío de "correos cadena", que suelen ser de humor o curiosidades que se envían mediante ficheros adjuntos de PowerPoint, supone un peligro potencial muy considerable, ya que muchos de estos ficheros están infectados

con algún tipo de malware y la propagación de los mismos únicamente depende del usuario.

2.2 Gusanos

Un gusano (también llamados IWorm por su apócope en inglés, I de Internet, WormWorm de gusano) es un malware que tiene la propiedad de replicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Son una evolución de los virus y uno de los más extendidos en la actualidad, con detalles técnicos que los diferencian de estos últimos. Su objetivo es infectar un ordenador y extenderse a otras máquinas de forma activa. Los gusanos, a diferencia de los tradicionales virus, se propagan por la red atacando distintas vulnerabilidades conocidas o utilizando ingeniería social para engañar al usuario.

No precisan alterar programas, sino que modifican parámetros del sistema para ejecutarse al inicio. Los gusanos casi siempre causan problemas en la red (ralentizándola), mientras que los virus siempre infectan o corrompen los archivos de la máquina que atacan. Muchos de estos gusanos, una vez infectado el sistema, intentan descargar malware adicional que les permita infectar un mayor número de sistema.

Entre los gusanos más conocidos podemos destacar Code Red, ***Conficker***[11], ***Sasser***[12] o Nimda, los cuales han aprovechado distintas vulnerabilidades para infectar un elevado número de máquinas en las que no se hayan aplicado los parches pertinentes.

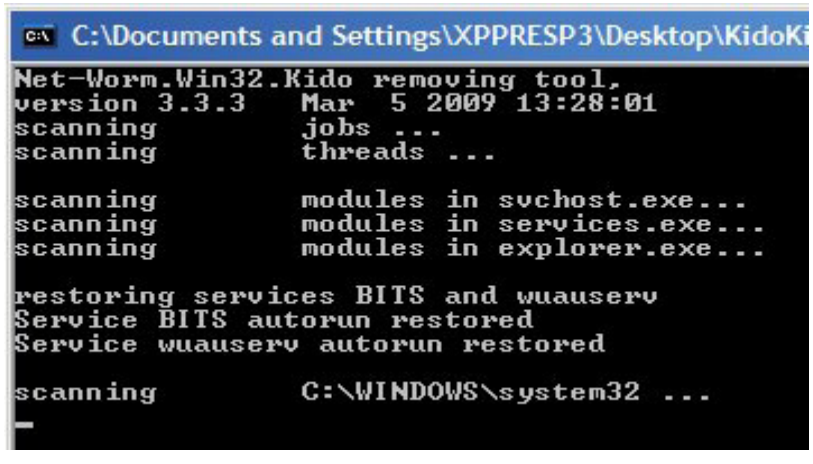


Ilustración 2 · Herramienta desinfección de gusano

Una buena práctica para evitar ser contaminados por dichos gusanos es aplicar las actualizaciones de seguridad en el momento en que son publicadas y reiniciar la máquina en caso de que dichas actualizaciones lo requieran, puesto que muchas de éstas no se aplican si no se reinicia el sistema una vez instalado el parche. De la misma forma, es necesario tener cuidado sobre qué cosas y de quién o de dónde se descargan y, cómo no, disponer de herramientas confiables para la desinfección de malware, así como herramientas de prevención generales, como ***firewalls***[13], antivirus y control de tráfico de la red (IDS/IPS).

11 Accesible en http://es.wikipedia.org/wiki/Conficker
12 Accesible en http://en.wikipedia.org/wiki/Sasser_%28computer_worm%29
13 Accesible en http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

2.3 Troyanos

Se denomina troyano al software que se enmascara con una falsa identidad ejecutando una tarea útil o conocida para el usuario, pero realizando a la vez actividades maliciosas en el sistema contaminado sin que el usuario sea consciente de las mismas; obviamente, el nombre "troyano" proviene del mito griego del Caballo de Troya (http://es.wikipedia.org/wiki/Caballo_de_Troya). De la misma forma que el Caballo de Troya, el troyano es un malware que intenta hacer creer al usuario que se trata de un software legítimo, para que éste lo ejecute en su máquina ocultando su intención original. Un caso típico de instalación de un troyano es aquél en el que se inicia la instalación de algún programa descargado de una página web o desde una red P2P, programa que aparentemente no funciona y da un error (incluso en muchos casos dicho programa se elimina a sí mismo); desde el punto de vista del usuario, no ha sucedido nada relevante, pero en realidad el falso programa ha dejado instalado un troyano en el sistema, troyano que realizará acciones como el robo de contraseñas o el ataque a otros usuarios de la red.

Ilustración 3 · Ejemplo Troyano Sub7

Dentro del gran número de troyanos existentes, fue muy conocido el que afectó al Banco de América. Este troyano modificaba la web que visualizaba el navegador, añadiendo un nuevo campo a un formulario de acceso web. Si en la página se solicitaba el número de tarjeta, usuario y contraseña, el troyano añadía un campo donde se solicitaba el pin de la tarjeta, de forma que el atacante obtenía todos los datos necesarios para provocar un fraude. Otros ejemplos conocidos de troyanos son Sub7, Downloader.GK, Mhtredir, Briss, StartPage, etc.

Para no vernos contaminados por este tipo de malware se recomienda no descargar software de lugares no confiables (redes P2P, páginas web de software ilegal...), así como emplear herramientas de prevención y desinfección de malware.

2.4 Spyware

Los Spywares o Programas espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas ("husmean" la información que está en nuestro equipo) para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad; en algunos casos lo hacen para obtener direcciones de email.

Normalmente el spyware suele instalarse al acceder a páginas web no confiables (***banners***[14] publicitarios de contenido erótico, viajes, regalos o compras de artículos a un precio muy inferior al establecido en el mercado, etc.).

Las recomendaciones para evitar este tipo de malware son las habituales: no instalar nada de sitios no confiables y emplear herramientas de desinfección y protección adecuadas.

2.5 Phishing

El ***phishing***[15] (del inglés fishing, "pescando") no es en sí un malware puro, aunque hay que citarlo como elemento software que causa un daño ejecutando acciones sin que el usuario las perciba. Podemos obtener más información del phishing en el capítulo dedicado a Delitos Tecnológicos, dentro de este mismo curso.

El objetivo de un ataque de phishing es intentar suplantar la identidad de una organización (típicamente un banco) para hacer creer al usuario que realmente está accediendo o enviando información a esa organización. Suele llegar en forma de correo informativo donde, de alguna forma, se ***incita al usuario***[16] a acceder, por ejemplo indicándole que si no envía sus datos personales se perderán en su banco, que una determinada entidad tiene una gran oferta, que ha sido el usuario X y ha sido premiado, etc. Al acceder al enlace se entra en una web que no es la auténtica, sino una copia idéntica de la web original realizada por el atacante, de forma que el usuario que no aprecia la diferencia entre la web original y la falsificada, accederá a ésta introduciendo sus datos como si de su banco real se tratara. De esta forma los atacantes obtienen la información necesaria para acceder posteriormente con las credenciales del usuario y robar dinero de su cuenta.

14 Accesible en http://es.wikipedia.org/wiki/Banner
15 Accesible en http://es.wikipedia.org/wiki/Phishing
16 Accesible en https://www.facebook.com/notes/csirt-cv/algunos-consejos-para-detectar-correos-maliciosos/146070748776981

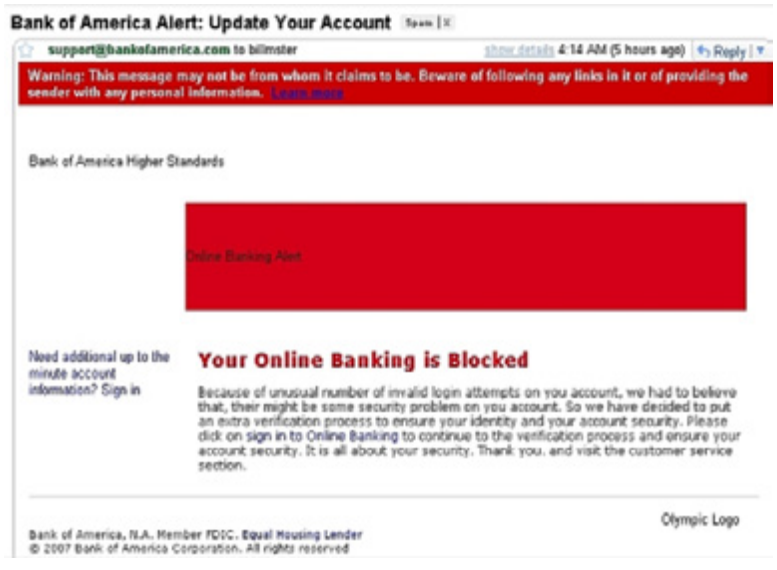


Ilustración 4 · Ejemplo de un correo falsificado

Recuerde que su banco, proveedor de correo electrónico o cualquier otra empresa jamás le pedirá introducir ese tipo de información que pueda comprometer su seguridad; por tanto siempre que reciba un correo de este tipo elimínelo e informe a la empresa afectada o a centros que se encargan de este tipo de ataques como el Centro de Seguridad TIC de la Comunitat Valenciana, ***CSIRT-cv***[17].

Es importante destacar que las direcciones origen de los correos se pueden falsificar, y por tanto, aunque el remitente sea correcto no indica que realmente el correo haya sido enviado por la empresa legítima de dicha cuenta de correo.

En la imagen adjunta se detalla el caso de un phishing a la Agencia Tributaria. En este correo se informaba de un error de la Agencia en la última declaración y que el afectado debía introducir sus datos bancarios o de tarjeta de crédito para que se le reembolsase el importe restante.

2.6 Rogue Software

El rogue software es un malware que aparenta ser una herramienta de desinfección (como un antivirus), pero que realmente no es más que un troyano que engaña al usuario haciéndole creer que primero tiene una infección y a continuación que este "antivirus" falso desinfecta la máquina. Realmente, el rogue software no realiza ninguna acción beneficiosa para el usuario y es un malware tan perjudicial -o más- como un troyano o un virus.

Estas aplicaciones maliciosas tienen un gran auge y están generando una gran cantidad de dinero en la actualidad. Hay que tener en cuenta que el beneficio para la organización que ha creado dicho malware es doble, ya que por un lado cobra por una falsa herramienta de desinfección y por otro instala malware para obtener información confidencial, pudiendo así, por ejemplo, obtener todas las contraseñas y datos que introduzca el usuario.

Normalmente este software se crea ***puntualmente***[18] incluyendo publicidad en páginas web para simular ante el cliente que realmente es un software legítimo

17 Accesible en http://www.csirtcv.gva.es/es/formulario/informar-de-un-phishing.html
18 Accesible en http://www.securityartwork.es/2010/05/21/rogueware-y-lost/

y correcto. Además, se modifican opciones de los buscadores más importantes para que, al buscar el nombre del malware acompañado de palabras clave (por ejemplo "antivirus"), salga esta falsa herramienta de desinfección como la primera en la búsqueda. Por ello es importante comprobar que se instala software reconocido, que no es nuevo en el sector y que lo descargamos de una web confiable. En esta ***sección***[19] del portal del CSIRT-cv se pueden encontrar varias herramientas reconocidas.

En la siguiente imagen se muestra un ejemplo de lo mencionado anteriormente; la herramienta realmente aparenta ser un antivirus legítimo donde se han detectado dos ficheros con malware. Realmente la aplicación en sí es malware, ya que se trata de un falso antivirus que primero cobra por registrar el antivirus (en caso contrario no permite desinfectar la máquina), y en segundo lugar registra las contraseñas del sistema.

Ilustración 5 · Ejemplo de Rogue Software

Puede encontrarse una ***lista***[20] completa de falsos antivirus, spyware, anti-troyanos, etc. que permiten comprobar si la herramienta que a instalar es realmente una herramienta legítima o una falsa herramienta.

2.7 Spam

El spam es un conjunto de correos publicitarios enviados de forma masiva a miles de usuarios de todo el mundo, usuarios que obviamente no han autorizado el envío de dicha publicidad a sus buzones de correo. Un correo publicitario legítimo debe tener en su asunto alguna palabra donde se indique claramente que se trata de un correo de publicidad, y en el mismo mail se debe informar de cómo darse de baja de la lista de distribución. La recepción de spam, tan habitual hoy en día, puede evitarse mediante filtros y listas negras bien en el servidor de correo, bien en el propio cliente (Outlook, Thunderbird...).

19 Accesible en http://www.csirtcv.gva.es/es/paginas/utilidades.html
20 Accesible en http://www.forospyware.com/t5.html

2.8 Rootkits y backdoors

Los ***rootkits***[21] son una una serie de aplicaciones que, o bien se encuentran ocultas en el sistema, o bien reemplazan aplicaciones reales del mismo. Así, cuando una aplicación contaminada por un rootkit se ejecuta, actúa como si realmente fuera la aplicación legítima, pero realiza acciones no legítimas que han sido diseñadas por el atacante. De esta forma, cuando un pirata consiga obtener acceso a una máquina vulnerable, intentará instalar un rootkit; una serie de aplicaciones que le permitan tomar el control del sistema aunque el usuario legítimo aplique a posteriori los parches pertinentes para evitar la vulnerabilidad. Estas herramientas también pueden ser instaladas mediante troyanos, y su peligrosidad radica en que para el usuario son difíciles de detectar, aparentemente todo funciona de forma correcta hasta que deja de hacerlo.

Existe un tipo especialmente peligroso de rootkit, los ***backdoors***[22] o puertas traseras, programas que permiten a un atacante acceder de forma remota a un sistema contaminado y administrarlo sin el consentimiento del usuario legítimo del mismo.

Para evitar este tipo de malware se deben aplicar herramientas preventivas de comprobación de integridad de los datos, así como herramientas activas que buscan en nuestro disco duro rootkits conocidos. Es conveniente emplear además algún tipo de firewall, para controlar el tráfico que entra y sale de nuestro sistema.

2.9 Adware

El adware es un malware que, más que dañar la máquina u obtener información confidencial del usuario, tiene como objetivo generar publicidad en el equipo de la víctima mediante múltiples ventanas sin que el usuario tenga ningún control sobre éstas.

Ilustración 6 · Adware

21 Accesible en http://es.wikipedia.org/wiki/Rootkit
22 Accesible en http://es.wikipedia.org/wiki/Backdoor

Habitualmente, el adware se instala en el equipo al acceder a webs de contenido sexual, software pirata o publicidad (aunque técnicamente puede instalarse al acceder a cualquier tipo de página web). Es fácilmente reconocible, ya que cuando se navega por Internet, se generan un gran número de ventanas publicitarias en el sistema infectado.

Las recomendaciones para evitar este malware de forma preventiva es que nunca se instale ni se acepte ningún tipo de Plugin o complemento cuando se navegue por páginas web de dudosa reputación o no confiables. De forma defensiva, se recomienda emplear herramientas de desinfección de adware o antivirus de propósito general.

2.10 Bots

Un bot es un programa que se hace pasar por una persona e intenta engañar al usuario mediante una serie de parámetros que le permiten simular, siguiendo unos patrones preestablecidos, una conversación con el usuario. Son muy habituales los bots de aplicaciones de mensajería instantánea (por ejemplo, ***MSN***[23]) que comienzan una conversación aparentemente real, interactuando con el usuario mediante frases concretas que tratan de que éste acceda a un enlace publicitario o a una descarga de malware.

Estos bots suelen ejecutarse desde el ordenador del atacante, intentando repetidamente que sus víctimas accedan a los enlaces enviados, o bien desde máquinas que han sido infectadas previamente; de esta forma, estos mensajes sospechosos pueden provenir de un contacto legítimo, lo que los convierte en algo más peligroso si cabe.

La mejor solución contra este malware es aplicar el sentido común; sus mensajes son fácilmente detectables, ya que responden como realmente lo haría la persona que supuestamente está escribiendo; por tanto, si alguien inicia una conversación por MSN y manda un enlace, es mejor preguntar por el enlace o el fichero al interlocutor, ya que los bots no suelen tener una respuesta correcta para preguntas "humanas". El mejor consejo para evitar posibles engaños por parte de un bot es, como decimos, usar el sentido común y por supuesto no interactuar con usuarios desconocidos a través de mensajería instantánea (y asegurarse de que los usuarios conocidos no están infectados por un bot).

2.11 Hoax

Los hoax son correos electrónicos cuyo contenido es falso -aunque el remitente sea legítimo- y son enviados de forma masiva por parte de usuarios que consideran como verdadero dicho contenido, generando así ruido en la red y en el buzón de quien lo recibe, y facilitando la captación de direcciones de correo electrónico por parte de un tercero malintencionado que, posteriormente, las utilizará para atacar a dichos usuarios. Aunque se trata de un malware especial que no realiza un daño directo sobre el equipo del usuario, sí que se considera nocivo por los motivos expuestos con anterioridad.

23 Accesible en http://es.wikipedia.org/wiki/Windows_Live_Messenger

Ejemplos típicos de hoax son las cadenas de correo electrónico que proporcionan datos falsos sobre atentados, campañas benéficas de grandes empresas a cambio de un simple correo electrónico o niños con enfermedades gravísimas que buscan apoyo; obviamente, se trata de datos falsos o rumores que, aprovechando la buena fe de los usuarios, se propagan por la red a través del correo electrónico y permiten a un atacante planificar un daño más directo contra los usuarios. Por supuesto, debemos desconfiar de cualquier información de este tipo que llegue a nuestro correo -incluso si proviene de personas conocidas- y notificar a estas personas que están enviando un hoax, un ***falso rumor***[24] en la red.

2.12 Keyloggers

Son programas espías, que toman el control de los equipos, para espiar y robar información, monitoriza el sistema, ***registrando***[25] las pulsaciones del teclado, para robar las claves, tanto de páginas financieras y correos electrónicos como cualquier información introducida por teclado, en el equipo utilizado para saber lo que la víctima ha realizado como conversaciones que la misma tuvo, saber donde ha entrado, qué ha ejecutado, qué ha movido, etc.

3 Prevención y desinfección de malware

Una vez explicados los distintos tipos de malware existentes vamos a realizar un breve resumen de las herramientas más destacadas para prevención y desinfección de los programas nocivos vistos con anterioridad. Es importante indicar que no se aconseja emplear distintas herramientas para un mismo propósito, ya que esto suele producir más problemas que beneficios. Incluso en algunos casos, como el de los antivirus, la instalación de más de uno de ellos puede dar lugar a funcionamientos incorrectos (por ejemplo, incompatibilidades entre sí), por lo que se aconseja instalar una única herramienta para cada tipo de malware y no emplear varias para una misma amenaza.

3.1 Actualización del software

Es muy importante tener habilitada la actualización automática de software en el sistema y aplicar las actualizaciones siempre que se informe de que existe una nueva versión (especialmente, en las actualizaciones referentes a seguridad). Si se solicita reiniciar el sistema, este reinicio debe hacerse lo antes posible, puesto que muchos parches sólo se aplican tras un reinicio del equipo (antes del mismo no tendrán efecto, aunque estén instalados correctamente).

En entornos Windows, desde el Panel de Control, debe seleccionarse la opción de actualizaciones automáticas y aplicarlas siempre que se requiera; en entornos Linux podemos aplicar las actualizaciones dependiendo de la distribución (emerge, apt-get, port, etc).

24 Accesible en http://www.csirtcv.gva.es/es/descargas/recomendaciones-b%C3%A1sicas-spam.html
25 Accesible en http://www.securityartwork.es/2011/06/13/pastebin-keyloggers/

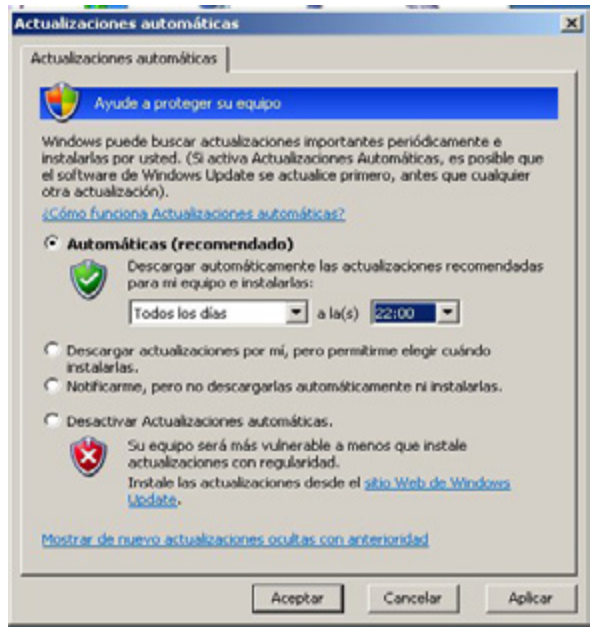


Ilustración 7 · Actualizaciones automáticas

No resulta solo importante actualizar el sistema operativo, sino que también se deben actualizar el resto de programas, sobre todo el navegador web y sus complementos puesto que si no están actualizados pueden ser un punto de infección al visitar páginas web maliciosas. Existen actualizadores que revisan los programas instalados en nuestro equipo recomendando su actualización con enlaces a las páginas de descarga originales. Se pueden encontrar herramientas de este tipo ***aquí***[26].

3.2 Cortafuegos

Se recomienda emplear en todos los equipos un firewall o cortafuegos con un doble objetivo: evitar que nuestro equipo sea plenamente accesible desde internet (para un malware o una persona que nos trate de atacar) y evitar también que un malware que nos ha contaminado pueda abrir puertos no controlados, accesibles desde Internet, al explotar alguna vulnerabilidad de nuestro sistema. Dentro de las distintas alternativas existentes, en cuanto a cortafuegos se refiere, se recomienda emplear el propio **firewall de Windows** o **ZoneAlarm** en entornos Windows o **Firestarter** (iptables) en entornos Linux.

3.3 Anti buffer overflow

En los sistemas operativos más modernos existen un gran número de controles que evitan que el software malintencionado explote vulnerabilidades en los programas y aplicaciones del sistema mediante protecciones de buffer overflow.

En entornos Windows se accede a este control desde la opción: Panel de Control → Sistema → Opciones Avanzadas → Rendimiento (configuración) → Opciones de rendimiento (Prev. De ejecución de datos → Activar Dep. → Aceptar (requiere reinicio).

26 Accesible en http://www.csirtcv.gva.es/es/paginas/actualizadores-de-programas.html

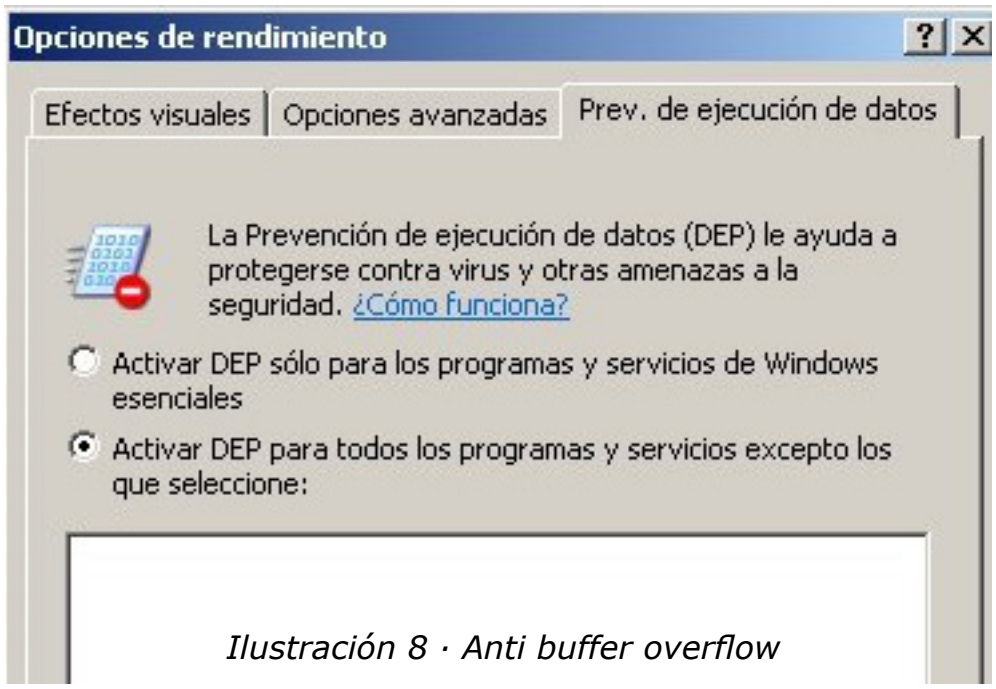


Ilustración 8 · Anti buffer overflow

En entornos Linux con núcleo 2.6 o superior se debe especificar una variable con valor "1" en el espacio del núcleo, de la siguiente forma:

```
# echo 1 > /proc/sys/kernel/randomize_va_space
```

3.4 Herramientas Anti Malware genéricas

En cuanto a herramientas genéricas para prevención y detección de malware, dentro de la distintas versiones disponibles se recomienda el uso de cualquiera de las siguientes: **Malwarebytes' Anti-Malware** (también se emplea para anti-spywire), **ComboFix, IniRem by InfoSpyware**. Específico para malware en soportes USB está disponible la herramienta **Panda USB Vaccine**.

3.5 Herramientas Anti Spywire

Existe un gran número de herramientas para evitar el spywire. Destacan las siguientes: **Ad-Aware Free Anti-Malware, Spybot - Search & Destroy, SpywareBlaster 4.2 y Windows Defender**. Existe también la herramienta **Hijackthis**, considerada como una de las mejores en la actualidad pero que requiere un nivel de conocimientos informáticos medio o alto.

3.6 Herramientas Anti Rootkits

Entre las ***múltiples herramientas disponibles***[27], se pueden destacar: **Sophos Anti-Rootkit, Panda Anti-Rootkit, F-Secure BlackLight Rootkit Eliminator y Rootkit Revealer de SysInternals(MS)**. Para entornos Linux se recomienda emplear adicionalmente herramientas de integridad de datos como **Tripwire** o **Aide**, así como herramientas de detección como **rkhunter**.

27 Accesible en http://www.csirtcv.gva.es/es/paginas/antivirus.html

3.7 Antivirus de escritorio

Los sistemas antivirus son tal vez la herramienta de seguridad más empleada por los usuarios, puesto que además de eliminar virus suelen incluir defensa contra todo tipo de malware actual. Es muy importante actualizar las bases de datos del antivirus diariamente y si el antivirus lo permite, seleccionar la casilla de actualización automática para que esta actualización se realice sin intervención humana.

Existen una gran cantidad de antivirus gratuitos y de pago en el mercado, de los que destacamos los siguientes: **Nod32** Antivirus System, **Panda** Antivirus Pro, **Kaspersky** Antivirus, Norton AntiVirus, **Avira** AntiVir Personal, **AVG** Anti-Virus Free Edition, **Avast** Home Antivirus Free Edition. Una recopilación de estos antivirus podemos encontrarla en ***http://www.inteco.es/landing/Seguridad/*** y en ***http://www.csirtcv.gva.es/es/paginas/antivirus.html***.

Debido al funcionamiento de los antivirus solo se debe emplear un único antivirus de escritorio a la vez y nunca emplear varios, ya que esto puede originar problemas entre ellos y verse afectado su correcto funcionamiento.

3.8 Antivirus Online y sandbox

Existen una serie de páginas Web que permiten analizar ficheros mediante un gran número de motores de antivirus. Puede resultar útil cuando se tengan dudas sobre un cierto fichero y deseen obtener el resultado de más de un antivirus. Recomendamos los siguientes recursos para dicha tarea:

- ***Virus Total***
- ***Jotti MalwareScan***
- ***VirScan***
- ***Filterbit***

Puede darse el caso que incluso auditando el fichero mediante varios motores antivirus se desconozca la naturaleza del fichero, por ejemplo, cuando solo tres de cuarenta antivirus nos catalogan el fichero como un virus. Para ello existen máquinas virtuales Online, llamadas sandbox, de tal forma que se sube el fichero y éste es ejecutado en un sistema controlado, notificando de todas las acciones llevadas a cabo por el fichero. A partir de su comportamiento los entornos nos pueden identificar si el fichero se comporta como un malware o no. Recomendamos los siguientes entornos:

- ***Anubis***
- ***Comodo***
- ***CWSandBox***
- ***Eureka***
- ***Norman SandBox***
- ***ThreatExpert***
- ***Xandora***
- ***Cuckoosandbox***

Acerca de este último entorno (Cuckoosandbox) os recomendamos una lectura interesante sobre el mismo en ***http://www.securityartwork.es/2012/01/23/cuckoosandbox/***

3.9 Última versión del sistema operativo

Se recomienda disponer de la última versión del sistema operativo empleada. Por ejemplo, para plataformas Windows se aconseja el empleo de la versión Vista o superior, debido a las mejoras de seguridad desarrolladas tales como la separación de niveles de privilegios y la implementación del UIPI (User Interface Privilege Isolation) que evita que procesos con menor nivel de integridad (IL) puedan realizar acciones sobre procesos de mayor integridad tales como SetWindowsHookEx() o CreateThreadEx() bloqueando de esta forma algunas versiones de malware que intentan registrar las acciones del usuario: números secretos, cuentas bancarias, redirección a falsas webs, etc.

4 Links de interés

Para más información relativa al malware y las defensas frente al mismo se recomienda consultar los siguientes enlaces:

Listado de herramientas adicionales

Foro con mucha información de malware

Actualidad Microsoft Windows

4

NAVEGACIÓN SEGURA

De los diferentes servicios que Internet proporciona, es la navegación por páginas web la más utilizada (junto con el correo electrónico) a nivel mundial. Esta popularidad provoca que exista una cantidad enorme de potenciales víctimas para personas que intentar realizar actividades delictivas (ciber-delincuentes), o simplemente satisfacer sus deseos de molestar al resto de usuarios de la Web.

Ante esta amenaza, cada vez más presente, es muy aconsejable seguir una serie de pautas que permitan acceder y navegar por la Web de forma segura.

En este apartado se presentarán una serie de consejos y varias herramientas muy sencillas que ayudarán al usuario a navegar por Internet protegidos de las muchas amenazas que se encuentran presentes en la red.

1 Consejos para realizar una navegación segura

1.1 Usar el sentido común

Aunque pueda parecer un consejo básico e innecesario, es habitual que un gran número de usuarios naveguen por Internet sin unos conocimientos mínimos de los peligros residentes en la web. Gracias a la confianza con la que la mayoría de los usuarios acceden a multitud de páginas y servicios, la ciber-delincuencia encuentra una enorme cantidad de víctimas para sus propósitos. Es necesario tratar Internet como una herramienta delicada que es muy útil, pero que puede convertirse en peligrosa si no se maneja con cuidado.

1.2 Actualizar frecuentemente las aplicaciones con los parches de seguridad

Las vulnerabilidades (http://www.csirtcv.gva.es/es/paginas/alertas.html) que se detectan en los programas informáticos más utilizados (navegadores de Internet, procesadores de texto, programas de correo, antivirus, etc.) suelen ser, precisamente por su gran difusión, un blanco habitual de los creadores de virus. Para evitarlo, una vez detectada una vulnerabilidad, las compañías fabricantes de software publican las soluciones a estos fallos en forma de actualizaciones o parches.

Normalmente estas mejoras se realizan mediante mensajes automáticos emitidos por el propio programa, pero es aconsejable comprobar si existen nuevas versiones del software que manejamos en la página web de la propia aplicación o desde la opción de comprobar actualizaciones (updates en Inglés) disponible en la mayoría de los programas.

Hay disponibles aplicaciones que comprueban constantemente las versiones instaladas en un sistema y si existen actualizaciones para ellas. Algunos ejemplos

pueden descargarse en la sección de Actualizadores de Programas http://www.csirtcv.gva.es/es/paginas/actualizadores-de-programas.html) del portal web de CSIRT-CV.

1.3 Usar software legal

Es importante que el software instalado en los equipos sean legales. Las copias de software pirata, además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles entre diferentes ordenadores, lo cual provocaría la inestabilidad en el mismo. Tampoco se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus. En cualquier caso, debemos analizar con el antivirus cualquier fichero que nos descarguemos de una página web.

1.4 Precaución con el correo electrónico

Analizar, antes de abrir, los correos electrónicos recibidos y sospechar de los mensajes no esperados, incluso si provienen de algún conocido. Los virus utilizan la libreta de direcciones de la máquina infectada para enviar sus réplicas y tratar de infectar a otros usuarios haciéndoles creer que están recibiendo un mensaje de un conocido. Más información sobre la seguridad en el correo electrónico en el capítulo 3.

1.5 Prudencia con los archivos

No descargar de Internet (ni de adjuntos de correos electrónicos) ficheros ejecutables (.exe, .dat ...), documentos, etc, que no provengan de una fuente confiable. Analizar con el antivirus cada nuevo elemento que trate de incorporarse a nuestro ordenador. No abrir ningún archivo con doble extensión (como archivo.txt.vbs). En condiciones normales no se necesitan nunca este tipo de archivos. Configurar el sistema para que muestre las extensiones de todos los archivos.

1.6 Copias de Seguridad

Realizar de forma periódica copias de seguridad de la información más valiosa (fotos, documentos y cualquier fichero imposible recuperar). En caso de sufrir un ataque de un virus o una intrusión, las secuelas serán mucho menores si es posible restaurar fácilmente estos datos.

1.7 Criticidad de los datos personales

No deben facilitarse datos personales como nombre, dirección o número de tarjeta de crédito, si no es en páginas de absoluta confianza. Estas páginas nunca deben ser accedidas desde el correo electrónico. Tampoco facilitar la dirección de e-mail en páginas web desconocidas.

2 Elementos de seguridad

En este apartado se enuncian y explican brevemente cuáles son las características del navegador en las que es más importante fijarse bien y aprender a utilizar.

2.1 Protección frente a atques

Cuando navegamos, existen ciertas páginas que intentan, incluso solo visitándolas (sin llegar a descargar nada), infectar el equipo. Para evitar estos ataques, los desarrolladores de navegadores han ido incluyendo diferentes herramientas que ayudan a minimizar el riesgo de éxito de dichos ataques, algunas de estas características se solapan con otras como modo de reforzar la seguridad.

Filtro contra la suplantación de identidad

Se trata de una funcionalidad que se utiliza para que el navegador indique si la página que se está visualizando está intentando suplantar la identidad de otra, por ejemplo: se ve la página del banco, aunque en realidad se trata de otra que se hace pasar por la del banco para intentar recopilar datos sensibles (el número de cuenta, números secretos, etc). También se puede llamar filtro antiphishing.

Bloqueador de elementos emergentes

Con este elemento evitamos que surjan ventanas con publicidad no deseada (también conocidas como pop-ups), y que en algunas ocasiones, intentan infectar el ordenador. Algunos navegadores poseen diferentes niveles de funcionalidad (listas blancas/negras, etc) para permitir algunas (bancos, páginas de confianza, etc) y restringir otras.

Java/JavaScript

Se tratan de dos lenguajes de programación que se utilizan para programar las páginas web, y que les hacen adquirir nuevas funcionalidades y en ocasiones, son aprovechadas por los atacantes para realizar alguna actividad maliciosa (robar información del equipo, infectarlo, etc).

Información de seguridad de la página

Este elemento no se trata de una funcionalidad en sí misma, sino que indica los datos de seguridad de la página actual y sirve para que el usuario determine si el nivel de seguridad es suficiente, o si se trata de la página legitima (y no se trata de una suplantación de identidad) entre otras cosas.

Personalización de reglas según el sitio

En este apartado se pueden configurar reglas particulares de privacidad y seguridad en función del sitio, por ejemplo pueden no permitirse cookies en ningún sitio, excepto los que se añadan manualmente con esta función.

Carga automática de imágenes

Mediante esta característica se consigue evitar la aparición de publicidad no deseada en las páginas que visitadas, además, en ocasiones, dichas imágenes se utilizan para dirigir al usuario a páginas con software malicioso.

Personalización de notificaciones

Las notificaciones ayudan a ser conscientes de las zonas por las que se navega, cuando es posible sufrir algún ataque o si el navegador está teniendo un comportamiento extraño (por la aparición de estas notificaciones), pone en alerta al usuario sobre situaciones peligrosas para su equipo.

2.2 GESTION DE LA INFORMACIÓN PRIVADA

La información privada se refiere a toda aquella que está protegida por la LOPD (Ley Orgánica de Protección de Datos), así como aquella que no se desea que sea conocida por otros usuarios o entidades (sitios visitados, correo electrónico, etc).

Navegación privada

Este modo de uso sirve para que el navegador no almacene la información que se genera respecto a la navegación (cookies, usuarios y contraseñas, historial, caché…). Es recomendable usarla cuando se necesita un nivel de privacidad muy alto.

Sesiones

Las sesiones que almacena el navegador sirven para recuperar páginas visitadas y que tal vez no se han guardado en favoritos, hay que saber administrar dichas sesiones para que otros usuarios no puedan acceder a esas páginas sin consentimiento.

Borrar información privada con un clic

Se trata de una funcionalidad que simplifica la tarea de borrar los datos sensibles y que da una visión completa de cuáles son los datos importantes respecto a la privacidad.

Contraseñas

En muchas ocasiones hay que recordar multitud de usuarios y contraseñas para poder acceder cada vez a más páginas (correo electrónico, redes sociales, redes internas, etc). Existe una característica que facilita enormemente la tarea de recordarlas, donde es el propio navegador el que almacena esta información.

Pero debemos tener en cuenta que esta es una información muy sensible y debemos administrarla correctamente para que otros usuarios no puedan acceder a la misma, por ejemplo con el establecimiento de una contraseña maestra en los navegadores que lo permitan.

En algunos navegadores existe la posibilidad de proteger las contraseñas guardadas con una contraseña maestra, tanto para poder verlas, como para utilizarlas, de tal modo que cada vez que se quiera acceder a las diferentes páginas en las que nos solicitan el usuario y contraseña, solo haya que introducir la contraseña maestra.

Cookies

Las cookies (también llamadas galletas o huellas) son unos archivos que se guardan en el sistema con cierta información del usuario respecto a la página (accesos, personalización de la página, etc) cada vez que visitamos una página (no en todas, pero sí en la mayoría) de tal manera que la siguiente vez que se visita, ésta tiene la información personalizada (colores, usuario y contraseña, mensajes leídos, etc). Estos pequeños ficheros, en ocasiones pueden llegar a ser leídos por otras páginas para poder conseguir información sobre los hábitos en Internet de un usuario: pautas de navegación, nombres de usuario e incluso información más sensible, llegando a poder manipular las cookies con intenciones fraudulentas.

Historial

Como su nombre indica se trata de la información que guarda el navegador de las páginas que se visitan, y cuándo se ha hecho, si no se quiere que se conozca esta información, porque utilizamos un ordenador compartido, por ejemplo, es importante saber administrar el historial.

Descargas

Del mismo modo que el Historial, las descargas que se realizan desde el navegador también pueden recordarse, de estas listas puede extraerse información sensible que también es importante saber cómo borrar u ocultar a otros usuarios.

Formularios y búsquedas

De manera análoga a la funcionalidad de "recordar contraseñas", esta característica simplifica la tarea de introducir datos en los formularios, pero puede darle acceso a usuarios no autorizados a información privada.

Caché

Esta característica le sirve al navegador para almacenar ciertos ficheros (imágenes de páginas web, páginas web enteras, etc) que le permiten cargar más rápido las páginas solicitadas y por lo tanto realizar una navegación mucho más fluida. En la carpeta de caché se almacena mucha información relacionada con la navegación del usuario y que es susceptible de ser robada por atacantes o software malicioso.

2.3 Fortalecer la seguridad de los navegadores

El navegador web es la ventana al mundo de la Web. Desde él se accede a la mayoría de servicios que Internet nos ofrece, por esto es muy importante que su configuración esté encaminada a la seguridad y permita la confidencialidad de los usuarios y evite, por ejemplo, que el equipo resulte infectado al visitar una página maliciosa o que haya una fuga de datos por una mala gestión de nuestra información privada.

Al igual que en la vida real, en el mundo virtual de Internet existen los engaños, timos o estafas, y es muy importante usar el navegador con precaución y sentido común.

Independientemente de por donde se navegue, siempre es recomendable configurar el navegador con la máxima seguridad posible, pero esto puede afectar a la eficacia del tránsito por Internet, por lo que es aconsejable mantener un compromiso entre la seguridad y la calidad de la experiencia del usuario, de este modo, si se quiere entrar a la página del banco es fundamental tener la máxima seguridad posible. En cambio para la mayoría de las páginas por las que navegamos normalmente, basta con tener unos niveles menores de seguridad. Por último, es muy importante que tengamos en cuenta el ordenador que estamos utilizando (personal, en el trabajo, en un lugar público…) para saber qué niveles de seguridad debemos configurar y esperar que tenga el navegador.

Como se comentaba en un punto anterior, es fundamental mantener actualizado el software del sistema. En el caso de los navegadores estas actualizaciones son más importantes si cabe. Los navegadores más habituales se actualizan automáticamente ellos mismos (Firefox y Opera) o a través de un gestor de actualizaciones automáticas: Internet Explorer con Windows Update en Microsoft Windows y Safari con Apple Software Update en Mac OS X. En ambos casos (sea automático o mediante gestor), solicitan permiso para instalar las actualizaciones.

Así mismo, si el navegador no está correctamente configurado, cuanto más se navega, más posibilidades existen de que se produzca una infección con un software malicioso que podría afectar a la calidad de la navegación e incluso, la privacidad del equipo o su integridad. Para cada opción, se indica a continuación cómo acceder a ella desde el menú del navegador.

Seguidamente se explica como configurar dos niveles de seguridad (alta y media) en los dos navegadores más habituales (Internet Explorer de Microsoft y Firefox de Mozilla)

INTERNET EXPLORER

Ilustración 9 · Internet Explorer

La práctica totalidad de la configuración de este navegador pasa por dos elementos fundamentales:

- las zonas de seguridad
- las zonas de privacidad

Mediante el control de la barra deslizante se configuran las principales opciones de seguridad y privacidad, además, en ambos casos se pueden personalizar los

diferentes niveles para usuarios más expertos, así como configurar las opciones avanzadas.

Como elemento común a ambos niveles está la información de seguridad de la página, que permite conocer la autenticidad de la página (para saber si no es una suplantación) y con conocimientos más avanzados, qué nivel de seguridad posee dicha pagina.

