Seguridad Informática en la Empresa

Teoría y Práctica de Seguridad para Empleados y Gerentes no Técnicos

Fernando Durán Valenzuela

Seguridad Informática en la Empresa

Teoría y Práctica de Seguridad para Empleados y Gerentes no Técnicos

Fernando Durán Valenzuela

Aviso

El autor no garantiza la exactitud o adecuación de la información aquí presentada. El autor no será responsable de ningún daño, directo o indirecto que pueda resultar de la aplicación de los consejos aquí presentados.

Sobre el Autor

Fernando Durán Valenzuela -nacido en Cádiz, España- tiene más de quince años de experiencia profesional informática tanto en Europa como Norteamérica en los ámbitos de gobierno, universidad y empresa privada.

Es licenciado en Física por la Universidad de Sevilla y *Master of Science* en *Computer Science* por la University of Louisville, contando con publicaciones para conferencias internacionales y revistas profesionales de computación. Así mismo es acreditado por el International Information Systems Security Certification Consortium, Inc., $(ISC)^2$.

Actualmente es Director de Tecnología de la empresa de seguridad informática WaterlooSecurity Inc., donde entre otras actividades audita y asesora a empresas sobre seguridad de la información.

Primera edición, diciembre 2010.

Andando, andando.
Que quiero oír cada grano
de la arena que voy pisando.

Juan Ramón Jiménez

Tabla de Contenidos

Introducción

Como cada lunes Luisa llega a su moderna oficina en el centro de la ciudad temprano y revisa su correo electrónico mientras saborea su segundo café de la mañana. Pero hoy pasa algo raro. La bandeja de entrada de su correo electrónico muestra varios mensajes tanto de amigos como de desconocidos advirtiendo de ataques provenientes de un computador de su propia empresa. ¿qué está pasando?

La mayoría de nosotros dependemos más cada día de las computadoras y de Internet para realizar nuestro trabajo; las empresas y la sociedad están más informatizadas y la complejidad de los sistemas aumenta. A esta mayor dependencia de las redes de computadoras y sistemas informáticos hay que añadir el hecho de que cada vez los *hackers* malignos aumentan tanto en número como en sofisticación, haciendo de la seguridad informática un área cada vez más importante en nuestras vidas.

Casi a diario podemos ver noticias de sitios web y organizaciones y empresas de todo tipo que tienen sus páginas web vandalizadas o a las que les roban datos confidenciales. Esto ocurre a grandes empresas con grandes presupuestos de seguridad y muchos (probablemente la mayoría) de incidentes no son reportados porque dañarían la reputación de la empresa. Si las grandes empresas tienen problemas de seguridad, ¿cree que su empresa está segura?

Si no hacemos nada o no tenemos en cuenta sólidos

principios de seguridad entonces tenemos un gran riesgo de que nos ocurra un incidente de seguridad. La seguridad informática se trata del manejo de este riesgo.

Vamos a suponer que en la organización o empresa existe un departamento o persona encargado de los temas técnicos como el manejo de spam, virus, amenazas externas, infraestructura de red, sistemas operativos y áreas técnicas en general. En este texto nos centraremos no en los detalles de tecnología concretas sino en principios generales y recomendaciones dirigidas al personal no técnico de la organización.

Este curso está dirigido a todos los empleados y directivos de empresas u organizaciones que usan Internet en su quehacer diario. Trataremos principios generales de seguridad en vez de detalles particulares de la tecnología, ya que ésta cambia muy rápidamente.

Estructura

Este libro está dividido en tres partes.

La primera parte hace un recorrido por los principales puntos teóricos de la seguridad informática. Esta parte trata más de conceptos generales y encaja especialmente con los gerentes o jefes que necesiten tener una visión amplia para tomar decisiones, pero también puede ser interesante para muchos

empleados.

La segunda parte es más práctica y algunos consejos sirven para todo el mundo mientras que otros sólo tienen sentido para los que tienen poder de decisión dentro de una organización.

Finalmente en la tercera y última parte se describe un caso de un estudio de seguridad de una empresa ejemplo. Esta parte está dirigida a los gerentes.

Este es un libro corto a propósito. La seguridad es un tema complicado y lleno de matices que se extiende a todas las áreas de la computación. Hemos querido simplificar lo más posible y destilar los conceptos y consejos más importantes sin intentar hacer un libro "para tontos" (sin ningún elemento técnico pero que sirva de poco). Hemos evitado añadir diagramas o dibujos que no añaden mucho valor y tampoco hemos querido "inflar" el libro para que tenga más páginas con largas parrafadas y verborrea. De hecho y para que sirva de ejemplo irónico éste es uno de los párrafos más largos del libro.