Ver > Informe de seguridad

Seguridad Media

Para poder obtener un nivel de seguridad aceptable para la mayoría de las situaciones de navegación (es decir, no incluye la conexión a bancos, transacciones, compra en línea,etc) es necesario:

1. Establecer la zona de seguridad en nivel Medio-alto desde Herramientas > Opciones de Internet > Seguridad

2. Establecer la zona de privacidad en nivel Medio-alto desde Herramientas > Opciones de Internet > Privacidad

3. Configurar el bloqueador de elementos emergentes: Posee diferentes niveles de bloqueo y notificación, además de la posibilidad de añadir una lista blanca. Las diferentes opciones son:

Activar

Herramientas > Bloqueador de elementos emergentes > Activar el bloqueador de elementos emergentes

Administración

Herramientas > Bloqueador de elementos emergentes > Configuración del bloqueador de elementos emergentes > Notificaciones y nivel de bloqueo

Herramientas > Bloqueador de elementos emergentes > Configuración del bloqueador de elementos emergentes > Excepciones

4. Configurar el uso del administrador de contraseñas: Se trata de una funcionalidad que hay que usar con cuidado ya que si otro usuario utiliza el navegador podría acceder a zonas privadas sin autorización. Tareas relacionadas con el administrador de contraseñas son:

Activar

Herramientas > Opciones de Internet > Contenido > Autocompletar > Configuración > Nombres de usuario y contraseñas en formularios

Borrar

Herramientas > Opciones de Internet > General > Historial de exploración > Eliminar > Contraseñas

Administración

Herramientas > Opciones de Internet > Contenido > Autocompletar > Configuración > Preguntar antes de guardar las contraseñas

5. Administrar el Historial: Es recomendable borrar el historial completo cada cierto tiempo, y establecer una política de guardado del historial, que en este navegador se realiza por el número de días que desee el usuario. Las opciones disponibles para el historial son:

Borrar

Herramientas > Opciones de Internet > General > Historial de exploración > Eliminar… > (seleccionar solo Historial) > Eliminar

Ver

Ver > Barras del explorador > Historial

Borrado selectivo

Ver > Barras del explorador > Historial > (seleccionar un elemento) > (botón derecho) > Eliminar

Política

Herramientas > Opciones de Internet > General > Historial de exploración > Configuración > Historial > Conservar páginas en el historial por estos días

Por último es importante conocer la funcionalidad que permite borrar toda la información privada en un solo cuadro, porque simplifica enormemente la limpieza de estos archivos.

Herramientas > Eliminar el historial de exploración > (seleccionar todos) > Eliminar

Alta seguridad

La configuración de este nivel de seguridad se puede utilizar en parte (o totalmente) según el criterio del usuario, para realizar la navegación más habitual, pero es imprescindible cuando se quiere realizar actividades en Internet que requieren un mayor nivel de seguridad. En cualquier caso este tipo de configuración es un complemento a la de seguridad media, por lo que es imprescindible configurar primero el nivel de seguridad medio para obtener este nivel.

1. Establecer la zona de seguridad en nivel Alto

Herramientas > Opciones de Internet > Seguridad

2. Establecer la zona de privacidad en nivel Alto

Herramientas > Opciones de Internet > Privacidad

3. Administrar la información que se guarda de formularios y búsquedas. En muchas ocasiones los datos de los formularios son personales y es importante protegerlos adecuadamente:

Activación

Herramientas > Opciones de Internet > Contenido > Autocompletar > Configuración > Formularios

Borrado

Herramientas > Eliminar el historial de exploración… > Eliminar formularios… > Eliminar

4. Administrar la caché: Se pueden administrar las diferentes opciones de la caché en función del espacio que exista en el disco, aunque, en la mayoría de los casos es suficiente con dejar que lo haga el navegador.

Borrado

Herramientas > Eliminar el historial de exploración… > Archivos temporales de Internet y Cookies > Eliminar

Gestión

Herramientas > Opciones de Internet > General > Historial de exploración > Configuración

Ver

Herramientas > Opciones de Internet > General > Historial de exploración > Configuración > Ver archivos

5. Activar el filtro SmartScreen. Este ayuda a detectar sitios potencialmente peligrosos (más información sobre el filtro en ***http://windows.microsoft.com/es-eS/windows-vista/SmartScreen-Filter-frequently-asked-questions***)

Herramientas > Opciones de Internet > Opciones Avanzadas > Configuración > Seguridad > Filtro SmartScreen > Activar el filtro SmartScreen

6. Administración del Java/JavaScript: Se tratan de los más importantes puntos de ataque en las páginas web y el elemento que más influye en

la presentación de muchas, por lo que es importante saber manejarlo con precisión.

Herramientas > Opciones de Internet > Seguridad > Nivel personalizado… > Automatización de los applets de Java

Por último, Internet Explorer posee la característica de navegación privada, que en este navegador se denomina InPrivate y permite que el navegador no almacene ningún tipo de información privada, y que de la posibilidad de tener un nivel de seguridad alto sin tener que configurarlo manualmente.

Herramientas > Exploración de InPrivate

FIREFOX

Ilustración 10 · Firefox

Navegador con múltiples opciones de configuración que podemos reducir a dos: seguridad media y alta seguridad.

Como elemento común a ambos niveles está la información de seguridad de la página, que permite conocer la autenticidad de la página (para saber si no es una suplantación) y con conocimientos más avanzados, qué nivel de seguridad posee dicha página. Además es importante saber configurar los múltiples niveles diferentes de notificaciones y que son importantes para saber si existe alguna situación de riesgo.

Información de seguridad

Herramientas > Información de la pagina > Seguridad

Personalización de notificaciones

Herramientas > Opciones > Seguridad > Configuración…

Seguridad Media

Para poder obtener un nivel de seguridad aceptable para la mayoría de las situaciones de navegación (es decir, no incluye la conexión a bancos, transacciones, compra en línea) es necesario:

1. Activar el filtro antiphising.

Herramientas > Opciones > Seguridad > Mostrar si el sitio que se está visitando es sospechoso de engaño

2. Configurar el bloqueador de elementos emergentes: Se puede incluir una lista blanca con las paginas donde no se desee que esté activado el bloqueador.

Activar

Herramientas > Opciones > Contenido > Bloquear ventanas emergentes

Excepciones (Lista blanca)

Herramientas > Opciones > Contenido > Bloquear ventanas emergentes > Excepciones…

3. Configurar el uso del administrador de contraseñas: Es muy importante que se utilice una contraseña maestra para evitar que otros usuarios no autorizados puedan ver las contraseñas. También se puede configurar una lista negra en la que el administrador no recordara la contraseña nunca.

Activación

Herramientas > Opciones > Seguridad > Recordar contraseñas de los sitios

Ver

Herramientas > Opciones > Seguridad > Contraseñas guardadas…

Borrar

Herramientas > Limpiar datos privados... > Contraseñas guardadas

Borrado selectivo

Herramientas > Opciones > Seguridad > Contraseñas guardadas… > (seleccionar contraseña) > Eliminar

Excepciones (Lista negra)

Herramientas > Opciones > Seguridad > Excepciones…

Contraseña maestra

Herramientas > Opciones > Seguridad > Usar una contraseña maestra

4. Configurar una política de almacenado de cookies: Para ello, aceptaremos "cookies de las webs", pero no aceptaremos "cookies de terceros". Por último, es recomendable guardarlas hasta que caduquen.

Activar

Herramientas > Opciones > Privacidad > Aceptar cookies de las webs

Ver

Herramientas > Opciones > Privacidad > Mostrar cookies…

Eliminar

Herramientas > Limpiar datos privados… > Cookies

5. Administrar el Historial: Es recomendable borrar el historial completo cada cierto tiempo, y establecer una política de guardado del historial, que en este navegador se realiza por el número de días que desee el usuario.

Ver

Historial > Mostrar todo el historial

Política

Herramientas > Opciones > Privacidad > Guarda mi historial por al menos

Eliminar (varios puntos)

1. Herramientas > Opciones > Privacidad > Configuración... > Historial de navegación

2. Herramientas > Opciones > Privacidad > Limpiar ahora…

3. Herramientas > Limpiar datos privados

Borrado selectivo

Historial > Mostrar todo el historial > (seleccionar historial) > Eliminar

6. Administrar las Descargas: Al igual que el historial es una opción de privacidad borrar cada cierto tiempo las descargas almacenadas.

Ver

Herramientas > Descargas

Borrado selectivo

Herramientas > Descargas > (seleccionar descarga) > Eliminar

Eliminar

Herramientas > Limpiar datos privados… > Historial de descargas

Por último, es importante conocer la funcionalidad que permite borrar toda la información privada en un solo cuadro, porque simplifica enormemente la limpieza de estos archivos.

Herramientas > Limpiar datos privados…

Alta seguridad

La configuración de este tipo de seguridad se puede utilizar en parte (o totalmente) según el criterio del usuario, para realizar la navegación más habitual, pero es imprescindible cuando queremos realizar actividades en Internet que requieren un mayor nivel de seguridad. En cualquier caso este tipo de configuración es un complemento a la de seguridad media, por lo que es imprescindible configurar primero el nivel de seguridad medio para obtener este nivel.

1. Administrar las sesiones: Aunque en este navegador las opciones de sesión son simplificadas, cuando al cerrar el navegador pregunta si se quiere guardar, es importante saber que se guarda y quien tiene acceso al equipo.

2. Eliminar selectivamente las cookies: Además de la administración que se hace en el nivel de seguridad media, existe la posibilidad de borrar las cookies que se deseen.

Herramientas > Opciones > Privacidad > Mostrar cookies… > (seleccionar cookie) > Eliminar cookie

3. Administrar la información que se guarda de formularios y búsquedas: En muchas ocasiones los datos de los formularios son personales y es importante protegerlos adecuadamente.

Activación

Herramientas > Opciones > Privacidad > Recordar la información introducida en formularios y barra de búsqueda

Eliminar

Herramientas > Limpiar datos privados… > Formularios guardados e historial de búsquedas

4. Administrar la caché: Se pueden administrar las diferentes opciones

de la caché en función del espacio que exista en el disco, aunque, en la mayoría de los casos es suficiente con dejar que lo haga el navegador.

Borrado

Herramientas > Limpiar datos privados… > Caché

Gestión

Herramientas > Opciones > Avanzado > Red

5. Administración del Java/JavaScript: Se trata de los más importantes puntos de ataque en las páginas web y el elemento que más influye en la presentación de muchas páginas, por lo que es importante saber manejarlo con precisión.

1. Herramientas > Opciones > Contenido > Activar JavaScript

2. Herramientas > Opciones > Contenido > Activar Java

6. Por último este navegador tiene la posibilidad de personalizar el nivel de seguridad según la página web en la que nos encontremos.

Herramientas > Información de la página > Permisos > (Se eligen las opciones para el sitio)

2.4 HERRAMIENTAS Y COMPLEMENTOS PARA NAVEGACIÓN SEGURA

No Script

Ilustración 11 · No Script

Este complemento para el navegador Firefox evita que se carguen JavaScript, Java y otros PlugIns en la página web visitada ya que este tipo de tecnología es susceptible a vulnerabilidades que afectan la seguridad del usuario. De esta forma, el navegador evitará la carga a menos que le indiquemos explícitamente que confiamos en esa web y permitimos el uso de dicha tecnología. Al principio es un proceso algo pesado (deberemos aceptar el acceso a las webs que

típicamente visitamos), pero una vez estén permitidas ya no será necesario volver a indicárselo.

Instalación:

1. Accedemos a la web de Mozilla para adquirir el complemento NoScript y pulsamos añadir a Firefox.

https://addons.mozilla.org/es-ES/firefox/addon/722

2. Aparecerá una pantalla similar a la siguiente donde deberemos pulsar a Instalar ahora y esperar a que se instale en la zona de complementos. Seguidamente aparecerá el mensaje para Reiniciar Firefox.

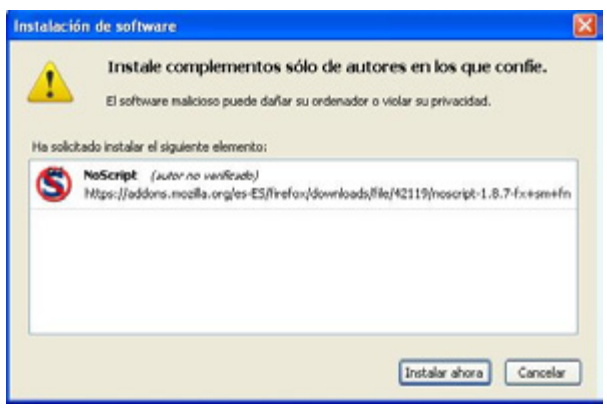


Ilustración 12 · Instalación de software

3. Una vez reiniciado, Firefox cargará la web de NoScript en una pestaña nueva y veremos en la parte inferior del navegador la barra del nuevo complemento. Donde nos indica si hay elementos bloqueados.

Uso:

1. Como ejemplo para permitir una web de confianza veremos como permitir el buscador ***www.google.es***.

2. Pulsaremos en el botón de Opciones y seleccionaremos Permitir google.es como se muestra a continuación.

Ilustración 13 · Uso de No Script

3. De esta forma indicamos que nos fiamos del JavaScript que google.es nos proporciona para mostrarnos su web.

ADBLOCK PLUS

Ilustración 14 · AdBlock Plus

El complemento AdBlock Plus para Firefox nos permite bloquear una imagen o banner dentro de una página web, ayudándonos a evitar este tipo de publicidad (que en ocasiones son fraudes que nos redirigen a páginas con contenido indeseado). Al contrario que el complemento anterior, este no bloquea por defecto, sino que debemos especificar que imagen o grupo de imágenes no queremos que nos muestre.

Instalación:

1. Accedemos a la web de Mozilla para adquirir el complemento AdBlock Plus y pulsamos añadir a Firefox.

2. De igual modo que la instalación del complemento anterior, aparecerá una pantalla donde deberemos pulsar a Instalar ahora, esperar a que se instale y pulsar en Reiniciar Firefox.

3. Una vez reiniciado, Firefox cargará la web de AdBlock Plus en una pestaña nueva y veremos en la parte superior derecha del navegador un icono con forma de señal de STOP con las letras ABP (AdBLockPlus) en su interior.

Ilustración 15 · Icono AdBlock Plus

Uso:

1. El icono tiene una flecha apuntando hacia abajo en la parte derecha con la que podemos acceder a las diferentes opciones; pero simplemente pulsando el icono de la señal aparece en la parte inferior del navegador el contenido de la web que puede ser bloqueado.

2. Como ejemplo vamos a tratar de bloquear la imagen del portal de

la Generalitat Valenciana.

3. Al acceder y pulsar sobre el icono de la señal, aparece una lista compuesta por diferentes lineas; cada una indica un recurso de la web, pueden ser imágenes o no. Por ahora solo nos interesan las imágenes y la dirección de donde proceden. Esto será muy importante a la hora de bloquear.

Ilustración 16 · Uso AdBlock Plus

4. Al seleccionar una de las líneas en la parte inferior, nos aparecerá una linea de puntos alrededor de la imagen en la propia web para poder identificarla correctamente, ya que por el nombre suele ser complicado.

5. Una vez seleccionada la imagen que deseamos bloquear, hacemos doble-click sobre la línea de la parte inferior y accedemos a un menú de acciones a realizar sobre la imagen seleccionada.

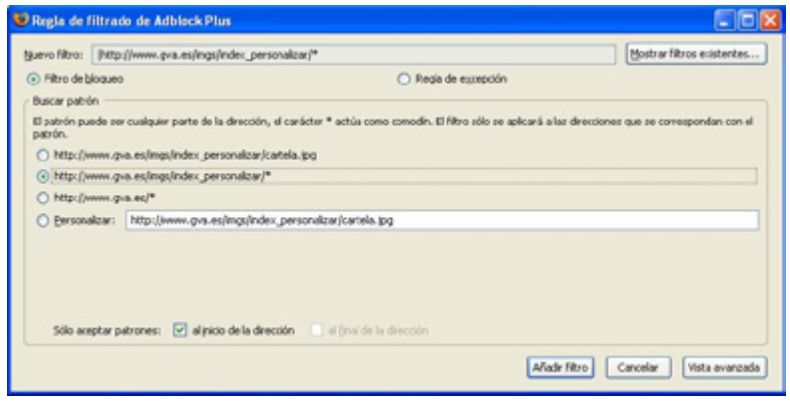


Ilustración 17 · Regla de filtrado de Adblock Plus

6. En esta ventana elegiremos la opción que más se aproxime a lo queremos hacer con la imagen. De las cuatro opciones que nos aparecen en el centro de la imagen, nos interesan principalmente las dos primeras. Una bloquea solo la imagen seleccionada, la otra (que es la marcada en la imagen y la que nos aparece por defecto) nos bloquea todas las imágenes que procedan de esa parte del dominio*. Pulsamos Añadir filtro para aplicar la opción elegida y vemos como desaparecen las imágenes que hemos seleccionado.

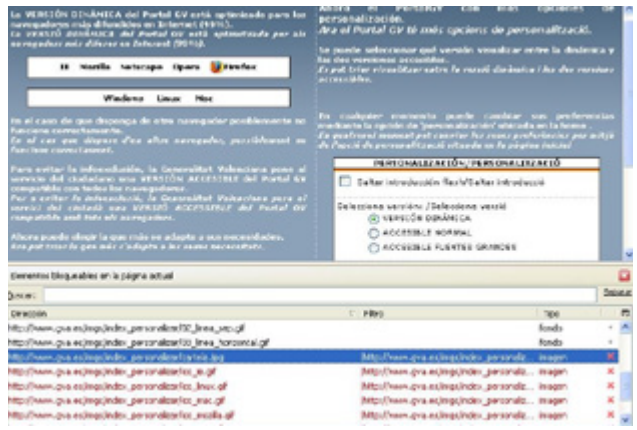


Ilustración 18 · Opciones filtrado de Adblock Plus

**Se aconseja usar esta opción ya que normalmente se incluyen en la misma carpeta las imágenes del mismo tipo, y si la imagen seleccionada es de publicidad, existirán más imágenes similares en esa carpeta, evitándonos así tener que bloquear las imágenes una a una.*

WOT

WEB OF TRUST

Ilustración 19 · Web Of Trust

Panda Security y Against Intuition han creado Web of Trust. WOT es un complemento de seguridad en Internet sencillo y gratuito, válido para Internet Explorer y Firefox. Logra mantener al usuario a salvo de los timos online, el robo de identidad, sitios de compra no fiables, spyware, correo no deseado, virus y sitios de compra poco fiables. Es fácil y gratis.

Los símbolos con código de color de son iconos de valoración, con colores de semáforo fáciles de entender (verde para continuar, amarillo para tener cuidado y rojo para detenerse) y se muestran junto a los resultados de búsqueda en Google, Yahoo!, Wikipedia, Digg y otros sitios conocidos. Las cuentas de correo de Google Mail, Hotmail y Yahoo también están protegidas del phishing, el correo no deseado y otros timos por correo electrónico. Las valoraciones se actualizan periódicamente y ya se han valorado más de 22 millones de sitios web.

Instalación (para Internet Explorer)

1. Acceder a la web en castellano desde ***http://www.mywot.com/es*** y pulsar la opción de descarga gratuita.

2. Se mostrará la página de descarga para el navegador usado y el idioma por defecto del sistema, en este caso pulsar "Descarga

Gratuita de Internet Explorer" comprobando que está seleccionado el idioma Español. Seguidamente elegir la opción deseada (instalar directamente o descargar el instalador).

3. Una vez ejecutado el instalador, aceptar las condiciones del Contrato de licencia y pulsar Instalar.

4. Finalmente aparece la opción de Finalizar y cuando se pulsa, el navegador carga automáticamente una página web como la que se muestra en la imagen, donde se debe seleccionar la configuración deseada para la aplicación. Seleccionar la configuración básica (la recomendada) y pulsar Finalizar.

Ilustración 20 · Descarga de WOT

5. Por último carga una página web donde se explica los significados de los símbolos introducidos por WOT y como valorarlos.

Uso:

Las dos funcionalidades principales son:

• Clasificación por parte de WOT y sus usuarios de una página web: En los resultados de los buscadores más populares podemos observar un anillo de color (verde para continuar, amarillo para tener cuidado y rojo para no acceder). Ver la imagen de ejemplo.

• Valorar la página según diversos criterios: Confiabilidad, Fiabilidad del vendedor, Privacidad y Seguridad para menores. Esta clasificación puede realizarse desde el anillo que aparece a la derecha de la barra de herramientas del navegador. V*er la imagen de ejemplo.*

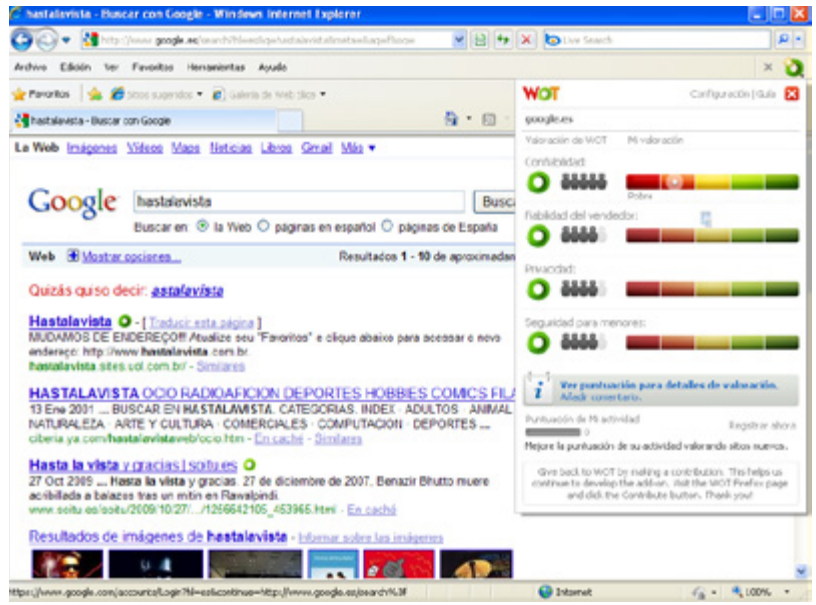


Ilustración 21 · Uso de WOT

La instalación para Firefox es muy similar a la de los dos complementos anteriores.

Otras Herramientas

SiteAdvisor:

La compañía McAfee ha desarrollado un complemento para los navegadores Internet Explorer y Firefox (para Windows y MacOS) muy similar a WOT (con iconos de valoración), que somete a los sitios Web a determinadas pruebas para localizar una posible presencia de spyware, spam o timos. De este modo, el usuario podrá efectuar búsquedas, navegar y realizar compras con mayor seguridad. Descargar desde aquí ***http://www.siteadvisor.com/***

SafeWeb:

Desde la web proporcionada por la compañía Symantec, fabricante de Norton Antivirus, es posible comprobar la seguridad de una página web antes de acceder a ella. Mediante una codificación de colores similares a WOT y Site Advisor, muestra un análisis realizado por Norton basado en la seguridad de la página web (si ha sido analizada anteriormente, sino se programa para un próximo análisis).***http://safeweb.norton.com/***

Proxies de Navegación Segura y Anónima:

Una forma de navegar de forma segura y anónima es a través de proxies. Entre otras muchas ventajas, de esta forma logramos enmascarar la dirección IP con la que estamos navegando y evitamos el uso de cookies por parte de servidores web sin nuestro consentimiento.

Varias listas de estos servidores Proxy pueden encontrarse en:

Hide My Ass ***http://hidemyass.com/proxy-list/***

Public Proxy Servers ***http://www.publicproxyservers.com/proxy/list_rating1.html***

Centurian ***http://www.centurian.org/***

5

CORREO ELECTRÓNICO

Con la llegada de las nuevas tecnologías al gran público, a casi todos los hogares, el uso del correo electrónico, también conocido como e-mail, ha crecido enormemente.

Cada vez nos resulta más extraño enviar cartas a conocidos y amigos, y poco a poco una gran parte de nuestro correo tradicional está migrando al correo electrónico (publicidad, facturas, notificaciones de la administración, etc).

Este hecho, debería de conlleva una formación de los usuarios sobre el uso y la seguridad en el correo electrónico ya que, a la vez que nos brinda muchas ventajas respecto al correo tradicional, también nos expone a algunos riesgos que antes no existían.

Es por ello que dedicamos este capitulo del curso, en el que explicaremos algunas medidas de seguridad para utilizar correctamente el correo electrónico.

1 Las cuentas de correo electrónico: principales consideraciones según la forma de acceso.

Una cuenta de correo está formada por un usuario y un dominio siguiendo la estructura **nombre@dominio.** Generalmente, una cuenta "pertenece" a un único usuario que se conecta al servidor para consultar su correo electrónico autenticándose mediante su nombre de usuario y su contraseña.

Esta conexión se realiza generalmente de dos formas: con un programa o cliente (Mozilla Thunderbird, Microsoft Outlook, Eudora...), o accediendo a una página web a través de un navegador de Internet (webmail). Este último se conoce como Webmail (hotmail.com, gmail.com, Yahoo correo, etc).

Ambas formas de conexión tienen características distintas en cuanto a funcionalidad y seguridad:

Clientes de correo: Al utilizar el correo electrónico mediante un cliente, los mensajes de correo se descargan al ordenador. Esto permite que si otros usuarios tienen acceso al ordenador, y los correos no están cifrados, otros usuarios puedan consultar los correos que hayan han sido descargados. Para evitar esto se recomienda el uso de distintos usuarios en el sistema operativo, ya que estos acostumbran a incorporar medidas para evitar que se puedan consultar las carpetas del resto de usuarios (donde generalmente se guardan los correos).

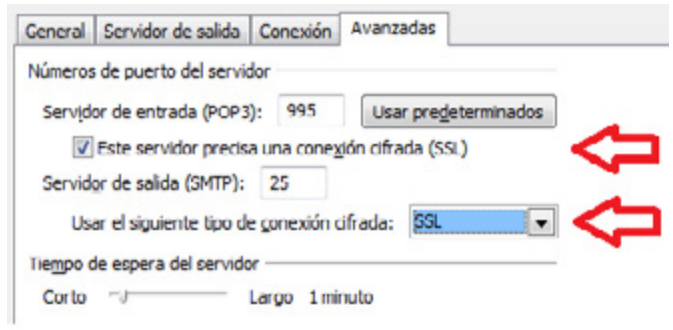


Ilustración 22 · Configuración correo

Otro punto a tener en cuenta es que las comunicaciones entre nuestro ordenador y el servidor, por defecto acostumbran a no ser cifradas, por lo que es posible interceptar tanto los correos electrónicos como las contraseñas de acceso. Para ello, los clientes tienen opciones para evitar estas situaciones aunque no todos los servidores soportan estas funcionalidades. Recomendamos contactar con el administrador de correo para informarse sobre estas opciones.

Webmail: en este caso los correos son almacenados en el servidor y se consultan online.

Al no almacenarse en el equipo no hay problema de que usuarios con acceso al ordenador puedan consultar el correo. No obstante, algunos de los servidores de webmail utilizan el protocolo http sin cifrar, por lo que si alguien está monitorizando la red, puede interceptar los correos que enviemos y recibamos o incluso las contraseñas de acceso. Es por ello que al escribir la dirección del servidor de correo es mejor poner https:// en lugar de http:// aunque no todos los servidores lo soportan.

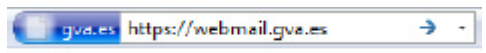


Ilustración 23 · Detalle Navegador

En lo referente a las contraseñas de acceso, generalmente en los accesos mediante webmail tienen la opción de cambiar la contraseña y establecer una pregunta secreta para recuperar la contraseña en caso de olvidarla (esta funcionalidad no está disponible en los clientes de correo). Se ha de tener en cuenta que si nuestra respuesta a la pregunta secreta es excesivamente fácil, algún usuario que nos conozca puede cambiar nuestra contraseña y acceder a nuestro correo electrónico, por lo que se desaconsejan el uso de nombres de mascotas, fechas de cumpleaños,lugar de nacimiento o preguntas similares.

Por último, se han de tomar las mismas medidas de seguridad que se tomarían al acceder a cualquier otro servicio web:

- **Evitar conectarse a webmail desde equipos públicos** como cibercafés para evitar que nuestra contraseña sea robada mediante programas maliciosos (keyloggers).

- **Cerrar siempre la sesión al abandonar el correo** en lugar de limitarse a cerrar el navegador o la pestaña.

• **Evitar el uso de respuestas sencillas para la opción "recordar contraseña".**

• **Utilizar un ordenador seguro:** sistema operativo y navegador actualizados, software antivirus, etc...

2 Enviando correos: Para, CC y CCO

Cuando enviamos un correo electrónico podemos elegir entre 3 campos para incluir la dirección del/los destinatarios.

En caso de que el correo tenga un único destinatario, bastará con escribir su dirección en el campo "para", pero si vamos a enviar el correo a varios destinatarios hay que tener en cuenta la diferencia entre los campos "Para","CC" y "CCO".

Nota: en algunos casos el campo CCO también se conoce como BCC.

Los campos Para y CC tienen la misma funcionalidad, indicar varios destinatarios, y la única diferencia entre ellos es a nivel formal o de protocolo: se entiende que el correo va destinado a quién figura en el campo "Para" y que se envía una copia a los destinatarios del "CC" para que estén informados (se trata de una formalidad). En este caso todos los destinatarios del correo, ya figuren en el "para" o en el CC, podrán ver a quien se ha enviado el correo electrónico.

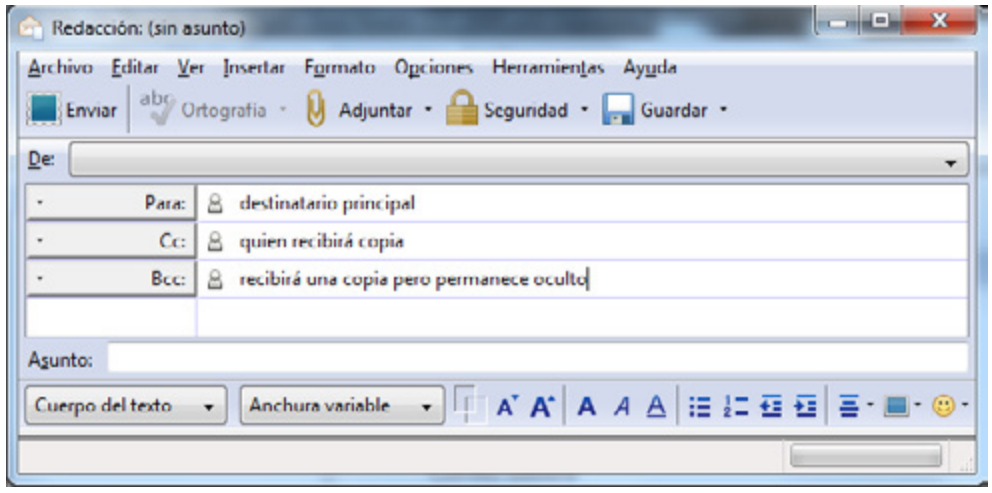


Ilustración 24 · Detalle campos de envío

Sin embargo, dependiendo del entorno, esto puede ocasionar algunos problemas a la hora de hacer envíos masivos ya que están quedando expuestas las direcciones de correo de todos los destinatarios.

Esto conlleva la revelación del correo electrónico del resto de receptores (dato de carácter personal), generalmente sin consentimiento de los afectados, y por ello puede desencadenar problemas legales.

Para evitar esta situación existe el campo CCO: si enviamos un correo a múltiples contactos, y para introducir sus direcciones utilizamos el campo CCO, ninguno de los destinatarios verá a que otros usuarios se les ha enviado el correo.

Vamos a proporcionar una serie de ejemplos de como se debería actuar en cada caso y el porqué:

Ejemplo1:
Enviamos un informe a un compañero y queremos que un segundo compañero también reciba la información.

Para: compañero1@nuestrodominio.com

CC: compañero2@nuestrodominio.com

Explicación: ambos compañeros recibirán el correo electrónico, compañero1 comprenderá que él es el destinatario del correo y verá que también se ha enviado a compañero2 porque ha de estar informado.

Ejemplo2:
Hacemos una consulta por correo electrónico a dos compañeros.

Para: compañero1@nuestrodominio.com, compañero2@ nuestrodominio.com

Explicación: ambos recibirán el correo y comprenderán que los dos son los destinatarios y que se espera una respuesta de cualquiera de ellos o de ambos.

Ejemplo3:
Enviamos un correo a un compañero y queremos que un segundo compañero esté informado, pero sin que el primero lo sepa.

Para: compañero1@nuestrodominio.com

CCO: compañero2@nuestrodominio.com

Explicación: compañero1 creerá que es el único destinatario del correo y compañero2 recibirá una copia en la que verá que el correo se ha enviado a compañero1 y que este desconoce que ha sido enviado a compañero2.

Ejemplo4:
Enviamos un correo masivo a una lista de amigos con una invitación a un evento:

CCO: amigo1@dominioamigo.com, amigo2@dominioamigo.com,

amigo3@dominioamigo.com, amigo4@dominioamigo.com,

Explicación: todos los amigos recibirán el correo pero nadie podrá consultar quienes más han sido invitados, salvaguardando de esta forma la privacidad del resto de los invitados.

Ha de hacerse hincapié en que el correo electrónico es un dato de carácter personal y no debe ser difundido sin el consentimiento expreso del propietario del mismo.

3 Firma Digital y cifrado: ¿qué son y para qué se utilizan?

Los correos electrónicos generalmente son enviados en texto claro (sin firmar ni

cifrar), por lo que no podemos tener la certeza de que el remitente sea autentico (autenticidad), ni de que el correo no haya sido modificado (integridad) ni de que no haya sido leído por terceras personas (confidencialidad).

Para garantizar estos 3 principios de la seguridad (autenticidad, integridad y confidencialidad) disponemos del cifrado y de el firmado digital (que son dos cosas distintas).

Existen muchas formas de utilizar estas dos técnicas por lo que nos vamos a centrar en el uso de certificados, por ser la práctica más extendida y aceptada.

Certificados

Para empezar a cifrar y firmar correos necesitaremos ante todo un **certificado digital**, que podemos entender como un "carnet de identidad digital" para, entre otras funciones, identificarnos en transacciones electrónicas.

Estos certificados pueden ser creados por el propio usuario pero generalmente se utilizan certificados emitidos por organismos oficiales, y en la Comunidad Valenciana son expedidos por la Autoritat de Certificació de la Comunitat Valenciana (ACCV) y por la Fabrica Nacional de Moneda y Timbre (FNMT).

Para solicitar un certificado digital bastará con acudir a uno de los puntos de registro con el DNI en vigor (se dispone de toda la información en la web ***www.accv.es*** o ***www.fnmt.es***).

Los certificados se pueden entregar a los usuarios en distintos formatos, como disquetes, memorias USB, o tarjetas criptográficas. Dependiendo de este soporte y del sistema operativo, la instalación será de forma diferente, quedando ese proceso fuera del alcance de este curso.

Una vez configurados los certificados en nuestro equipo siguiendo las pautas de la autoridad de certificación, veamos dos de sus diferentes usos, como son la firma digital y el cifrado de correos electrónicos:

Firma digital: Al enviar un correo electrónico firmado, garantizamos al receptor que somos el autor del correo electrónico y garantizamos que el correo no ha sido modificado. Nótese que al garantizar que somos el autor, añadimos la cualidad de **no-repudio**, por lo que no podremos negar que hemos sido los autores del correo.

Esto se consigue mediante un proceso criptográfico que combina el propio correo electrónico con una parte de nuestro certificado digital llamada "clave privada", la cual solo nosotros conocemos.

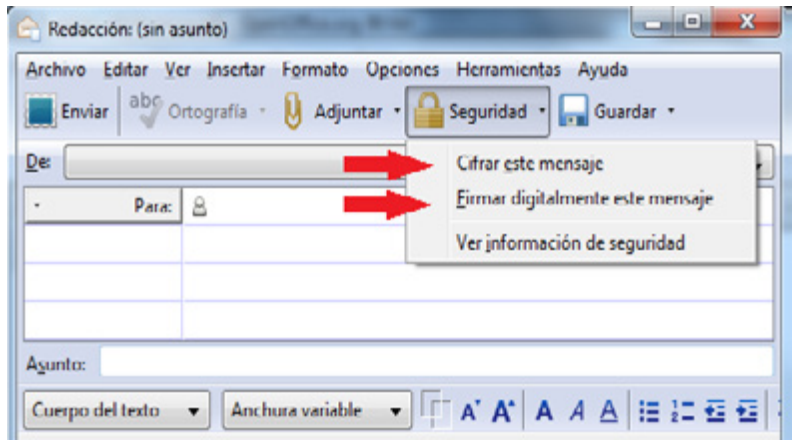


Ilustración 25 · Cifrar y firmar correo

Al recibir el correo, el remitente utilizará otro proceso criptográfico combinando el correo firmado con otra parte de nuestro certificado llamada "clave pública" que como indica el nombre es pública y cualquiera puede consultar, obteniendo como resultado la verificación de si el correo es original o no.

Si los certificados digitales están correctamente instalados, al seleccionar la opción "Firmar este mensaje", tanto el proceso de firmado, como el de comprobación se realizan automáticamente, sin necesitar ninguna acción por parte del usuario.

Cifrado digital: Al enviar un correo electrónico cifrado garantizamos que únicamente el receptor pueda ver el contenido del correo electrónico.

La explicación tecnológica es similar a la anterior: en este caso, se aplica otro algoritmo criptográfico utilizando la clave pública del receptor sobre el correo, con lo que obtendremos un mensaje ilegible, que al aplicarle el receptor otro algoritmo combinándolo con su clave privada, que únicamente él conoce, obtendrá el correo en un formato legible. Nótese que de esta forma, no es necesario que ambos usuarios intercambien ninguna contraseña para descifrar el correo, como sucede en el cifrado tradicional.

Al igual que en el caso anterior, tanto el cifrado como el descifrado son automáticos.

Hay que tener en cuenta dos aspectos importantes:

- Hay que ser consciente de que es relativamente sencillo falsificar el campo del remitente en un correo electrónico, de igual forma que las comunicaciones pueden ser interceptadas, por lo que según la información que compartamos por correo electrónico, han de tomarse unas u otras medidas de seguridad.

- No confundir la firma digital con el texto que se incluye al final de los correos electrónicos a modo de tarjeta de contacto, que también se conoce como firma.

4 Spam o publicidad no deseada: ¿Qué es y como evitarlo?

En algún momento, todo usuario de correo electrónico ha recibido o recibirá correos electrónicos con publicidad no solicitados, lo que conocemos como spam.

Según Viruslist.com, más del 80% de los correos electrónicos enviados durante el primer trimestre del 2009 fue spam. Este gran volumen supone unos importantes costes a las empresas y organismos que ofrecen servicios de correo electrónico ya que son la primera barrera para eliminar el spam.

La segunda barrera son los propios usuarios, que han de aprender a distinguir el spam, no fiarse de él, y aprender a evitarlo.

El spam acostumbra a ser fácil de distinguir a pesar de que puede ser de lo más variado: productos ilegales, medicamentos a bajo precio, viagra, páginas web con contenido para adultos, artículos de lujo, subastas...

A pesar de que nos pudiese interesar cualquiera de estos artículos nunca hemos de responder a los correos ni pulsar sobre los enlaces que hay en el correo ya que en los casos que no se trata de un virus, suele tratarse de estafas.

Estos son algunos ejemplos:

Usted ha sido premiado con un viaje a DisneyLand con su familia.

Llame urgentemente al número xxx xxx xxxx xxx

Realice llamadas telefónicas mitad de precio.

Marque el número xxx y obtendrá un descuento de 50 % de sus llamadas.

Acelere la velocidad de su conexión a Internet...

Generalmente, los encargados de enviar spam "compran" listas de correos electrónicos a terceros y envían de forma masiva correos a todos ellos. Estas listas son recopiladas mediante consultas a buscadores, búsquedas en foros, correos "cadena" donde todos pulsa en reenviar a todos, etc..., por lo que la primera recomendación para prevenir el spam es no difundir nuestro correo electrónico mediante unas sencillas pautas:

No publicar el correo electrónico en páginas web

En lugar de poner el correo tal cual se puede utilizar una imagen en la que esté escrito el correo, de forma que al no ser texto, un buscador no lo mostrará como resultado. Otra opción es no escribir la arroba, sino cambiarla por la propia palabra: micorreoARROBAmidominio.com. De estas dos formas evitamos que nos puedan localizar haciendo búsquedas por ejemplo en Google.

No publicar el correo electrónico en foros

Igual que en el caso anterior, no es recomendable escribir el correo electrónico en un foro. Es una mala práctica habitual responder en foros públicos solicitando información a otro usuario e indicando nuestro correo. En lugar de publicar un comentario con nuestra dirección, debemos enviarle un mensaje privado indicándole nuestro correo de forma que solo sea visible por él.

Utilizar una cuenta de correo distinta para los sitios de no confianza

Cuando nos registramos en una página, ya sea un foro, una comunidad, o una red social, acostumbran a solicitarnos el correo electrónico. Si proporcionamos

nuestro corre electrónico personal nos arriesgamos que el administrador de la página venda esas listas de correos, legal o ilegalmente, a spamers para que nos envíen publicidad, por lo que según la confianza que tengamos en la web, podemos utilizar una segunda cuenta de correo a la que no nos importa que nos envíen spam y que solo utilizaremos para este tipo de registros. Hay que destacar que en algunos casos, al registrarnos en algún foro/página, y hacer click en "acepto las condiciones y términos" estamos dando el consentimiento para que se nos envíe publicidad. Es por ello que conviene leer las condiciones que acostumbramos a aceptar ciegamente.

No responder a correos de spam

Cuando un spamer compra una lista de correos electrónicos no tiene la certeza de que esas cuentas sean validas, ya que estas pueden haber sido borradas, dadas de baja, o simplemente que no las lea nadie. Sin embargo, si respondemos a un correo de spam estamos anunciando que esa cuenta está activa y que alguien la lee, por lo que es muy posible que veamos incrementada la cantidad de correo basura.

Filtrado en los clientes

Los usuarios que descargan su correo electrónico al equipo mediante clientes (recordamos, Mozilla Thunderbird, Microsoft Outlook, Eudora...), tiene la posibilidad de crear sus propias reglas de filtrado a mano. Una buena práctica es el filtrado mediante palabras clave. Así pues podemos crear un filtro para que todos los correos que contengan palabras típicas de correos de spam (viagra, rolex, free, etc) se archiven en una carpeta especial destinada al spam. Adicionalmente existen aplicaciones gratuitas o comerciales dedicadas a bloquear spam que instalan plugins en nuestros clientes y realizan esta tarea por nosotros, e incluso resulta cada vez más frecuente que estas funcionalidades se incluyan como opciones extra en suites antivirus.

Filtrado en webmail

En el caso de utilizar webmail, la mayoría de proveedores dispone de herramientas para marcar el correo como no deseado o spam. De esta forma, el sistema aprenderá que tipo de correos ha de identificar como spam, haciendo que a largo plazo este se vea reducido.

Contactar con el administrador del correo

Generalmente, en entornos profesionales, los administradores del correo electrónico disponen de herramientas para filtrar el spam. Conviene informarse de si existe algún mecanismo para notificarles el spam recibido para que lo incluyan en una lista negra, por ejemplo reenviándolo a cierta cuenta de correo. De esta forma ningún usuario volverá a recibir ese correo de spam.

Puede obtenerse más información sobre como provenir y evitar las Cadenas de Correos y el SPAM en el este informe del CSIRT-CV.

5 Engaños y estafas

Junto con el auge del correo electrónico han surgido numerosas amenazas que debemos conocer y saber identificar para protegernos.

A diferencia del spam, el cual se puede frenar con medidas tecnológicas, las estafas utilizan lo que se denomina "ingeniería social" que no es otra cosa que mentir para engañar y estafar a la antigua usanza, pero jugando con las principales ventajas que proporciona Internet: conectividad con todo el mundo y anonimato.

Noticias engañosas (hoax)

Se trata de correos en forma de cadena que generalmente persiguen conseguir la mayor difusión posible.

La temática es muy variada y cada día surgen nuevas cadenas, aunque todas comparten una serie de características.