El sitio web oficial del libro es: **http://seguridadinformati.ca** , en él puede encontrar más información como errata, actualizaciones etc.

Nota sobre el estilo

Este texto va dirigido a todos los hispanohablantes. Es difícil si no imposible acomodar los términos (especialmente técnicos) a todos los países de habla castellana (es irónico que incluso el mencionar "castellano" o "español" puede ser problemático).

Por ejemplo en España hablan del "ratón del ordenador" e "informática" y en Hispanoamérica es más común decir el "mouse de la computadora" y "computación"; en general en España hay más términos de influencia francófona y en Latinoamérica de influencia anglosajona.

Hemos optado por tratar de usar los términos que creemos se entiendan más en todos los países, de forma que aunque suenen raros aún se comprendan y a veces repetimos el mismo concepto con dos palabras distintas o similares (como *computador* y *computadora*). A menudo hemos decidido dejar el término técnico en su original en inglés antes que usar una palabra en español que no parece establecida.

A los puristas de la lengua les ruego nos perdonen; como decía en un chiste el estudiante que se fue a aprender inglés al extranjero en un telegrama a sus padres: "INGLES NO APRENDER ESPAÑOL OLVIDO".

Malware

El *malware* es software malicioso creado con la intención de introducirse de forma subrepticia en los computadores y causar daño a su usuario o conseguir un beneficio económico a sus expensas.

Existe una gran cantidad de malware y nuevos programas maliciosos son creados a diario; la empresa Sophos, en su informe "Mid-year 2010 threat report" dice que recibe una media de 60.000 muestras de malware nuevo diariamente. Considere que aunque tenga un antivirus actualizado algunos especialistas consideran que el software antivirus detecta solamente alrededor de un tercio de los posibles virus.

Principales tipos de malware:

- Virus. Un virus se activa al ejecutar un programa y además de intentar reproducirse lleva a cabo actividades como borrar archivos, mostrar una broma etc.
- Gusano o *worm*. Análogo al virus pero se transmite de forma automática por la red, aprovechando una vulnerabilidad.
- *Spyware*. Monitorean su actividad online y venden esta información a anunciantes. A menudo usan una barra de herramienta en el navegador para ello. Si usted dió permiso para que se instalara el programa entonces la empresa de publicidad no estaría en principio haciendo nada ilegal, aunque a menudo es un área gris ya que las condiciones de uso puede no estar claras para el usuario o estar

escondidas.

- *Adware.* Relacionado con spyware, son programas que instalándose sin permiso hacen publicidad, típicamente con *pop-ups* (ventanas emergentes).
- *Scareware*, *crimeware.* Este tipo de malware intenta asustar al usuario y convencerlo para que haga pago por tarjeta de crédito u otros engaños. Por ejemplo pueden hacen aparecer en su navegador un mensaje de que su computador está infectado.
- Trojanos y *backdoors*. Los Troyanos son aplicaciones malignas que se disfrazan como algo inofensivo y atractivo para que el usuario lo ejecute. Cuando se instala realiza su actividad maliciosa como borrar archivos o propagar gusanos por la red local. Los *backdoors* o puertas traseras son aplicaciones que ocultándose del usuario permite a atacantes conectarse a su computadora. Esto es extremadamente peligroso ya que los hackers pueden tener control total de su computadora, ver lo que usted hace etc. (los programas que capturan lo que el usuario teclea se llaman keyloggers).
- *Rootkits*. Es una serie de modificaciones en el sistema operativo del computador, por ejemplo para que el malware que se está ejecutando no aparezca en la lista de procesos.
- *Botnet* software. Cuando un computador cae bajo el control de los hackers a través de malware que contiene una puerta trasera se dice que es un esclavo o "*zombi*". Estos esclavos pueden formar parte de una red o "botnet".

Las motivaciones de los creadores de malware son principalmente económicas:

- Anuncios o redirección a sitios web con publicidad que les reportan ingresos.
- Obtención fraudulenta de datos financieros (datos de tarjeta de crédito etc).
- Controlar el computador y usarlo como esclavo o *zombi* para atacar otros sistemas ("*Denial of Service*" o *DoS*).
- Fraude haciendo clic en anuncios (de Google u otros anunciantes).