1. Todas acaban solicitando ser reenviados a todos los contactos, para de esta manera llegar al mayor número de usuarios posibles. Un riesgo de esta práctica es, como ya se ha visto en un apartado anterior, que al reenviar se acostumbra a no incluir los destinatarios en copia oculta (CCO), por lo que las cuentas de correo que aparecen en estas listas son propensas a caer en manos de spamers.

2. Son intemporales por no llevar la fecha de cuando se inició la cadena. En caso de que la cadena pida ayuda para una operación médica, salvar una perrera, o participar en una promoción, es muy posible que la cadena empezase meses antes o incluso años, por lo que si fuese real, la perrera habría cerrado o la promoción finalizado.

3. Muchas veces requieren reenviarlo a un número concreto de contactos para cumplir con la finalidad del correo, ya sea participar en una promoción o que una empresa pague dinero por motivos solidarios en base al impacto de la cadena. Se ha de tener en cuenta que si reenviamos un correo a nuestros contactos, ninguna empresa o servicio externo tiene forma de saberlo, por lo que lo que se promete en estos correos no tiene sentido. En los casos que realmente existen campañas publicitarias que requieren recomendaciones a conocidos, estas se realizan desde paginas web con formularios para que el anunciante tenga la certeza de que la recomendación se ha realizado.

Estos son algunos ejemplos:

- ¡¡Peligro!! hay un nuevo virus informático muy peligroso descubierto por la compañía X. Si tienes el fichero Y en la carpeta Z estás infectado. Borrarlo lo antes posible!! Reenvía este correo a todos tus contactos!!!

- ¡¡Ayuda!!l hijo de una amiga padece la enfermedad X. Se trata de una enfermedad muy rara y el tratamiento vale Y. La compañía Z se compromete a pagar un euro de la operación por cada persona que reenvíe este correo. Reenvía este correo a todos tus contactos!!!

• ¡¡Atención!! Este es un método infalible para ganar al poker en casinos online. Garantizado!! Solo hay que hacer lo siguiente […] Reenvía este correo a todos tus contactos!!!

• ¡¡Portátiles gratis!! HP está promocionando sus nuevos portátiles y para ello los está regalando. Para conseguir uno solo tienes que reenviar este correo a 10 contactos y recibirás una respuesta con información de donde recogerlo. Reenvía este correo a todos tus contactos!!!

• ¡¡Cierran messenger!! Messenger se está quedando sin cuentas y van a borrar todas las de los usuarios que no sean activos. Para salvar tu cuenta reenvía este correo a todos tus contactos!!

• ¡¡Cuidado!! Hay nueva banda criminal en la ciudad. Si por la noche ves un coche circulando con las luces apagadas no le hagas luces!! El rito de iniciación de esta nueva banda consiste en conducir a oscuras y si alguien le hace luces deben perseguirle y robarle. Avisa a todos tus contactos!!!

• ¡¡Peligro!! Si recibes una llamada telefónica en dónde en lugar de un número de teléfono aparece la palabra "INVIABLE!!"es una estafa. Si aceptas o rechazas la llamada el extorsionador accede a la SIM de tu teléfono, la duplica y la usa para llamar desde la cárcel

Estafas

Estas son muy similares a las estafas tradicionales y buscan siempre el beneficio económico.

Destacan, por ejemplo, las "cartas nigerianas", correos en los que se nos informa que algún pariente lejano ha fallecido y nos ha dejado una importante herencia en otro país, pero que se requieren muchos tramites internacionales para cobrarla y se solicita una pequeña cantidad de dinero para agilizar los trámites. Una vez los estafadores reciben el dinero, solicitan más, alegando que las gestiones se han complicado y así sucesivamente el tamaño de la esta aumenta.

Una variante del caso anterior es informar de que el usuario ha ganado un premio de lotería de otro país, y se requieren gestiones para tramitar el cobro.

También merece especial mención el "scam". Son correos que llegan generalmente de mujeres de países de Europa del este, que buscan pareja. Los correos acostumbran a estar mal redactados y adjuntan fotografías de las supuestas mujeres. En realidad, tras estos correos hay mafias organizadas que buscan que el receptor del correo crea que realmente está estableciendo una relación, para más adelante pedir pequeñas cantidades de dinero para gastos que les surgen a las supuestas mujeres: educación, multas, hipotecas... las relaciones se establecen únicamente por Internet y evitan las webcam y el teléfono.

6 Phishing

El phishing es una técnica por la cual se suplanta la identidad de los administradores de un servicio (generalmente banca online, paypal, ebay o correo electrónico) para solicitar las credenciales de acceso al usuario. Los ataques más sencillos consisten en correos electrónicos haciéndose pasar por los administradores, ya sea del banco o del servicio de correo que, alegando problemas técnicos, solicitan a las potenciales víctimas las cuentas de usuario y contraseña de acceso.

En otros casos más elaborados, los atacantes clonan íntegramente la página web del banco o servicio y la alojan en un dominio parecido (de su propiedad o un servidor vulnerado para este propósito). Esta página nada tiene que ver con la del banco y por lo tanto, si introducimos nuestro usuario y contraseña, estaremos ofreciendo a los atacantes todo lo necesario para acceder a nuestra cuenta real. Para hacernos llegar a estas páginas engañosas lo más frecuente es el envío de correos electrónicos fraudulentos, también con el mismo diseño que los enviados por un banco real, que contienen enlaces a dicha página fraudulenta

En ambos casos hay que seguir una serie de pautas para evitar ser engañados:

- Nunca revelar las contraseñas. Los administradores de un servicio nunca nos pedirán la contraseña por ningún motivo.

- Nunca hacer click en los enlaces de correos electrónicos relacionados con banca online. siempre escribir la dirección en el navegador, ya que aunque en el texto del enlace parezca que la dirección es correcta, es posible que seamos redirigidos a un sitio web fraudulento.

- Comprobar el certificado del servidor web (consultar capítulo 4).

La Asociación de Internautas ha publicado una guía para detectar este tipo de páginas: http://www.seguridadenlared.org/61.html En el caso de detectar un correo o un sitio web sospechosos de albergar phishing, es posible reportarlo a la entidad afectada o hacer uso del servicio de ***Reporte de Phishing***[28] ofrecido por CSIRT-CV.

28 Accesible en http://www.csirtcv.gva.es/es/formulario/informar-de-un-phishing.html

6

COMPRAS ONLINE

1 Introducción

El comercio, actividad ancestral del ser humano, ha evolucionado de muchas formas. Pero su significado y su fin es siempre el mismo. Según el diccionario consultor de economía, el Comercio es "el proceso y los mecanismos utilizados, necesarios para colocar las mercancías, que son elaboradas en las unidades de producción, en los centros de consumo en donde se aprovisionan los consumidores, último eslabón de la cadena de comercialización. Es comunicación y trato".

La popularización de Internet ha hecho que muchos de los hábitos de la gente estén cambiando, incluido el del consumo. Cada vez son más las personas que se animan a comprar a través de Internet cualquier tipo de producto o servicio.

Viajes, entradas para espectáculos, material informático y audiovisual... y casi cualquier cosa que se pueda pensarse, se puede comprar a través de Internet, ya sea en tiendas "oficiales" o en portales de subastas.

Pero al realizar estas compras, como en cualquier otra que realizamos por el "método tradicional", deben seguirse unas ciertas indicaciones que ayudarán a que estas sean lo más seguras posible.

Al finalizar esta unidad del curso se espera que el alumno:

- Tenga un conocimiento básico sobre el fraude en Internet y los métodos usados por los ciber-delincuentes para llevar a cabo grabes delitos.

- Entienda la importancia de la seguridad en las transacciones por Internet y las relacione con los conceptos de transmisiones seguras que se verán en los apartados de HTTPS y Certificados.

- Compruebe y exija los derechos y garantias que conllevan una compra online así como las leyes que les afectan.

- Conozca los diferentes métodos de pago para compras online, sus características principales y los métodos que utilizan, para que de esta forma sea capaz de elegir la que mejor se adapta a sus necesidades.

2 Fraude / Ingeniería Social

No todo lo que se lee en Internet tiene porque ser cierto. Además, los defraudadores aprovechan la credulidad de los usuarios para su provecho, por lo que conviene usar el sentido común y contrastar la información.

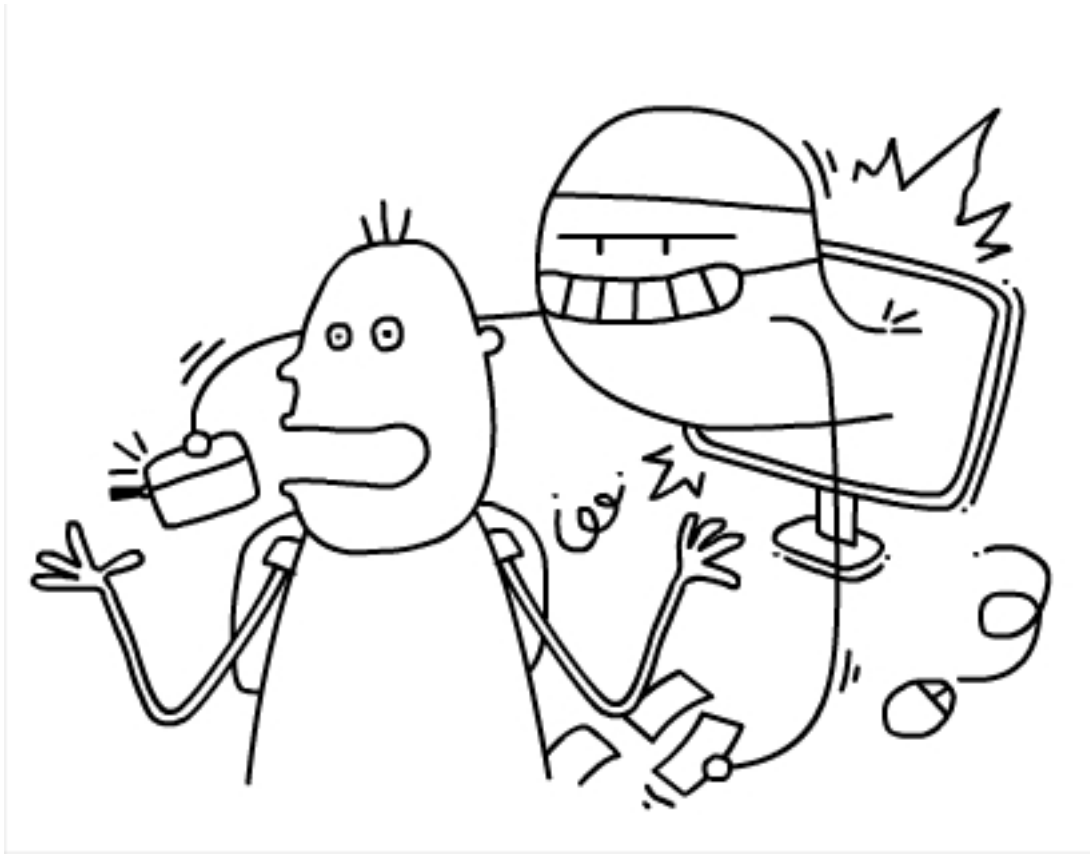


Ilustración 26 · Ingeniería social

En quien y que confiar

Del mismo modo que en la vida real cuando se lee una revista, se ve la televisión o se habla directamente con una persona se tiene en cuenta una serie de factores que ayudan a poner en valor la información obtenida, en Internet debe actuarse de idéntica manera.

Que este publicado en Internet no quiere decir que sea veraz

Tener una reputación contrastada a lo largo del tiempo, haber confiado en ella en anteriores ocasiones o transmitir la información de forma clara y concisa son aspectos que ayudaran a valorar una fuente como confiable. Otra opción siempre aconsejable es contrastar la información en una fuente alternativa.

No asegurarse de en quien confiar puede suponer tomar como ciertos contenidos falsos o faltos de rigor. Pero se tiene que tener en cuenta que los ciberdelincuentes también aprovechan la credulidad del usuario para embaucarle a realizar determinadas acciones en su beneficio, lo que se conoce como **ingeniería social.**

El engaño puede conllevar grabes consecuencias, desde aceptar sin miramientos la ejecución de un fichero que contiene un virus, hasta suministrarles inocentemente las claves del banco.

Asegurarse que realmente es quien dice ser

Además de saber en quien confiar, también se debe asegurar que el interlocutor es quien dice ser. Sobre todo en los servicios de banca y comercio en los que el dinero esta en juego.

No confiarse es siempre el mejor consejo. Antes de realizar cualquier operación a través de una web verificar la legitimidad de la página. Y del mismo modo, antes

de responder a un remitente de correo electrónico desconocido, asegúrarse de que no se trata de un mensaje fraudulento.

El peligro de la suplantación de la identidad

La mayoría de fraudes actualmente pasan por suplantar la identidad en línea de un tercero. Para ello los estafadores se apoyan en la ingeniería social, con la que conseguir las credenciales de acceso -o como paso previo la suficiente información privada- de los servicios de banca, comercio, etc.

No ponerlo fácil a los estafadores. Si se conocen los elementos que se utilizan para el fraude en internet se podrá reconocer más fácilmente los principales tipos de fraude que se pueden encontrar y no caer en su trampa.

3 Fraude en Internet

Los estafadores que predominan en Internet se aprovechan de los servicios y la facilidad de comunicación que proporciona la red para construir el engaño y conseguir su beneficio. Aunque, dependiendo del tipo de fraude se utilizan diferentes elementos, a continuación se resume cuáles son sus principales herramientas:

- La **Ingeniería Social** es la herramienta más utilizada para llevar a cabo toda clase de estafas, fraudes y timos sobre los usuarios más confiados a través del engaño. Estas técnicas consisten en utilizar un reclamo para atraer la atención del usuario y conseguir que este actue de la forma deseada, por ejemplo convenciéndolo de la necesidad de que reenvíe un correo a la lista de direcciones, que abra un archivo que acaba de recibir y que contiene un código malicioso, o que, como ocurre en el phishing, utilice un enlace que ellos proporcionan para visitar su banco e introducir sus códigos y claves. Para captar su atención, utilizan referencias a temas de actualidad, nombres de personajes famosos, denuncias de injusticias o catástrofes humanitarias o fechas significativas como la Navidad. Además, los timadores presionan o incluso amenazan al usuario que no siga sus indicaciones.

- El **correo masivo y no deseado**, conocido como **spam**, proporciona el mejor y más barato mecanismo de difusión de cualquier información y, por lo tanto, de cualquier intento de fraude. Los estafadores aprovechan la posibilidad de enviar gratis millones de correos con una misma estafa para aumentar la probabilidad de que alguien caiga en su trampa.

- Los **virus** y **códigos maliciosos** en general, también pueden ser diseñados para capturar información personal, como por ejemplo, los datos que se intercambian con una determinada entidad o las pulsaciones del teclado cuando se accede a una determinada página web.

4 HTTPS – Transferencia segura de datos

En la barra de direcciones del navegador se ve muchas “http://” y luego la dirección de la página. Esto, sin entrar en tecnicismos, está indicándole al navegador que debe usar el protocolo HTTP para llegar e interpretar la web que se le introduce. Si no existiera http, no se podría acceder e interactuar en la red de redes como se hace actualmente.

Pero este protocolo no es del todo seguro y puede ser capturado y leído por cualquier persona que intercepte la comunicación. Es por eso que se mejoró el protocolo añadiéndole a los datos un cifrado con el objetivo de hacerlo más seguro, generando de esa forma un protocolo de seguridad.

Es por esta razón por la que se aconseja introducir en el navegador “https://” antes de introducir direcciones de webs críticas (bancos, páginas de compras, agencias de viajes o incluso la web donse se consulta el correo) o de realizar un envío de datos críticos.

Se puede comprobar que al conectar a un sitio Web crítico, como puede ser un banco o alguna página donde se realicen pagos o transferencias monetarias, cambia en la barra de direcciones al llegar a cierta página dentro del dominio visitado. Esto indica que se ha llegado a una “zona segura” con una sesión segura.

Los navagadores suelen indicar la presencia en una web con conexión segura mostrando un color diferente en la barra de direcciones, la cadena “https://” antes de la dirección web y con un candado cerrado en el navegador.

Para entender este sistema se muestra un ejemplo cuando se accede a la web de la Agencia Tributaria:

En primer lugar se muestra como el entorno es no seguro, por lo que la información transmitida puede ser captura y leída por un tercero. En la barra de direcciones aparece ‘http’ y no se observa ningún cambio de color en la barra de direcciones..

Cuando se pulsa en el enlace de “Tramitación: Servicio de Cálculo de Retenciones”, se abre una nueva pestaña como la que muestra la segunda imagen. En ella se puede comprobar como aparecen tanto el prefijo ‘https’ como el nombre de la dirección en fondo azul. Si pulsamos sobre dicho campo, aparece información relacionada con el certificado que autentica esa dirección.

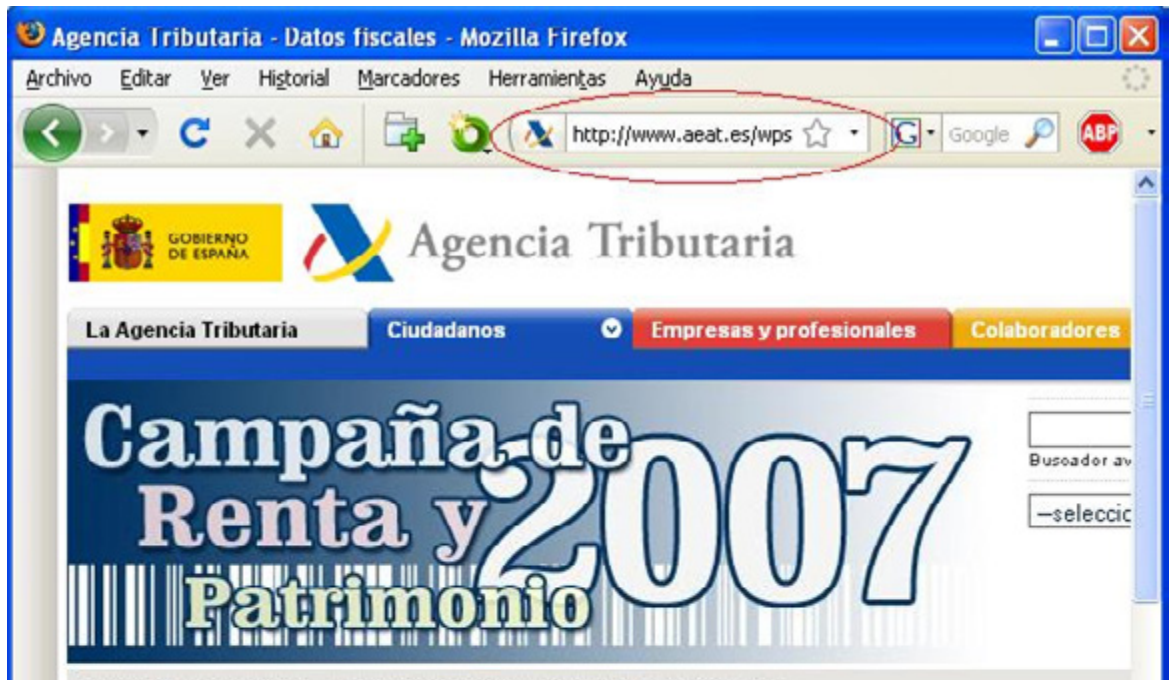


Ilustración 27 · Detalle navegador http

Ilustración 28 · Detalle navegador https

Este cambio de protocolo se debe a que la web actual tiene un formulario en el que se van a introducir y enviar datos de carácter personal que, para garantizar la seguridad, serán enviados de forma cifrada.

5 Certificados

Uno de los problemas que surgen en Internet es el de la identificación de las personas o entidades. ¿Cómo asegurarse de que una clave pública que se recibe o encuentra en Internet pertenece realmente a quién dice pertenecer?

Una posible solución es la utilización de un certificado digital. Este es fichero digital intransferible y no modificable, emitido por una tercera parte de confianza (Autoridad de Certificación), que asocia a una persona o entidad una clave pública.

Un certificado digital standard, utilizado por los navegadores, contiene la siguiente

información:

- Identificación del titular del certificado: Nombre, dirección, etc.
- Clave pública del titular del certificado.
- Fecha de validez.
- Número de serie.
- Identificación del emisor del certificado.

Un detalle muy importante a tener en cuenta es que en muchas ocasiones se detecta como lugares inseguros páginas web totalmente legítimas. Normalmente es debido a que no se reconoce la Autoridad de Certificación que emite el certificado que la auntentica. Esto es debido a que estas AC no están incluidas entre las que incluye el navegador por defecto, pero esto no significa que no sean Acs legítimas. Lo aconsejable es obtener el certificado, verlo y comprobar que la AC es de confianza. Los mensajes que muestra el navegador son similares a los siguientes. En esta caso la AC que en la que el navegador no confia es la Autoridad de Certificación de la Comunitat Valenciana (ACCV).

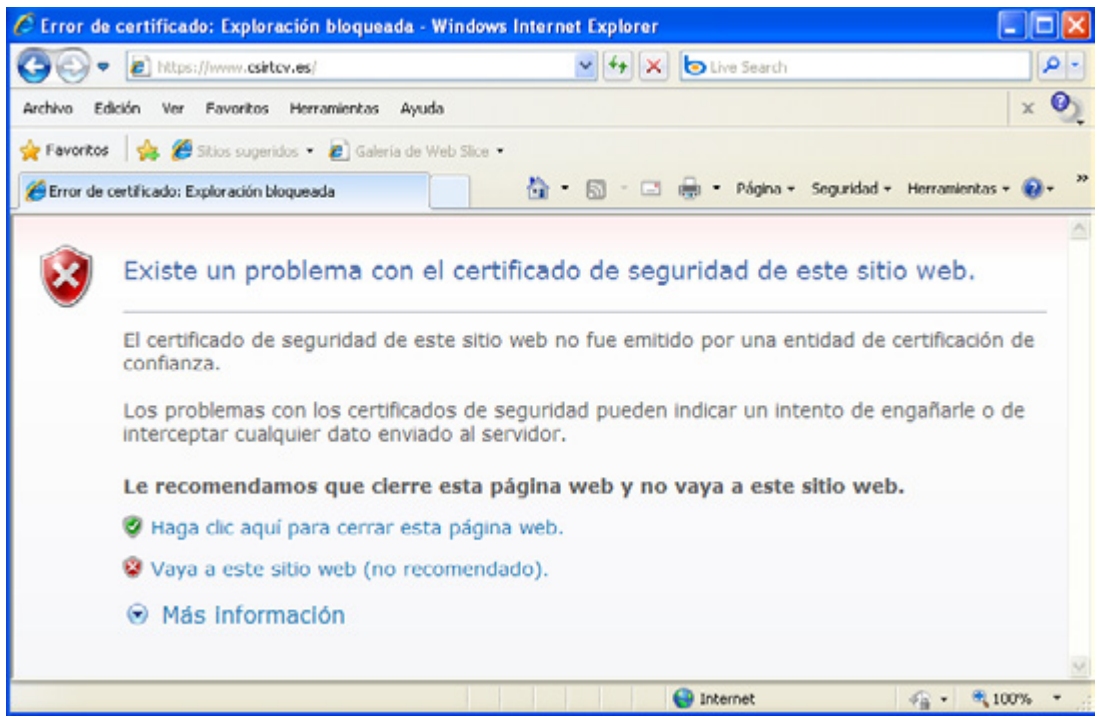


Ilustración 29 · Detalle error de certificado

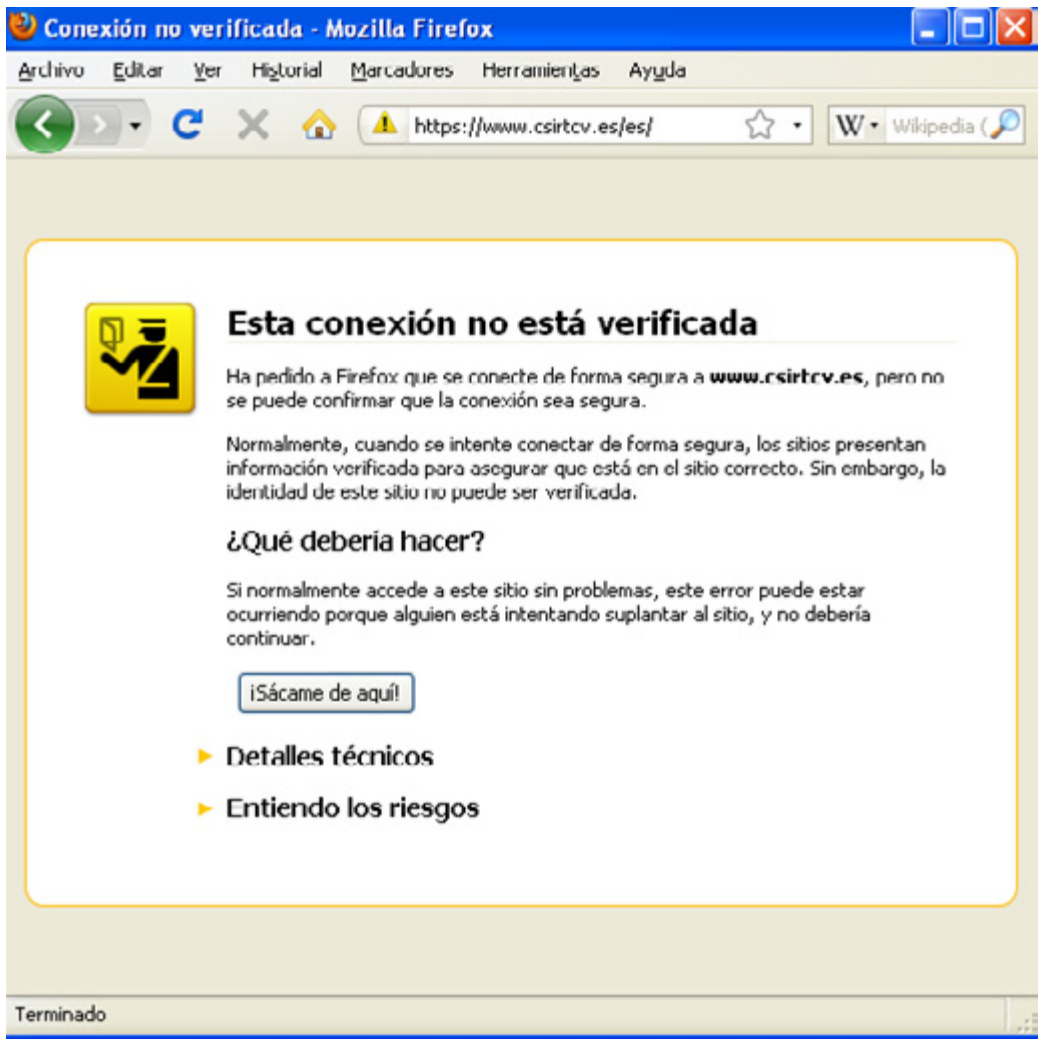


Ilustración 30 · Detalle conexión no verificada

Más información sobre los certificados (como crearlos, como obtenerlos, como usarlos...) en ***http://www.accv.es***

6 Banca Online

Ilustración 31 · Banca online

En este punto se indican una serie de consejos a seguir a la hora de realizar cualquier operación bancaria a través de Internet. La lógica y el sentido común, como siempre, son un gran aliado en el desarrollo de una navegación segura por la Web, pero hay que hacer incapie en ciertos aspectos y seguir unas normas

básica como las que se exponen a continuación:

• Observar que la dirección empieza por **https**, lo que indica que se trata de una conexión segura.

• Observar que aparece un **candado** en la parte inferior derecha del navegador. 

• Asegurarse de la validez de los **certificados** (pulsando en el candado), que coinciden con la entidad solicitada y sean vigentes y válidos.

• Tener en cuenta que el banco **NUNCA** solicita información confidencial por correo electrónico ni por teléfono.

• Evitar el uso de **equipos públicos** (cibercafés, estaciones o aeropuertos, etc) para realizar transacciones comerciales.

• Desactivar la opción **autocompletar** si se accede desde un equipo distinto al habitual o se comparte el equipo con otras personas.

• **Cerrar la sesión** cuando se termine, para evitar que alguien pueda acceder a los últimos movimientos, cambiar claves, hacer transferencias, etc.

• Instalar alguna herramienta **antifraude** para evitar acceder a páginas fraudulentas. Dos ejemplos de estas herramientas son:

1. *Netcraft*[29]: Protege de los ataques de phishing. Vigila donde se hospeda y proporciona un índice de riesgo de los sitios que visitas. Ayuda a defender a la comunidad internauta de fraudes. Disponible para Firefox e Internet Explorer.

2. Diagnóstico Google: Para saber si un sitio Web es seguro, Google dispone de una página de consulta basada en el número de páginas que Google ha indexado de ese sitio y lo que haya encontrado en ella. Por ejemplo, hemos consultado si www.csirtcv.gva.es es una página peligrosa, para ello se contruye está URL: ***http://www.google.com/safebrowsing/diagnostic?site=csirtcv.gva.es***

Para consultar la web que desee comprobar, sustituya la cadena "csirtcv.gva.es" tras "site=" por el nombre de dominio de la web (quitando las www).

7 Compras Seguras

Debido a varios casos de fraude y estafa, se ha extendido entre los consumidores en general un excesivo temor a las compras por internet. Como en cualquier otro tipo de compra se debe ser cauto y saber exactamente qué se quiere comprar y a quién.

29 Accesible en http://news.netcraft.com/

Ilustración 32 · Compras seguras

Conexiones Seguras

Los portales de internet que ofrecen la posibilidad de realizar compras a través de ellos, utilizan para sus conexiones protocolos seguros, por lo que se debe comprobar que en el navegador aparece https delante de la dirección y el icono de un candado en la parte inferior, para asegurarnos de que los datos sensibles son codificados antes de transmitirlos. Esto indica que esa web cuenta con una acreditación de una Autoridad de certificación que garantiza que es quien dice ser. La Autoridad de certificación más extendida en la red es VeriSign y en España se ha creado el programa ***Confianza Online***[30].

Como siempre, los sitios web con más renombre aportan un nivel extra de confianza. Pero también son el objetivo más suculento para todo tipo de estafas, por lo que se debe tener especial cuidado al acceder a estos portales introduciendo la dirección directamente en el navegador en lugar de acceder desde un correo electrónico o desde un enlace en otra página web.

Condiciones de compra

Los sistemas de seguridad electrónicos no deben ser los únicos que deben tenerse en cuenta. Los sistemas de garantías deben ser los mismos o mayores que en una compra ordinaria, por lo que las condiciones de garantía, devolución y gastos de envío deben quedar muy claras ya que cualquier fallo o defecto requerirá un reenvío del producto y un desembolso por el mismo.

Por otra parte, el no poder ver físicamente el producto hasta que se recibe, hace a los usuarios vulnerables a engaños o estafas ya que una foto del producto puede no corresponder al mismo (puede ser de otro modelo, puede venir directamente de la web del fabricante, etc...). Por ello es importante obtener la máxima información sobre el artículo a comprar, comparando precios y características en otras páginas web.

LOPD (Ley Orgánica de Protección de Datos)

Otro punto a tener en cuenta y que es importante que el comerciante cumpla es la LOPD, por lo que se debe exponer claramente el uso y tratamiento que se

30 Accesible en http://www.confianzaonline.es/

le va a dar a los datos personales. Los sitios web están obligados a indicarlo y a garantizar la seguridad de los mismos.

Ley de Propiedad Intelectual: LPI

Por otro lado, la Ley de Propiedad Intelectual indica que los programas de ordenador (aplicaciones y juegos) pirateados son delito y prevé multas por ello. El portal de venta debe cumplir esta ley y no comerciar con material pirata. Recordar que el software pirateado son aquellos programas -excluyendo los gratuitos y libres- que se utilizan sin haber pagado previamente su licencia de uso.

Atención al Cliente

Por último, para asegurar la legalidad o autenticidad del portal de compra, deben comprobarse los medios que la página disponga para la comunicación. Lo normal es un número de teléfono o una dirección de correo electrónico para el contacto. Si el sistema a usar resulta sospechoso (p.e. hablar por messenger), se debe desconfiar del portal.

Es imposible acudir a los diferentes organismos existente para consultar los derechos en materia de consumo o conseguir asistencia o asesoramiento en el caso de ser necesario realizar una reclamación. Si el producto está comprado en España es posible dirigirse al ***Instituto Nacional del Consumo***[31] o al ***Sistema Arbitral de Consumo***[32]. Si ha sido adquirido en otro país de Europa se puede hacer en el ***Centro Europeo del Consumidor***[33].

8 Métodos de pago

En este apartado se exponen los diferentes métodos de pago de los que se pueden hacer uso para realizar compras en la Web.

Principales métodos de pago Online:

Tarjetas Bancarias

Tarjetas de Crédito o débito. Además del número y la fecha de caducidad, es necesario introducir el código adicional CVV (Valor de Validación de la tarjeta de Crédito) como garantía de que se encuentra en poder del usuario. Algunos bancos ofrecen el sistema de pago seguro, donde el usuario añade una contraseña extra, necesaria antes de validar definitivamente la compra

Tarjetas Virtuales

Son ofrecidas por algunos bancos o cajas para el pago online. Para ello se genera un número de tarjeta (asociado a la cuenta del usuario) para una compra determinada. Deja de ser válido y es eliminado una vez la transacción se realiza

PayPal

Método novedoso y adecuado para pequeños pagos online. El usuario se da de alta en el portal de la empresa, donde debe introducir de forma segura los

31 Accesible en http://www.consumo-inc.es/
32 Accesible en http://www.consumo-inc.es/Arbitraje/home.htm
33 Accesible en http://cec.consumo-inc.es/

datos bancarios. Luego puede comprar desde cualquier página que acepte este tipo de medio de pago (cada vez hay más páginas asociadas a este sistema) sin necesidad de volver a introducir el número de tarjeta, ya que es suficiente con usar los datos de la cuenta asociada a PayPal. Son ellos los encargados de mandar el importe al vendedor

Mobipay

Sistema de pago a través del teléfono móvil que se asocia previamente a una tarjeta de crédito emitida por la entidad del usuario. Facilita las compras ya que solo hay que enviar un mensaje de texto y las operaciones se gestionan a través de las redes de los operadores de telefonía móvil y de los sistemas de medios de pago financieros, que gestionan diariamente millones de transacciones en las más altas condiciones de seguridad

Transferencia Bancaria

Transacción de dinero de la cuenta del usuario a la del vendedor. En algunos bancos o cajas este servicio es gratuito. Algunas entidades mandan un SMS al teléfono móvil del usuario para confirmar la operación

Ukash

Bonos que se adquieren en oficinas de Correos o Telecor para poder efectuar un pago en internet. Se introduce el código de 19 dígitos en la web y se descuenta automáticamente el importe del saldo del cupón

Firma Electrónica

Sistema de acreditación que permite asociar la identidad de las personas, con el mismo valor que la firma manuscrita. Es necesario un hardware y un software específico para realizar el pago. El nuevo DNI electrónico incorpora ya este sistema

Contra reembolso

Sistema de pago por el que el usuario abona el importe del producto a un cartero, mensajero o transportista al recibirlo en su domicilio. Deben quedar claras las condiciones (quién paga los gastos y a cuanto ascienden) antes de realizar la operación.

7

SEGURIDAD EN CHAT, MENSAJERÍA INSTANTÁNEA Y REDES SOCIALES

Resulta indiscutible que la formas de comunicación han cambiado. La tecnología ha sido capaz de revolucionar algo tan arraigado como el correo tradicional o incluso el teléfono. El concepto del correo fue inventado hace siglos y realmente ha quedado obsoleto por ser unidireccional y no instantáneo, mientras que las opciones que nos brindan las nuevas tecnologías se han posicionado como fuertes competidores destacando el chat, la mensajería instantánea y más recientemente, las redes sociales.

Existen multitud de tecnologías y protocolos para comunicarse a través de la red, y cada una de ellas tiene características muy diferenciadas que hacen que, dependiendo del servicio que busquemos, utilicemos una tecnología u otra.

Entre las posibilidades que se nos brindan las más utilizadas son el chat, la mensajería instantánea, videoconferencia o compartición de ficheros.

1 Acoso a través de la red

Aparte de las características técnicas y funcionales de cada tecnología, que más adelante se detallaran, existe un riesgo común en todas ellas: el acoso a los usuarios.

Generalmente se trata de desconocidos, o conocidos con malas intenciones, con los que se establece algún tipo de relación a través de la red, y que buscan principalmente la extorsión con amenazas de difundir fotografías comprometidas, vídeos grabados con webcam, o similar y que a cambio, exigen dinero o material pornográfico.

En algunos casos más extremos, hay quienes se llegan a obsesionar con gente que conocen a través de la red, y que al ser rechazados toman represalias online o incluso físicamente.

Es por ello que igual que en la vida real no damos nuestros datos a cualquier desconocido, en la red hemos de actuar igual, o incluso ser más cautelosos, ya que el anonimato que ofrece internet, juega de parte de los usuarios maliciosos.

En caso de ser víctima de acosos de esta índole, es recomendable no ceder a los chantajes y denunciarlo lo antes posible, ya que se trata de un delito, igual que en la vida real. Para ello está a disposición de los ciudadanos la ***web de la policía***[34]

2 Chat

El chat es un servicio que nos permite enviar y recibir texto en tiempo real con otros usuarios de la red. Estos nos pueden responder también al instante por lo que a una sesión de chat se le llama "conversación".

34 Accesible en http://www.policia.es/org_central/judicial/udef/bit_alertas.html

Esta comunicación puede realizarse de muchas formas entre las que destacan el ***IRC***[35]y el chat web, por ser las que más usuarios han captado.

2.1 IRC (Internet relay chat)

Es un protocolo que se utiliza para comunicarse mediante texto en tiempo real creado en 1988.

Ilustración 33 · IRC

Se trata de un ***protocolo***[36] estándar, que utilizan varios programas para que sus usuarios puedan comunicarse. Es un protocolo que bien utilizado ofrece buenos niveles de seguridad, aunque no siempre se implementa correctamente, por lo que es en el programa que se utiliza para conectar a la red donde se encuentran la mayoría de los problemas de seguridad.

A pesar de ello, para poder utilizar IRC con un buen nivel de seguridad basta con seguir unas sencillas indicaciones:

Utilizar siempre las últimas versiones de los clientes de IRC. Históricamente, la mayoría de los usuarios utilizaban clientes muy básicos a los que añadían ***scripts***[37] para poder utilizar nuevas características. Posteriormente se descubrió que la mayoría de estos scripts eran vulnerables a diversos ataques por lo que se tomó conciencia del riesgo y en las versiones recientes de los clientes de IRC han quedado solventados estos problemas.

Comprobar las opciones de cifrado. Por defecto, las conexiones de IRC no viajan cifradas por lo que cualquier usuario que intercepte estas comunicaciones puede ver todas las conversaciones. Las versiones actuales de ***mIRC***[38], el cliente más popular de IRC, admite que las comunicaciones se cifren mediante ***SSL***[39], pero esta opción depende de que el servidor y todos los usuarios del canal dispongan de esta opción. Además, las comunicaciones van cifradas desde nuestro equipo al servidor, pero si este reenvía la información a

35 Accesible en http://es.wikipedia.org/wiki/Internet_Relay_Chat
36 Accesible http://es.wikipedia.org/wiki/Protocolo_(inform%C3%A1tica)
37 Accesible en http://es.wikipedia.org/wiki/Script_(inform%C3%A1tica)
38 Accesible en http://es.wikipedia.org/wiki/Mirc
39 Accesible en http://es.wikipedia.org/wiki/Ssl

otro servidor, estos datos viajarán en texto plano. Es por todo ello que no se recomienda utilizar el protocolo de IRC para transmitir información sensible, aunque en caso de necesitar garantías de confidencialidad, es posible utilizar scripts o clientes que permitan directamente las conexiones cifradas entre los usuarios.

No utilizar enlaces sospechosos. Existen programas o scipts que simulan ser usuarios normales, que ya sea respondiendo cuando se establece comunicación con ellos, o bien de forma automática, se dedican a enviar enlaces publicitarios a los usuarios. En muchas ocasiones se trata de enlaces a sitios maliciosos, por lo que es recomendable no pulsar sobre ellos.

Evitar utilizar nombres reales o el mismo nick/alias que se utiliza para mensajería instantánea. Al entrar a un servidor de IRC se solicita un nick o nombre de usuario. Es recomendable evitar utilizar el nombre real o el mismo nick de cuentas de correo, ya que como muchos usuarios siguen esta práctica, es muy posible que si buscamos en un buscador el nick de un usuario seguido de @hotmail.com o @gmail.com encontremos entradas suyas en foros, pudiendo saber sus aficiones e intereses (foros de deportes, ocio...), o llegar a encontrar fotos.

2.2 Webchat

Es una alternativa más popular y usable que IRC ya que no es necesario el uso de ningún cliente, sino que es suficiente con utilizar un navegador web y acceder a alguna de las muchas salas públicas que hay en la red. Generalmente utilizan Java, Flash, Ajax, o tecnologías similares, por lo que la seguridad al acceder a estos servicios, depende directamente del navegador y la versión de los plugins, si bien es cierto que es posible que aparezcan vulnerabilidades en el servicio, pero queda en mano de los administradores solucionarlo.

Dada su similitud con el chat tradicional se aplican las mismas recomendaciones de seguridad:

- **Utilizar navegadores web actualizados**, ya que en estos casos es en el propio navegador donde se ejecuta la sesión de chat.

- **Comprobar las opciones de cifrado:** por defecto, las conversaciones de webchat no tienen porqué ser cifradas, por lo que si deseamos cierto grado de confidencialidad debemos investigar las opciones que nos brinda el servicio. Hay que revisar las condiciones de uso del servicio, ya que es posible que por defecto se utilice cifrado (depende del servidor). También podemos intentar conectar mediante el protocolo seguro SSL, incluyendo una “S” en la dirección de la página de forma que quede “https” en lugar de ”http”. Si la página no

se carga querrá decir que el servidor no soporta esta opción.

• **No utilizar enlaces sospechosos,** ya que al ser ejecutados en el navegador, es posible que nos redirijan a servidores con contenidos maliciosos, o incluso que nos roben la sesión del chat de forma que perdamos nuestro usuario y contraseña.

• **No utilizar siempre el mismo nick,** por los mismos motivos que en el caso de conectarse a servidores IRC.

• **Evitar conectarse desde equipos públicos como cibercafés** para evitar que nuestra contraseña sea robada mediante programas maliciosos (***keyloggers***[40]).

• **Cerrar siempre la sesión al abandonar la chat** en lugar de limitarse a cerrar el navegador o la pestaña.

3 Mensajería instantánea

El concepto de mensajería instantánea se distingue principalmente de los chat tradicionales en que aporta el concepto de "contacto". Mientras que en un chat tradicional todos los usuarios pueden comunicarse entre ellos, en la mensajería instantánea previamente se debe solicitar al usuario el inicio de la comunicación y que este acepte. De esta forma, además se consigue disponer de una red de contactos más sólida, y cerrada.

Funcionalmente también operan de formas distintas a los chats tradicionales ya que, en la mayoría de los casos, es necesario utilizar un programa específico para utilizar el servicio, aunque algunos también disponen de interfaz web.