Al principio de la revolución de los computadores personales los motivos de muchos creadores de virus eran más para ganar fama, como reto o broma y el efecto del malware era muy obvio pero desde hace unos años la principal motivación de los creadores de malware es económica (frecuentemente estas personas viven en países en vías de desarrollo). A menudo este nuevo tipo de malware intenta pasar más desapercibido para pasar más tiempo en el computador infectado.

Por dónde entran los programas maliciosos a su computador:

- Páginas web: cuando se visitan o bajándose un fichero de ellas.
- Incluido en otro programa (típicamente uno gratuito) que ha sido descargado de Internet.
- A través de archivos bajados con una utilidad "*peer-to-peer*" P2P.

- En un archivo adjunto en un mensaje de correo electrónico.
- En un fichero enviado por mensajería instantánea o *chat*.

Peligros que conllevan:

- Pérdida económica
- Espionaje de su actividad, pérdida de privacidad.
- Degradación del rendimiento de la computadora.
- Uso de su computador para atacar a otros.

Indicios de que malware está instalado en su computador:

- El uso del computador va más lento.
- Anuncios “pop-ups”.
- Mensajes o errores inesperados.
- El computador se queda sin memoria o sin espacio en disco.
- El computador se apaga sólo de forma inesperada.
- El computador no arranca de forma normal o produce mensajes extraños.
- Se producen cambios inexplicables en ficheros, como que desaparecen o cambian de nombre .
- El computador tiene comportamientos erráticos o inesperados.
- Hay procesos corriendo (en Windows se ven en el “Gestor de Tareas”) que son sospechosos (son nuevos, no se sabe cuál es su función etc).

- Cambios en el navegador como:
    - Página de inicio del navegador distinta.
    - Nuevo enlace “favorito”.
    - Nueva barra de herramientas.

Consejos para protegerse del malware:

En parte el administrador de lo sistemas o departamento técnico es responsable del mantenimiento técnico que protege del malware, como es mantener los computadores actualizados, con firewall o cortafuegos y con software anti-virus. Por su parte tiene que tener cuidado y seguir unas precauciones básicas para evitar que código maligno entre en su computador:

- No abra ficheros incluidos en mensajes de correo de personas desconocidas o incluso si conoce el remitente no lo abra si le parece sospechoso (hay virus que utilizan la libreta de direcciones de correo para propagarse).
- Use contraseñas fuertes como explicamos en la sección de contraseñas.
- Tenga cuidado con archivos obtenidos por P2P o no use P2P.
- Mantenga su software de anti-virus actualizado.
- Mantenga su navegador y los “*plugins*” que usa actualizados (use por ejemplo https://browsercheck.qualys.com para comprobarlo)
- Familiarícese con la lista de programas que su computador procesa normalmente (en Windows se ve en el “Gestor de Tareas”) y

cuando tenga sospechas de malware revise la lista para comprobar si hay procesos nuevos corriendo. Puede buscar en Internet por el nombre del programa sospechoso. Otro indicio es la ubicación del fichero (presunto malware) que se está ejecutando; si está en un directorio de descargas de Internet Explorer por ejemplo es más sospechoso que si está en un directorio de sistema de Windows. Este es un tema tema más técnico de forma que si no está seguro avise al encargado de informática o similar.

- Esté a la defensiva y use el sentido común.

Veamos un caso basado en un hecho real que ilustra la necesidad de estar siempre alerta:

Francisco fue a Google a buscar información sobre un anti-virus. Fue a la página web de uno de los resultados e inmediatamente un pop-up le advirtió de que se había detectado un virus en su computador y que debía comprar la suscripción para el antivirus que le solucionaría el problema. De manera que Francisco introdujo los datos de su tarjeta de crédito para comprar el producto.

Resulta que todo era un timo. Los defraudadores habían imitado una página web de una empresa conocida de anti-virus y habían conseguido que apareciera como uno de los primeros resultados en Google al buscar por ciertos términos (ésto fue la parte difícil para ellos). Cuando cualquiera visitaba este sitio web se le aparecía el mensaje advirtiendo falsamente de que su computador tenía un virus y animándole a usar de inmediato su tarjeta de crédito.

La lección es que los criminales en Internet tienen una gran inventiva y siempre están desarrollando nuevas formas de timos. Por este motivo es importante estar a la defensiva siempre y usar principios generales sólidos, como no hacer una compra en Internet como reacción a un mensaje de una página web o un email.