Los clientes de mensajería instantánea acostumbran a soportar más servicios de forma predeterminada que los chat o los canales de IRC, permitiendo realizar llamadas de voz, videoconferencias o envío de ficheros.

Estas cualidades, sumadas al hecho de que algunos clientes permiten instalar plugins de terceros, hace que sea necesario seguir ciertas normas de seguridad:

• **No aceptar como contactos a desconocidos.** La mayoría de estos servicios ofrecen perfiles del usuario que pueden ser consultados por el resto de contactos, por lo que es posible que revelemos información personal a desconocidos.

• **Comprobar qué información está accesible en los perfiles públicos.** Por el motivo anterior, conviene comprobar que información sobre nosotros muestra el perfil, ya que es posible que en la página de registro nos soliciten el teléfono, dirección, o incluso fotografías, información que no es recomendable que pueda ser consultada por usuarios fuera de nuestra red de contactos y que por descuido hayamos configurado de forma pública.

40 Accesible en http://es.wikipedia.org/wiki/Keylogger

• **Antes de aceptar la transferencia de un fichero, asegurarse de que no se trata de un envío fraudulento.** Existen virus que envían ficheros automáticamente a otros contactos utilizando nombres de fichero o textos automáticos que pueden engañar a los receptores. En estos casos el usuario recibirá un texto automático como puede ser "hola, aquí tienes mis últimas fotos" acompañados de un fichero "mis_fotos.zip", que realmente contiene un virus. En caso de recibir estos mensajes de usuarios con los que no se tenga contacto frecuente o de los que no se espere este tipo de envío, preguntad al usuario si realmente ha sido él quien lo ha enviado.

• **Comprobar que el antivirus analiza los ficheros transmitidos.** La mayoría del software antivirus actual incluyen esta opción por defecto, pero se recomienda comprobarlo consultando las opciones.

• **No introducir la contraseña de acceso en portales de terceros.** Existen portales de terceros que ofrecen servicios adicionales para los programas de mensajería, ya tengan fines maliciosos, o no. A pesar de que algunos de ellos informen de que no se van a almacenar las contraseñas, estamos proporcionando nuestros datos de acceso a desconocidos, cosa que algunos casos puede llevar al secuestro de la cuenta, o al uso de la misma para fines maliciosos. Un claro ejemplo de esta situación está en el tipo de portales para saber si algún usuario te ha bloqueado como contacto, para lo cual se solicita el usuario y contraseña de acceso para poder utilizar la cuenta, por ejemplo, para enviar spam. Por el contrario, un ejemplo que presuntamente no tiene fines maliciosos, es proporcionar el nombre de usuario y la contraseña para importar los usuarios de mensajería instantánea a una red social: existen métodos alternativos, como importarlos desde un fichero de texto por lo que se desaconseja proporcionar las credenciales de acceso de no ser estrictamente necesario. En caso de haber utilizado en alguna ocasión estos servicios se recomienda cambiar la contraseña de acceso.

• **Utilizar sólo software oficial.** Cuando hablamos de software NO oficial nos referimos a los programas clones de los más populares programas de mensajería instantánea, los cuales dicen ofrecer algunas funcionalidades extra, o que simplemente son más atractivos visualmente. Estos programas han sido desarrollados por "compañías" desconocidas, por lo que es posible que se cometan delitos como el robo de contraseñas, capturas de las conversaciones o infecciones de equipo. Igualmente no se aconseja el uso de ***complementos***[41] o plug-ins para este tipo de aplicaciones ya que, en su mayoría, se trata de malware que provoca un comportamiento no deseado. Un ejemplo de esto son complementos que, al instalarlos, envían mensajes a los contactos de un usuario, en su nombre y sin su consentimiento, con invitaciones (en ocasiones muy convincentes) de visitar ciertos enlaces a páginas web maliciosas. Para evitar posibles peligros, se aconseja descargar las aplicaciones de mensajería instantánea desde las páginas web oficiales y no desde páginas web de descargas, con todo tipo de software.

41 Accesible en http://es.wikipedia.org/wiki/Complemento_(inform%C3%A1tica)

Es posible recurrir a programas alternativos que sean de código libre. Estos no suelen ser objetivo de los ciberdelincuentes dada su baja popularidad, aunque también su imagen suele ser menos atractiva.

Estos son algunos ejemplos de los principales clientes de mensajería instantánea de código libre. Una serie de alternativas a los populares ***Windows Live Messenger***[42], ***Yahoo!Messenger***[43] o ***Google Talk***[44]:

- **Amsn:** Programa para la red de MSN disponible para Windows y Linux. Es de ***código libre***[45] y dispone de la mayoría de características del software oficial.

- **Pidgin:** Aplicación para Windows y Linux que soporta también la mayoría de servicios: AIM, ICQ, GoogleTalk, Yahoo, MSN, Skype...

- **Kopete:** Software para linux de los principales servicios de mensajería: AIM, ICQ, GoogleTalk, Yahoo, MSN, Skype...

- Informarse de las opciones de cifrado. Dependiendo del programa usado, las comunicaciones no se transmiten cifradas por lo que, según el nivel de privacidad que queramos mantener, conviene consultar esta cualidad.

- No guardar trazas en caso de no ser necesario. Algunas aplicaciones disponen de la opción de registrar todas las conversaciones y almacenarlas para más adelante poder consultarlas. Dependiendo de la configuración, de donde se guardan, y del cliente utilizado, esta información podría ser consultada por otros usuarios del equipo, por lo que en caso de no necesitarlo, se recomienda no almacenarlos. Por ejemplo, es muy recomendable no guardar los logs si se utiliza este tipo de software en equipos compartidos, o públicos, como pueden ser locutorios o equipos de bibliotecas.

En ***este enlace***[46] pueden consultarse detalles sobre el uso correcto de la Mensajería Instantánea, con una serie de preguntas y respuestas muy interesantes.

En ***este otro***[47] se indican una serie de consejos para el correcto uso de la Mensajería Instantánea y los Chats.

4 Redes Sociales

En la cadena evolutiva de la comunicación en Internet que estamos siguiendo, actualmente nos encontramos en el eslabón de las redes sociales. Son portales en los que, al igual que en la mensajería instantánea, formamos una comunidad de contactos con la que podemos interactuar no solo chateando o enviando mensajes, sino publicando fotos, vídeos, aplicaciones, etc...

---

42 Accesible en http://windowslive.es.msn.com/messenger/
43 Accesible en http://es.messenger.yahoo.com/
44 Accesible en http://www.google.com/hangouts/
45 Accesible en http://es.wikipedia.org/wiki/Codigo_libre
46 Accesible en http://geekotic.com/2007/03/12/12-cosas-que-siempre-quisiste-saber-sobre-msn-pero-te-mias-preguntar/
47 Accesible en http://www.csirtcv.gva.es/es/descargas/utilizar-la-mensajer%C3%ADa-instant%C3%A-1nea-y-chats-de-forma-segura.html

Ilustración 34 · Redes sociales

Existen numerosas redes sociales de distintas temáticas y ámbitos. Las hay de ámbito profesional, destinadas a afianzar relaciones entre trabajadores y empresas; otras informales, dirigidas a compartir vivencias personales y mantener el contacto con amistades, y finalmente existen otras enfocadas a conocer gente con similares inquietudes o aficiones y ampliar la red de amigos.

En todas ellas, principalmente en las destinadas al ocio, el mayor problema es la privacidad. Se trata de portales de servicios en los que cualquier usuario puede publicar imágenes y vídeos que serán vistos por el resto de sus contactos, o por el total de los usuarios de la red, según se configure. Esto hace posible que se publiquen imágenes sobre personas que no desean aparecer en la red con la consiguiente pérdida de privacidad. En la mayoría de estas redes está disponible la posibilidad de "etiquetar usuarios", mediante la cual, cada usuario que aparezca en una foto/vídeo recibe una notificación, y en caso de no desear aparecer, puede retirar las etiquetas o solicitar la retirada de las imágenes. El problema es que, en caso de querer retirar la foto, desde que esta es publicada hasta que el usuario la encuentra y solicita la retirada, pueden pasar días o incluso meses, por lo que el contenido ya ha sido visto por el resto de usuarios.

Frente a este problema no existe una solución tecnológica directa, únicamente la prevención, una buena configuración y algunas recomendaciones:

- **Solicitar expresamente a los contactos que cierto tipo de contenidos no sean publicados,** ya sea en el momento de hacer las fotos, o posteriormente al ver el contenido publicado. Del mismo modo, no debemos publicar contenido que creamos que puede ser ofensivo o molesto para terceros, ya sean usuarios de esa red o no.

- **Habilitar la notificación por correo de contenido multimedia en el que el usuario aparece etiquetado,** para poder acceder lo antes posible a la red social y comprobar la naturaleza de las imágenes/vídeos.

- **Comprobar si la red social dispone de utilidades para validar el etiquetado** de documentos multimedia, de forma que cuando somos etiquetados, antes de que la etiqueta sea visible por el resto de usuarios, tengamos que autorizarlo.

• **Configurar las opciones de privacidad con el resto de usuarios,** ya que muchas veces por defecto, todos nuestros contactos pueden ver todo nuestro contenido, o incluso los contactos de nuestros contactos. Esto puede no ser deseable cuando en una misma red se dispone de contactos personales y contactos laborales.

• **Configurar las opciones de privacidad con aplicaciones y terceros.** Algunas redes sociales disponen de pequeñas mini-aplicaciones desarrolladas por terceros que nos solicitan autorización expresa para poder acceder a nuestro perfil. Es posible que al permitir este acceso, estemos revelando más información de la deseada o necesaria, por lo que es necesario leer las condiciones del servicio.

• **No admitir a usuarios desconocidos.** Es posible que usuarios maliciosos creen perfiles falsos para captar nuestra atención, ser agregados y poder así acceder a nuestros datos, contactos y elementos multimedia. Generalmente estos casos no están relacionados con hechos delictivos, sino con asuntos personales o familiares: exparejas, problemas familiares, celos, desconfianzas...

• **No publicar contenido comprometido.** Si no deseamos que algunos usuarios vean cierto contenido lo mejor es no publicarlo, ya que aunque existen medios para salvaguardar los contenidos no sean accesibles por ciertos usuarios, un error humano, o un usuario con permiso para acceder a ese contenido, pueden acabar haciéndolo público. Además, según la política de privacidad de la red social, es posible que por el simple hecho de publicar una imagen, esta pase a ser propiedad de dicha red, además de estar cediendo los derechos de uso para campañas publicitarias o fines similares.

• **No publicar contenido con derechos de autor.** Al publicar contenido multimedia es posible que por desconocimiento, o de forma intencionada, estemos cometiendo un delito contra la propiedad intelectual. Recomendamos no publicar nada a no ser que tengamos la certeza de que no está protegido por las leyes, ya que, además de poder ser sancionados en la propia red social, puede acarrear problemas legales.

A continuación se definen las diferentes opciones relacionadas con la privacidad para tres tipos de redes sociales con diferentes enfoques. Si se desea profundizar en otros aspectos de la plataforma, se puede obtener más información en forma de ***guías y manuales***[48] en el apartado dedicado a las redes sociales en la página web de INTECO.

4.1 Privacidad en Facebook

Facebook[49] es una de las redes sociales que más fuerza tiene hoy en día. Fue creada para la comunidad universitaria, pero su uso se ha extendido a grandes sectores de la población. Sus usuarios pueden compartir principalmente fotos,

48 Accesible en http://www.inteco.es/guias/guia_ayuda_redes_sociales
49 Accesible en https://www.facebook.com/

vídeos, eventos y aplicaciones y dispone de la opción de etiquetar a otros usuarios.

El principal problema de privacidad de sus usuarios consiste en controlar qué fotos y vídeos de sus perfiles son visibles por sus contactos. Sin embargo dispone de la posibilidad de poder separar distintos ámbitos (amigos/familia/trabajo...) para evitar que, por ejemplo, compañeros de trabajo, vean fotos del ámbito familiar.

Para todo esto, Facebook dispone de opciones de privacidad que pocos usuarios se dedican a investigar.

• Limitar información del perfil público: La primera barrera que debemos levantar para salvaguardar nuestra privacidad es limitar la información disponible a los usuarios que no son contactos nuestros, siendo recomendable limitar esta información a un nombre de usuario, alguna referencia geografía genérica (por ejemplo la provincia) y si lo deseamos, una fotografía. De esta forma si algún contacto nos busca puede reconocernos para agregarnos. Para cambiar esta opción, una vez hemos iniciado la sesión acceder a: "Configuración" > "Configuración de la privacidad" > "Información del perfil" Ahí estableceremos todos los parámetros (información personal, cumpleaños, creencias...) a "solo mis amigos". Pulsaremos en volver, y repetiremos los pasos para los parámetros de la sección "Información de contacto", configurando como "Todos" aquellos datos que queramos dejar públicos (como pueden ser el sitio web, la ciudad, la posibilidad de agregar como amigo, o la de enviar un mensaje).

• Evitar que buscadores (como Google, Bing, o Yahoo), muestren tu perfil de usuario en sus resultados. Para evitar esta situación basta con acudir a las opciones de privacidad de Facebook y el apartado "Búsquedas" desmarcar la opción "Resultados públicos de búsqueda". De esta forma, nuestro perfil de usuario de Facebook no aparecerá en los resultados de los buscadores.

• Controlar de forma cómoda, qué usuarios, pueden ver qué contenido. Si se desea hacer una separación entre tipos de usuarios, como puede ser familia/trabajo, es posible crear listas de usuarios y asignarles permisos para ver los álbumes. Para ello, acudir a la pestaña "Amigos", seleccionar a la izquierda de nuevo "Amigos" y pulsar en "Nueva lista" en la parte superior. A esta lista le asignaremos un nombre y los usuarios que deseemos incluir. Por ejemplo se puede crear una lista llamada "familia" y otra "trabajo" donde incluiremos a los usuarios según corresponda (nótese que es posible incluir usuarios en ambas listas). Una vez creadas las listas, acudiremos a nuestras fotos y pulsaremos sobre alguno de los álbumes para los que queramos cambiar las condiciones de privacidad, y seleccionaremos "Editar información". A continuación desplegaremos la lista "Quien puede ver esto" y seleccionaremos "personalizar". En el menú que aparece, podremos seleccionar que solo alguna de las dos listas pueda ver las fotos, o impedir que una de las listas pueda verlas. Esta configuración es muy recomendable para el conjunto de fotos en las que el usuario

es etiquetado, ya que de esta forma, podemos evitar que una foto etiquetada con "mala fe" sea vista por el resto de usuarios antes de que le demos el visto bueno.

Es una realidad que los usuarios de esta popular red social son víctimas de múltiples engaños donde los ciberdelincuentes encuentran una gran difusión de sus estrategias para posteriores beneficios. Como ejemplo de sus estrategias es posible encontrar estos ataques en noticias de personajes públicos o famosos, en grupos de fans, en rumores falsos, incluso virus específicamente diseñados para la plataforma de Facebook como el popular ***Koobface***[50].

Desde este enlace puede descargarse un ***resumen de la política de privacidad de Facebook***[51] con algunas de las recomendaciones más importantes para privatizar tu perfil .También se puede obtener un ***cortafuegos***[52] específico para esta aplicación.

4.2 Privacidad en Tuenti

Tuenti es una red social muy similar a Facebook que se ha extendido principalmente entre gente joven. A diferencia de Facebook, se trata de una red social española, por lo que el volumen de usuarios es mucho menor.

Ilustración 35 · Privacidad Tuenti

Tal vez este sea el motivo por el que Tuenti no dispone de aplicaciones ni juegos directamente en su plataforma, por lo que resulta más segura ante la posibilidad de poder ejecutar código malicioso.

De igual forma, las opciones de privacidad son más limitadas que en Facebook en cuanto a flexibilidad, pero a la vez son mucho mas sencillas de configurar

50 Accesible en http://www.csirtcv.gva.es/es/noticias/desmantelan-banda-que-propagaba-malware-en-redes-sociales.html
51 Accesible en http://www.csirtcv.gva.es/es/noticias/resumen-de-la-pol%C3%ADtica-de-privacidad-de-facebook.html
52 Accesible en http://www.defensio.com/?cmpid=prnr

para usuarios poco experimentados.

Para cambiar las opciones de privacidad basta con acudir en la parte superior de la pantalla a la opción "mi cuenta" → "privacidad" donde nos aparecerá un sencillo menú donde podemos asignar que usuarios (todos, mis amigos, o amigos de mis amigos), pueden acceder a qué contenido (perfil, fotos, tablón, mensajes y teléfono).

Una de las principales peticiones de los usuarios de Tuenti, es que se incluya la posibilidad de evitar ser etiquetado, ya que con las opciones actuales, únicamente se puede des-etiquetar la foto una vez publicada, pero no se incluye ninguna herramienta preventiva.

Una guía con más detalle sobre la seguridad en Tuenti puede descargase desde la ***web de INTECO***[53].

4.3 Privacidad en LinkedIn

Linkedin es una red social muy diferente de las anteriores, ya que está enfocada principalmente a los contactos laborales. Permite establecer relaciones basándose en intereses comunes, empresas, organizaciones o currículum y dispone de una amplia red de grupos de discusión que acostumbra a tener mucho tráfico.

En otras redes sociales, es recomendable ofrecer la mínima información posible a desconocidos, pero en LinkedIn se da el caso contrario: interesa "que te encuentren". Interesa compartir intereses laborales, proyectos o experiencias con el fin de formar una solida red de contactos. Sin embargo, igual que en otras redes sociales, hay algunos parámetros que se deben tener en cuenta.

Para configurar los detalles de privacidad hay que dirigirse al apartado de "configuración" → "mi foto del perfil" y seleccionar si deseamos que toda la red pueda verla o solo nuestros contactos.

Si no se desea que los cambios en el perfil sean notificados al resto de usuarios, bastará con cambiarlo en el apartado "Visibilidad de tu actualización personal". De igual forma, existen fáciles opciones para permitir o denegar la participación en estudios de investigación, permitir que nuestros contactos sean públicos para otros usuarios, o configurar las preferencias de publicidad.

Para profundizar sobre el manejo de la seguridad en LinkedIn, descargar el ***manual publicado por INTECO***[54].

53 Accesible en http://www.inteco.es/file/0GJXYRVkJXlG7-0ggHlozQ
54 Accesible en http://www.inteco.es/file/nVpd_oWQO0ZRK6a0e7iZKg

8

SEGURIDAD INALÁMBRICA

1 Introducción

En este capítulo se van a abordar todos aquellos aspectos de seguridad que conciernen a las tecnologías inalámbricas ***WiFi***[55] y ***Bluetooth***[56].

Cada vez más, las tecnologías inalámbricas van ganando protagonismo en la vida diaria de las empresas, instituciones y entornos personales. Las redes WiFi y Bluetooth agrupan un conjunto de estándares de comunicación inalámbrica que ofrecen soluciones de compartición de la información sin hacer uso de medios cableados. Obteniendo la posibilidad de establecer canales de datos entre entornos móviles y estáticos, eliminando las barreras arquitectónicas.

Ilustración 36 · WiFi

Las soluciones WiFi y Bluetooth suponen dos de los estándares de comunicación por radiofrecuencia más utilizados y populares para redes de área local. No es extraño que dispositivos como ordenadores portátiles, PDA's, consolas de videojuegos, móviles o incluso maquinaria industrial hagan uso de estos estándares como solución inalámbrica para interconectar y transferir cualquier tipo de información, datos, voz o vídeo. Como ejemplo de ello, basta con realizar una búsqueda mediante su ordenador portátil de las redes inalámbricas disponibles en su entorno, para darse cuenta de la gran acogida que esta tecnología ha tenido en la sociedad.

Todo apunta a que el crecimiento y despliegue de este tipo de redes seguirá aumentando en los próximos años. Encuestas realizadas por la Asociación para la Investigación de los Medios de Comunicación (AIMC) reflejan que el 52 % de los usuarios de Internet en 2007 obtuvo acceso a la red de redes a través de este tipo de tecnología, frente al 43% del año anterior. Pero no solo los usuarios domésticos adquieren productos de estas normas, instituciones, PYMEs y grandes compañías, cada vez más hacen uso de estos estándares como solución de comunicación inalámbrica.

Ilustración 37 · Bluetooth

55 Accesible en http://es.wikipedia.org/wiki/Wifi
56 Accesible en http://es.wikipedia.org/wiki/Bluetooth

Es por ello que no debe descuidarse la seguridad al hacer uso de dispositivos que implementen estas normas, puesto que pueden suponer una ventana abierta al exterior por donde cualquier persona maliciosa pueda robar información personal o confidencial, pudiendo incluso obtener el control de los dispositivos del usuario. Este capitulo esta orientado a la protección del canal inalámbrico.

2 Seguridad WiFi

ORIGENES

Principalmente existen tres normas o grupos de trabajo que definen los estándares WiFi a nivel comercial: 802.11b, 802.11g, 802.11n.

802.11b

En 1999, el ***IEEE***[57] aprueba el estándar 802.11b (también llamado Wi-Fi), consiguiendo un ancho de banda de 11Mbps.

Ilustración 38 · Router WiFi I

Los primeros productos 802.11b aparecieron muy rápidamente en el mercado debido a su gran potencial. Este repentino salto de rendimiento comparado con el del estándar original (802.11 legacy), así como un descenso de los precios debido a la rápida aceptación del producto por parte de los usuarios produjo el asentamiento de la norma como la tecnología inalámbrica definitiva para redes de área local. Por lo que respecta a su cobertura, los valores típicos del área que puede llegar a cubrir en localizaciones interiores son 30 metros a 11 Mbps y 90 metros a 1 Mps.

802.11g

En 2003 se hizo público el estándar 802.11g,totalmente compatible con la norma "b" presenta un avance significativo en cuanto al ancho de banda proporcionando un menor consumo y un mayor alcance que 802.11b. La norma "g" utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia.

57 Accesible en http://es.wikipedia.org/wiki/IEEE

Ilustración 39 · Router WiFi II

Como ya se ha comentado es compatible con el estándar "b" ya que utiliza las mismas frecuencias. Aunque cabe hacer notar que el rango en el cual puede operar a máxima velocidad es menor en comparación con el de 802.11b. Buena parte del proceso de diseño del estándar se fundamentó en hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar 802.11g la presencia de nodos bajo el estándar "b" reduce significativamente la velocidad de transmisión.

802.11n

Ilustración 40 · Router WiFi III

En la actualidad, la mayoría de productos son de la especificación b y/o g , sin embargo ya se ha ratificado el estándar 802.11n que sube el límite teórico hasta los 600 Mbps. Actualmente ya existen varios productos que cumplen el estándar N con un máximo de 300 Mbps (80-100 estables).

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5,4 Ghz. Las redes que trabajan bajo los estándares 802.11b y 802.11g, tras la reciente ratificación del estándar, se empiezan a fabricar de forma masiva y es objeto de promociones de los operadores ***ADSL***[58], de forma que la masificación de la citada tecnología parece estar en camino. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre si, de forma que el usuario no necesitará nada mas que su adaptador wifi integrado, para poder conectarse a la red.

58 Accesible en http://es.wikipedia.org/wiki/ADSL

PROTOCOLOS DE SEGURIDAD

El estándar inalámbrico de comunicaciones IEEE802.11 y sus diversos grupos de trabajo posteriores establecen la posibilidad de conferir a esta tecnología, capacidades de integridad de datos, confidencialidad y autenticidad de las estaciones. De esta manera existen 3 protocolos de seguridad basados en la norma IEEE802.11 y IEEE802.11i:

- **WEP** como parte de la norma IEEE802.11
- **WPA** como borrador de la norma IEEE802.11i
- **WPA2** como parte de la norma IEEE802.11i

De esta manera y con el objetivo de poder comprender las consideraciones de seguridad que afectan a cada uno de estos protocolos es necesario definir muy escuetamente su funcionamiento.

WEP

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a , 802.11b y 802.11g, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de cifrado estándar soportado por la mayoría de las soluciones inalámbricas.

Pero, ¿por qué cifrar las comunicaciones inalámbricas?. El entorno de Radio Frecuencia es un canal de comunicación inseguro, ya que cualquier estación dentro del rango de la señal puede recibir los datos emitidos por otra. Conscientes de ello el IEEE implemento un mecanismo de seguridad que pudiera otorgar al medio inalámbrico las características del cableado, todo ello sin demasiado éxito, como en secciones posteriores comprobaremos.

Aunque en los entornos de ***RF***[59] (Radio Frecuencia) pueden residir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas inalámbricos dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Cabe destacar que un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes ***WLAN***[60] (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo.

WEP utiliza una misma clave simétrica (se usa la misma contraseña para cifrar que para descifrar) y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto

59 Accesible en http://es.wikipedia.org/wiki/Radiofrecuencia
60 Accesible en http://es.wikipedia.org/wiki/WLAN

genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El sistema de cifrado WEP presenta numerosas vulnerabilidades de seguridad que hacen que este protocolo sea altamente inseguro. Es por eso que **no se recomienda** el uso de este tipo de cifrado en la configuración de los dispositivos inalámbricos. Con las herramientas oportunas, un atacante podría llegar a descifrar la contraseña de acceso a la red en tan solo 30 segundos. Este protocolo solo debe utilizarse en caso de extrema necesidad, es decir, es mejor que ningún cifrado.

WPA

WPA (Wi-Fi Protected Access) fue desarrollado por la Wi-Fi Alliance y el IEEE en 2003 como resultado de aplicar el borrador del estándar IEEE 802.11i. Su principal objetivo era cubrir todas aquellas carencias de seguridad detectadas en el protocolo de seguridad nativo de 802.11 WEP. Cabe destacar que WPA no representa un protocolo que pueda asegurar una protección cien por cien del medio inalámbrico ya que como en muchos casos esto depende en gran parte del usuario final. WPA es un estándar orientado tanto al mundo de la pequeña oficina y el usuario domestico como a grandes empresas.

Prestaremos especial atención al método empleado por WPA para autenticar a las estaciones ya que supone uno de los puntos débiles de este protocolo de seguridad. Por lo que respecta a la autenticación, en función del entorno de aplicación, es posible emplear dos modos de autenticación diferentes WPA-PSK (Pre Shared Key) o WPA EAP (Extensible Autentication Protocol).

En entornos personales, como usuarios residenciales y pequeños comercios, se utiliza WPA con clave pre-compartida o también llamada WPA-PSK. En estos entornos no es posible contar con un servidor de autenticación centralizado . Es este contexto WPA se ejecuta en un modo especial conocido como "Home

Mode" o PSK, que permite la utilización de claves configuradas manualmente y facilitar así el proceso de configuración del usuario domestico.

El usuario únicamente debe introducir una clave de 8 a 63 caracteres, conocida como clave maestra, en su punto de acceso, módem o router inalámbrico residencial, así como en cada uno de los dispositivos que quiere conectar a la red. De esta forma solo se permite acceso a aquellos dispositivos que son conocedores de la contraseña, lo que evita ataques basados en escuchas así como acceso de usuarios no autorizados. En segundo lugar se puede asegurar que la clave proviene de una relación de acuerdo único para generar el cifrado ***TKIP***[61] (Temporal Key Integrity Protocol) en la red, el cual describiremos más a delante. Por lo tanto la contraseña preestablecida para la autenticación es compartida por todos los dispositivos de la red, pero no son las claves de cifrado, que son diferentes para cada dispositivo, lo que representa una mejora en cuanto a WEP.

61 Accesible en http://es.wikipedia.org/wiki/TKIP

En general WPA parece representar un nivel superior en cuanto a la seguridad que ofrecía WEP.

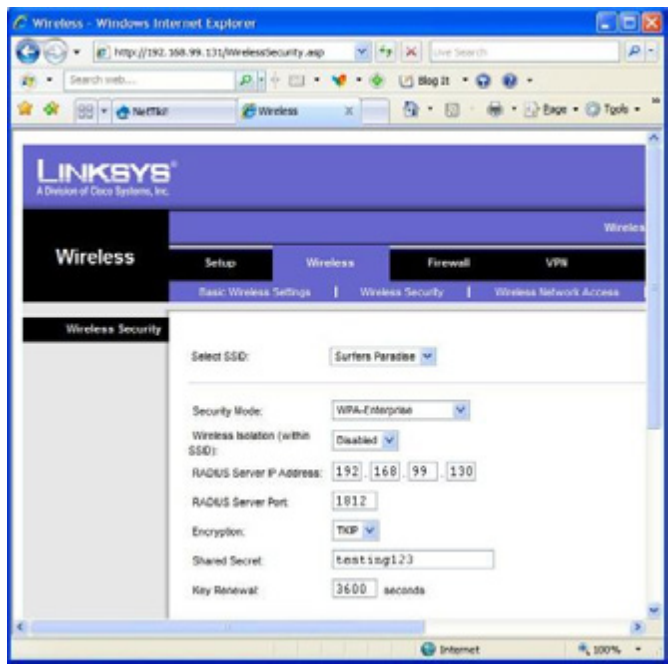


Ilustración 41 · Configuración router

Como se ha comentado una de las vulnerabilidades que presenta este protocolo de cifrado reside en el modo en que autentica el punto de acceso a las estaciones (ordenadores, PDA's...). Un usuario mal intencionado podría capturar el dialogo inicial de conexión y realizar un ataque de fuerza bruta sobre la contraseña. Es decir, un atacante mediante el uso de un computador, podría ir probando reiteradamente posibles contraseñas validas. Hay que destacar que los ordenadores permiten la ejecución de tareas repetitivas de una forma muy rápida. Esto quiere decir que un atacante podría probar del orden de 350 contraseñas por segundo hasta dar con la correcta. Un punto a favor del protocolo WPA es que obliga a que la contraseña sea de al menos 8 caracteres y hasta un total de 63. Es por esto que, al utilizar WPA es muy importante el tamaño de la contraseña y que esta no este en un ***diccionario***[62]. De esta manera contraseñas como: "casacasa", "juan2009" o "12345678" serían extremadamente débiles. Credenciales como "EstaC4SaEs1ruin4." o "/me-Gusta-LasWIFIS/" se considerarían de una buena fortaleza.

Por lo tanto cuando se configure este tipo de protocolos se ha de introducir contraseñas no obvias y que no se encuentren en un diccionario.

WPA2

La alianza Wi-Fi lanzó en septiembre de 2004 el protocolo de seguridad WPA2, que suponía ser la versión certificada interoperable de la especificación completa del estándar IEEE802.11i, que fue ratificado en junio de 2004. Para llevar a cabo la certificación se basa en las condiciones obligatorias de la última versión del estándar IEEE802.11i. WPA2 es, por tanto, la implementación aprobada por la Wi-Fi Alliance interoperable con el estándar IEEE802.11i.

Aunque los productos WPA siguen siendo parcialmente seguros, muchas organizaciones han estado buscando una tecnología interoperable y certificada

62 Accesible en http://es.wikipedia.org/wiki/Ataque_de_diccionario

basada en el estándar IEEE802.11i o han requerido de la utilización de cifrados mas robustos por razones internas o reguladoras. WPA2 resuelve estas necesidades, basándose en su predecesor WPA (con el que es completamente compatible hacia atrás) y ha sido específicamente diseñado para cumplir los requisitos más exigentes de entornos empresariales.

En cuanto a su relación con WPA, la principal las diferencias de WPA2 respecto a WPA es que emplea, al igual que IEEE802.11i un mecanismo de cifrado mas avanzado como AES. No obstante, WPA2 es compatible con WPA. Por ello, algunos productos WPA pueden ser actualizados a WPA2 por software. Otros en cambio, requieren de un cambio en el hardware debido a la naturaleza de cómputo intensiva del cifrado requerido para WPA2, AES.

Por lo tanto y siempre que sea posible, **utilizaremos este protocolo de seguridad** para configurar nuestros dispositivos WiFi. Destacar que WPA2 no esta exenta de vulnerabilidades, de hecho el ataque de recuperación de contraseña por fuerza bruta, explicado para WPA también sirve para este protocolo. Es por eso que debemos ser cuidadosos a la hora de establecer la contraseña, utilizando como se ha explicado, una longitud adecuada e incluir juegos de caracteres especiales (*,:./&).

Otras consideraciones de seguridad

Hemos hecho especial hincapié en la importancia de elegir un protocolo de seguridad robusto así como unas contraseñas de una complejidad aceptable, pero existen otras consideraciones de seguridad que se deben tener en cuenta a la hora de utilizar esta tecnología.

En primer lugar y aunque pueda parecer tentador, **no es aconsejable conectarse a puntos de acceso no confiables** (como por ejemplo el del vecino), dado que nunca podemos saber que se encuentra en la red destino. Por ejemplo, un atacante podría colocar un punto de acceso sin contraseña para atraer a posibles víctimas y en él instalar numerosas herramientas de captura de información. De esta manera mientras estuviéramos navegando a través de su red, de igual forma que un espía, este podría ver la información que recibimos y transmitimos, capturando nuestras contraseñas y por ejemplo cuentas bancarias. De la misma manera, no es recomendable visitar o acceder a paginas web o recursos de un alto valor para nosotros (páginas bancarias, correo electrónico, hotmail, gmail), cuando nos encontremos en cibercafés (Starbucks coffe, bares, etc...) o puntos de acceso libres, mas allá de las fronteras de nuestra casa. En resumen hay que huir de la tentación de conectarse a redes inalámbricas no seguras.

Por otra parte se debe **tener limpia la lista de redes inalámbricas favoritas** de nuestro Windows XP. ¿Qué quiere decir esto?, pues el sistema Windows XP y sus predecesores, cada vez que nos conectamos a una red inalámbrica guardan el nombre de la red en una lista de favoritos. Por ejemplo, si en algún momento hemos conectado a la red de un amigo “Casa” y esta no tenia habilitado ningún protocolo de seguridad, cuando abandonemos la red, Windows XP intentará conectarse de forma periódica, siempre y cuando no estemos conectados ya a otra. Pero, ¿qué tiene esto de peligroso? Pues existen aplicaciones que

pueden funcionar en forma de punto de acceso WiFI y que están a la espera de peticiones de conexión como la mencionada anteriormente. Al recibir esa petición el punto de acceso ilícito puede capturar nuestra computadora en su red, pudiendo proceder a vulnerar el sistema aprovechando otros fallos en el software de nuestro ordenador. Por todo lo anterior, se recomienda tener en la lista de redes favoritas solo la red de nuestra casa/oficina y configurada con un protocolo de seguridad robusto.

3 Seguridad Bluetooth

ORÍGENES

La tecnología Bluetooth fue desarrollada por la empresa Ericsson en 1994 y posteriormente en 2002 fue utilizado para definir la norma 802.15. Bluetooth permite, mediante una conexión inalámbrica de corto alcance, conectar entre sí móviles, ordenadores, PDAs, y un gran abanico de dispositivos. Mediante este sistema, los usuarios pueden interconectar sus dispositivos móviles y fijos también. El alcance que logran tener estos dispositivos es de 10 metros para ahorrar energía, ya que generalmente estos dispositivos utilizan mayoritariamente baterías. Sin embargo, se puede llegar a un alcance de hasta 100 metros similar a WiFi, pero con un aumento del consumo energético considerablemente.

Para mejorar la comunicación es recomendable que ningún objeto físico, como por ejemplo una pared, se interponga. El primer objetivo para los productos Bluetooth de primera generación eran los entornos de la gente de negocios que viaja frecuentemente, pero hoy en día esta ampliamente extendido a cualquier tipo de usuario.

La especificación de Bluetooth define un canal de comunicación de máximo 720 Kbps (1 Mbps de capacidad bruta).La frecuencia de radio con la que trabaja está en el rango de 2,4 a 2,48 GHz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1Mhz; esto permite dar seguridad y robustez.

La potencia de salida para transmitir a una distancia máxima de 10 metros es de 1 mW, mientras que la versión de largo alcance transmite entre 20 y 30 dBm entre 100 mW y 1 W de potencia.

Ilustración 42 · Ejemplo Bluetooth

Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideó una solución que se puede implementar en un solo integrado utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9 mm y que consume aproximadamente 97% menos energía que un teléfono celular común. Hoy en día existen 3 versiones del estándar la v1.1, v1.2 y v2.0. La versión 1.2, a diferencia de la 1.1, provee una solución inalámbrica complementaria para co-existir con WiFI en el espectro de los 2.4 GHz, sin interferencia. Por otra parte la versión 1.2, usa la técnica "Adaptive Frequency Hopping (AFH)", que ejecuta una transmisión más eficiente y un cifrado más segura. Para mejorar las experiencias de los usuarios, la V1.2 ofrece una calidad de voz (Voice Quality - Enhanced Voice Procesing) con menor ruido ambiental, y provee una más rápida configuración de la comunicación con los otros dispositivos Bluetooth dentro del rango del alcance. Por último la versión 2.0, creada para ser una especificación separada, principalmente incorpora la técnica "Enhanced Data Rate" (EDR), que le permite mejorar las velocidades de transmisión en hasta 3 Mbps a la vez que intenta solucionar algunos errores de la especificación 1.2 .

MEDIDAS DE SEGURIDAD

Bluetooth incorpora varios mecanismos de seguridad que permiten securizar las comunicaciones frente a ataques y capturas de datos. Se definen mecanismos de seguridad en las siguientes capas de protocolo:

- Seguridad a nivel de la capa física
- Seguridad a nivel de la capa de enlace

Capa física

Bluetooth trabaja en la frecuencia de 2.4 GHz de la banda ISM (Industrial, Scientific and Medical) disponible a nivel mundial y que no requiere licencia de operador. Con el fin de evitar interferencias con otras tecnologías que operen en la misma banda de frecuencias, Bluetooth emplea la técnica de salto de frecuencias (FHSS, Frequency Hopping Spread Spectrum), que consiste en dividir la banda de transmisión en 79 canales (23 en España, Francia y Japón) de longitud 1 MHz y realizar 1600 saltos por segundo.

Durante el proceso de establecimiento una conexión, uno de los dispositivos funciona en modo maestro y los demás en modo esclavo. El maestro genera una tabla pseudoaleatoria con la secuencia o patrón de saltos de frecuencia que deben utilizar todos los dispositivos durante las comunicaciones. El intercambio de la tabla de saltos desde el maestro hacia el esclavo (o esclavos) se realiza en un canal determinado del espectro de frecuencias, de forma que todos los dispositivos pueden acceder a ésta.

Una vez comenzada la comunicación, el intercambio de paquetes de datos se realiza de acuerdo con el patrón de saltos de frecuencia establecido y a una velocidad marcada por el reloj interno. Esto significa que en cada instante de tiempo cada dispositivo escribirá o escuchará durante su intervalo en un determinado canal.

En definitiva, la técnica de saltos de frecuencia empleada por Bluetooth garantiza, en principio, la participación exclusiva de dispositivos autorizados y una comunicación libre de escuchas por parte de usuarios ajenos a la misma. Sin embargo, esta tabla de frecuencias podría ser capturada por un atacante, haciendo necesaria la introducción de elementos de seguridad en las capas superiores, como por ejemplo la capa de enlace.

Capa de enlace

Principalmente existen 3 mecanismos de seguridad en la capa de enlace:

- Autenticación
- Autorización
- Cifrado de los datos

La **autenticación** es el proceso por el cual un dispositivo Bluetooth verifica su identidad en otro dispositivo para poder acceder a los servicios que ofrece. La primera vez que dos dispositivos intentan comunicarse, se utiliza un procedimiento de inicialización denominado emparejamiento (pairing) para crear una clave de enlace común de una forma segura. Para la primera conexión entre dos dispositivos, el procedimiento estándar de emparejamiento requiere que el usuario de cada dispositivo introduzca un código (cadena ASCII) de seguridad Bluetooth de hasta 16 bytes de longitud que debe ser el mismo en los dos casos. En primer lugar un usuario introduce el código de seguridad y en segundo lugar, el otro usuario debe confirmar el mismo código de seguridad.

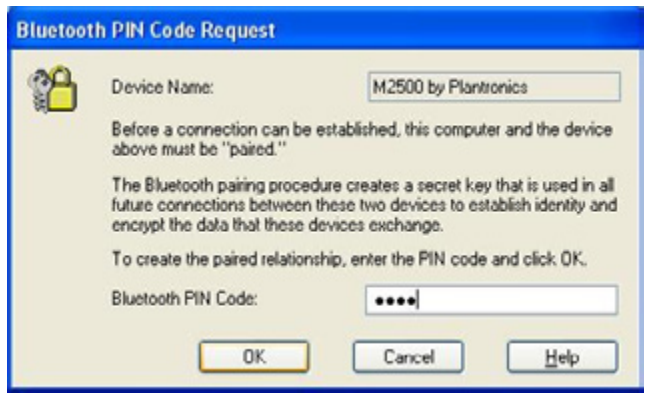


Ilustración 43 · Bluetooth PIN Code request

La **autorización** es el procedimiento que determina los derechos que tiene un dispositivo Bluetooth para acceder a los servicios que ofrece un sistema. El mecanismo de autorización en dispositivos Bluetooth se lleva a cabo mediante niveles de confianza. Los dispositivos tienen cuatro niveles de confianza, los cuales determinan la capacidad de acceso a los servicios: total, parcial o restringida y nula. En el caso de que un determinado dispositivo de confianza (se ha emparejado previamente) intente acceder a un servicio autorizado, no se requiere ningún procedimiento de confirmación, accede de forma transparente. En el caso de que un determinado dispositivo no confiable intente acceder a un servicio restringido, se requiere un procedimiento explícito de confirmación por parte del usuario para permitir o denegar el

acceso a ese dispositivo durante la sesión de conexión actual. Nótese que, para algunos servicios, es posible conceder permisos de acceso temporal a dispositivos no emparejados previamente.

Ilustración 44 · Cifrado

El **cifrado** de la información protege los datos que se transmite en un enlace entre dispositivos Bluetooth. Garantiza la confidencialidad del mensaje transmitido, de forma que si el paquete es capturado por un usuario que no posea la clave de descifrado, el mensaje le resultará ininteligible. Su implementación es opcional, pero necesita que se haya producido anteriormente una autenticación. El maestro y el esclavo deben ponerse de acuerdo en utilizar cifrado o no. En caso afirmativo, deben determinar el tamaño de la clave de cifrado, para lo cual, maestro y esclavo intercambian mensajes hasta alcanzar un acuerdo. Para ello utiliza un sistema de cifrado E3 de 128 bits.

RECOMENDACIONES DE SEGURIDAD

Se recomienda adoptar las siguientes medidas de seguridad con el fin de evitar ataques a dispositivos Bluetooth. Estas medidas son simples y de aplicación inmediata y deberían formar parte de la conducta habitual de un usuario de dispositivos Bluetooth.

1. Activar Bluetooth en el dispositivo sólo cuando sea necesario para realizar algún tipo de comunicación a través de este interfaz y desactivarlo cuando no se vaya a utilizar.

2. Configurar el dispositivo en modo oculto o non discoverable. De esta forma disminuyen las probabilidades de que un supuesto atacante detecte la presencia del dispositivo al escanear en búsqueda de equipos Bluetooth.

3. Configurar el dispositivo para que utilice la función de cifrado en todas las comunicaciones. De esto modo, se garantiza la confidencialidad del intercambio de mensajes

4. Utilizar un nombre de dispositivo que no sea representativo de la marca y modelo del mismo, por ejemplo: Nokia 6600. Esto implica, en la mayoría de los casos, modificar el nombre de dispositivo asignado por el fabricante.

5. No aceptar bajo ningún concepto conexiones entrantes de

dispositivos desconocidos. Esto implica también intentos de conexión de personas en las que no se confía aunque el pretexto pueda parecer inofensivo, por ejemplo: Emparejar dos dispositivos para transferir una fotografía.

6. Configurar todos los perfiles soportados por el dispositivo para que requieran autenticación ante cualquier intento de acceso .

7. Verificar periódicamente la lista de dispositivos de confianza y eliminar aquellas entradas de dispositivos con los que habitualmente no se establece conexión.

8. Aunque actualmente todavía no se ha descubierto una forma de romper la seguridad del emparejamiento realizando fuerza bruta sobre un código de seguridad Bluetooth (clave PIN) que hayan empleado dos dispositivos emparejados, utilizar en la medida de lo posible claves PIN de longitud extensa, a partir de 8 caracteres y siguiendo las recomendaciones del apartado WiFi.

9

EQUIPOS Y DISPOSITIVOS PORTÁTILES

Durante los últimos años se han producido diversos cambios en las costumbres de los usuarios en cuanto a la adquisición de ordenadores se refiere. Si bien durante la pasada década reinaron los equipos de sobremesa, a mediados de la misma irrumpieron con fuerza los portátiles, llegando en 2007 a venderse más ordenadores portátiles. Al respecto, en los últimos 2-3 años el mercado volvió a girar hacia los ***nettop***[63]: portátiles pequeños de hasta 12 pulgadas, de potencia limitada y que destacan por la duración de su batería y su bajo coste. Por último, durante 2011 llegaron los famosos ***tablets***[64] principalmente de la mano de Apple y Android los cuales prometen sustituir a corto plazo a los ordenadores, al menos para realizar tareas cotidianas como navegar por internet o leer el correo, dejando para tareas más complicadas paso a los nuevos ultrabooks(ordenadores con tamaños de pantalla cercanos a las 15' extremadamente ligeros).

Así pues, este curso se centra en los ordenadores portátiles, independientemente de si se trata de portátiles tradicionales, nettops o ***ultrabooks***[65].

1 Protección lógica

La seguridad lógica en ámbitos informáticos se refiere a la seguridad en el uso del software. Esto implica desde la protección de la información mediante controles para evitar el accesos, hasta las medidas necesarias para restaurar un equipo en caso de avería o robo.

1.1 Copias de seguridad

Las pérdidas de datos por falta de copias de seguridad es un problema mucho mayor en dispositivos portátiles que en los tradicionales equipos de sobremesa, ya que, además de los errores de software que comparten ambas plataformas, han de añadirse los riesgos asociados a pérdida/robo del equipo y averías físicas del hardware.

Hardware

Algunos componentes informáticos, especialmente los discos duros, tienen partes móviles que pueden sufrir daños si se mueve el equipo o si recibe golpes mientras están en funcionamiento.

Existen alternativas, como los discos ***SSD***[66], los cuales no contienen partes móviles, reduciendo así el riesgo de pérdida de datos aunque su coste actual es bastante superior a los discos duros tradicionales. A pesar del uso de estos discos, y dado que continua la posibilidad de robo o perdida del equipo, resulta necesario el uso de copias de seguridad.

63 Accesible en http://es.wikipedia.org/wiki/Nettop
64 Accesible en http://es.wikipedia.org/wiki/Tableta
65 Accesible en http://es.wikipedia.org/wiki/Ultrabook
66 Accesible en http://es.wikipedia.org/wiki/SSD

Windows

En los equipos con Microsoft Windows en entornos corporativos, la medida más sencilla es el uso de **perfiles móviles en el dominio**. Esta opción es habilitada por el administrador del dominio y consiste en que al cerrar el equipo, todos los documentos y ficheros modificados por el usuario son enviados a un servidor. De igual forma, cuando se enciende el equipo, se contrasta la información del disco duro con la del servidor, y si algo ha sido modificado se sincroniza. Así, en caso de que se pierda el equipo, o que haya que reinstalarlo, el usuario puede iniciar sesión en cualquier otro equipo del dominio y disponer ahí de sus documentos y configuraciones de programas.

Si esta opción no está disponible por no tratarse de entornos corporativos, disponemos de varias alternativas:

- **Copiar los datos del usuario en un soporte externo:** se puede hacer una copia de seguridad directamente copiando y pegando los ficheros en una memoria USB, o disco duro, pero se ha de tener en cuenta que ay información que tal vez olvidemos guardar que no se almacena en la carpeta "mis documentos", como puede ser la libreta de direcciones, los favoritos del navegador o las opciones particulares de cada programa. En caso de que se produzca una perdida del equipo o haya que formatearlo, tendremos que reinstalar el sistema operativo, instalar de nuevo los programas y luego restaurar los datos y documentos.

  Este mecanismo tiene la ventaja de que la copia de seguridad es sencilla de realizar y ocupa mucho menos que con otros medios, pero en caso de tener que restaurar el sistema, el proceso es largo y tedioso.

- **Realizar una copia completa del disco duro.** En este caso crearemos una "imagen" del disco duro, es decir, copiaremos íntegramente el disco duro y lo almacenaremos en un fichero que sacaremos del equipo. Para ello existen múltiples herramientas comerciales, como puede ser Norton Ghost, Nero o Backup4. Acostumbran a ser programas muy intuitivos que pueden incluso programarse para ejecutarse automáticamente siguiendo sencillos asistentes.

La única peculiaridad de la mayoría de programas de copia de seguridad que causa dudas entre usuarios poco experimentados es el concepto de las copias incrementales: si realizamos una copia incremental, cuando queramos realizar una nueva copia, el sistema comparará los ficheros de la copia previa y solo incluirá los que hayan sido modificados desde la última copia. Mientras que si no elegimos esta opción, la copia se hará íntegramente nueva. En caso de realizar la copia sobre unidades de solo escritura, como pueden ser DVD's, la única opción es utilizar copias integras, mientras que si utilizamos un disco duro externo, es mejor utilizar la copia incremental para ahorrar tiempo en el proceso. Otra opción independientemente de los programas mencionados es la propia utilidad de copias de seguridad de Windows. Dependiendo de la versión

del sistema operativo, el proceso de crear una copia de seguridad puede cambiar ligeramente:

• Abrimos el programa de copias de seguridad que se encuentra en "Inicio->Todos los programas-> Herramientas del sistema -> copia de seguridad". En caso de no encontrarlo es posible que no esté instalado, para lo cual insertamos el disco de Windows y navegamos hasta la carpeta "\valueadd\msft\ntbackup", por último ejecutamos el instalable.

• Pulsamos sobre la opción "modo avanzado" y acudimos a la pestaña "backup" . Creamos un nuevo trabajo. A continuación seleccionamos los elementos que deseamos incluir en la copia de seguridad y seleccionamos también la casilla de verificación "estado del sistema" que hay debajo de "Mi Pc".

• Para concluir, seleccionaremos el destino, preferiblemente un dispositivo externo como un disco duro o una unidad de memoria USB, y lanzaremos la copia de seguridad.

Linux

En entornos Linux existen también multitud de herramientas dependiendo de si queremos hacer una copia integra o una copia parcial de nuestros datos.

Una de las opciones más sencillas para las copias de seguridad de nuestros datos es ***rsync***[67] con su aplicación gráfica Grsync(no muy atractiva a la vista, por cierto). Basta con seleccionar el origen y el destino de la copia de seguridad, elegir los atributos que deseamos que se almacenen y pulsar sobre "Ejecutar". Con esto, todos los datos seleccionados se copiarán al destino elegido, pudiendo ser este un disco duro externo o un destino de red. La próxima vez que se ejecute el software, la copia se realizará de forma incremental, por lo que los datos que no se hayan modificado, no se sobrescribirán, con el consiguiente aumento de velocidad en el proceso.

Para realizar copias integrales del disco duro podemos utilizar las herramientas ***"mondo"***[68] y ***"mindi"***[69]:

Tras instalarlos, primero crearemos un CD de arranque con mindi para asegurarnos que es compatible con nuestro sistema. Para ello ejecutaremos en una terminal "mindi" el cual nos pedirá ciertos parámetros mediante un asistente:

67 Accesible en http://es.wikipedia.org/wiki/Rsync
68 Accesible en http://blogdrake.net/node/7088
69 Accesible en http://www.mondorescue.org/

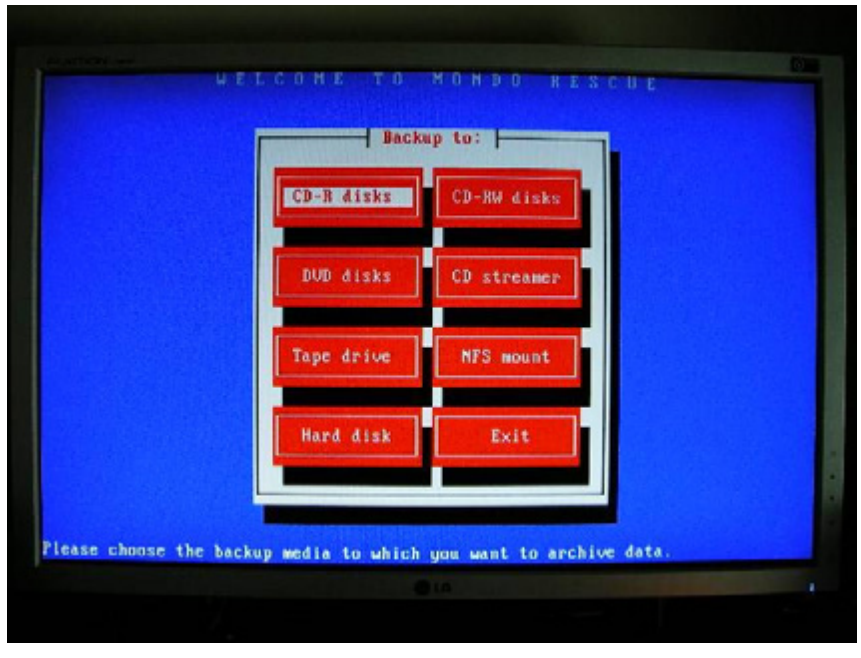


Ilustración 45 · Terminal mindi

```
Do you want to use your own kernel to build the boot disk (y/n) ? Y

Would you like to use LILO (instead of syslinux) for your boot CD/
floppies (y/n) ? N

Would you like to create boot+data floppy disks now (y/n) ? N

Shall I make a bootable CD image? (y/n) Y
```

Tras ejecutar esto, nos creará un cd en el directorio /root/images/mindi/mindi.iso que meteremos en un CD/DVD y reinicaremos. Si este proceso se completa correctamente estamos listos para hacer nuestra copia con "mondo". Bastará con ejecutar "mondoarchive" y aparecerá un menú algo arcaico pero sencillo de seguir.

1.2 Contraseñas de acceso

En caso de robo o pérdida del equipo, además de salvaguardar la información para restaurar el servicio lo antes posible, es necesario tener la tranquilidad que la información almacenada en el dispositivo extraviado esté protegida para evitar que pueda ser utilizada con fines fraudulentos.

El primer control de seguridad que se debe implantar es una contraseña, siendo la contraseñas de la ***bios***[70] la mejor opción.

70 Accesible en http://es.wikipedia.org/wiki/BIOS

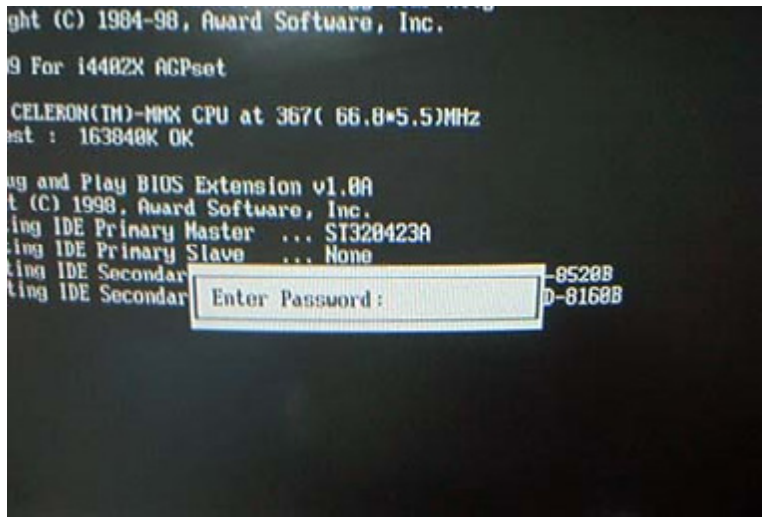


Ilustración 46 · Contraseña BIOS

Se trata de una contraseña que se requiere antes de cargar cualquier tipo de sistema operativo por lo que no es posible evitarla mediante el uso de ningún cd de arranque ***liveCD***[71] o usb de arranque ***liveUSB***[72].

Esta contraseña se establece desde el menú de la bios que aparece generalmente al pulsar F2 o Suprimir, durante el arranque del equipo.

En caso de no estar familiarizado con las opciones de la bios recomendamos solicitar soporte al administrador del sistema, ya que se administran parámetros delicados que pueden causar que el equipo no arranque correctamente. Una de las opciones debe ser la introducción de contraseña mediante USER PASSWORD o similar.

Aquí introduciremos la contraseña que elijamos. Posteriormente habrá que configurar el sistema para que pida la contraseña cada vez que el equipo arranque. Dentro del apartado de BIOS FEATURES SETUP (o similar) debe haber una opción de seguridad (Security Option). Donde se configura para que la pida siempre (System).

Después de esto, se guardan los cambios 'SAVE & EXIT SETUP' y se sale de la BIOS. El equipo se reiniciará y nos pedirá la clave introducida anteriormente.

Aparte de la contraseña de la bios existen contraseñas para los sistemas operativos, la clásica contraseña de usuario de Windows o linux, las cuales pueden proteger nuestros datos de usuarios poco experimentados, pero que para usuarios avanzados no suponen un problema. En la mayoría de los casos bastaría con arrancar con un liveCD y entrar al disco duro para que toda la información esté disponible.

1.3 Controles avanzados de acceso

Una vez introducida la contraseña de la bios (en caso de haberla), se pasa a cargar el sistema operativo, en el cual se pueden implementar controles de acceso más sofisticados que las tradicionales contraseñas como pueden ser

71 Accesible en http://es.wikipedia.org/wiki/Livecd
72 Accesible en http://es.wikipedia.org/wiki/Live_USB

dispositivos USB con un certificado de usuario, tarjetas criptográficas, lectores de huella digital o incluso sistemas de reconocimiento de imágenes.

Nota: A pesar de que estas medidas pueden interpretarse como medidas e seguridad físicas, realmente no lo son ya que no impiden el acceso físico al equipo, sino que se trata de medidas lógicas.

- **Utilizar memorias USB como contraseña:** existen herramientas del tipo USB Lock, mediante la cual convertiremos una unidad USB en una "llave" para poder iniciar sesión sin necesidad de contraseñas.

- **Tarjetas criptográficas:** en entornos corporativos, en caso de disponer de una tarjeta criptográfica, como puede ser el DNI electrónico o los certificados de la ACCV, y un lector, es posible configurarlo para utilizar el certificado de la tarjeta en lugar de la contraseña de acceso.

  En la siguiente url se explica como configurarlo en entornos Windows: ***http://support.microsoft.com/kb/281245/es***[73]

- **Lectores de huella dactilar:** existen equipos portátiles que incorporan un pequeño lector de huella dactilar con el cual es posible utilizar la huella para acceder al equipo o desbloquear la cuenta de usuario.

- **Sistemas de proximidad:** Los sistemas de proximidad constan de dos partes físicas, las cuales una se conecta al equipo y la otra la posee el usuario (enganchada al móvil, cartera o bolsillo). Estos dispositivos se comunican de forma inalámbrica de modo que detectan si se encuentran cercanos. Se caracterizan por su comodidad para el usuario ya que en cuanto este se aleja del equipo (o el equipo es sustraído), el sistema se bloquea automáticamente y al volver al puesto de trabajo se desbloquea.

Ilustración 47 · USB

1.4 Cifrado

Con las contraseñas de acceso evitamos que se acceda al equipo, pero no evitamos que se extraiga el disco duro, se coloque en otro equipo y entonces se acceda a la información. Para evitar esta situación se ha de recurrir al cifrado de los datos.

El cifrado consiste en, mediante técnicas matemáticas codificar la información para que no sea posible leerla sin conocer una clave. Las técnicas criptográficas han evolucionado y esta clave ya no tiene por que ser una clave o contraseña

73 Accesible en http://support.microsoft.com/kb/281245/es

clásica, siendo posible utilizar un certificado digital, tarjeta criptográfica, huella digital o un USB.

Dependiendo de la naturaleza de la información contenida podemos optar por dos opciones, cifrar todo el sistema o cifrar únicamente los datos sensibles.

La mayoría de sistemas operativos ofrecen la opción de cifrar las carpetas personales de los usuarios de forma nativa.

Windows

En sistemas Microsoft Windows basta con seleccionar la carpeta o el archivo a cifrar y pulsar botón derecho → propiedades → general → avanzadas → atributos de compresión y cifrado" y marcar "cifrar contenido para proteger datos". Solo quedará elegir si deseamos cifrar solo el contenido de la carpeta o también todas las subcarpetas.

Si una carpeta está cifrada, el nombre de la misma aparecerá en color verde.

Este sistemas no utiliza ninguna contraseña, sino un certificado que se "activa" al iniciar sesión con nuestro nombre de usuario y contraseña a la hora de arrancar el equipo. De esta forma, cada usuario podrá acceder de forma transparente a sus carpetas cifradas sin necesidad de volver a introducir la contraseña, mientras que si se intenta abrir el fichero de otro usuario no se tendrá acceso por estar utilizando un certificado distinto.

El problema de esta técnica es que si se se reinstala el sistema y se migran los datos, estos serán ilegibles por perderse el certificado de cifrado/descifrado. Para evitar esta situación hay que exportar este certificado y almacenarlo fuera del equipo, por ejemplo en una memoria USB.

Para exportar el certificado de cifrado/descifrado pulsaremos en inicio-ejecutar, escribiremos CMD, y se abrirá una sesión de ms-dos donde habrá que escribir "cipher/r fichero" con lo que se solicitará una contraseña para proteger el certificado.

Linux

Ya que en los sistemas linux, la mayoría de los datos de usuarios se almacenan en la carpeta home, una buena opción es centrarse en cifrar esta carpeta. Al igual que en sistemas Windows, existe la posibilidad de cifrar la carpeta de forma transparente para el usuario de forma que cuando inicie sesión se solicite la clave de descifrado que permanecerá activa durante toda la sesión.

Para ello, necesitamos instalar el paquete ecryptfs-utils, con lo que se creará una carpeta cifrada en el directorio /home/ y bastará ejecutar en una terminal ecryptfs-setup-private para establecer la contraseña que deseemos.

Cifrado seguro independiente del sistema operativo

Aparte de las opciones anteriores, existe un estándar de cifrado de código abierto muy extendido llamado GnuPG o GPG. Se trata de una evolución libre de su predecesor PGP. Se caracteriza por utilizar certificados digitales que pueden ser utilizados tanto para correo electrónico como para cifrar ficheros.

Se trata de una plataforma muy versátil con multitud de opciones y que cuenta con mucha documentación en su sitio web ***www.gnupg.org***[74] por lo que no consideramos necesario incluir aquí todo su contenido.

Otras consideraciones

Ciertas medidas adicionales han de tomarse en cuenta si vamos a viajar al extranjero con nuestros equipos o dispositivos portátiles, ya que algunos países, como Estados Unidos, pueden exigirnos examinar el contenido del equipo, realizar una copia integra para su posterior análisis o incluso requisarlo si lo consideran oportuno.

Se conocen casos en los que han solicitado las contraseñas para descifrar ficheros protegidos, por lo que para evitar problemas o retrasos en los vuelos internacionales, se recomienda cifrar los datos sensibles que no quieran ser revelados y depositarlos en algún servidor de Internet para descargarlos y descifrarlos una vez llegados al destino.

1.5 Recuperar equipos robados

Gracias a las nuevas prestaciones de los equipos portátiles han surgido numerosos programas que nos pueden ayudar a recuperar nuestro portátil en caso de robo. Estos programas se ayudan de las cámaras web, GPS, y redes inalámbricas integrados en los portátiles de forma que cuando el equipo tienen conectividad a Internet puede enviar a una dirección de correo electrónico capturas de pantalla, fotos tomadas desde la webcam, o incluso las coordenadas del GPS marcando la posición en la que se encuentra.

Una buena utilidad es ***"Prey"***[75] por ser libre y multiplataforma disponible para Windows, Mac Os, Android, iOS y Linux.

Ilustración 48 · Prey

El buen funcionamiento de la aplicación depende de las características del portátil (GPS, WebCam), de la conectividad a Internet, y de que el equipo no sea formateado, además de que el software ha de ser instalado antes de que el portátil sea robado.

74 Accesible en http://www.gnupg.org/
75 Accesible en http://preyproject.com/

1.6 Información susceptible de ser robada

Es posible que algunos usuarios crean que la información que contienen sus equipos portátiles no es crítica y que no es necesario tomar medidas de seguridad para salvaguardar los datos que contiene el equipo, pero acostumbran a no tener en cuenta casos como estos:

- **Currículum:** es frecuente tener el currículum en formato electrónico en las carpetas de documentos. De no estar cifrado, quedan públicos datos relevantes como nuestra profesión, dirección, teléfono y fotografías. De esta forma estamos ofreciendo información a desconocidos que les puede hacer intuir cuanto ganamos, donde vivimos, si tenemos pareja y edad situación muy poco recomendable ya que si el equipo ha sido robado esta información puede ser utilizada para preparar incluso robos en el domicilio particular.

- **Fotografías y vídeos:** en caso de disponer de fotografías personales en nuestro equipo, dependiendo de la índole de las mismas es posible que estas sean publicadas en Internet violando la privacidad de familiares y amigos. En caso de contener fotografías intimas, es posible que sean utilizadas para extorsionar y chantajear, bajo la amenaza de que se hagan publicas.

- **Ficheros con contraseñas:** Existen usuarios que almacenan sus contraseñas en ficheros descifrados u hojas de calculo. De ser el caso, todas estas contraseñas quedarían expuestas posibles usuarios maliciosos. Si además de contraseñas de acceso a servicios de correo, mensajería o similar, contienen también contraseñas de acceso a banca electrónica es posible que sean utilizadas con fines fraudulentos.

- **”Recordar contraseñas” en navegadores:** Muchos usuarios utilizan la opción “recordar contraseña” que tienen los navegadores para no tener que escribir las contraseñas de acceso en los servicios online que más utilizan. Mediante las opciones del navegador es posible visualizar estas contraseñas con el importante riesgo que ello conlleva. La mayoría de los navegadores disponen de la opción de establecer una contraseña maestra, de forma que para editar, agregar y consultar las contraseñas almacenadas, es necesario introducir la contraseña maestra.

- **Correo electrónico almacenado:** Los usuarios que utilizan clientes de correo como Microsoft Outlook o Mozilla Thunderbird, almacenan el correo electrónico directamente en el equipo, por lo que en caso de robo/perdida, si el correo no está cifrado, queda expuesto a ser consultado por usuarios maliciosos. Dependiendo de la índole de los correos, esto puede acarrear problemas laborales o personales.

- **Información bancaria:** cada día es más frecuente recibir las facturas cotidianas (móvil, luz de casa, gas, justificantes de transferencias) en formato electrónico, generalmente PDF, y que los usuarios las almacenen en el ordenador. De esta forma, en caso de perdida/robo del equipo, nuestros datos bancarios, últimos movimientos o incluso

saldo de las cuentas quedan expuestos. Toda esta información puede ser utilizada para realizar compras por internet, contratar servicios a cuenta del usuario y realizar movimientos bancarios ilícitos.

1.7 Deshabilitar conectividad innecesaria

Dada la movilidad de los equipos portátiles, es posible que al utilizarlos fuera del puesto de trabajo o del hogar, coincidamos con otros usuarios de equipos con conectividad inalámbrica.

En caso de que nuestro equipo sea vulnerable, ya sea mediante Bluetooth o wireless, estaremos expuestos a ser víctimas de un ataque por lo que siempre se recomienda deshabilitar estas conexiones inalámbricas en caso de no estar utilizándolas, ya que además aumentaremos la duración de las baterías.

2 Protección física

La mayoría de los controles de seguridad explicados en puntos anteriores hacen referencia a la posibilidad de salvaguardar la confidencialidad de la información y o la integridad del sistema en caso de robo, pero también se disponen de medidas de protección físicas para evitar que el equipo sea sustraído.

Ilustración 49 · Protección física I

Los elementos de seguridad física más comunes son los candados con cable de acero, los cuales es enganchan por un extremo al portátil y por el otro a algún elemento no móvil del puesto de trabajo. Los hay con llave o combinación, e incluso con alarmas sonoras como medida disuasoria.

Otra opción algo más disuasoria es “secury it”, una etiqueta con nuestros datos de contacto, la cual dispone de un arnés para conectarle un cable de seguridad. Se trata de una pegatina resistente que se coloca en la tapa de forma que para retirar esta etiqueta es necesario dañar físicamente la tapa del ordenador, haciéndolo más difícil de vender.

Ilustración 50 · Protección física II

Especialmente enfocado a entornos laborales, cabe la posibilidad de utilizar la tecnología RFID para evitar robos por parte de empleados o visitantes. Para ello hay que etiquetar todos los equipos portátiles con pegatinas RFID las cuales contienen información sobre el dispositivo, como puede ser tipo, identificador, o características del mismo, además de colocar escáneres en las entradas y salidas, de forma que en caso de que se produzca una salida no autorizada de un dispositivo, suene una alarma, o se tome una imagen.

3 Otras consideraciones

Información de contacto: Puede parecer una propuesta algo ingenua, pero es recomendable dejar un teléfono de contacto adherido al portátil. De esta forma en caso de ser extraviado y encontrado, sea posible contactar con el dueño para devolverlo.

No mostrar excesivamente el equipo: en lugares públicos es recomendable no exhibir en exceso el portátil si no es necesario

Evitar en la medida de lo posible los maletines de portátil. Es recomendable utilizar mochilas o maletines que no induzcan a pensar que contienen equipos portátiles.

10

TELÉFONOS MÓVILES, MÓVILES INTELIGENTES Y PDA

Los teléfonos móviles quedan ya lejos del concepto inicial de teléfono para pasar a ser dispositivos en el que almacenamos información de todo tipo, desde contactos, citas, eventos, fotos, vídeos, correos electrónicos, ficheros personales o incluso contraseñas. Resulta muy cómodo disponer de toda esta información en cualquier lugar pero como en el resto de nuevas tecnologías, en ocasiones no se recibe la formación necesaria para conocer y tomar conciencia de los riesgos que puede implicar su uso.

Estos dispositivos se clasifican en 3 grandes grupos:

Teléfonos móviles: son los dispositivos más comunes y sencillos. Disponen de las funciones básicas para comunicarse, como llamadas de voz, SMS e incluso videollamadas. También pueden disponer de sistemas para reproducir contenido multimedia o realizar fotografías,

Teléfonos inteligentes, o smartphone: además de tener las cualidades de un teléfono móvil tradicional disponen de herramientas avanzadas de gestión y comunicación como pueden ser conectividad continua con internet, gestión de correo electrónico, redes sociales, juegos online, o acceso a servicios en la nube.

Por último encontramos las **PDA**, las cuales han caído en desuso con la introducción de los smartphones en el mercado domestico. Se caracterizaron por ser los primeros dispositivos móviles con pantallas táctiles, generalmente con la ayuda de un lápiz, y disponían de los primeros sistemas operativos que permitían editar documentos o navegar por internet.

Muchas de las funcionalidades descritas en este capitulo dependerán del dispositivo utilizado, sistema operativo, u operadora de telecomunicaciones.

1 PIN, PUK e IMEI

En los primeros teléfonos el mayor de los problemas era que fuese extraviado o robado y se utilizase para realizar llamadas a cargo del dueño del dispositivo, para lo cual se creó el código PIN (Personal Identification Number). Se trata de un código numérico encargado de activar la tarjeta SIM del dispositivo para que el dispositivo pueda conectarse a la red de telefonía y así poder enviar y recibir información.

Nota: en caso de no conocer el código PIN, la única comunicación posible es con el número 112 de emergencias.

Este código PIN puede ser desactivado por parte del usuario aunque no se recomienda. Adicionalmente puede ser modificado por el usuario ya que se cambia directamente desde el propio terminal. Al tratarse de un número generalmente entre 4 y 6 dígitos, es relativamente fácil de averiguar por ***fuerza bruta***[76],

76 Accesible en http://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta

por lo que al tercer intento consecutivo fallido de activar la ***SIM***[77], esta queda bloqueada, requiriendo el código PUK para el desbloqueo. El código PUK es otro código que también se proporciona junto con la tarjeta y que debe guardarse en lugar seguro por si se bloquease la tarjeta.

El código IMEI es el número de serie del dispositivo (nada tiene que ver con la tarjeta SIM). Este código debe ser anotado en lugar seguro ya que en caso de perdida o robo del móvil, es recomendable proporcionárselo a la operadora o fuerzas de seguridad del estado para que bloquee el terminal y no sea posible utilizarlo en con otra tarjeta SIM. Suele constar en la caja del teléfono, pero en caso de no tenerla se puede consultar gratuitamente pulsando en el teléfono la combinación *#06# con lo que obtendremos el número por pantalla.

2 Bloqueo del terminal

En los primeros móviles era necesario introducir el código PIN para que el dispositivo funcionase, independientemente de si se iba a realizar alguna llamada. Hoy en día los teléfonos móviles disponen de muchas funcionalidades para las que no es necesario el uso de la red, por lo que se puede configurar un código de bloqueo adicional que se introduce para desbloquearlo y resulta conveniente utilizarlos. De esta forma en caso de robo o pérdida, no será posible acceder a los datos almacenados en el teléfono, por lo que si se desea utilizar el dispositivo, sería necesario hacer un ***reset***[78] del móvil eliminando toda la información del dispositivo.

Este código normalmente coincide, según el sistema operativo del dispositivo, con el código de seguridad. Se trata de otro código del propio dispositivo que se utiliza para realizar cambios importantes en el teléfono, como restringir llamadas, realizar desvíos, o cambiar las redes a las que se conecta.

Ciertos dispositivos, como el ***Iphone***[79] de Apple, disponen de un programa especial mediante el cual, si se introduce mal cierto número de veces el código de bloqueo, el equipo procede a borrar automáticamente el contenido de todo el teléfono para salvaguardar los datos privados que pueda contener.

Otros dispositivos, con el sistema ***Android***[80], tienen la posibilidad de establecer códigos de bloqueo gestuales. Se diferencian de los códigos clásicos en que en lugar de tener que introducir un código alfanumérico, deberemos realizar ciertos trazos uniendo puntos de una matriz cada vez que encendamos el teléfono o queramos desbloquear la pantalla. Para crear este patrón de bloqueo en Android, accedemos al menú de “Settings” y luego “Security & location”, allí dibujaremos nuestro patrón de seguridad conectando al menos cuatro puntos en vertical, horizontal y/o diagonal, confirmamos y activamos el patrón.

77 Accesible en http://es.wikipedia.org/wiki/Tarjeta_SIM
78 Accesible en http://es.wikipedia.org/wiki/Reset
79 Accesible en http://es.wikipedia.org/wiki/Iphone
80 Accesible en http://es.wikipedia.org/wiki/Android

3 Seguridad de las comunicaciones en telefonía móvil

La mayoría de los terminales móviles utilizan para comunicarse la tecnología GSM(2G), o su evolución UMTS(3G). Se trata de dos tecnologías muy diferentes aunque para un usuario pueda parecer que hacen lo mismo.

Cuando se diseñó GSM, se utilizaron nuevos ***algoritmos de cifrado***[81] para estas comunicaciones los cuales estaban rodeados por secretismo bajo la creencia de que si se ocultaban los detalles del algoritmo aumentarían su seguridad. Con el tiempo se demostró que fue una mala opción ya que aparecieron vulnerabilidades que permiten descifrar sin mucho esfuerzo conversaciones y SMS transmitidos mediante GSM casi en tiempo real. Se trata pues de una tecnología insegura que debe evitarse en caso de ser utilizada para transmitir información confidencial.

Más adelante surgió UMTS por la necesidad de mayores velocidades de transmisión de datos a través de las redes de telefonía móvil y se aprovecho para cambiar los algoritmos de cifrado siendo estos publicados antes de su implantación para que su seguridad fuese discutida abiertamente antes de implantarlo. De esta forma, en lugar de ser un desarrollo privado, participaron científicos de todo el mundo para conseguir un cifrado mucho más seguro que su predecesor.

Parece ser que ante la expectativa de que los usuarios migren a terminales con soporte para UMTS y que el GSM caiga en desuso, se espera que con tiempo el problema se solucione por si mismo.

4 Actualizaciones de software

En algunas ocasiones se descubren fallos en el software que controla los dispositivos móviles que pueden desde hacer que no responda como es debido, hasta comprometer la seguridad del dispositivo.

Dado que, como se ha comentado, frecuentemente contienen información sensible, y ya que existe riesgo de que se instale algún código malicioso es muy recomendable solucionar estos problemas. Para ello los fabricantes publican actualizaciones del software del sistema, también llamado ***firmware***[82] en los teléfonos móviles o Rom en los smartphones.

Mientras que en los smartphones es el propio terminal el que advierte al usuario de que existen actualizaciones, muy pocos usuarios comprueban si existen actualizaciones del firmware de sus teléfonos móviles, por lo que en caso de disponer de un terminal vulnerable quedan expuestos a numerosos peligros.

Generalmente, para comprobar si existen actualizaciones será necesario acceder directamente a la web del fabricante del dispositivo y dirigirse al apartado de descargas o soporte donde acostumbran a estar estas actualizaciones. Además resulta frecuente que se introduzcan mejoras en cuanto a usabilidad o nuevas funciones para el dispositivo.

No obstante, los últimos sistemas operativos para dispositivos más avanzados,

81 Accesible en http://es.wikipedia.org/wiki/Algoritmo_de_cifrado
82 Accesible en http://es.wikipedia.org/wiki/Firmware

como pueden ser ***Windows Mobile***[83] o Android, disponen de gestores de actualizaciones que pueden acceder directamente a Internet en busca de nuevo firmware o ***parches***[84] publicados.

5 Conectividad de dispositivos móviles

Una mala práctica habitual de los usuarios es tener activadas todas las conexiones de los dispositivos móviles, como pueden ser el Bluetooth, redes Wireless, o GPS, práctica que puede acarrear además de un consumo de batería excesivo, riesgos como los siguientes.

Ilustración 51 · Conectividad

5.1 Bluetooth

Bluetooth es una tecnología por la cual es posible conectar pequeños dispositivos para que puedan interactuar o intercambiar información.

Desde el punto de vista de la seguridad, se trata de una tecnología fiable que implemente sistemas y mecanismos para proteger las comunicaciones y que dispone de métodos robustos de autenticación. Los principales problemas de seguridad en Bluetooth, son debidos a las implementaciones de terceros que realizan los fabricantes de dispositivos.

Un claro ejemplo de estas malas implementaciones es el hecho de no poder cambiar las contraseñas por defecto que tienen algunos dispositivos como los manos libres de los vehículos, GPS externos o similar, lo cual propicia que al tener contraseñas como 0000 o 1234, cualquier dispositivo pueda emparejarse con ellos y acceder a los datos almacenados.

Las conexiones Bluetooth disponen de multitud de posibilidades entre las que destacan transmisión de ficheros, acceso a la tarjeta SIM para realizar llamadas y sincronización de contactos y agenda, por lo que ante un ataque satisfactorio contra un dispositivo vulnerable, sería posible utilizar el dispositivo para realizar llamadas a costa del propietario del dispositivo, descargar sus ficheros y fotos, robar los contactos y agenda, e incluso infectar el dispositivo.

83 Accesible en http://es.wikipedia.org/wiki/Windows_Mobile
84 Accesible en http://es.wikipedia.org/wiki/Parche_(inform%C3%A1tica)

Para evitar esta situación lo más sencillo es deshabilitar el Bluetooth y activarlo únicamente cuando vaya a ser utilizado.

Una alternativa a apagarlo, es configurar el terminal para que trabaje en **modo oculto**. De esta forma no será posible que otros dispositivos enlacen con el nuestro, mientras que el nuestro si que podrá contactar con otros.

Otro motivo para desactivar el Bluetooth, o habilitar el modo oculto, es que en grandes aparcamientos o por la noche en calles donde aparcan muchos coches, es posible pasear entre los vehículos con un dispositivo Bluetooth activado en busca de dispositivos encendidos olvidados en los coches. De esta forma en caso de detectar una señal potente desde el interior de un vehículo es evidente que se ha olvidado algún GPS o móvil dentro de un vehículo e intentar sustraerlo. Como se ha indicado, la mejor forma de evitar esta situación es desactivamos el Bluetooth o lo configuramos en modo oculto.

Ilustración 52 · Bluetooth

Además de todo lo expuesto se han de tomar en cuenta las siguientes recomendaciones:

- **No enlazar o conectar con dispositivos desconocidos,** de igual forma que no se debe aceptar ningún fichero que no hayamos solicitado.

- **Cambiar el nombre por defecto del dispositivo.** En ocasiones el nombre del dispositivo coincide con el modelo del dispositivo, por lo que si se hubiese descubierto alguna vulnerabilidad para dicho dispositivo, quedaríamos excesivamente expuestos.

- **Cambiar las contraseñas por defecto de los dispositivos Bluetooth,** especialmente GPS, y manos libres.

- **Evitar utilizar el Bluetooth para enviar información sensible,** ya que existen alternativas más robustas como pueden ser conexiones inalámbricas cifradas.

5.2 Wireless

Al contrario de lo que pueda parecer, poco se parecen los problemas de seguridad de la tecnología wireless con los propios del Bluetooth. En el wireless no se difunde el nombre del dispositivo, de forma general no se permiten las conexiones directas entre dispositivos, ni siquiera el envío y recepción de ficheros, al menos

de forma sencilla.

Los riesgos de las conexiones wireless son más propias de ordenadores compartiendo con estos ciertas recomendaciones básicas de seguridad:

- **No conectarse a redes sin cifrado,** ya que de esta forma la información viaja desde nuestro dispositivo hasta el router sin protección y puede ser fácilmente interceptada por usuarios maliciosos.

- **Evitar el uso de redes con cifrado débil como WEP,** ya que se trata de un cifrado nada robusto mediante el cual es muy sencillo capturar y descifrar la información transmitida.

- **No conectarse a redes desconocidas,** ya que entonces estaremos compartiendo la misma red que otros usuarios desconocidos sin la protección de cortafuegos ni medidas similares, arriesgándonos a ser víctimas de ataques.

- **Disponer de las últimas actualizaciones del firmware y software de acceso a la red,** ya que los dispositivos móviles que utilizan tecnología wireless acostumbran a ser mucho más complejos que simples teléfonos móviles y es posible que se descubran vulnerabilidades importantes.

- **Desactivar la conectividad inalámbrica en caso de no utilizarla,** ya que, además de alargar la vida de la batería, evitaremos que mediante un análisis de tráfico nuestro dispositivo sea descubierto.

- **No utilizar la opción de almacenar contraseña de las redes inalámbricas** a las que nos conectemos ya que en caso de robo o perdida del dispositivo, y dependiendo del sistema operativo, puede ser posible extraerla del dispositivo.

5.3 GPS

A pesar de que a priori pueda parecer que el GPS en los dispositivos móviles no puede resultar una amenaza conviene dedicar unos minutos a estudiar la configuración del terminal para hacer algunas comprobaciones. La mayoría de nuevos smartphones disponen de módulos GPS que pueden trabajar conjuntamente con la cámara de fotos del dispositivo con el fin de registrar donde se toma una fotografía. Esto puede resultar muy útil cuando se está de viaje para recordar de donde es cada fotografía aunque puede ser peligroso si no le prestamos atención: si hacemos fotos en nuestro ámbito cercano (casa, trabajo, lugar de veraneo, etc...) con esta funcionalidad activada y publicamos la foto en internet, cualquiera con acceso a la foto podría acceder a la información de la foto y averiguar donde vivimos, donde trabajamos o si cuando hemos hecho la foto estamos en casa. Esta información, según con quien sea compartida, puede entrañar riesgos como robos en periodo vacacional, o que gente ajena a nuestro circulo más cercano sepa donde vivimos. Conviene pues desactivar está característica en caso de no utilizarla.

6 Copias de seguridad

Dada la gran cantidad que se almacena en dispositivos móviles y lo critica que puede ser esta información para nosotros resulta necesario hacer copias de seguridad de los datos de nuestros dispositivos como si de un ordenador se tratase.

Uno de los mayores quebraderos de cabeza de un usuario al perder su teléfono móvil acostumbra a ser el reconstruir la libreta de direcciones ya que muy pocos realizan copias de seguridad periódicamente.

La gran mayoría de los dispositivos actuales incorporan la opción de volcar los datos a un PC mediante un proceso llamado "sincronización". De esta forma, según se configure, es posible exportar contactos, SMS, correos electrónicos, imágenes tomadas, vídeos o grabaciones de audio.

En caso de que el teléfono no admita estas copias de seguridad, es posible llevar la tarjeta SIM a una tienda de teléfonos móviles para que se haga una copia de los datos de la misma.

Este proceso puede simplificarse según las características de los dispositivos, ya que algunos incorporan integración con servidores de correo ***Exchange***[85], donde es posible sincronizar mediante Internet los datos con un servidor de correo.

De forma similar, con las llegadas de las tarifas planas de datos a los teléfonos móviles, están surgiendo servicios en los que las compañías unifican todos los contactos bajo una misma plataforma propietaria y a la cual se puede acceder desde los terminales o ordenadores personales.

Si el dispositivo incluye una tarjeta ***minSD***[86] o ***microSD***[87], se puede acceder copias directamente en un ordenador personal que disponga de un lector de tarjetas de este tipo.

7 Cifrado de información sensible

Esta característica acostumbra a estar disponible de forma nativa en pocos sistemas operativos móviles, si bien es cierto que algunos, como Symbian, disponen de aplicaciones "cartera" en las que podemos guardar datos cifrados y protegidos por contraseña. Hay que tener en cuenta que por este método no es posible cifrar ficheros, únicamente información confidencial, como cuentas bancarias, contraseñas de acceso o similares.

Además, los sistemas operativos avanzados para móviles, como Symbian, Windows Mobile, Android o Limo, ofrecen aplicaciones para poder cifrar ficheros completos.

En Windows Mobile, podemos utilizar "Resco File Explorer", un gestor de archivos que soporta el cifrado. Para ello, seleccionaremos el fichero deseado, y mediante el botón derecho pulsaremos "codificar". A continuación estableceremos la

85 Accesible en http://es.wikipedia.org/wiki/Exchange
86 Accesible en http://es.wikipedia.org/wiki/Minisd
87 Accesible en http://es.wikipedia.org/wiki/MicroSD

contraseña y finalizaremos el asistente. Este programa admite cifrado mediante RC2, RC5, DES, 3DES, y AES de 128,192 y 256 bits, por lo que es posible descifrarlo en otros dispositivos.