Si ha sido infectado o sospecha que ha sido infectado por un virus de cualquier tipo:

- Si tiene más de un computador desconecte la unidad infectada de la red para evitar posibles propagaciones del malware.
- Cierre la aplicación de email (Outlook o Thunderbird por ejemplo).
- Haga un scan con anti-virus, usando un antivirus online o si el computador está desconectado de Internet, con un CD.

Algunos sitios web con anti-virus online:

http://www.pandasecurity.com/activescan/
http://security.symantec.com/sscv6/home.asp
http://www.bitdefender.com/scanner/online/free.html
http://www.kaspersky.com/virusscanner
http://onecare.live.com/site/en-us/center/howsafe.htm

Si usa Internet para acceder a cuentas bancarias u otros sitios web a los que transmite información secreta considere usar un computador dedicado de forma exclusiva para esta actividad. Dicho computador no debe usar otro software que el mínimo para usar el navegador y no se debe usar para correo electrónico o para acceder a otros sitios de Internet. Tenga en cuenta

que con un software de virtualización como VMware o VirtualBox puede crear una “máquina virtual” o sistema aislado dentro de otro sistema operativo, de forma que no tiene que usar el hardware de una PC física.

Considere usar un computador (o máquina virtual) dedicado exclusivamente a la navegación a sitios web críticos como los de bancos.

Navegación Segura por Internet

Ya vimos en la sección anterior de malware riesgos al navegar a sitios web y dimos recomendaciones. En esta sección vamos a ver algunos conceptos y daremos más consejos para minimizar los riesgos cuando uno está recorriendo páginas web de Internet.

Privacidad

Veamos qué información puede recolectar un sitio web acerca de usted cuando lo visita.

Cuando nos conectamos por Internet a un sitio web (o cualquier otro tipo de conexión como mensajería instantánea o *chat* etc) cada computador que está conectado enviando o recibiendo información tiene asignada una dirección (de forma análoga a los números de teléfono cuando llamamos por teléfono o la dirección postal para las cartas por correo), ésta dirección se llama *dirección de IP* (IP significa *Internet Protocol* en inglés; Protocolo de Internet).

Esta dirección de IP es capturada por la página web que visita y con este dato a menudo se puede saber desde qué casa o edificio se conectó.

Los sitios web pueden recolectar otro tipo de información como qué navegador o sistema operativo usa e incluso en qué páginas ha estado antes, por ejemplo vaya a la dirección http://watsec.com/myip para tener una idea de la información que transmite.

Cuando la gente habla de “navegación anónima” se pueden referir a dos cosas:

- Que no quede rastro en el computador que está usando de los sitios en los que ha estado (su historia). Esto se puede conseguir usando un navegador como Chrome o Firefox que tengan esa propiedad.
- Que no quede rastro en los servidores que visitamos de quienes somos (específicamente, desde que dirección IP nos estamos conectando). Esto se consigue conectándose a través de un servidor “*proxy*” o intermediario, hay varias empresas en Internet que ofrecen este servicio de anonimato.

Mientras navega por Internet toda la información que manda o recibe a través de la red puede ser espiada por alguien con acceso a ella a menos que la sesión esté usando el protocolo encriptado SSL, esto es, cuando la dirección URL empieza por https:// (fíjese en la “s” extra) en vez de http:// . Cuando usa esta navegación con HTTPS el navegador (Internet Explorer, Firefox, Chrome etc) se lo indica con un icono de un candado o cerrojo en la barra de dirección o en la barra de estado (en el borde inferior).

Sea consciente de que toda la información que manda por Internet (indagaciones en buscadores etc) **y también información sobre su computador es posiblemente grabada por los sitios web que visita.**

Navegando

Tenga en cuenta que sólo hace falta un clic en el sitio equivocado para ser infectado.

Como consejos generales para evitar infectarse con malware mientras se visita un sitio web:

- Chequee que su navegador y las aplicaciones o *plugins* que tiene instalados están actualizados. Para esto puede usar la aplicación en: https://browsercheck.qualys.com/
- Cierre los pop-ups haciendo clic en el botón X de cerrar la ventana, no presione ningún botón de “cerrar” ya que puede ser falso e instalar un programa malicioso en su computador.
- No haga clic en anuncios de empresas que no conozca o que sean muy llamativos o que clamen regalar productos atractivos como iPods. Note que el malware puede venir también en anuncios insertados en sitios web prestigiosos.
- Use aplicaciones que le protegen o avisan e sitios peligrosos como *WOT* (http://www.mywot.com), *SiteAdvisor* (http://www.siteadvisor.com) y O*penDNS* (http://www.opendns.com).
- Evite hacer clic en enlaces a juegos o videos con el enganche de que aparezca gente famosa de actualidad ya que a menudo tienen spyware u otros problemas.
- Cuando termine de usar un servicio que requiere contraseña termine la sesión antes de visitar otros sitios web.