En Symbian podemos utilizar programas como "MediaSafe", mediante el cual podemos cifrar automáticamente las carpetas de fotos, vídeos, audio y notas, de forma que es necesaria una contraseña para poder acceder. Este programa soporta SHA1 y Blowfish.

BlackBerry dispone de la opción de cifrar de forma nativa todo el contenido multimedia desde el menú de "opciones > memoria> modo de cifrado> contraseña de seguridad" además de cambiar el campo "cifrar archivos multimedia" a "si".

8 Virus en dispositivos móviles

Dependiendo del sistema operativo del móvil es posible que este pueda ser comprometido por algún tipo de software malicioso. Afortunadamente en la actualidad no es una situación frecuente, pero con la rápida evolución que están teniendo estos sistemas, es de esperar que aumente el número de virus circulando por nuestros terminales. Algunos conocidos fabricantes de antivirus para ordenadores ya disponen de versiones para algunos sistemas operativos móviles, como pueden ser "Kaspersky" o "Symantec".

El principal foco de infección en los móviles es la instalación por parte del usuario de programas descargados de fuentes no confiables que pueden contener algún código malicioso. Puede ser el caso de supuestas herramientas de cracking para móviles, versiones "desbloqueadas" de software propietario, o aplicaciones descargadas de redes P2P.

Otros posibles modos de infección pueden ser la navegación por Internet desde el dispositivo, la recepción de ficheros adjuntos desde el correo electrónico en el móvil y el intercambio de ficheros por Bluetooth con otros usuarios.

A pesar de que parece que comparten muchas coincidencias con los virus tradicionales de ordenador, dada la gran diferencia entre cada sistema operativo y dispositivos, es prácticamente necesario que el virus esté adaptado a cada tipo de terminal para que sea efectivo. Esto hace, que de momento, sea complicado infectarse, pero como ya hemos comentado, es previsible que a medio plazo la situación se vuelva más delicada.

Por todo ello es recomendable seguir unas sencillas pautas de comportamiento, comunes con el resto de plataformas informáticas:

- Mantener el sistema operativo del móvil actualizado.
- No instalar programas de dudosa procedencia.
- No abrir ficheros ni enlaces a páginas web enviados por desconocidos.
- Desactivar el Bluetooth cuando no se utilice.

11

INTERNET Y LOS MENORES

1 Introducción

Internet se ha convertido en una revolución en la última década, haciendo realidad aspectos que hace algunos años para la mayor parte de las personas eran únicamente una cuestión de ciencia ficción. No obstante, existe una clara diferencia entre los usuarios que hemos "adoptado" Internet como medio de comunicación y aquellos que, primero Prensky y ahora el ***Berkman Center for Internet and Society***[88], llaman "nativos digitales". Es decir, usuarios para los que no hubo una época de su vida en la que Internet tal y como la conocemos hoy en día no existía.

Ilustración 53 · Caperucita y el lobo

Éstos son, como es natural, los menores, especialmente aquellos ubicados en el rango de edad entre ocho y quince años y constituyen no sólo aquellos que definirán el futuro de la red, sino aquellos que, por el hecho de nacer en un mundo ya conectado, consideran este hecho de manera más natural y menos extraordinaria, reduciendo al máximo la distancia que establecen entre su vida "electrónica" y su vida "física"; su identidad digital es únicamente una dimensión más de su identidad personal. Internet es una parte más de su vida social, igual que lo es ir al cine o hablar con los compañeros de clase.

Mientras que esto tiene indudablemente aspectos muy positivos para estos usuarios, les genera una dificultad añadida a la hora de aplicar patrones de comportamiento diferentes dependiendo del entorno en el que se relacionan. No hay ninguna duda de que las redes sociales, servicios de mensajería instantánea, o correo electrónico son herramientas positivas para los menores que incorporan una dimensión vital necesaria hoy en día en sus relaciones sociales, pero sobre las que es necesario educarlos para que sean conscientes de los riesgos a los que se enfrentan y dispongan de las herramientas para hacerles frente. En definitiva, al igual que una persona no se comporta del mismo modo en una cena de

88 Accesible en http://cyber.law.harvard.edu/research/youthandmedia/digitalnatives

amigos que en una reunión de negocios, se trata de educar a los menores para que sean consciente de que enseñarle fotografías del verano a un amigo no es lo mismo que colgarlas en tu tablón de Facebook, aunque tu amigo lo sea también en Facebook.

Los principales problemas relativos a la utilización de Internet por parte de menores radican en la ingenuidad, buena fe o simple desconocimiento de lo que puede esconderse al otro lado de la red; es famosa una viñeta en la que un perro simula utilizar un ordenador mientras dice "En Internet, nadie sabe que eres un perro". La moraleja es simple: debemos desconfiar de lo que hay (o de quién hay) al otro lado de una conversación, de una página web o de un correo electrónico, ya que a ese otro lado puede haber un perro... o un delincuente.

Ilustración 54 · Viñeta

2 Seguridad en el correo electrónico

El correo electrónico es probablemente el medio más utilizado de comunicación entre los usuarios de Internet, aunque en el espectro de población que nos centramos no tiene tanta importancia como en otros ámbitos, por lo que su nivel de amenaza no es tan elevado. Al respecto, cabe destacar que el correo electrónico, aun cuando sus ventajas son innumerables (rapidez, asincronía, facilidad de comunicación, etc.), implica algunos problemas que no sólo desconocen los menores, sino que también lo hacen los adultos; vamos a comentar los más destacados en este punto.

El correo electrónico es, por defecto, un medio eminentemente inseguro para el envío de información. Su contenido se transmite, excepto si este hecho no ha sido resuelto de manera intencionada por el usuario (aspecto que no es trivial

no habitual), en claro por la red. Si visualizamos mentalmente Internet, la red está compuesta por una serie de elementos centrales que reciben los datos y los distribuyen hacia el destino apropiado (***"encaminadores", o "enrutadores"***[89] en su traducción literal del inglés "routers"), y otros elementos "periféricos" que constituyen los usuarios finales (es decir, su PC o el mio). Asimismo, debe tenerse en cuenta que a menudo, no existe una similaridad entre aspectos geográficos del mundo real y el "virtual"; es obvio que para ir de Valencia a Madrid en un medio de transporte carece de sentido atravesar París o Londres, pero eso no se aplica a los datos informáticos. Un correo electrónico enviado a otro usuario que se encuentra en Madrid puede implicar que los datos que contiene atraviesen una docena de sistemas ubicados en Francia, Alemania e Italia, alguno de cuyos sistemas puede haber sido "comprometido" y los datos que recibe ser grabados o modificados.

El correo electrónico es, en aspectos de autenticación, un medio eminentemente inseguro. Esto quiere decir que el hecho de que A reciba un correo de B no siempre implica que ese correo haya sido enviado efectivamente por B; resulta relativamente sencillo para un usuario experimentado modificar los campos de un correo para hacer creer al destinatario que el emisor del correo es alguien que no es. Aunque la implicación de este hecho para los menores es pequeña, es un aspecto que hay que tener en cuenta.

Prácticamente todo usuario de Internet ha recibido un correo que forma parte de una cadena. A causa del bajo coste (en principio) que supone el envío de un e-mail, hace mucho tiempo que se popularizaron las cadenas de correos electrónicos. Más allá de la molestia que suponen estas cadenas de correos, de la pérdida de tiempo que suponen para muchos usuarios y de la sobrecarga de los servidores de envío y recepción que implican, su principal riesgo reside en el uso que se le da al campo del destinatario (Para:) o copia (Cc:). Es frecuente recibir correos de este tipo cuyos emisores lo envían a unas cuantas docenas de usuarios y ni siquiera han eliminado las direcciones que contiene el cuerpo del correo, lo que implica que el correo recibido puede contener con facilidad un centenar o más de direcciones de correo electrónico. Estas cadenas son utilizadas por personas malintencionadas para construir bases de datos a las que enviar no sólo correo basura (que incrementa la pérdida de tiempo y la sobrecarga indicada previamente), sino también e-mails conteniendo spyware, malware, virus, y enlaces a páginas web de phising.

El phising (podemos consultar el capítulo dedicado a delitos) puede considerarse como una composición de correo electrónico y entorno web. Aunque en general está orientado a conseguir credenciales bancarias, existe también la versión menos perjudicial desde el punto de vista financiero pero que puede implicar el inicio de un problema psicológico serio para el menor. Esta versión está basada principalmente en enviar al usuario un correo en el que se describe un medio para averiguar qué "amigos" del ***MSN***[90] le tienen bloqueado, pretendiendo aprovechar un problema de seguridad o una funcionalidad escondida de este programa de mensajería instantánea. Dicho correo le redirecciona a una página

89 Accesible en http://es.wikipedia.org/wiki/Enrutador
90 Accesible en http://es.wikipedia.org/wiki/Windows_Live_Messenger

web que solicita al usuario que introduzca su usuario y clave de MSN. Como es obvio o no existe dicha funcionalidad oculta o ésta no tiene nada de oculta, lo que a todos los efectos implica que el usuario ha introducido sus credenciales de acceso a su correo de Hotmail y cuenta de MSN, donde puede existir información sensible del menor: fotografías, conversaciones, intimidades, etc. Aunque dicha información es habitualmente utilizada para la construcción de bases de datos de destinatarios de ***spam***[91], no hay que descartar la posibilidad de que se utilice para chantajear al usuario, siendo en este caso los menores especialmente sensibles por su mayor dependencia de las opiniones de los demás.

Por último, caben destacar los correos electrónicos que "simplemente" contienen Spyware, pero cuyo contenido está diseñado de tal forma que para un usuario poco precavido puede parecer legítimo. Debe tenerse en cuenta que una parte no despreciable de los usuarios que reciben un correo de un desconocido con un ejecutable que aparenta ser para otra persona intenta abrirlo, lo que supone automáticamente en la infección del equipo, y de nuevo, puede implicar la instalación de software y troyanos que faciliten el control del equipo por parte de un tercero, quien puede llevar a cabo chantaje, intimidación o abuso, como se ha comentado en el punto anterior. En este punto, el menor debe ser consciente de que no debe abrir los ficheros adjuntos de correos de emisores desconocidos, por muy interesantes que éstos aparenten ser.

3 Seguridad en navegación web

Compitiendo con el correo electrónico, la web es el servicio estrella de Internet, en especial tras la aparición de la ***web 2.0***[92], donde el usuario no es ya un mero espectador sino que dispone de todos los medios para convertirse en un componente activo de la web.

Dejando las ***redes sociales***[93] para un punto posterior, la principal figura a destacar en este caso son los ***blogs***[94], cuyo crecimiento en los últimos años ha sido espectacular. Un blog no es otra cosa que un espacio web tradicional donde los contenidos se cuelgan de manera secuencial a modo de diario personal, y donde se reflejan opiniones, fotografías y vivencias de la persona. En el caso de los menores, es fácil que éstos utilicen el blog para comunicarse con otros usuarios tanto de su esfera social local como global, y que este contenga información sensible tanto desde el punto de vista de la protección del menor como desde el punto de vista de la intimidad.

El menor debe ser consciente de la importancia, visibilidad y perdurabilidad de cualquier contenido que "cuelga" en Internet. Aunque publicar una confidencia pueda parecer una buena idea en un determinado momento, quizá una semana después esa "entrada" o "post" ya no sea tan buena idea, por sus implicaciones para el propio autor o para terceras personas. No hay que olvidar en ningún momento que cualquier cosa que un usuario pone en Internet se convierte en eterno, y cuyo control escapa al propio autor; el menor debe saber que una

91 Accesible en http://es.wikipedia.org/wiki/Spam
92 Accesible en http://es.wikipedia.org/wiki/Web_2.0
93 Accesible en http://es.wikipedia.org/wiki/Red_social
94 Accesible en http://es.wikipedia.org/wiki/Blog

fotografía colgada en un blog deja de estar bajo su control, ya que es posible copiarla y colgarla en otro blog, en una red social, enviarla por correo o guardarla en el ordenador de cualquier usuario

Asimismo, es importante saber que al igual que no le damos nuestra dirección postal ni teléfono móvil a cualquiera, tampoco debemos hacerlo en Internet (ni en un blog ni en cualquier otro medio). Aunque parezca que nuestros visitantes son los amigos de siempre, en realidad no es así. Otras muchas personas, curiosos, amigos de otros amigos, o personas con las que no nos llevamos bien, pueden acceder a nuestro espacio personal y por tanto a nuestros datos personales. Los problemas de privacidad que puede acarrear un blog donde el menor da detalles de sus amistades, lugares frecuentados, horarios... son algo a tener muy en cuenta por los propios menores, pero especialmente por los padres: es necesario estar muy atento a la utilización de nuestros datos en Internet, por ejemplo, a la hora de registrarse en webs no confiables que nos pueden llegar a solicitar hasta el teléfono o la dirección de nuestra casa.

Ilustración 55 · Google

De la misma forma que ningún padre abandonaría a sus hijos en el centro de una gran ciudad, a merced de todo tipo de delitos, es muy importante no abandonar "digitalmente" a los menores; aunque en ocasiones nos resulte cómodo que nuestros hijos conecten a internet, y a primera vista parezca inofensivo, debemos tener siempre presente que en la red hay gente buena y mala, contenidos apropiados e inapropiados, excelentes amigos y delincuentes... exactamente igual que en la vida real. Los problemas de pérdida de privacidad, acceso libre a contenidos pornográficos, las páginas que sin que el menor pueda darse cuenta permiten a un tercero tomar el control de nuestro ordenador... son simplemente algunos de los ejemplos que nos pueden suceder si permitimos que nuestros hijos accedan libremente a Internet, sin ningún tipo de control.

4 Seguridad en mensajería instantánea

La mensajería instantánea es, junto con las redes sociales, el principal medio de comunicación de los menores en Internet. Este medio permite una comunicación inmediata y síncrona, además de proporcionar múltiples funcionalidades de intercambio de información, tanto de ficheros como de conexión a la WebCam del interlocutor. Aunque existen multitud de protocolos y programas de mensajería

instantánea, sin duda el más utilizado en la actualidad por los menores es Microsoft Messenger (MSN); en cualquier caso, los problemas comentados en el presente punto son extrapolables a cualquier sistema de mensajería.

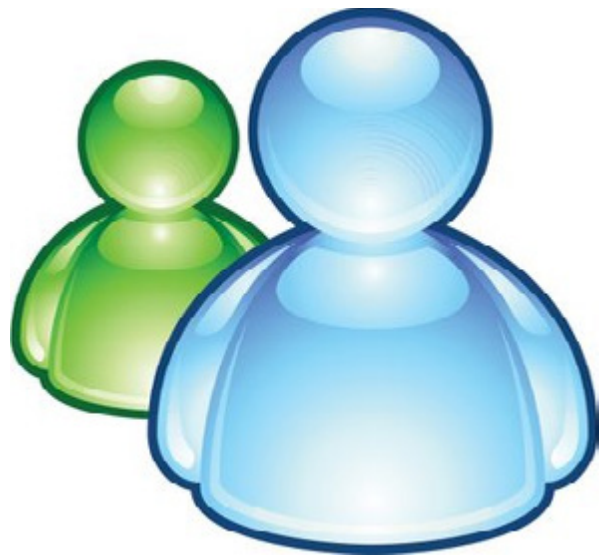


Ilustración 56 · Messenger

El principal problema relativo a la utilización de sistemas de mensajería instantánea en los menores -tal y como hemos dicho al principio, en general, en el uso de Internet por parte de éstos- es la ingenuidad y el desconocimiento de lo que puede esconderse en una inocente conversación; la primera regla de oro es **no admitir a cualquiera que nos añada como amigo,** ya que a priori no sabemos quién está detrás de una dirección de correo. Para una persona malintencionada, es muy sencillo conseguir una dirección de correo aparentemente inocente, entablar conversación con un menor y ganarse su confianza hasta obtener datos de su vida privada muy relevantes, incluso de cara a realizar delitos "físicos" contra el menor. Por tanto, la segunda regla de oro es **no fiarse de cualquiera** que nos esté hablando a través de MSN: incluso aunque aparentemente sea un amigo, a ese amigo pueden suplantarle la identidad (por ejemplo, mediante el ***robo de la contraseña***[95] de acceso a MSN). De hecho, hay gusanos que inician conversaciones automáticas con los contactos MSN de su víctima con el objetivo de propagarse; es muy importante no aceptar ficheros enviados por MSN y que puedan resultar sospechosos, aunque aparentemente sean legítimos: si nuestro amigo, sin mediar palabra, nos trata de enviar un archivo, o inicia una conversación en inglés cuando habitualmente hablamos en castellano, debemos sospechar.

Otra regla muy importante a la hora de utilizar mensajería instantánea, al igual que cuando utilizamos redes sociales o correo electrónico, es **no facilitar nunca datos de carácter personal** que puedan comprometer nuestra seguridad (teléfono móvil, dirección, instituto, horarios...); recordemos, tal y como hemos indicado, que esta información puede ser muy útil para un tercero malintencionado. Por supuesto, **tampoco debemos facilitar nuestra clave** MSN a cualquiera que nos la pida, ya que esta contraseña proporciona el acceso directo a nuestros contactos -y probablemente a nuestro correo electrónico-; esta regla, que parece obvia, no lo es tanto: aunque poca gente daría su clave al

95 Accesible en http://geekotic.com/2007/03/12/12-cosas-que-siempre-quisiste-saber-sobre-msn-pero-te-mias-preguntar/

primero que se encuentra en Internet, existen multitud de webs malintencionadas que, con la excusa de proporcionar al usuario información acerca de amigos que lo bloquean -por poner un ejemplo-, solicitan el nombre de usuario y la contraseña MSN aprovechando la ingenuidad del usuario. Obviamente, se trata de páginas falsas cuyo único objetivo real es disponer de acceso al correo electrónico y a la mensajería del menor.

Cualquier sistema de mensajería actual (por supuesto, también MSN) permite no sólo intercambiar conversaciones o ficheros, sino también utilizar la webcam del usuario para entablar videoconferencias; por supuesto, esto constituye un riesgo añadido a la utilización habitual de la mensajería instantánea, ya que no sólo estamos transmitiendo texto, sino vídeo y audio; debemos concienciar al menor para que **no active jamás la webcam con un contacto desconocido**, ya que es habitual la utilización de estos sistemas por parte de pederastas que, haciéndose pasar por menores, tratan de ganarse la confianza de un tercero y obtener así imágenes -incluso comprometidas- de éste.

Muchas cámaras web actuales pueden ser activadas por control remoto, tal y como veremos en el capítulo dedicado a la seguridad de los sistemas, lo que implica que el menor puede ser grabado incluso no estando conectado a MSN si alguien ha comprometido la seguridad de su equipo. Adicionalmente, siempre que se inicia una videoconferencia, estamos proporcionando a un tercero la posibilidad de grabar o capturar las imágenes transmitidas, con las implicaciones que el mal uso de estas imágenes puede acarrear: las imágenes pasan a estar fuera de nuestro control, y a partir de ese momento pueden ser publicadas en webs, foros, o distribuidas de cualquier otra forma por Internet.

Para acabar este capítulo, es necesario hacer especial hincapié en el **riesgo de chantaje y extorsión** a menores que puede implicar el mal uso de la mensajería instantánea; si fuera este el caso, debemos recomendar que el adulto esté siempre accesible y dispuesto a tratar estos problemas con el menor, transmitiéndole confianza para que le cuente cualquier incidencia de este tipo, y por supuesto prestándole todo su apoyo para resolverla. Y obviamente, ese apoyo debe comenzar con la denuncia del hecho ante las Fuerzas y Cuerpos de Seguridad del Estado (ver capítulo relativo a delitos).

5 Seguridad en P2P

El P2P es sin duda el protocolo de intercambio de ficheros más ampliamente utilizado hoy en día, tanto por menores como por adultos; todos los riesgos generales de utilización de este tipo de mecanismos, comentados en diferentes capítulos del presente curso, en el caso de los menores estos riesgos se agravan, ya que entran en juego, una vez más, factores como la inocencia, las ganas de hacer amigos o el afán de protagonismo.

Para comenzar, es necesario hacer hincapié en la falta de confianza de cualquier archivo descargado desde una red P2P; lo que a primera vista es un vídeo inocente, puede resultar no sólo un contenido inapropiado para un menor (pornografía, violencia...), sino que puede convertirse en el medio de transporte de cualquier

tipo de malware: virus, gusanos, troyanos... Es necesario hacer hincapié, una vez más, en la necesidad de utilizar sistemas antivirus correctamente actualizados y, en este caso concreto, de validar por parte de un adulto los contenidos que el menor descarga de redes P2P.

Especialmente en el caso de los menores, una precaución básica en la utilización de redes P2P consiste en **no compartir jamás material propio** (fotografías, vídeos, documentos...) a través de estos mecanismos; si colgamos una foto, un trabajo del instituto, o un vídeo personal en eMule, es muy difícil garantizar que sólo quien nosotros queramos podrá descargarlo. Lo más probable es que este material acabe en manos de terceros, que como siempre podrán hacer con él lo que estimen oportuno (y no siempre será bienintencionado). En este sentido, es necesario configurar correctamente cualquier programa P2P, para garantizar que no estamos compartiendo archivos que realmente no queremos compartir: un sencillo error de configuración puede llevarnos a dejar accesible a Internet todo nuestro disco duro, con lo que esto puede implicar para nuestra privacidad, reputación, etc.

6 Seguridad en redes sociales

Facebook y Tuenti son hoy en día las dos redes sociales más utilizadas por los menores de todo el mundo. A través de ellas, los usuarios intercambian fotos, comentarios, datos personales, tendencias, aficiones, y todo tipo de características, creando (o tratando de crear) una identidad digital lo más similar posible a su identidad real.

Ilustración 57 y 58 · Facebook y Tuenti

Como en tantos otros ejemplos, el principal problema de la utilización por parte de menores de estas redes sociales es la pérdida de privacidad. Es necesario, una vez más, hacer hincapié en la necesidad de no proporcionar jamás datos que puedan comprometer la seguridad del menor: teléfonos de contacto, direcciones, etc. Cualquier dato publicado en una red social, al igual que los publicados en una página web, es susceptible de saltar al dominio público y, a partir de ese momento, será imposible de controlar (los mecanismos de seguridad de las redes sociales para evitar ésto suelen ser ineficientes). Debemos tener presente que la información que publicamos en una red social permanecerá en algún sitio de la red, de una u otra forma, por un tiempo indefinido.

Al igual que sucedía en los sistemas de mensajería instantánea, debemos tener

en cuenta que no todo el mundo que te agrega en Facebook o Tuenti, por poner unos ejemplos, tiene por qué ser un amigo real; por tanto, es necesario tener especial cuidado en qué conexiones aceptamos o dejamos de aceptar en estas redes sociales -o en cualquier otra-, ya que estos contactos, en caso de ser aceptados, pueden tener acceso a información que no queremos que vean.

El uso responsable de las redes sociales -como de cualquier otro elemento, en Internet o en el mundo real- es otro de los aspectos a destacar a la hora de hablar de menores en la red; al igual que las imágenes o los vídeos, cuando se publica una opinión o un comentario en una red social, es necesario pensar dos veces lo que se va a escribir antes de hacerlo. Ese comentario u opinión potencialmente puede ser leído por miles de personas, y el autor puede perder el control de quién accede al mismo y de qué forma lo hace (algo similar a lo que sucedía cuando hablábamos de blogs); por supuesto, no podemos utilizar comentarios que atenten contra los demás (xenofobia, racismo, insultos...), y debemos siempre preservar la privacidad de terceros (de nuevo, no facilitar datos privados, no colgar fotografías de otras personas...). Un mal uso de Internet en este sentido puede llegar a considerarse delito, por lo que los menores -y por supuesto los adultos- deben ser cuidadosos con lo que cuelgan en una red social.

Para finalizar los aspectos dedicados a redes sociales, es necesario hacer hincapié, una vez, en el apoyo que los adultos debemos prestar al menor en caso de problemas en la red (chantajes, amenazas...), mostrándole nuestra confianza y apoyándole en lo que sea necesario (de nuevo, inicialmente, en una denuncia de cualquier hecho que pueda llegar a considerarse delictivo).

Toda aplicación de redes sociales debe tener un apartado de configuración que permita limitar la visibilidad de la información que ofrecemos, de forma que ésta solo sea accesible por amigos e incluso limitar lo que los buscadores pueden recabar de nuestra información.

7 Seguridad y sistemas

Los aspectos relevantes para un menor cuando hablamos de la seguridad de los sistemas en Internet son obviamente los mismos que para un adulto, pero con el agravante, no sólo del desconocimiento o del exceso de confianza a los que hemos hecho referencia en varias ocasiones a lo largo del presente capítulo, sino también, con el del uso intensivo que los menores hacen de la red, en la que con frecuencia pasan muchas más horas que los adultos y llegan a convertirse en los expertos tecnológicos de cara a sus padres. De esta forma, los capítulos del presente curso dedicados a malware, seguridad en WiFi, etc. son de total aplicación al menor, y por tanto no vamos a repetir aquí estos aspectos de seguridad en sistemas, tratados con mayor profundidad en otros capítulos de este curso. No obstante, en el presente apartado del capítulo dedicado a los menores, debemos romper una imagen idealista que muchos menores tienen de la seguridad en Internet, en concreto de los hackers (entendidos como piratas informáticos).

La ciberdelincuencia en los últimos años ha evolucionado considerablemente,

tanto en complejidad, como en alcance. Los ataques ya no son fruto de la curiosidad y de demostrar la valía de ciertos adolescentes que actuaban desde sus dormitorios. Esa idea ya pertenece al pasado. Se ha pasado a las mafias organizadas de delincuentes, que refinan día a día sus técnicas de ataque, y tienen un claro ánimo de lucro.

En la actualidad, un pirata informático no es más que un delincuente -equivalente a un estafador, un gamberro o incluso un atracador- que suele actuar por dinero y que utiliza todos los recursos y tecnologías presentes en Internet para garantizar su anonimato y cometer todo tipo de fraudes. Pertenecen a mafias organizadas de cibercriminales, cuyas actividades cuestan a las empresas y al propio estado millones de euros al año.

Ojo con los menores que, alentados por películas como "Hackers", "The Net", o similares, pueden "jugar" a convertirse en piratas y pueden meterse en problemas penados incluso con cárcel. De la misma manera que ningún padre permitiría a su hijo robar en un centro comercial, ningún padre debe permitir que su hijo se convierta en un delincuente desde su propia habitación.

Pasamos a detallar una serie de buenas prácticas que el menor -y por supuesto el adulto- debe seguir en el uso habitual de su equipo y de Internet.

Son las siguientes:

- Jamás debemos ejecutar programas desconocidos o que provengan de una fuente no fiable (y no todas las páginas web lo son).

- Mantengamos actualizados nuestros sistemas (parches, actualizaciones del sistema operativo, navegador y complementos, ...) y activado nuestro cortafuegos.

- Siempre que conectemos a nuestro correo electrónico debemos asegurarnos que, cuando tecleamos el usuario y la contraseña, el protocolo que utiliza el navegador es HTTPS, no HTTP. De esta forma, nuestros datos viajarán cifrados por la red, lo que evitará que un tercero no autorizado pueda leerlos.

- Ten siempre en ejecución el antivirus (que incluya antispyware, antitroyanos, antiadware...) en tu equipo, y por supuesto mantenlo actualizado para que pueda detectar nuevo malware.

- No utilices ordenadores compartidos (instituto, biblioteca...) para conectar a Internet utilizando tu usuario y contraseña (por ejemplo, para conectar a redes sociales, correo electrónico...). Otras personas pueden haber intervenido el equipo para robarte la información.

- El ordenador debe permanecer en una zona común de la casa para evitar que se haga un mal uso.

- Por supuesto, no compartas tu contraseña con nadie: con frecuencia es lo único que te identifica en la red -como el DNI en el mundo real-, así que mantenla en privado.

• Cada vez que publiques algo en Internet (una foto en Facebook, un comentario en un blog, una modificación de tu página web...) piensa que cualquier persona, desde cualquier parte del mundo, podrá acceder a esta información y utilizarla de muchas maneras, no todas correctas.

• Si detectas cualquier amenaza contra ti o contra cualquier otro menor, notifícalo a los adultos que corresponda en cada caso (padres, tutores, profesores...). Esta recomendación incluye todas las amenazas comentadas aquí, desde la infección por virus hasta el chantaje.

• Recuerda que en Internet puede suceder lo mismo que en el mundo real... por tanto, ten el máximo cuidado cuando conectes, igual que lo tienes cuando cruzas una avenida o sales con los amigos.

8 Seguridad y telefonía móvil

Aunque los móviles no son actualmente parte activa de Internet, tal y como la conocemos hoy en día, no hay duda alguna de que estos dispositivos son otro de los principales medios de comunicación de los jóvenes, con sus ventajas y riesgos. En este caso, se detallarán las ventajas del móvil tanto para situaciones de emergencia (112) como para mantenerse en contacto con la familia, amigos, etc. De la misma manera, se describirán los problemas y amenazas a los que se enfrentan los usuarios de móviles: robo del dispositivo, robo de información personal, sistemas de suscripción, descargas para móviles, etc. La idea es trasladar que el móvil es, desde cierto punto de vista, casi una tarjeta de débito de la que servicios malintencionados pueden abusar sin el consentimiento del usuario.

El teléfono móvil puede ser para los menores, al igual que para los adultos, una ayuda indispensable ante situaciones de riesgo de cualquier índole: desde un accidente de tráfico hasta una pelea callejera, pasando por un atraco o una pérdida de la orientación -por ejemplo, en excursiones-. Podemos decir, sin duda, que en la actualidad un teléfono puede llegar a salvar vidas con una simple llamada: no tenemos más que pensar en el número de emergencias (112) detrás del que se encuentra el Centro de Coordinación de Emergencias de la Generalitat Valenciana, centro que con una simple llamada es capaz de poner en marcha a Fuerzas y Cuerpos de Seguridad del Estado, Protección Civil, servicios sanitarios, bomberos, y un largo etcétera de servicios que pueden ser indispensables para que el menor -o de nuevo, un adulto- salve una situación de riesgo. Desde luego, disponer de un teléfono móvil es a día de hoy una garantía en estas situaciones, pero por supuesto, cualquier elemento tecnológico, desde el punto de vista de la seguridad, tiene su parte positiva y su parte negativa.

Cada vez más frecuentemente, los teléfonos móviles son pequeños ordenadores de bolsillo, pequeños ordenadores que se ven afectados por los mismos problemas que hemos comentado en otros capítulos del presente curso, pero con un agravante: siempre van con el menor. Hoy en día, desde muchos teléfonos es posible conectar con nuestro banco online, navegar por Internet o chatear

con nuestros amigos, posiblemente fuera del control de los adultos y desde cualquier parte del mundo (con la sensación de anonimato, o el anonimato real, que esto implica). El teléfono no sólo nos sirve para hablar, sino que es agenda, lista de contactos, navegador... de esta forma, los problemas de phishing, robo de información, delitos... comentados durante este curso, se extrapolan casi directamente a muchos teléfonos móviles de los utilizados a diario por los menores: sólo imaginemos que quien accede al teléfono móvil de un menor con toda probabilidad tendrá acceso no sólo a su lista de contactos, sino a su agenda personal (lugares frecuentados, citas, horarios...), a información confidencial de muchos amigos o conocidos, e incluso a imágenes privadas (teléfonos con cámara digital).

Caso aparte son estos teléfonos con cámara, de nuevo muy habituales, y que con demasiada frecuencia son utilizados para grabar peleas, vejaciones, abusos... en centros educativos, en centros de ocio, o en la propia vía pública. Aparte del delito cometido en estos casos, en el que de nuevo entra la tecnología -aunque sea colateralmente- las cámaras en los móviles pueden constituir un peligro contra la intimidad de nuestros menores, ya que en caso de robo o pérdida del dispositivo, quien lo encuentre puede tener acceso a imágenes personales, con las implicaciones que esto supone para los menores.

En definitiva, a la hora de hablar de la seguridad de los menores, es imprescindible hablar de la telefonía móvil, y en especial de sus implicaciones en la intimidad del menor; es importante la concienciación en este sentido, y no sólo de los adultos, sino sobre todo de los propios menores: a fin de cuentas, casi ningún padre puede controlar el uso que su hijo hace del teléfono cuando no está con él, y debemos explicar claramente a nuestros hijos las connotaciones que puede suponer el robo o la pérdida del teléfono o un mal uso del mismo. La mejor medida de seguridad es, de nuevo aquí, la concienciación adecuada acerca de los peligros que el uso de las nuevas tecnologías implica.

9 Herramientas gratuitas

A continuación se referencian algunas herramientas gratuitas que permiten a los padres conocer y controlar los contenidos a los que sus hijos acceden en la Red :

Protegits

Enlace: ***http://www.protegits.gva.es/lang/es/***

Idioma:Español

Características:

A diferencia de otras iniciativas en este campo, limitadas a un enfoque principalmente pasivo, ProtegiTs abarca tres áreas de acción bien diferenciadas:

- Clases formativas, dirigidas tanto a menores como a padres. El propósito de esta iniciativa es dar una visión real de las amenazas a los menores, con un contenido adaptado a los diferentes grupos de edad diseñados en el proyecto.

- El Kit ProtegITs, formado actualmente por un complemento para navegadores y una aplicación, tiene la función de prevenir, detectar y facilitar la respuesta frente a potenciales amenazas a las que el menor pueda verse expuesto en su utilización de Internet.

- La página web del proyecto, un medio a través del cual, además de divulgar el proyecto, se ofrece información relevante, descargas de aplicaciones y recursos tanto para menores como para padres y docentes.

Asesor de contenidos de Internet Explorer

Enlace: ***http://www.microsoft.com/spain/windows/ie/using/howto/contentadv/config.mspx***

Idioma: Español

Características:

- Es una opción en el navegador Internet Explorer.

- Puede configurarse de tal forma que active diferentes filtros y detecte los contenidos según haya sido etiquetada la página.

- Da la posibilidad de crear listas de páginas "permitidas" para incluir los sitios que consideras adecuados para tus hijos (listas blancas).

- Permite agregar "filtros adicionales" más complejos que simplemente las etiquetas en la página.

Parental control bar

Enlace: ***http://www.aboutus.org/ParentalControlBar.org***

Idioma: Inglés

Características:

- La instalación se hace de la misma forma que una "barra de herramientas" en los navegadores Internet Explorer, Firefox y Safari en computadoras con sistema operativo Windows 98/ME/2000/XP.

- Cuando se activa el Child Mode, automáticamente se bloquean las páginas etiquetadas con contenidos no aptos, las que no estén clasificadas (esto es configurable) y las que se agreguen a la lista negra.

- Permite la creación de listas de páginas blancas para incluir los sitios que consideras adecuados para tus hijos.

- Permite colocar páginas que estén etiquetadas como aptas dentro de las listas negras si contienen información inadecuada.

- Da la opción de saber en qué páginas ha entrado tu hijo.

Leopard
Enlace: ***http://www.faq-mac.com/noticias/node/26785***

Idioma: Español

Características:

- Permite la configuración de cuentas de usuario específicas para los niños

- Permite la restricción de contenidos de tres formas diferentes: acceso ilimitado, limitación selectiva y aprobación selectiva.

- Control del acceso a mail e iChat (aplicaciones de mensajería instantánea relacionadas con MSN aparecerán como otras aplicaciones.)

- Permite un control del tiempo de uso.

- Da la opción de saber en qué páginas ha entrado su hijo.

10. Resumen de recomendaciones

Por otro lado, tal y como se ha presentado anteriormente, resulta necesario poner al servicio de los usuarios una serie de recomendaciones para evitar que los menores sean víctimas o accedan a contenidos ilícitos e inapropiados. En esa línea, desde INTECO se ofrece a todos los usuarios las siguientes recomendaciones:

- Eduque al menor sobre los posibles peligros que puede encontrar en la Red.

- Acompañe al menor en la navegación cuando sea posible, sin invadir su intimidad.

- Advierta al menor de los problemas de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.

- Aconséjele no participar en charlas radicales (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.

- Infórmele de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad.

- Preste atención a sus "ciber-amistades" en la misma media que lo hace con sus amistades en la vida real.

- Pídale que le informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.

- Vigile el tiempo de conexión del menor a Internet para evitar que

desatienda otras actividades.

• Utilice herramientas de control parental que le ayudan en el filtrado de los contenidos accesibles por los menores.

• Cree una cuenta de usuario limitado para el acceso del menor al sistema.

12

REDES P2P

Las redes P2P (peer to peer), son redes formadas por equipos que trabajan a la vez como ***cliente***[96] y ***servidor***[97] por las que se permite el intercambio de información entre usuarios de forma descentralizada. Esto significa que no existe un servidor centralizado donde se encuentra toda la información al que acudan los usuarios para descargar, sino que la información está almacenada en cada uno de los clientes.

1 Como funcionan las redes P2P

Esta tecnología se utiliza con diversos fines, como puede ser el popular software de voip Skype, pero sin duda la utilidad más extendida es el intercambio de ficheros de forma gratuita, como pueden ser archivos multimedia, juegos, o software.

Fue utilizada como solución en ciertos ámbitos para evitar que, en caso de compartir ficheros con derechos de autor, las autoridades cerrasen el servidor principal cortando el servicio (como sucedió con Napster), de forma que con esta tecnología han de perseguir a cada uno de los usuarios. Existen numerosas redes de P2P, cada una con sus clientes (programas como Emule, Kazaa, Ares, BitTorrent, etc...) para conectarse y descargar contenido, si bien es cierto que algunas de estas no son totalmente distribuidas por disponer de servidores que almacenan información sobre qué usuario dispone de qué fichero.

Nota: Estas redes son un concepto totalmente diferente a los servicios de descarga directa, como pueden ser Megaupload (***actualmente cerrada***[98]) o Rapidshare, donde toda la información está almacenada en servidores centralizados.

1.1 Edonkey2000

Se trata de un ***protocolo***[99] utilizado por el programa que lleva su nombre, además de otros conocidos como Emule, Shareaaza o Lphant.

Se trata de un sistema semi centralizado, ya que no existe un servidor principal, pero sí una red de servidores que coordinan la red. Estos servidores únicamente se encargan de transmitir la lista de archivos que los clientes comparten y no contienen directamente los ficheros a compartir .

Existen servidores falsos que se encargan de recolectar información de qué usuarios comparten qué ficheros, por lo que es recomendable descargar las listas de servidores desde sitios de confianza.

Una vez un cliente se conecta a un servidor, el cliente transmite la lista de

96 Accesible en http://es.wikipedia.org/wiki/Cliente_(inform%C3%A1tica)
97 Accesible en http://es.wikipedia.org/wiki/Servidor_inform%C3%A1tico
98 Accesible en http://www.csirtcv.gva.es/es/noticias/el-fbi-cierra-la-web-de-descargas-megaupload-aparecen-ya-p%C3%A1ginas-falsas-que-simulan-un-nuev
99 Accesible en http://es.wikipedia.org/wiki/Protocolo_de_comunicaciones

ficheros que contiene junto con un identificador del fichero (***hash***[100]) del fichero, por si otro usuario dispone del mismo fichero con otro nombre. De esta forma, cuando se solicita un fichero se envían peticiones a todos los clientes que el servidor conoce que tienen ese fichero. Cuando cada cliente recibe la petición, añade al otro cliente a una lista de espera de forma que cuando es su turno, empieza la descarga del fichero.

Los servidores de la red ***Edonkey2000***[101] evolucionan constantemente ya que dependiendo del país en que se encuentran, autoridades y sociedades de autores toman medidas legales para que los principales servidores sean cerrados. De esta forma los clientes de dicho servidor han de migrar masivamente a servidores alternativos, dejando muchas descargas de otros clientes sin ser terminadas o con muy pocas fuentes, por lo que la descarga se ralentiza.

Otra forma de luchar contra este protocolo que utilizan algunas discográficas consiste en buscar qué usuarios comparten contenido protegido y enviar de forma masiva mensajes privados avisando que en caso de no dejar de compartirlo se tomarán acciones legales.

Este protocolo fue creado inicialmente para la aplicación Edonkey2000, la cual fue abandonada por motivos judiciales, siendo hoy el programa eMule el que más adeptos ha captado sobre este protocolo. eMule dispone de ciertas características que lo diferencian del resto de clientes de la red Edonkey2000: ofuscación de protocolo (función que evita que las conexiones de eMule sean detectadas), transferencias de ficheros comprimidas, sistema de créditos en las colas (a más se comparte, antes avanzas en las colas de descarga), comentarios en los ficheros, previsualización de archivos multimedia o servidor web (entre otros).

Aparte de sus cualidades técnicas cabe descartar que el protocolo Edonkey2000 actualmente es el que ofrece mayor comodidad y variedad en la descarga de ficheros, aunque han surgido competidores mucho más rápidos.

1.2 BitTorrent

Se trata de un protocolo algo diferente del resto de protocolos P2P ya que no dispone de buscador integrado, sino que requiere de un pequeño fichero .torrent (o recientemente enlaces "magnet") que contiene la dirección de un servidor que se encargará de buscar fuentes para el fichero y comunicar a los clientes entre ellos para que descarguen el fichero. Estos ficheros pueden encontrarse en páginas web, foros, o listas de distribución.

A diferencia de la red edonkey2000, este protocolo no permite compartir carpetas enteras, de forma que ante la necesidad de crear archivos .torrent para poder publicar un contenido elimina el riesgo de que publiquemos por descuido contenido del disco duro por configurar mal la carpeta de archivos a compartir. Esto hace que en la red hayan muchos menos ficheros compartidos ya que para descargar un fichero alguien lo tiene que haber subido explícitamente.

100 Accesible en http://es.wikipedia.org/wiki/Hash
101 Accesible en http://es.wikipedia.org/wiki/EDonkey2000

De esta forma, cuando descargamos un pequeño fichero .torrent y lo añadimos al cliente de descargas, empieza a descargarse en pequeñas partes o bloques. Cuando se descarga una parte de un fichero, este pasa automáticamente a ser servido a otros clientes dando siempre prioridad a las partes que menos usuarios tienen (interesa que todas las partes estén descargadas en varios clientes). De esta forma se pretende evitar que cada vez que un usuario descargue completamente el fichero y deje de compartirlo, llegue el momento en que los últimos usuarios no consigan nunca todas las partes que les faltan ya que no quedan usuarios con todas las partes completas. Inevitablemente esto acaba sucediendo por lo que es posible que un usuario descargue de una web un fichero .torrent que nadie continúe compartiendo (o que falte alguna parte) y que nunca vaya a poder conseguir todas las partes.

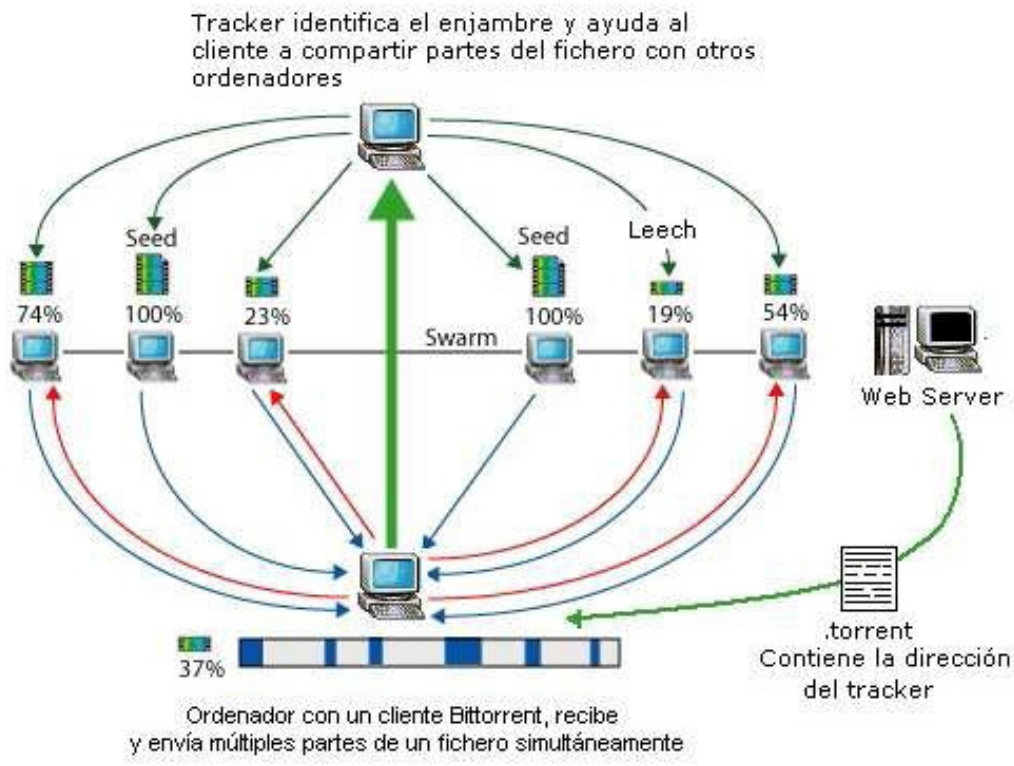


Ilustración 59 · Sistemas Bittorrent

Su principal ventaja frente al otros protocolos de P2P radica en su velocidad a la hora de descargar grandes ficheros, aunque es poco recomendable para ficheros de poco tamaño.

A pesar de que de forma nativa el protocolo no admite realizar búsquedas, existen clientes que han implementado sus propios buscadores generalmente haciendo búsquedas sobre los buscadores web o sobre comunidades de usuarios que comparten ficheros.

Otra peculiaridad a tener en cuenta es la existencia de servidores privados a los cuales es necesario acceder mediante un usuario y contraseña. La principal diferencia es que en estos servidores se tiene en cuenta el ratio entre datos descargados y datos publicados, de forma que se penaliza a los usuarios que únicamente utilizan la red para descargar sin compartir con el resto de usuarios.

Ya que en los protocolos torrent resulta muy complicado perseguir los servidores que almacenan la información sobre qué clientes tienen ficheros para compartir, la

lucha de las industrias audiovisuales contra el intercambio de ficheros protegidos se centra en buscadores especializados en búsquedas de ficheros .torrent.

Dos de los casos más relevantes de estas acciones contra servidores de ficheros .torrent fueron los casos de mininova.org y thepiratebay.org:

Mininova: se trataba de uno de los portales de enlaces torrent más grande de Internet, el cual operaba desde Holanda. Surgió como sustituto a supernova.org el cual cerró también por problemas legales. En mayo de 2009 la organización holandesa Brein denunció a mininova.org. Mininova respondió que eliminaría todo el contenido con derechos de autor que Brein solicitase, pero este movimiento no impidió que las presiones aumentasen desembocando en que se eliminasen todos los ficheros torrent. Desde entonces mininova únicamente publica ficheros que los propios autores piden explícitamente que sean publicados.

Thepiratebay: es el mayor motor de búsqueda de ficheros torrent del mundo. Su historia ha estado llena de trabas legales, pero de momento siguen funcionando, motivo por el cual se autodefinen como "el sitio BitTorrent más resistente del mundo". Thepiratebay ha soportado la presión legal en parte gracias a la mentalidad social que se ha creado en torno a esta página, que ha acabado desembocando en la creación del "partido pirata" en diversos países. Ante cada demanda y orden de cierre contra Thepiratebay, el portal ha respondido trasladando sus servidores a centros de proceso alternativos, cambiando de país, incluso, tal como indica wikipedia, trasladándose a servidores secretos accesibles mediante direcciones IP alemanas desde el famoso Cyberbunker.

1.3 Ares

Ares es otro cliente P2P que utiliza una red propia para descargas. En un principio utilizó la red Gnutella, pero a finales de 2002 comenzó el diseño de su nueva red descentralizada.

Algunos usuarios son reacios a utilizarlo ya que en un principio contenía ***adware***[102], pero más adelante los desarrolladores decidieron eliminarlo por lo que hoy en día se trata de software limpio. A pesar de que en un principio se publicó como software gratuito pero privado, la magnitud que tomó el proyecto, junto con el temor a ser perseguidos hizo que sus desarrolladores decidiesen convertirlo en software libre (***GLP***[103]).

Actualmente dispone de soporte para descargar ficheros torrent, navegador web y chat, además de previsualización de archivos, radio sobre internet, reproductor multimedia.

Dada su facilidad de de uso, su interfaz todo en uno, y su alta velocidad de descarga se ha convirtiendo en competidor directo de eMule en cuanto a numero de clientes y ficheros.

102 Accesible en http://es.wikipedia.org/wiki/Adware
103 Accesible en http://es.wikipedia.org/wiki/GNU_General_Public_License

1.4 Direct Connect

Direct Connect es un protocolo P2P basado en ***FTP***[104] diseñado para transmitir ficheros grandes a altas velocidades, generalmente en entornos locales y con grupos de usuarios homogéneos.

Al igual que en otros sistemas P2P, los clientes han de conectarse a servidores (llamados hubs) e informar de los ficheros que contienen para compartir. Una vez un usuario encuentra un fichero que desea descargar de otro usuario, se inicia una transferencia directa mediante FTP, por lo que se alcanzan altas tasas de transferencia.

Esta velocidad, se debe en parte al hecho de que los servidores acostumbran a requerir registrarse e iniciar sesión de forma similar a los servidores privados de torrent. Además, pueden requerir compartir cierta cantidad de datos, no permitiendo compartir ficheros duplicados, o de contenido inválido (por ejemplo un fichero de 10 GB que solo contiene la letra A muchas veces).

Este tipo de software acostumbra a ser utilizado en eventos u organismos con conectividad directa por ***LAN***[105], como concentraciones de internautas o universidades.

1.5 Skype

Skype es un conocido programa de voz sobre Internet (VoIP) que permite realizar llamadas tanto entre equipos informáticos (teléfonos móviles con conectividad a Internet, ordenadores, equipos portátiles...), equipos tradicionales de telefonía y centrales telefónicas (PBX).

Una de sus características que lo hacen peculiar es que está basado en un modelo P2P, a pesar de no ser utilizado para descargar ficheros.

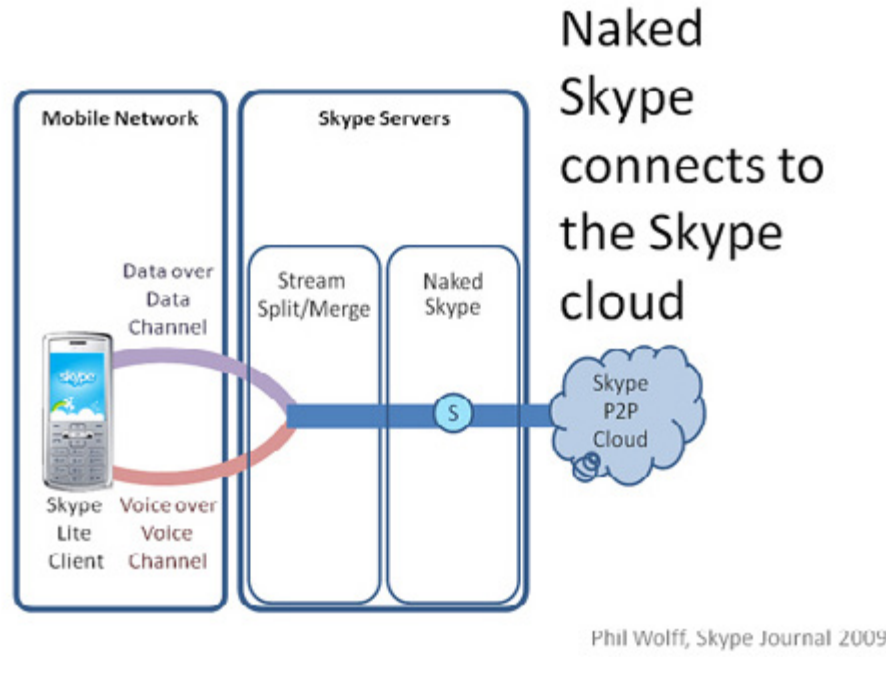


Ilustración 60 · Skype

104 Accesible en http://es.wikipedia.org/wiki/Ftp
105 Accesible en http://es.wikipedia.org/wiki/Lan

El programa fue desarrollado por los creadores de Kazaa, los cuales quisieron llevar sus conocimientos sobre redes P2P al campo de la voz sobre IP. Al conectarse a la red, cada usuario es catalogado por el cliente como nodo o como un super-nodo en base a ciertos parámetros como pueden ser si dispone de dirección IP pública, ancho de banda o recursos del equipo donde se ejecuta el cliente. Los super-nodos se encargan de almacenar información sobre qué usuarios están conectados a la red, a la vez que realizan las búsquedas de usuarios.

Según sus desarrolladores, la principal ventaja de esta topología es que se autoescala a medida que crece el número de usuarios ya que a la vez que surgen clientes van surgiendo nuevos super-nodos. Sin embargo los detractores de está tecnología alegan que puede entrañar problemas de saturación en el caso de que cada usuario, al acabar de realizar sus llamadas cierre el cliente ya que se pierde capacidad de computo y comunicación en la red.

Por último, también existen teorías que apuntan a que cuando un usuario instala skype, está permitiendo que un código privado se ejecute en su equipo y realizando funciones de servidor, de forma que es posible ser víctima de ataques de denegación de servicio, ya sea por congestión de red o saturación de la CPU ante volúmenes excesivamente grandes de peticiones.

1.6 Pando

Pando es un programa de descargas de ficheros, que a pesar de no seguir una estructura P2P, comparte algunas cualidades con estas redes.

De cara a los usuarios funciona de forma similar a los clientes torrent: es necesario descargar un pequeño fichero que a al abrirlo en el cliente inicia la descarga. Sin embargo en lugar de descargarlo de otros usuarios, los ficheros son descargados de un servidor donde previamente se han cargado los ficheros por parte de los usuarios.

Aunque parezca una estructura puramente cliente-servidor, los clientes tienen la posibilidad de servir los ficheros desde sus equipos para aumentar así las fuentes de los ficheros, aunque no es la practica habitual.

2 Legalidad de las redes P2P

Este es un tema en constante discusión en varios círculos que enfrenta principalmente a internautas con las sociedades de autores, incluyendo en el debate a políticos, jueces y teleoperadoras.

El uso de programas de P2P esta permitido ya que se trata de un servicio más de la red en que se intercambia todo tipo de información, incluyendo material basado en licencias que permiten su difusión, programas de código libre, ficheros con derechos de autor o ficheros personales de los usuarios.

El foco de discusión está principalmente en las descargas de audio y vídeo, donde existen muchos usuarios que descargan películas y canciones con derechos. El

software y los juegos no se contemplan directamente en esta lucha ya que se rigen según otras normativas. Aparte quedan también los contenidos ilegales, como la pedofilia, vídeos racistas, violencia de genero, apología del terrorismo y otros materiales similares.

Desde el 25 de abril del 2007, la Unión Europea se pronunció al respecto estableciendo como infracción **penal** toda infracción internacional de un derecho de propiedad intelectual cometida a escala comercial[106]. Esto excluye el castigo a los usuarios privados que descarguen contenidos con fines personales y no lucrativos, dejando en el punto de mira a los portales que ofrecen enlaces a descargas y que contienen publicidad, ya que en caso de denuncia, queda en manos del juez el decidir si los beneficios obtenidos en concepto de publicidad son considerados como "animo de lucro" o simples gastos de mantenimiento del servicio. Desde entonces cada país ha evolucionado en lineas diferentes, como es el caso de la ley Hadopi en Francia, o la conocida popularmente como "ley Sinde" en España.

Lo cierto es que la situación actual resulta caótica, más ahora con la propuesta de que comisiones gestoras puedan solicitar el bloqueo a páginas web sin la orden de un juez.

Ante esta situación, la mejor recomendación es no utilizar redes P2P para descargar contenidos protegidos, ya que a pesar de que según la Unión Europea no se puede perseguir a los usuarios, es cierto que se han dado casos de denuncias a usuarios que utilizan intensamente estos servicios, indiferentemente de que después el juez haya decidido si se trata de una actividad punible o no.

2.1 P2P en el trabajo

En entornos de trabajo (generalmente entornos grandes) es habitual la monitorización del tráfico de red, ya que los clientes P2P acostumbran a consumir mucho ancho de banda, pudiendo llegar a congestionar la red y crear latencias importantes.

Desde la dirección se debería recomendar no utilizar o limitar estas redes, especialmente del tipo Edonkey2000 o Ares en entornos laborales ya que el material que contienen no pasa ningún filtro de calidad, ya sea para comprobar la existencia de virus o la legalidad del material descargado pudiendo incurrir en delitos contra la propiedad intelectual o comprometiendo la seguridad de la red.

Ante esta situación, muchos usuarios plantean sus dudas sobre la legalidad o no de que las comunicaciones de sus equipos informáticos del trabajo sean monitorizadas por la directiva (mediante algún departamento técnico), ya sea para monitorizar la navegación, el correo corporativo o el uso de redes P2P.

Ya que tanto las comunicaciones como los equipos informáticos son recursos corporativos, estos pueden ser monitorizados siempre y cuando se informe a los empleados de estas prácticas y se justifiquen. Esta información debe constar en la política interna de la organización y ha de ser accesible para todos los miembros.

106 Fuente ***www.bufetalmeida.com***

3 ¿Qué ficheros compartir?

Al instalar programas P2P, generalmente completamos un asistente que recoge información sobre la conexión, opciones que se desean activar por defecto y acostumbra solicitar al usuario que indique qué carpetas desea compartir.

En este paso, que puede parecer trivial es donde muchos usuarios cometen un gran fallo de seguridad ya que comparten carpetas personales de documentos, fotos privadas o incluso todo el disco, de forma que toda su información queda a disposición de todos los usuarios de la red.

Se conocen numerosos casos de denuncias de la Agencia Española de Protección de Datos a empresas por el hecho de que sus empleados han compartido sin saberlo datos de carácter personal de clientes.

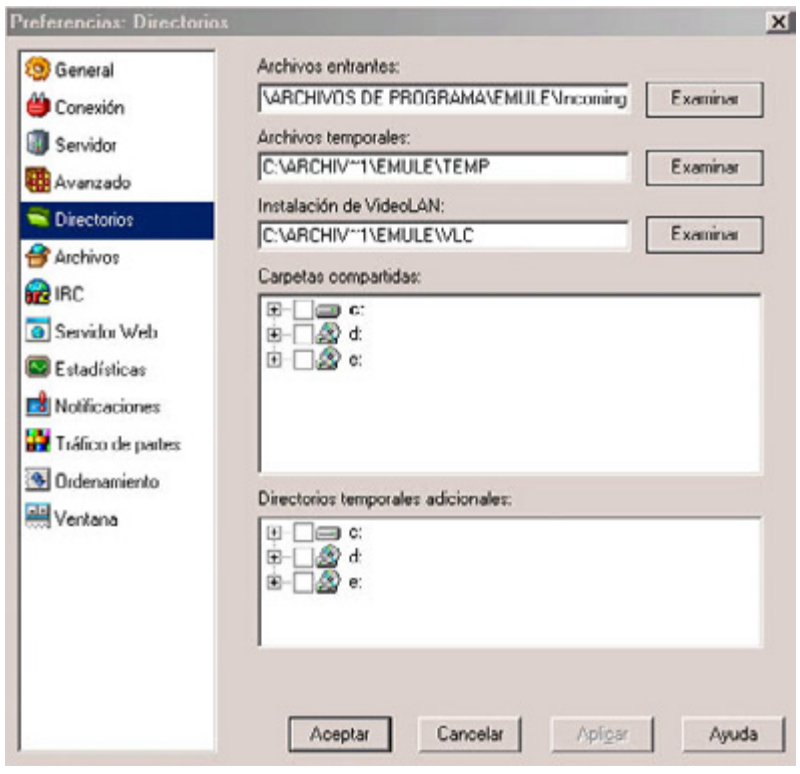


Ilustración 61 · Configuración sistema P2P

Esto queda demostrado si buscamos en un programa de P2P palabras clave como “Factura”, “Currículum” o “backup”, y veremos gran cantidad de resultados de usuarios que están compartiendo esta información, seguramente sin saberlo.

4 Peligros de utilizar P2P

Al igual que cualquier otro software, y en especial los que se utilizan para intercambiar información por la red están expuestos a las amenazas procedentes de Internet, como virus o ataques.

Dada la naturaleza de los programas P2P, (usuarios poco experimentados, mentalidad “descargar todo porque si”), algunos desarrolladores crearon clientes P2P maliciosos, que además de servir para descargar ficheros, infectan los equipos donde se instalan.

Dada la constante evolución de estos programas resulta muy complicado

mantener una lista actualizada de qué programas están libres de malware, por lo que recomendamos analizar los equipos con un software antimalware una vez instalados estos programas.

El siguiente listado muestra un listado de programas P2P, algunos descontinuados, que en algún momento han tenido software malicioso[107]:

Ares (tiene una versión "Lite" limpia)

Audiogalaxy (obsoleto)

Bearshare (la versión gratuita)

BitTorrent (varios clientes, ver detalles)

BitTorrent Ultra

Blubster (Piolet)

Computwin (FileNavigator) (ver detalles)

E-Donkey (Overnet) (la versión gratuita)

Exeem

FileCroc

FreeWire

Grokster (la versión gratuita)

Imesh

KaZaa (la versión gratuita)

Kiwi Alpha

Limewire (versiones antiguas)

MediaSeek (ver detalles)

Morpheus

OneMX

RockItNet

Warez P2P

Xolox

107 Fuente ***www.adslzone.net***

Dada la gran cantidad de usuarios que utilizan estas aplicaciones son un claro objetivo para los usuarios maliciosos en busca de vulnerabilidades que explotar, por lo que hay que seguir estas pautas:

• **Actualizar los clientes con las últimas versiones disponibles,** siendo la actualización automática una buena solución.

• **No desactivar el cortafuegos del sistema operativo.** En muchos equipos Windows, los puertos que utilizan los clientes de P2P están cerrados por lo que no pueden llegar a conectarse a los servidores. Ante esta situación muchos usuarios optan por deshabilitar el cortafuegos desconociendo que es posible añadir reglas concretas para cada programa. Para ello, acudiremos al "panel de control → firewall de windows" y asegurarse de que se encuentra activo. El siguiente paso será acceder a "configuración → excepciones → agregar programa" y seleccionaremos el programa que deseamos abrir en el cortafuegos.

• **Analizar todos los ficheros descargados en busca de virus,** ya que al proceder de otros usuarios es posible que estén infectados.

• **Descargar los clientes de P2P desde las páginas originales,** ya que es frecuente encontrar sitios de descarga que además de cobrarnos una pequeña cantidad por un programa gratuito, descargan el programa con código malicioso, publicidad, o barras de navegación.

• **Utilizar las opciones de cifrado de los clientes,** ya que de esta forma, además de proteger la información transmitida, evitaremos ser víctimas de equipos priorizadores de tráfico que utilizan algunas compañías u organizaciones. La mayoría de clientes ofrecen tecnologías para esta tarea

• **Revisar los comentarios de los ficheros antes de descargarlos.** Según el cliente que utilicemos es posible consultar los comentarios que los usuarios aportan sobre los ficheros ya que hay ocasiones en que no son lo que creemos. Existen usuarios que publican contenidos, especialmente para adultos, y los renombran con nombres populares, por ejemplo los últimos estrenos de cine. Estos ficheros son denominados "fakes". Si por culpa de uno de estos ficheros descargásemos por error algún fichero que resultase ilegal (pornografía infantil, grabaciones de maltratos, etc...) debemos eliminarlo lo antes posible para no compartirlo con el resto de usuarios y notificarlo a las autoridades para que puedan proceder a su retirada. De no notificarlo, ni borrarlo nos arriesgamos a que la descarga haya sido monitorizada por las autoridades con lo que tendríamos serios problemas legales.

• **Configurar cuidadosamente las opciones de arranque automático del software.** La mayoría de clientes de P2P acostumbran a configurarse para ser iniciados automáticamente con el arranque del equipo. Si no vamos a utilizarlos intensamente es recomendable deshabilitar esta opción ya que aunque no los estemos utilizando, estos estarán compartiendo nuestros ficheros con el resto de usuarios, con el consumo de ancho de banda que esto conlleva, lo cual puede

hacer que la conexión con Internet sea más lenta de lo habitual.

• **No utilizar nombres de usuario personalizados en los clientes.** En la mayoría de redes P2P se utilizan nombres de usuario, los cuales son utilizados únicamente para utilizarse en sus servicios de chat, mensajes privados o similar. Acostumbran a llevar un nombre por defecto del estilo "Usuario", los cuales es recomendable no cambiar para ser confundido con el resto de usuarios. Esto no nos hará invisibles ante el resto de usuarios, pero es una salvaguarda más que añadir a todo lo anterior.

13

JUEGOS ON-LINE

Es frecuente pensar, equivocadamente, que la seguridad de los sistemas de información es algo que afecta principalmente al software para navegar por Internet, a los programas de P2P, y a los sistemas operativos, pero en pocas ocasiones se tienen en cuenta otros tipos de software, que igual que los citados anteriormente, también se conectan a la red y que por ello pueden ser una puerta más de entrada a nuestro sistema: **los videojuegos**.

Son mucho mas complejos que la mayoría de los programas que acostumbramos a utilizar, se conectan a servidores donde hay miles de usuarios que pueden interactuar con nosotros, pueden ser utilizados por usuarios sin experiencia en ordenadores, y en ocasiones son descargados ilegalmente desde sitios web de dudosa reputación y seguridad.

Todas estas características hacen que, a pesar de que no sean considerados como tal por muchos usuarios, se conviertan en el objetivo de usuarios maliciosos.

Recomendar por último en esta pequeña introducción el reciente informe sobre seguridad en los juegos online elaborado por la empresa ***S2 Grupo***[108] y que puede consultarse en este enlace ***http://www.securityartwork.es/2011/12/22/informe-sobre-seguridad-en-juegos-online-2011/***[109]

1 Videojuegos masivos en linea

Se trata de juegos donde cada usuario crea un personaje virtual que interactúa con otros personajes de otros jugadores en un mundo virtual.

Los hay de temáticas variadas, desde aventuras espaciales, de estética medieval o mística, o realistas.

Simuladores de realidad: Años atrás el más conocido fue "Second Life", donde el personaje vive en un mundo virtual similar al real donde se simula una "segunda vida". En este mundo virtual el usuario puede buscar un trabajo virtual, comprar una casa o moda virtual, y establecer relaciones virtuales con otros jugadores. Tal fue el boom de este tipo de juegos que muchas marcas conocidas de ropa ofrecen sus productos virtuales que pueden ser comprados con dinero real en sus tiendas virtuales. Son juegos sin inicio y un final, y pocas veces con un objetivo, se trata simplemente de "vivir" una segunda vida paralela.

108 Accesible en http://www.s2grupo.es/
109 Accesible en http://www.securityartwork.es/2011/12/22/informe-sobre-seguridad-en-juegos-online-2011/

Frente a estos videojuegos surgieron casos de jugadores que desarrollaron fuertes adicciones pasando más tiempo viviendo esa vida paralela que la vida real. Hay que tener en cuenta que en estos juegos cada uno elije quien quiere ser y es una vía para evadirse de los problemas reales. Es por ello que se recomienda tomar conciencia de lo que son: videojuegos. Deben ser un medio para ocupar parte del tiempo libre, siempre sin dejar de lado la vida cotidiana. En caso de descubrir que se es adicto y no conseguir dejarlo, es posible recurrir a ayuda profesional.

Cuando estos juegos toman relevancia, es frecuente que aparezcan saboteadores: en los principios de este tipo de juego, en un intento de acercamiento a los ciudadanos, numerosos políticos crearon sus propios personajes en estos juegos, llegando incluso a dar mítines online, por lo que usuarios maliciosos aprovecharon para sabotear estos encuentros de las formas más diversas (provocando denegaciones de servicio sobre el juego, causando errores deliberadamente, robando las cuentas de usuario de los políticos, etc...).

Otro tema a tratar es la posibilidad de que los menores utilicen estos juegos de forma incorrecta. Si un menor de edad crea un perfil de jugador de estética adulta, el resto de jugadores no pueden saberlo, ¿que sucedería entonces si un usuario le propone tener cibersexo y el menor acepta? De forma similar se plantean otros dilemas. Si un jugador adulto crea un perfil con estética infantil, simplemente porque le gusta, y propone cibersexo a otros jugadores adultos, sabiendo los dos que se trata de personas adultas ¿se está promoviendo la pedofilia?. Algunos de estos juegos dieron solución a estas situaciones prohibiendo participar a menores de edad y eliminando la posibilidad de crear perfiles con esta estética, pero realmente no existe una forma de garantizar que un menor de edad se registre.

Recomendaciones:

- No establecer relaciones personales a no ser que se tenga certeza de la edad del otro usuario para evitar posibles problemas legales con menores.

- No compartir nuestra cuenta de usuario con otros jugadores y establecer contraseñas robustas.

• En caso de que el juego sea de pago, no realizar pagos online en páginas no oficiales, para evitar estafas.

• En caso de que el juego requiera instalación, mantener el software actualizado para evitar que posibles vulnerabilidades descubiertas no sean solucionadas.

• No confiar nuestros datos personales reales a desconocidos de igual modo que no se los entregaríamos a algún desconocido en la calle (sentido común).

Videojuegos de rol multijugador masivos en linea (MMORPG): Se trata de videojuegos, similares a los anteriores pero de estética generalmente medieval, fantástica o futurista en la que los jugadores tienen misiones a cumplir, las cuales pueden llevar a cabo en solitario, en grupo, o contra otros usuarios. Aquí la finalidad ya no es socializarse, si no vivir aventuras explorando mundos extraños. Generalmente el jugador va ganando puntos de experiencia y mejorando su personaje lo que le permite acceder a misiones más difíciles. El más conocido es el World Of Warcraft, ambientado en un mundo de enanos, bárbaros, elfos y magos, el cual ronda los 10 millones de usuarios activos.

Igual que en el caso anterior, estos juegos acostumbran a crear adicción, hasta tal punto que incluso se le ha dedicado un capítulo en la conocida serie estadounidense “South Park”.

Alrededor de este juego, y otros similares, ha surgido un mercado ilegal de objetos y dinero virtuales. En ciertos países como china, existen mafias que explotan a gente sin recursos, para que estén largas horas jugando y recogiendo “oro virtual”, que venden a usuarios generalmente de otros países, a cambio de dinero real.

Son llamados “farmers” o granjeros, y trabajan hacinados en pisos en condiciones poco salubres. Es muy poco recomendable acudir a estos usuarios para conseguir dinero virtual “fácil”, ya que además de poco ético, y de no tener garantías de ningún tipo, estaremos propiciando este modo de esclavitud. Existe incluso

un mercado negro de personajes, de modo que puedes comprar una cuenta de usuario de un jugador con cierto nivel para ser más poderoso que otros jugadores.

Es muy desaconsejable recurrir a este mercado para comprar bienes virtuales, ya que además de que el comprador no dispone de ningún mecanismo para garantizar su compra,

En cuanto a las recomendaciones de seguridad sobre los sistemas se aplican las mismas que a los juegos realistas.

2 Juegos offline con modo online

La gran mayoría de los juegos ya tienen modos para jugar online contra otros usuarios. Esta capacidad está potenciada en parte para evitar la piratería, ya que generalmente requieren crear un usuario asociado al número de serie del juego original, de modo que si es descargado, o copiado del original, únicamente el propietario del original podrá jugar online.

Una vez más se hace hincapié en la necesidad de mantener todo el software, especialmente el que se conecta a Internet, actualizado con los últimos parches de seguridad, para evitar ser víctimas de ataques contra vulnerabilidades conocidas a pesar de que en estos entornos los ataques acostumbran a ir dirigidos a robar cuentas de usuario o a modificar el juego para hacer trampas.

Es importante registrar la copia del juego lo antes posible ya que es posible que algún usuario malicioso descubra como crear un generador de números de serie válidos y registre nuestro número antes que nosotros (no ocurre frecuentemente pero es posible).

Evidentemente la situación anterior toma relevancia en caso de que vayamos a prestar el juego a otro usuario (recomendamos comprobar la licencia de usuario para ver si esta opción es legal), ya que al comprar software de segunda mano, aunque sea original, si el dueño anterior ha registrado el número de serie no podremos jugar online.

3 Minijuegos online

Los minijuegos online son una modalidad de videojuego muy extendida en redes sociales en la cual, generalmente, se accede a una web en la que se juega directamente a juegos desde el navegador utilizando tecnologías como Flash o Java. Se trata de juegos en los que predomina la jugabilidad, diversión e interactividad con el resto de usuarios, por encima de los gráficos realistas y los efectos especiales.

Alrededor de estos juegos es frecuente encontrar comunidades de usuarios frecuentes, los cuales interactúan, envían mensajes y compiten por escalar posiciones en rankings de puntos, y es precisamente por estas competitividad por lo que en ocasiones, usuarios intentan engañar al sistema con métodos

fraudulentos para subir posiciones en la clasificación general. Téngase en cuenta que los portales de videojuegos acostumbran a disponer de mecanismos para detectar comportamientos anómalos, y que en caso de detectar trampas es posible que se tomen medidas contra el usuario que pueden ir desde el veto a volver a entrar al servicio, hasta la toma de acciones legales.

Las trampas acostumbran a dirigirse contra el propio juego y el servidor, por lo que como usuarios, únicamente podemos denunciar y avisar a los administradores de la plataforma de que sospechamos que se están haciendo trampas si detectamos cambios repentinos de puntuaciones, o actividades sospechosas.

Dada la tecnología de estas páginas web, ante la posibilidad de que haya sido creada por un usuario malicioso, debemos comprobar que las opciones de privacidad son correctas(por defecto lo son). Para ello, en una página que tenga una animación en flash, pulsaremos sobre la animación con el botón derecho → configuración. En la segunda pestaña "privacidad", nos aseguraremos de que no se permita la utilización del micrófono, ni de la webcam.

Adicionalmente, y al igual que en el resto de servicios web, se recomienda utilizar las últimas versiones del software utilizado (navegador, ShokwaveFlash, sistema operativo y antivirus), y no revelar las contraseñas de acceso bajo ningún concepto.

4 Apuestas online

Existen numerosas páginas web que nos permiten apostar online. Muchos usuarios de Internet tienen dudas a la hora de apostar online ya que desconfían de entregar sus números de tarjeta de crédito a páginas web desconocidas para ingresar el dinero con el que más adelante apostarán o por si se trata de servicios fraudulentos.

Aunque existen páginas web fraudulentas, existen muchos servicios que han conseguido la confianza de los clientes y son utilizados por millones de usuarios en el mundo. Acostumbran a tener la ventaja de permitir realizar apuestas mucho más variadas que las apuestas tradicionales aunque tampoco están exentas de ciertas desventajas funcionales, como que las sedes están en otros países para que los premios estén exentos de impuestos, por lo que si se desea denunciar algún tipo de fraude resulta complicado por ser denuncias de carácter internacional.

La seguridad y privacidad en las páginas de apuestas online se rige por los mismos principios que el resto de paginas web, por lo que se han de tomar en

cuenta las siguientes consideraciones:

• Investigar la reputación de una página web antes de ingresar dinero. Generalmente con una búsqueda en un buscador basta para descubrir si los usuarios acostumbran a estar contentos con el servicio, si se trata de una estafa, o si tiene alguna peculiaridad que aparezca solo en "la letra pequeña".

• En caso de que existan, mejor utilizar los servicios oficiales antes que acudir a intermediarios. En España, existen administraciones de lotería que disponen de la opción de jugar a las loterías del estado online. A pesar de que se trata de administraciones oficiales, tal vez no dispongan de todos los medios tecnológicos necesarios o garantías. Ya que el servicio oficial de apuestas del estado, dispone de su ***propia web para apostar online***[110], es recomendable utilizar este servicio, frente a otros similares.

• Utilizar métodos de pago seguros, como puede ser PayPal o similar, los cuales ofrecen garantías en caso de engaño. Si se ha de introducir el número de tarjeta de crédito, asegurarse que este proceso se realiza desde una página cifrada (que la dirección de la web comience por https, en lugar de http), y nunca pagar por métodos como Western Union o similar, ya que estos servicios no ofrecen acuse de recibo ni garantía ninguna.

• Leer las condiciones de uso del servicio, ya que es posible que existan clausulas con respecto a situaciones fiscales según países, puede que para retirar dinero sea necesario que el premio acumulado sea mayor a cierta cantidad, o que la edad mínima para jugar sea distinta de la mayoría de edad en España.

• Disponer de un navegador y sistema operativo actualizado además de software antivirus en el equipo que se utiliza para navegar por la web de apuestas, ya que en caso de tener algún virus o código malicioso en el equipo, es posible que nuestras contraseñas de acceso o numero de tarjeta de crédito sean robados.

• Ser cauteloso con páginas web falsas y phishing, ya que al manejar dinero desde las propias web, son objetivos interesantes para usuarios maliciosos.

110 Accesible en https://loteriasyapuestas.es/

• Evitar conectarse a webs de apuestas desde equipos públicos como cibercafés para evitar que nuestra contraseña sea robada mediante programas maliciosos (keyloggers).

• Cerrar siempre la sesión al abandonar el correo en lugar de limitarse a cerrar el navegador o la pestaña.

• Evitar el uso de respuestas sencillas para la opción "recordar contraseña".

5 Copias ilegales de videojuegos

5.1 Juegos de PC

Por todos es sabido que existen técnicas para copiar videojuegos sin el consentimiento de los fabricantes.

Cuando Internet estaba lejos de ser lo que es hoy en día y los módems trabajaban a 56k o menos, resultaba impensable descargar un videojuego completo desde internet, por lo que la opción más utilizada para grabar juegos era el mano a mano. Ante esta practica los fabricantes de videojuegos incluyeron mecanismos anticopia en los juegos de forma que al intentar jugar a un juego no original este no funcionaba.

Esta tendencia se ha mantenido hasta hoy en día, por lo que existen grupos de usuarios que se dedican a publicar parches (llamados cracks) que modifican el juego, generalmente algún ejecutable, de forma que se consigue evitar la protección anticopia.

Estos ejecutables, según de donde se descarguen, pueden estar infectados por programas maliciosos que pueden comprometer los equipos, además de poder incurrir en delitos por el hecho de estar diseñados explícitamente para burlar las medidas de seguridad, por lo que se desaconseja su uso.

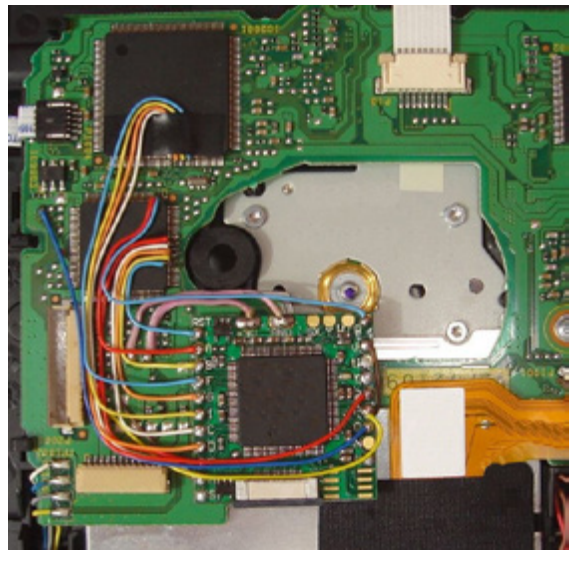
5.2 Videoconsolas

En el mundo de las videoconsolas también existen riesgos similares ya que generalmente los videojuegos "piratas" se descargan desde sitios web de dudosa reputación o desde redes p2p, donde tenemos pocas garantías en cuanto a calidad o integridad.

De igual forma que los fabricantes de software ofrecen actualizaciones para sus sistemas software, en el mundo de las videoconsolas sucede lo mismo: generalmente existen actualizaciones para el software de las consolas, sobre todo en las de última generación, en las que se resuelven problemas encontrados, se añaden nuevas funcionalidades o se cierran posibles agujeros de seguridad.

Una consideración relevante a tener en cuenta es que norma general, las consolas no pueden ejecutar juegos no originales, por lo que deben ser modificadas.

Generalmente, estas modificaciones se realizan por usuarios particulares o tiendas especializadas que rara vez ofrecen facturas o garantías del servicio.



Al modificar la consola, los cambios acostumbran a no ser reversibles por lo que si tenemos algún problema con la videoconsola, seguramente la garantía no cubra la reparación alegando que ha sido manipulada por personal ajeno a la compañía.

Además existen ciertas videoconsolas que toman medidas contra los usuarios que modifican sus videoconsolas como puede ser vetar el acceso a los juegos online o bloquear el uso de ciertos accesorios.

14

DELITOS TECNOLÓGICOS

1. Introducción

Sin duda, estaremos todos de acuerdo en que las nuevas tecnologías han aportado a nuestras vidas soluciones y posibilidades impensables hace tan sólo unos años. ¿Quién podría pensar quince años atrás que podría hacer la compra desde su ordenador, intercambiar ficheros con personas al otro lado del mundo, o pasear virtualmente por las calles de casi cualquier ciudad? Por supuesto, en 1995 -ya no hablamos de 1950- los conectados a Internet eran una minoría afortunada, pero la red era desconocida para el público en general.

La proliferación del uso de Internet y las nuevas tecnologías, como casi cualquier cambio en nuestras vidas, tiene un apartado positivo, pero también uno negativo: los delitos tecnológicos. Con la expresión **delito tecnológico** se define a todo acto ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes. Se trata, en definitiva, o bien de delitos tradicionales, cometidos ahora mediante tecnología e informática, o bien de nuevos delitos que han surgido al amparo del uso generalizado de Internet.

La clasificación de delitos tecnológicos que hace la Brigada de Investigación Tecnológica, la Unidad de la Policía Nacional destinada a responder ante estos delitos (ver el último punto del presente capítulo) es la siguiente:

- Ataques que se producen contra el ***derecho a la intimidad***[111]. Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos.

- Infracciones a la ***Propiedad Intelectual***[112] a través de la protección de los derechos de autor. Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas.

- **Falsificación de documentos.** Entendiendo documento como todo soporte material que exprese o incorpore datos, aunque se extiende también a la falsificación de moneda y a las tarjetas de débito y crédito. También pertenece a este grupo la fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.

- **Sabotajes informáticos.** Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos.

- **Fraudes informáticos.** Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito.

111 Accesible en http://es.wikipedia.org/wiki/Derecho_a_la_intimidad
112 Accesible en http://es.wikipedia.org/wiki/Propiedad_intelectual

• **Amenazas.** Realizadas por cualquier medio de comunicación.

• **Calumnias e injurias.** Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión.

• **Pornografía infantil.** Existen varios ***delitos***[113] en este epígrafe:

• La inducción, promoción, favorecimiento o facilitación de la prostitución de una persona menor de edad o incapaz.

• La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido.

• La facilitación de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...).

• La posesión de dicho material para la realización de dichas conductas.

Actualmente, el único delito que no puede ser cometido a través de la tecnología es la violación; incluso el homicidio puede ser ejecutado a través de tecnología (interfiriendo de forma remota los pulsos de un marcapasos, por ejemplo). Con esta situación, es necesario estar atento a casi todo tipo de delitos, en especial a estafas o robos, siempre que utilicemos Internet; de la misma forma que en nuestra vida "real" tomamos ciertas precauciones (desconfiamos de desconocidos, no transitamos a determinadas horas por determinados lugares...), en Internet debemos seguir unas pautas de conducta equivalentes para no cometer delitos, ni de forma directa ni como cómplices, ni por supuesto para ser víctima de los mismos.

2 Delitos informáticos

Se detallan en este punto los delitos tecnológicos más habituales, haciendo especial hincapié en los delitos informáticos derivados del uso de Internet. Como ***precauciones***[114] generales, aparte del sentido común, se recomienda a todos los usuarios que adopten las siguiente medidas:

• Ante la recepción de un correo electrónico cuyo remitente desconocemos, debemos borrar de forma inmediata el correo.

• Si el remitente es alguien conocido, pero el correo electrónico nos puede hacer sospechar (por ejemplo, un amigo que de repente nos envía correo en inglés con adjuntos o información para hacerse millonario), borraremos el correo y contactaremos con la persona por otro medio, indicándole que hemos recibido el correo.

113 Accesible en http://www.securityartwork.es/2010/02/01/emule-pornografia-y-justicia/
114 Accesible en https://www.facebook.com/note.php?note_id=146070748776981

• Si se nos solicita llamar por teléfono al extranjero, no hacerlo bajo ningún concepto.

• Nadie regala dinero; si nos ofrecen millones, seguramente perderemos unos cientos de euros.

• Si un alto cargo de un país extranjero se comunica con nosotros para hacer negocios, seguramente estamos ante un intento de estafa.

• Para compras o transacciones online, es muy importante fijarse en el dominio de la web (que sea el original y no una imitación), así como en el modo seguro de la página.

• Ningún banco solicita datos confidenciales (nombre de usuario, PIN, tarjetas de coordenadas...) por correo electrónico.

PHISHING

El phishing ("pescando datos") es una técnica de captación ilícita de datos personales, principalmente relacionados con claves para el acceso a servicios bancarios y financieros, a través de correos electrónicos o páginas web que imitan y copian la imagen o apariencia de una entidad bancaria o financiera (o cualquier otro tipo de empresa de reconocido prestigio). Basándose en la confianza que ofrece la entidad suplantada solicitan los datos de acceso, por lo que generalmente no se sospecha de aquellos correos electrónicos que piden información de carácter bancario con urgencia.

Ilustración 67 · Phishing

Las técnicas más habituales para realizar ataques de phishing son:

• Explotar vulnerabilidades que permiten superponer una imagen de la entidad de confianza asociada a una dirección fraudulenta.

• Invitar a pinchar en enlaces en ***correos***[115] electrónicos que dirigen hacia la dirección fraudulenta, por lo que es conveniente dirigirse directamente, a través de su navegador, a la página web de la entidad o empresa.

115 Accesible en https://www.facebook.com/note.php?note_id=221532294564159

Estos ataques vienen acompañados de técnicas de "ingeniería social", para provocar el engaño. Por ejemplo, con el reclamo de ofrecer un 50% gratis en el importe de una carga de teléfonos móviles, se obtiene información de tarjetas de crédito de los usuarios. Tras la obtención de los datos, no se ofrece el servicio prometido sino que se comete el hecho delictivo.

Como variantes más llamativas o utilizadas de este delito podemos describir las siguientes:

Phishing-car: La peculiaridad de este fraude consiste en que se comete con la venta de coches a bajo precio. La víctima, atraída por la posibilidad de adquirir un coche a un precio ventajoso, consiente en adelantar una parte, entre un 30% y un 50%, a través de una empresa de transferencia de dinero.

Scam: Esta estafa se fragua a través de un anuncio de trabajo en Internet. En él se busca a personas que deseen ganar mucho dinero fácilmente trabajando desde casa. Lo único que necesitan es un ordenador con conexión a Internet y una cuenta bancaria. La función de esta persona, denominada "mulero", consiste en recibir del estafador una cantidad de dinero fruto de una previa estafa de phishing, en su cuenta bancaria. Posteriormente debe remitir dicha cantidad, menos un porcentaje de comisión que se queda por la gestión, a través de una empresa de envío de dinero, a quien el estafador indique.

Vising o fraude a través de la Telefonía IP: En este tipo de fraude, la víctima recibe un correo electrónico de su entidad bancaria, supuestamente, en el que se le ofrece un teléfono gratuito al que ha de llamar. Una grabación le pide los datos de su tarjeta y las claves de la misma. Otra modalidad es aquella en la que se recibe un SMS en el que se le informa que su banco le ha hecho un cargo de X euros y un número de teléfono en el que informarse. La víctima telefonea para informarse de lo que ocurre y aporta los datos bancarios que la voz de la grabación le solicita.

PHARMING

Consiste en la manipulación de las direcciones DNS logrando así que la URL tecleada en el navegador de Internet no nos lleve a la página web de la entidad bancaria buscada, sino a otra página web idéntica y que los delincuentes han creado expresamente para captar el tráfico desviado de la verdadera. Para que un equipo sea víctima del pharming es preciso que se introduzca en el sistema una aplicación maliciosa (virus, troyanos, etc.) la cual ha logrado colarse con algún e-mail, al descargar algún contenido de la Red, etc. Una vez instalada dicha aplicación maliciosa, se queda a la espera de que su usuario acceda de nuevo a su entidad bancaria, lo cual lo diferencia del phishing, que se perpetra en el momento concreto en que se realiza el envío y el usuario accede a su servicio bancario a través del enlace indicado en el e-mail fraudulento.

REDES ZOMBIES

Zombie es la denominación que se asigna a los ordenadores que tras haber sido infectados por algún tipo de software dañino, normalmente una puerta trasera, pueden ser usados por una tercera persona para ejecutar actividades hostiles.

Este uso se produce sin la autorización o conocimiento del usuario del equipo, que aunque no lo sabe, está participando activamente en la comisión de un delito.

Ilustración 68 · Redes Zombies

Las máquinas zombie se agrupan en los denominados botnets, y éstas se coordinan para por ejemplo gestionar el envío de correo basura (spam), pero sobre todo suelen ser culpables de los ataques de denegación de servicio distribuido.

PIRÁMIDES DE VALOR

Se trata de ***suculentos mensajes***[116] del tipo "consiga aumentar su beneficio en poco tiempo", con el fin de captar a usuarios que crean que pueden conseguir grandes comisiones sin hacer nada. Una vez que han deslumbrado al usuario suelen remitirle un correo electrónico o un enlace a una ***determinada página web***[117] en la que solicitan sus datos personales y cuenta bancaria para poder realizar los ingresos de las futuras comisiones. Lo único que los usuarios deben hacer es pagar una determinada cantidad de dinero e incluirse en una cadena de correos ya iniciada, remitiendo a su vez miles y miles de correos electrónicos para que sus destinatarios repitan el mismo procedimiento; en teoría cuantos más correos envíen, más comisión generan, pero obviamente esto no se corresponde con la realidad.

TIMO NIGERIANO

Esta estafa consiste en ilusionar a la víctima con una gran fortuna que, en realidad es inexistente, con objeto de persuadirla luego para que pague una suma de dinero por adelantado como condición para acceder a la supuesta fortuna. Típicamente, se recibe un correo no solicitado del tipo "Soy una persona muy rica que reside en Nigeria y necesito trasladar una suma importante al extranjero con discreción. ¿Sería posible utilizar su cuenta bancaria?" Así, se le promete a la víctima un porcentaje de una inexistente cantidad millonaria de

116 Accesible en http://www.csirtcv.gva.es/es/paginas/ingenier%C3%ADa-social-el-arte-del-enga%C3%B1o.html

117 Accesible en http://www.csirtcv.gva.es/es/descargas/enlaces-maliciosos-en-el-correo-electr%C3%B3nico.html

dinero, para luego convencerla - mediante excusas muy elementales inventadas - a adelantar cierta cantidad de dinero propio al estafador. Como en cualquier estafa por Internet, lo más adecuado es borrar el mensaje nada más verlo y, por supuesto, sin contestarlo.

DELITOS CONTRA LA PROPIEDAD INTELECTUAL

Un delito muy habitual en el que muchos ciudadanos incurren es la violación de la Ley de Propiedad Intelectual (LPI) mediante la distribución de archivos protegidos por dicha Ley, incluido el ánimo de lucro; en los programas de intercambio de ficheros P2P (ver capítulo dedicado a éstos) es habitual detectar la presencia de música, películas, libros... con derechos de autor compartidos por millones de usuarios, lo que a priori puede constituir una violación de la LPI.

DELITOS CONTRA LA INTIMIDAD Y EL HONOR

A la hora de ***participar***[118] en foros, chats, redes sociales, etc. es ***muy importante***[119] tener en cuenta el único límite que en democracia se pone a la libertad de expresión: el honor de las personas y la imagen de las organizaciones. Insultar en un blog o en un foro es delito, y también lo es verter afirmaciones categóricas sin pruebas que las sustenten: un comentario desafortunado en un foro político, en un periódico online, o en un blog deportivo pueden acarrear duras sanciones, como también pueden acarrearlas la publicación de fotografías sin consentimiento expreso de la persona que sale en ellas, o el mal uso de las imágenes de videocámaras de seguridad.

PORNOGRAFÍA INFANTIL

Sin duda, uno de los delitos que más revuelo mediático genera es la tenencia, producción o distribución de pornografía infantil. Con frecuencia, las Fuerzas y Cuerpos de Seguridad del Estado destapan redes de distribución de este material, en operaciones con detenidos de todas las edades, clases sociales, profesiones, etc.

Obviamente, no vamos a entrar en este curso a describir la pornografía infantil, porque es algo obvio para todos nosotros; no obstante, consideramos necesario realizar una anotación muy importante para el ciudadano al que, como a la mayoría de nosotros, le repugna este tipo de material: en estas operaciones contra la pornografía infantil a las que hemos hecho referencia, no sólo se captura a pedófilos que disponen de grandes volúmenes de material, sino que en muchas de ellas se puede intervenir el equipo de ciudadanos "normales" que han estado distribuyendo pornografía infantil sin ellos saberlo. Un ejemplo: si utilizando un programa P2P para compartir archivos, alguno de nosotros descargara una película -delito contra la propiedad intelectual, recordemos- con un título aparentemente inofensivo pero que en realidad fuera material pornográfico con menores, y lo mantuviéramos en el directorio de descargas del programa -que por defecto se comparte con el resto de usuarios del mismo-, estaríamos potencial acusados de distribución de pornografía infantil. Aunque luego se demostrara que el volumen de información es mínimo, y por tanto en

118 Accesible en http://www.csirtcv.gva.es/es/descargas/utilizar-la-mensajer%C3%ADa-instant%C3%A-1nea-y-chats-de-forma-segura.html
119 Accesible en http://www.inteco.es/guias/guiaManual_honor_internet

un juicio fuéramos absueltos, probablemente la Policía Nacional o Guardia Civil entrarían con una orden en nuestro domicilio, requisarían nuestros equipos, y tendríamos una denuncia por tenencia y distribución de pornografía infantil. Algo para nada deseable, por supuesto.

3 Otros delitos tecnológicos

Los nuevos delitos no son en exclusiva informáticos, sino que existen delitos basados en cualquier otra nueva tecnología; para el ciudadano de a pie, son especialmente relevantes los dirigidos a sistemas de medios de pago (cajeros automáticos, TPVs de comercios...), por lo que vamos a referenciar aquí los delitos más habituales contra este tipo de sistemas. Es muy importante, sobre todo al utilizar un cajero automático, tomar las siguientes precauciones:

- Estar atento a cualquier alteración general del cajero, en especial del lector de número secreto o de tarjetas.

- Jamás utilizar una tarjeta de crédito para acceder al interior del recinto donde se ubica el cajero. El acceso al mismo debe ser libre.

- En caso de cajeros interiores, bloquear el acceso físico al recinto donde se ubica el cajero durante su utilización (se dispone de un pestillo de seguridad en la puerta).

- Desconfiar de extraños que aparentan tener problemas con el cajero, o tratan de ayudarnos a solventar un problema que tenemos nosotros.

- En caso de problemas, utilizar el interfono de seguridad del que disponen todos los cajeros automáticos, o llamar a la Policía o Guardia Civil.

Ilustración 69 · Cajero

MICROCÁMARAS

Este ataque consiste en colocar un lector de tarjetas a la entrada del habitáculo donde se encuentra el cajero automático (el lector es similar al que utilizan algunas entidades bancarias para permitir el acceso a esta estancia). El aparato registra los datos de la banda magnética, lo que permite a los falsificadores hacer un duplicado de la tarjeta.

Para lograr la clave secreta, los delincuentes colocan también una microcámara de vídeo camuflada encima del teclado. Así consiguen el número PIN en un receptor de la señal que suele estar colocado a unos metros del lugar, en un coche o en una bicicleta. El último paso es hacer el duplicado de la tarjeta y sacar dinero de los cajeros o comprar objetos de marca (que son más fáciles de vender). La víctima, por lo general, tarda un tiempo en comprobar los movimientos de su cuenta, y los delincuentes pueden estar semanas o meses gastándose su dinero si la propia entidad no lo detecta antes.

LAZO LIBANÉS

Este ataque consiste en colocar un dispositivo mecánico para que la tarjeta de crédito se quede retenida en el cajero. Cuando la víctima está intentando recuperarla, llega un delincuente que simula ayudarle y le pide el número secreto para intentar sacarla, según le dice. Pero el cajero no la devuelve y llega un momento en que la víctima la da por perdida y se va. Entonces, la recuperan los delincuentes que sacan el dinero con el número secreto facilitado. Cuando al día siguiente la víctima va a la sucursal a recoger la tarjeta, le dicen que no está allí y descubre que su cuenta corriente ha sufrido una considerable merma.

SKIMMING

Se trata de una práctica novedosa para la cual no es preciso robar la tarjeta. Cuando un cliente paga en un comercio y la tarjeta pasa por el ***datáfono***[120], más frecuente si está fuera de su vista, un empleado desleal copia la información de la banda magnética con un lector de tamaño mínimo (puede llevarlo en una pinza, por ejemplo). Esa información se transfiere a otras tarjetas blancas mediante sencillos programas informáticos; a continuación se elaboran documentos a la carta para respaldarlas, de forma que a nombre de una sola persona pueden funcionar ocho o diez tarjetas falsas. En estos casos sólo sirven para compras en establecimientos y no para reintegros, dado que no se cuenta con el número secreto del estafado.

En el caso de ***skimming en un cajero***[121], se coloca un dispositivo que simula el lector de tarjetas y un teclado numérico para capturar el número secreto de la víctima. Tanto la banda magnética como el PIN se transmiten al delincuente (por ejemplo, por SMS desde una terminal móvil incluida en el mismo cajero), que puede duplicar fácilmente esta tarjeta y utilizarla con normalidad. Se trata de uno de los ataques más peligrosos, ya que el usuario mantiene su tarjeta original, y por tanto no es consciente de que ha sido víctima de este delito.

120 Accesible en http://es.wikipedia.org/wiki/Dat%C3%A1fono
121 Accesible en http://www.securityartwork.es/2011/10/03/%C2%BFayudando-al-cliente/

4 Denuncias

Según el artículo 259 de la Ley de Enjuiciamiento Criminal (LEC), la denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado es obligatoria siempre que se haya producido un delito. En España, es posible realizar esta denuncia bien en las comisarías del ***Cuerpo Nacional de Policía***[122], bien en los puestos o cuarteles de la ***Guardia Civil***[123], en cada caso en el ámbito de actuación de estos cuerpos y siempre de forma presencial: aunque en la actualidad es posible realizar el cuerpo de una denuncia "online", habremos de confirmarla con nuestra presencia en la comisaría o puesto de la Guardia Civil correspondiente.

Ilustración 70 y 71 · Cuerpo Nacional de Policía y Guardia Civil

Tanto la Guardia Civil como la Policía Nacional cuentan con grupos de Policía Judicial y de Policía Científica especializados en nuevas tecnologías (informática, electrónica, telefonía...); el incremento exponencial de este tipo de delitos en los últimos años -hemos visto algunos ejemplos de ellos aquí, pero hay muchos más- ha motivado que ambos cuerpos de seguridad formen especialistas en la materia, de la misma forma que hay especialistas en la lucha contra estupefacientes o bandas armadas. Hoy en día, en casi todas las Jefaturas Superiores de Policía y Comandancias de la Guardia Civil existe personal especializado en la lucha contra los delitos tecnológicos, que en ocasiones logran éxitos considerables en la lucha contra los delitos que hemos descrito en este capítulo.

A la hora de realizar la denuncia de un delito tecnológico -como de cualquier otro delito-, es muy importante aportar al funcionario toda la información posible sobre los hechos denunciados: direcciones IP que nos han atacado, URLs de material protegido que son públicamente accesibles, etc. Con este material, las Fuerzas y Cuerpos de Seguridad del Estado podrán ponerse a trabajar, y, con una orden judicial, las unidades correspondientes podrán solicitar información adicional a un proveedor de accesos a Internet, un ISP, o al administrador de una página web.

122 Accesible en http://www.policia.es/
123 Accesible en http://www.guardiacivil.es/

CUESTIONARIOS de AUTOEVALUACIÓN

SEGURIDAD GLOBAL

1 La seguridad se define como la combinación de...

A Integridad, confidencialidad y disponibilidad.

B Integridad, confidencialidad y verificación.

C Verificación, confidencialidad y contraseñas.

2. Utilizo Linux... ¿debo configurar un cortafuegos?

A No, el cortafuegos sólo es necesario configurarlo en Windows.

B Sí, siempre.

C No, porque en Linux no hay virus y por tanto estaré protegido sin firewall.

3. Me llega un correo de un amigo con un programa ejecutable. Debería...

A No ejecutar el programa si el correo está en inglés, porque mi amigo es de Albacete, pero si está en castellano no hay problema.

B No ejecutar el programa jamás.

C Ejecutarlo sin problemas, porque mi amigo es de total confianza.

4. En las redes sociales...

A Puedo poner cualquier información sobre mi persona, porque sólo es accesible con usuario y contraseña.

B Puedo poner cualquier información sobre mi persona, porque sólo la verán mis amigos y contactos.

C Jamás debo poner información que pueda comprometer mi seguridad.

5. Los ataques tecnológicos son raros, pero debo protegerme por si acaso.

A Falso, no debo protegerme porque no soy una multinacional.

B Falso, los ataques tecnológicos son muy habituales.

C Verdadero, es importante protegerse aunque no te vayan a atacar nunca.

Soluciones: 1A · 2B · 3B · 4C · 5B

MALWARE

1. En un equipo donde todo el software es original, no se emplean redes de intercambio de ficheros como emule (P2P), no se navega por sitios desconfiables y se emplea el ordenador únicamente para escribir documentos y para el correo electrónico. ¿Requiere usar herramientas anti malware?

A No. Si no se navega por sitios “peligrosos” ni se descarga nada no puede ser infectado.

B Sí, por que aunque se tengan todas las precauciones posibles, no se sabe si el correo que se recibe de contactos conocidos puede estar infectado o se dispone de alguna herramienta que pueda tener alguna vulnerabilidad.

C Sí, y adicionalmente deben instalarse varios antivirus a la vez.

2. Un ordenador realiza acciones extrañas, como ralentizarse, ocultar o eliminar ficheros, etc. y el usuario presupone que está infectado por algún tipo de malware. Revisando los programas en ejecución comprueba que tiene ejecutándose un programa X que desconoce. Lo busca en Internet y encuentra que dicho programa es un troyano. ¿Qué debería hacer?

A Buscar en Internet, empleando su buscador preferido, el nombre del troyano seguido de la palabra eliminar, antivirus, desinfectar, etc. y descargarse la primera herramienta que encuentre el buscador y de esta forma eliminar el troyano.

B Acceder a la página web de la herramienta anti-virus que emplea contra los troyanos y comprobar qué es ese troyano y por qué no ha sido detectado por la herramienta. Consultar en la web cómo poder eliminarlo.

C Como no emplea ninguna herramienta anti-virus porque no es recomendable tenerla , debe buscar en páginas Web como eliminar dicho troyano.

3. El banco informa a un cliente que requieren su nombre y DNI para asociarlo a su correo por una nueva ley y que, en caso contrario, tendrán que darle de baja del acceso online a la web del banco. El usuario comprueba que el remitente coincide con el banco. ¿Qué debe hacer?

A El correo es correcto y debe pinchar en el enlace.

B Pinchar en el enlace y reenviar el correo a todos los contactos por si alguno tiene alguna cuenta bancaria en el mismo banco.

C Suponer que es un correo falso ,notificarlo al banco del cual parece ser el mensaje y eliminar dicho correo.

4. Si un ordenador va lento y el usuario cree que es el antivirus. ¿Qué debe hacer?

A Detener el antivirus hasta que el rendimiento vuelva a ser el correcto.

B Desinstalar el antivirus.

C Comprar un nuevo ordenador.

D Consultar a un experto o consultar al fabricante del antivirus para averiguar el motivo por el cual el antivirus ralentiza la máquina.

5. Un usuario tiene un antivirus instalado en el ordenador. Quiere instalar uno nuevo porque el que tiene no le gusta. ¿Cómo debe hacerlo?

A Debe borrar el antivirus viejo e instalar el nuevo.

B Mantener el antivirus viejo e instalar el nuevo.

C Detener el antivirus viejo para que no se ejecute e instalar el nuevo. Una vez que compruebe el correcto funcionamiento del nuevo antivirus, desinstalar el viejo.

D No se puede hacer.

Solución: 1B · 2B · 3C · 4D · 5C

NAVEGACIÓN SEGURA

1. ¿Es recomendable aplicar los parches de seguridad las aplicaciones siempre?

A Si, las actualizaciones mejorarán la seguridad.

B No, eso hace que la aplicación corra el riesgo de no funcionar correctamente. Si funciona mejor no tocarla.

C No, eso hará que nos vaya más lenta.

2. Si se recibe un correo en la bandeja de entrada de un remitente conocido…

A Comprobar con nuestro antivirus cualquier adjunto que acompañe al correo antes de abrirlo.

B No hay que temer, si hubiese alguna posibilidad de que adjunte algún tipo de virus, el antivirus del correo lo hubiese eliminado.

C Si no contiene ningún fichero adjunto es totalmente seguro.

3. Una cookie…

A Almacena información personal del usuario en el equipo de este para ser usada en sesiones posteriores y solo puede leerla la página web que la crea.

B Almacena información personal del usuario en el servidor web para ser usada en sesiones posteriores y puede ser leída por páginas con intenciones fraudulentas.

C Almacena información de la página en el equipo del usuario para poder consultar la web cuando no está conectado a Internet.

4. ¿Cuáles de estos consejos son CORRECTOS cuando hablamos de seguridad informática? (Puede existir más de una respuesta correcta)

A Si una versión de un programa nos funciona correctamente no es aconsejable actualizarla.

B Si nuestro ordenador funciona correctamente no es necesario actualizar el Sistema Operativo, a no ser que nuestro antivirus detecte un virus.

C Es muy recomendable tener actualizado el antivirus permanentemente ya que sino puede resultar inútil.

D Los correos electrónicos que recibimos en nuestra bandeja de entrada son legítimos y no tenemos nada que temer ya que nuestro proveedor de correo se encarga de filtrar el correo que pueda resultar maligno o no deseado (SPAM).

E Es recomendable analizar todos los ficheros descargados de Internet ya que pueden contener algún tipo de malware.

F No es recomendable realizar copias de seguridad periódicamente ya que esto puede suponer la acumulación de muchos datos redundantes. Lo aconsejable es una vez cada año o cada dos años.

G Debemos asegurarnos que todo el software instalado en nuestro ordenador proviene de una fuente conocida y segura. Muchos de los programas descargados de la red pueden contener todo tipo de malware que puede infectar nuestro ordenador.

5. ¿Qué navegador es más seguro?

A Internet Explorer de Microsoft

B Firefox de Mozilla

C Safari de Apple

D Opera de Opera Sofware

E Chrome de Google

F Epiphany de Gnome (GNU/Linux)

G Konqueror de KDE (GNU/Linux)

H No hay ningún navegador completamente seguro, todo depende del uso que de él se haga y de como configuremos las diferentes medidas de seguridad que nos ofrece.

Solución: 1A · 2A · 3A · 4CEG · 5H

CORREO ELECTRÓNICO

1. En caso de recibir un correo electrónico desde la cuenta administrador@ mi_dominio solicitando confirmación de que la cuenta está en uso, mediante el envío del nombre de usuario y contraseñar como justificante de que se es el propietario de la cuenta...

A No conviene hacer nada ya que parece un engaño.

B Es recomendable enviar la contraseña ya que parece evidente que son los administradores.

C Hay que notificárselo a los administradores del correo para que tomen medidas al respecto.

D Hay que responder al correo indicando que no vamos a enviar la contraseña ya que parece un correo fraudulento, indicando que si es un correo real, contacten telefónicamente.

2. En caso de recibir un correo en el que el remitente es nuestra propia cuenta, y teniendo la certeza de que no lo hemos enviado, lo mejor es:

A Contactar con los administradores ya que parece que nuestra cuenta de usuario ha sido comprometida.

B Abrir el correo por si hemos olvidado que nos auto-enviamos un correo.

C No es necesario hacer nada, ya que es relativamente sencillo enviar correos suplantando una identidad. Lo mejor es borrarlo sin abrirlo y contactar con los administradores por si pueden rastrear su origen.

D Responder al correo indicando que, por favor, dejen de enviar correos suplantando la cuenta.

3. En caso de recibir un correo de nuestro banco, con una oferta muy interesante en la cual queremos participar:

A Hay que abrir un navegador y escribir la dirección del banco a mano para buscar la promoción, y en caso de no encontrarla solicitar información telefónicamente.

B Basta con hacer click en el enlace del correo, simplemente tomando la precaución de no dar nuestro usuario y contraseña de banca electrónica.

C Eliminar el correo directamente, ya que los bancos no envían publicidad.

D Contactar con CSIRT-cv para obtener información sobre si se trata de una estafa.

4. Al reenviar un correo “cadena“ entre tus contactos...

A No es necesario utilizar el campo CCO o BCC, ya que es un correo entre contactos personales.

B Es recomendable incluir a todos los usuarios únicamente en CCO.

C Es recomendable poner a todos los usuarios en el campo “para” y en el campo “CCO” al mismo tiempo.

D Es recomendable introducir direcciones de correo erróneas para despistar a posibles spamers.

5. Si firmamos un correo electrónico al enviarlo, la firma digital sirve para...

A Justificar que el correo ha sido enviado.

B Garantizar que nadie más que el destinatario podrá leerlo.

C Garantizar que el remitente es autentico y que el contenido no ha sido modificado.

D Garantizar que el remitente es autentico.

Solución: 1C · 2C · 3AD · 4B · 5C

COMPRAS ONLINE

1. Un certificado de seguridad es: (Puede haber más de una respuesta correcta)

A Una tarjeta que introducimos físicamente en el ordenador y que nos permite navegar solo por páginas web seguras.

B Un documento digital mediante el cual un tercero confiable garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

C Un título que acredita a una persona como usuaria de Internet con conocimientos de navegación segura.

D Un software que permite cifrar los datos que se envían por la red.

2. Marque todas las recomendaciones CORRECTAS relacionadas con la Banca Online

A La dirección web donde introducimos nuestro usuario y contraseña debe empezar siempre por https y no por http.

B Si aparece un candado en alguna parte del navegador deberemos cerrar el navegador inmediatamente.

C Debemos saber que nuestro banco NUNCA nos pedirá información confidencial mediante correo electrónico o teléfono.

D Es más seguro el uso de equipos públicos para realizar operaciones bancarias, ya que estos equipos están equipados con última tecnología.

E El método más seguro es que cuando terminemos de realizar las operaciones, cerremos el navegador, de esta forma simple se cierra automáticamente nuestra sesión.

3. Los portales web de las empresas con más renombre:

A Son completamente seguras y no debemos temer por la seguridad.

B En general tienen mejores medidas de seguridad que otras, pero también son más propensas a falsificaciones que otras menos conocidas.

C Es mejor acceder a este tipo de empresas a través de mensajes correo electrónico recibidos ya que se accede de forma más directa.

4. Escoja el método de pago que coincide con la definición. OPCIONES: 1 Tarjetas Virtuales, 2 Ukash, 3 PayPal, 4 Tarjetas Bancarias, 5 Firma Electrónica, 6 Mobipay, 7 Contra reembolso, 8 Transferencia Bancaria

A Tarjetas de Crédito o débito. A demás del número y la fecha de caducidad, es necesario introducir el código adicional CVV (Valor de Validación de la tarjeta de Crédito).

B Son ofrecidas por algunos bancos o cajas para el pago online. Para ello se genera un número de tarjeta (asociado a la cuenta del usuario) para una compra determinada. Deja de ser válido y es eliminado una vez la transacción se realiza.

C Método novedoso y adecuado para pequeños pagos online. El usuario se da de alta en el portal de la empresa, donde debe introducir de forma segura los datos bancarios. Luego puede comprar desde cualquier página que acepte este tipo de medio de pago sin necesidad de volver a introducir el número de tarjeta, ya que es suficiente con usar los datos de la cuenta asociada. Son ellos los encargados de mandar el importe al vendedor.

D Sistema de pago a través del teléfono móvil que se asocia previamente a una tarjeta de crédito emitida por la entidad del usuario. Facilita las compras ya que solo hay que enviar un mensaje de texto y las operaciones se gestionan a través de las redes de los operadores de telefonía móvil y de los sistemas de medios de pago financieros, que gestionan diariamente millones de transacciones en las más altas condiciones de seguridad.

E Transacción de dinero de la cuenta del usuario a la del vendedor. En algunos bancos o cajas este servicio es gratuito. Algunas entidades mandan un SMS al teléfono móvil del usuario para confirmar la operación.

F Bonos que se adquieren en oficinas de Correos o Telecor para poder efectuar un pago en Internet. Se introduce el código de 19 dígitos en la web y se descuenta automáticamente el importe del saldo del cupón.

G Sistema de acreditación que permite asociar la identidad de las personas, con el mismo valor que la firma manuscrita. Es necesario un hardware y un software específico para realizar el pago. El nuevo DNI electrónico incorpora ya este sistema.

H Sistema de pago por el que el usuario abona el importe del producto a un cartero, mensajero o transportista al recibirlo en su domicilio. Deben quedar claras las condiciones (quién paga los gastos y a cuanto ascienden) antes de realizar la operación.

5- Responda si las siguientes afirmaciones son vedaderas

A Las garantías de los productos adquiridos por Internet no son iguales que los adquiridos en tiendas. Normalmente las garantías son menores.

B Una foto del producto puede no corresponder al mismo, por lo que deberemos informarnos de las características del mismo en diferentes sitios de Internet.

C Los datos de caracter personal están protegidos por la LOPD (Ley Orgánica de Protección de Datos), pero en el ámbito de Internet existe otra ley diferente y se denomina LPDI (Ley de Protección de Datos en Internet).

D Lo mas usual es que en el comercio electrónico no exista el departamento de atención al cliente, aunque si existe, la comunicación será por Messenger.

Solución: 1BD · 2ACE · 3B · 4 A4-B1-C3-D6-E8-F2-G5-H7· 5B

REDES SOCIALES

1. Al descubrir que un amigo ha publicado una foto nuestra en una red social, si deseamos que sea retirada...

A Se ha de acudir al poder judicial para conseguir una orden de retirada.

B Conviene contactar con el usuario, y en caso de que se niegue, contactar con los administradores de la red.

C No podemos hacer nada, la libertad de expresión le ampara.

D No podemos hacer nada en caso de que la imagen solo esté disponible para su red de contactos.

2. Al utilizar un servicio de mensajería, si recibimos un mensaje privado con un enlace de un conocido en un idioma diferente del que solemos utilizar para contactar con él...

A Hemos de darle la enhorabuena ya que parece que está aprendiendo idiomas.

B Seguramente se trate de información sobre algún viaje o curso de idiomas por lo que no hemos de sospechar.

C No haremos nada, ya que parece un mensaje fraudulento.

D No utilizaremos el enlace e informaremos al usuario de la situación ya que parece que tiene algún tipo de código malicioso instalado.

3. Si queremos vengarnos de un conocido, ex-pareja o similar publicando fotos comprometidas en una red social para que sus contactos las vean, ¿cómo hay que actuar?

A Lo mejor es no etiquetarle para que no se dé cuenta.

B No hacerlo bajo ningún concepto ya que además de denigrante, está prohibido y nos puede llevar a denuncias y consecuencias legales.

C Tapar la cara para que no nos puedan acusar.

D Utilizar un ordenador público para no dejar rastro.

4. Si recibimos una transferencia de un fichero no solicitado mediante mensajería instantánea, pero tenemos curiosidad por abrirlo, ¿como se ha de actuar?

A Aceptarlo sin problemas, ya que tenemos un software antivirus que nos protegerá.

B Contactar con el usuario para saber si se trata de un envío automatizado y malicioso.

C Cancelar la transferencia y no hacer nada.

D Analizar con un antivirus nuestro sistema operativo, ya que la petición de transferencia puede haber infectado el equipo.

5-. Si nuestro cliente de IRC o de mensajería instantánea, admite la posibilidad de cifrar las comunicaciones.

A Es recomendable utilizarlo, aunque no lo consideremos necesario.

B Es recomendable no utilizarlo ya que al tener que descifrar las comunicaciones, el equipo consumirá mas energía.

C Es recomendable activarlo únicamente cuando se van a transmitir datos confidenciales.

D No hay que activarlo ya que sino, el receptor recibirá la información cifrada y no podrá leerla.

Solución: 1B · 2D · 3B · 4B · 5A

SEGURIDAD INALÁMBRICA

1. ¿Qué protocolo de seguridad WiFi es más aconsejable utilizar por lo que a su seguridad se refiere?

A WPA

B WPA2

C WEP

D Ninguna de las anteriores

2. ¿Cuál las siguientes acciones, conforma una buena práctica en el uso de redes WiFI?

A Conectarse a la red WiFi de mi vecino

B Consultar el estado de mi cuenta bancaria desde una red WIFI de un cibercafé

C Mantener limpia la lista de redes favoritas de mi Windows XP

D Configurar mi punto de acceso con un protocolo de seguridad WEP

3. ¿Qué ventajas tiene el protocolo de seguridad WiFI WPA2 frente a su predecesor WPA?

A Segundas partes nunca fueron buenas

B WPA2 utiliza un algoritmo de cifrado mas robusto (AES), que WPA

C WPA permite asociar tan solo a una estación, mientras que WPA2 permite múltiples estaciones

D WPA2 permite cifrar el tráfico desde la estación al punto de acceso.

4. ¿Qué medidas de seguridad aplica Bluetooth para la capa de enlace?

A Autenticación, autorización y cifrado de datos

B Autorización, discreción y cifrado de datos

C Cifrado de datos, autenticación y disponibilidad

D Disponibilidad, autenticación y autorización

5. ¿Cuál las siguientes acciones, conforma una buena práctica en el uso de dispositivos Bluetooth?

A Mantener encendido el Bluethooth de mi móvil permanentemente

B Aceptar conexiones entrantes anónimas

C Modificar el nombre por defecto de mi dispositivo Bluethooth

D No revisar la lista de emparejamientos periódicamente.

Solución: 1B · 2C · 3B · 4A · 5C

EQUIPOS Y DISPOSITIVOS PORTÁTILES

1. Al realizar una copia de seguridad de un dispositivo portátil, está debe guardarse:

A En un soporte (disco duro, DVD, memoria USB), que conviene llevar en la funda del portátil por si necesitamos recuperar la información.

B en un soporte (disco duro, DVD, memoria USB), que conviene dejar en casa o en la oficina.

C en el propio equipo ya que los soportes externos pueden perderse o dañarse.

2. Cual de las siguientes afirmaciones sobre el uso de contraseña en la bios es cierta:

A Es poco recomendable ya que basta con formatear el equipo o cambiar el disco duro.

B Es recomendable ya que sin ella es imposible acceder a los datos del disco duro.

C Puede ser delicada de configurar para usuarios noveles por lo que se recomienda pedir ayuda a algún usuario con conocimientos medios.

3. Al cifrar el disco duro...

A ...garantizamos que en caso de robo, sea imposible utilizar el equipo, ya que este queda bloqueado.

B ...garantizamos que la información que contiene el dispositivo no será accesible.

C ...garantizamos que la información que contiene será imposible de eliminar.

4. La conectividad inalámbrica en un equipo portátil...

A ...conviene desactivarla en caso de no utilizarla.

B ...puede estar siempre habilitada mientras no nos conectemos a ninguna red no segura.

C ...no debe deshabilitarse bajo ningún concepto con el ordenador encendido.

5. En Windows el cifrado de carpetas y ficheros, va asociado al usuario, por lo que no nos solicitan contraseña para acceder a los ficheros, pero esté método tiene una de las siguientes desventajas. Marcar la correcta.

A Si creamos un usuario con el mismo nombre en otro equipo y copiamos los ficheros, podrán ser descifrados.

B Si formateamos el servidor y no hemos exportado los certificados, la información cifrada será irrecuperable.

C Al no tener contraseña, si otro usuario inicia sesión con otra cuenta en el mismo equipo, podrá acceder a los datos.

Solución: 1B · 2C · 3B · 4A · 5B

Teléfonos móviles, móviles inteligentes y PDA

1. Si desde nuestro teléfono móvil nos conectamos a una web bancaria utilizando GSM:

A Nuestros datos podrán ser interceptados ya que GSM es inseguro.

B Nuestros datos estarán a salvo ya que las conexiones con los bancos disponen de mecanismos extra independientemente de la plataforma desde donde se acceda.

C Las conexiones GSM no permiten conexiones a Internet, solo las UMTS.

2. Si tenemos un fichero infectado por un virus corriente de ordenador, lo transferimos al móvil y lo abrimos ¿qué sucederá?

A El móvil quedará infectado ya que lo hemos abierto.

B El móvil no se infectará ya que le virus no está diseñado para funcionar en teléfonos móviles.

C El cortafuegos del móvil nos avisará de que el fichero está infectado.

3. ¿Cuál de las siguientes afirmaciones sobre teléfonos inteligentes es correcta?

A Los dispositivos sin pantalla táctil no permiten instalar programas por lo que no son vulnerables a los virus informáticos.

B Los virus para dispositivos inteligentes son multiplataforma, por lo que afectan por igual a todos los sistemas operativos.

C Ninguna de las anteriores.

4-. ¿Cuál de los siguientes no es un sistema operativo de dispositivos móviles?

A Symbian.

B Windows Mobile

C Ubuntu.

Solución: 1A · 2B · 3C · 4C

INTERNET Y LOS MENORES

1. Al descargar un programa de Internet...

A ...debo pasarle siempre el antivirus.

B ...no debo pasarle el antivirus si lo descargo de una web española, pero sí en el resto.

C ...no debo pasarle el antivirus si lo descargo de una web, pero sí si lo descargo del eMule.

D ...no hace falta pasarle el antivirus salvo que lo descargue por WiFi.

2. El correo electrónico.... ¿es una fuente de datos fiables?

A No lo es excepto con los correos de las personas que tengo identificadas como amigos.

B Sí, siempre y cuando no proporcione mi clave de correo a nadie.

C Sí, siempre que venga de una dirección conocida.

D No lo es, cualquiera puede enviar un correo falsificando mi dirección.

3. En las redes sociales...

A Puedo publicar cualquier contenido sin ningún problema.

B Debo estar atento a no publicar contenidos inapropiados (datos privados, mensajes ofensivos...).

C Siempre que publique algo que pueda poner en peligro mi seguridad, los sistemas de la propia red lo detectarán y eliminarán.

D Cualquier cosa publicada en una red social reconocida, como Facebook o Tuenti, es correcta.

4. La mejor forma de enviarle un documento privado a un amigo es...

A Mediante el uso de programas P2P.

B Compartiéndolo en una red social.

C Colgándolo en mi blog.

D Por correo electrónico.

5. Si creo que puedo tener un problema que comprometa mi seguridad en Internet, debo...

A Compartirlo con mis padres, tutores o profesores, para que puedan ayudarme.

B Compartirlo con mis amigos para que puedan ayudarme.

C Compartirlo sólo con expertos informáticos, que son quienes pueden echarme una mano.

D Buscar ayuda en la propia red (foros, redes sociales...).

Solución: 1A · 2D · 3B · 4D · 5A

REDES P2P

1. Si al instalar un programa P2P no sabemos exactamente conde están en nuestro equipo los ficheros que deseamos compartir, ¿cual de estas opciones será la mejor?

A No compartir nada.

B Compartir todo el disco y que sean los propios usuarios los que decidan qué descargar y qué no.

C Compartir la carpeta “Mis documentos” , ya que acostumbra a contener la carpeta de “Mi música” y “mis vídeos”.

2. Si desde una página web sigo un enlace a descargas P2P, ¿estoy a salvo de virus y fakes, ya que los administradores de la pagina están para hacer las comprobaciones previas?

A Si, ya que es precisamente la principal ventaja de estas páginas, comprueban los ficheros para ofrecer un mejor servicio a sus visitantes, ya que si no nadie las utilizaría.

B Si, ya que el servidor antivirus de la página web analizará los ficheros antes de que los descarguemos.

C No, ya que la web únicamente nos proporciona el enlace sin tener responsabilidad sobre los ficheros que contengan.

D No, ya que acostumbran a ser páginas fraudulentas creadas por las entidades de gestión de derechos de autor con el fin de perseguir a los usuarios que descargan contenido ilegalmente.

3. En caso de descargar por error contenidos prohibidos, como pedofilia, o violencia explicita real, ¿que debemos hacer?

A Borrar el contenido lo antes posible y no avisar a las autoridades, ya que podrían sospechar que lo hemos descargado intencionadamente.

B Borrar el contenido y notificarlo a las autoridades para que puedan bloquearlo a la vez de evitar problemas legales.

C Avisar a las autoridades, pero no borrarlo por si necesitan la muestra.

4. En caso de utilizar las redes de P2P para descargar material sin derechos de autor, (marcar la respuesta correcta).

A Estaremos infringiendo la ley, ya que el uso de estas redes está prohibido.

B Se trata de un servicio más de Internet, por lo que no sucederá nada.

C Estaremos a salvo de virus y otros códigos maliciosos, ya que estos ficheros siempre están limpios.

5. En caso de utilizar las redes de P2P para descargar material con derechos de autor, (marcar la respuesta correcta).

A Estaremos infringiendo la ley y seremos investigados por ello, arriesgándonos a fuertes multas, incluso a penas de prisión.

B Es recomendable no hacerlo ya que hay que apoyar a los autores, además de poder ser víctimas de denuncias de las sociedades de autores.

C Es imposible utilizar estas redes ya que solo contienen material libre.

Solución: 1A · 2C · 3B · 4B · 5B

JUEGOS ON-LINE

1. En los juegos masivos por Internet, en los que podemos interactuar con otros jugadores, ante la posibilidad de establecer una relación personal con algún otro jugador debemos:

A Evitarlo a toda costa ya que Internet puede ser un delincuente.

B Utilizar nuestro sentido común y actuar como lo haríamos con una relación normal.

C Evitarlo a toda costa ya que se trata de una actividad ilegal.

2. En los juegos masivos por Internet, en caso de querer comprar un bien virtual (dinero virtual, complementos para nuestro jugador, etc...), como debemos actuar.

A No hacerlo bajo ningún concepto, ya que además de fomentar la esclavitud en países asiáticos, es ilegal.

B Consultar las condiciones del juego para asegurarse de la legalidad de la transacción e informarse sobre la fuente de dicho bien virtual.

C Nada, ya que no es posible comprar algo virtual con dinero real.

3. Cuales de las siguientes afirmaciones son correctas con respecto a la posibilidad de jugar online a un juego adquirido en una tienda (solución múltiple).

A Conviene leer las condiciones de uso ya que es posible que incluya licencia para ser utilizado en más de un equipo.

B Es necesario “piratearlo” para poder utilizarlo online.

C No conviene revelar el número de serie para evitar que sea registrado por otros usuarios.

D No es necesario tomar medidas de seguridad ya que solo es un juego.

4. Sobre las páginas web de apuestas online cual de las siguientes afirmaciones es falsa.

A Ofrecen medidas de seguridad similares a las de banca online.

B Son ilegales por operar en paraísos fiscales.

C Están libres de impuestos al operar en paraísos fiscales.

5. Un usuario que utiliza habitualmente una páginas web de apuestas descubre cargos en su tarjeta de crédito procedentes del servicio de apuestas no solicitadas.¿Qué debe hacer?

A Nada. Será un error, y se arreglará solo.

B Cambiar sus contraseñas de acceso al servicio como medida preventiva y notificarlo al servicio de apuestas.

C Cancelar la cuenta bancaria ya que ha sido comprometida.

Solución: 1B · 2B · 3AC · 4? · 5B

DELITOS TECNOLÓGICOS

1. Si recibimos un correo electrónico de alguien desconocido, ofreciéndonos importantes cantidades de dinero, debemos...

A Borrar inmediatamente el correo.

B Responder al correo indicando que no estamos interesados porque puede tratarse de una estafa.

C Borrar inmediatamente el correo y responder al mismo indicando que es una estafa.

2. Nuestro banco suele enviarnos correos electrónicos donde se nos piden datos confidenciales, como el PIN:

A Verdadero

B Falso

3. Con respecto a los programas P2P y la pornografía infantil...

A Es imposible descargar pornografía infantil, está muy controlado.

B Es posible descargar, sin saberlo, pornografía infantil, incluso compartirla.

C Sólo descarga pornografía infantil el que la busca.

4. Si utilizando un cajero automático éste se traga mi tarjeta...

A No debo preocuparme, el banco se encarga de todo.

B Debo avisar a los servicios de atención del propio banco para notificarles de lo sucedido y bloquear la tarjeta.

C Si me ofrece ayuda un viandante, debo hacerle caso.

5. ¿Dónde podemos denunciar los delitos cometidos por Internet?

A En cualquier página web de seguridad informática.

B En las ubicaciones de la Guardia Civil o Cuerpo Nacional de Policía.

C En CSIRT-CV.

Solución: 1A · 2B · 3B · 4B · 5B

GENERALITAT VALENCIANA

CSIRT-CV
Centre Seguretat TIC de la Comunitat Valenciana

GRUPO S2

COLEGIO OFICIAL DE INGENIEROS EN INFORMÁTICA DE LA COMUNIDAD VALENCIANA

ADCV
Agenda Digital de la Comunitat Valenciana