Política de la Empresa

Pregunte o revise la política de la empresa sobre el uso personal de Internet.

Dependiendo de su jurisdicción, su empresa puede tener el derecho a revisar los correos electrónicos y la actividad en Internet de sus empleados.

Tenga mucho cuidado con acciones que pueden llevar **consecuencias legales** para usted o para su compañía:

- No escriba (en email, página web, chat etc.) vea, imprima, baje o retransmita nada que sea ofensivo o que pueda considerarse ofensivo o amenazador.
- No escriba nada (en email, página web, chat etc.) sobre la empresa sin la autorización de la misma.
- Los puntos anteriores incluyen el escribir de forma “anónima” ya que de ser necesario por acción judicial lo más seguro es que se pueda rastrear y encontrar al computador o a la empresa que fue empleado para dicha acción.
- No realice piratería; no descargue ni distribuya materiales con copyright (música, películas, libros, programas etc.) sin pagar o tener la correspondiente licencia.
- No realice ataques contra otros computadores (de dentro o fuera de la compañía), no intente acceder a sistemas para los que no tiene autorización.

Tenga extremada precaución con lo que escriba en Internet ya que en general la información permanecerá por siempre (no se puede borrar) **y se puede seguir la pista y averiguar quién la escribió.**

Phishing

El *phishing* (palabra que viene del inglés *fish* o pescar como en "pescar a un tonto") hace referencia a estrategias de criminales por Internet en las que haciéndose pasar por instituciones reputables engañan a víctimas de forma que éstas revelen información personal o confidencial (como sus nombres de usuario y contraseñas y relacionado por tanto con el **robo de identidad**). El objetivo del fraude es acceder a servicios que reporten beneficios económicos como bancos, cuentas de correos o cuentas de sitios sociales.

Típicamente los intentos de phishing vienen por correo electrónico e intentan atraer a las víctimas hacia páginas web falsas que imitan a las auténticas.

En el caso de cuentas de email o de sitios sociales como Facebook el beneficio para el criminal es usarlas para mandar mensajes de spam, para atraer tráfico a una página web o para capturar nuevas víctimas.

Ejemplos de correos electrónicos con gran probabilidad de ser un timo de tipo phishing son **mensajes pidiendo**

información de cuentas de bancos o sitios web famosos como Ebay o PayPal; un sitio web financiero o medianamente importante nunca le va a pedir su información secreta (como contraseñas) y tampoco le va a pedir dirigirse a una página para verificar sus datos o contraseña.

Estas son algunas frases en un email que indican una actividad de phishing:

- "Verifica tu cuenta", mencionando que hay un problema para darle mayor credibilidad.
- "Cancelaremos su cuenta si no actúa en 24 horas", u otros apremios y supuestas razones para actuar.
- "Ha ganado un premio" o "ha ganado la lotería" o "ha sido seleccionado" o similares también son indicativos de phishing u otros timos.
- Frases en las que le acusan de un delito (por ejemplo de piratería de música o películas) y le ofrecen una amnistía o cancelar la deuda a cambio de un pago.

No haga clic en un email o página web para ir a un sitio web crítico como su banco o institución financiera; escriba directamente la dirección en la barra de dirección de su navegador o guárdela como "favorita".

Si tiene dudas sobre si un email que recibe es legítimo o no, contacte directamente por teléfono o por email con la organización que se supone envió el mensaje de correo. No responda al mensaje sospechoso, sino que verifique independientemente el número de teléfono o dirección de correo de servicio al cliente de la

organización.

A medida que los usuarios se van familiarizando con estos engaños los timadores se van volviendo cada vez más sofisticados y los mensajes que mandan están más dirigidos y son más específicos a una persona o grupo de personas para darles mayo credibilidad. A este tipo de phishing se le llama “spear phishing”.

Por ejemplo si los timadores se hacen con una lista de correo de un club o asociación o de una ciudad o región determinada (por ejemplo a través de una página web social) entonces pueden mandar un email a los miembros del grupo con un mensaje relacionado con el tema del que trata el grupo.

Si recibe un mensaje que sospecha es un timo de phishing bórrelo inmediatamente. No conteste al email y no haga clic en ninguno de sus enlaces.

Tenga en cuenta que estos timos no están limitados a Internet sino que también se hacen por teléfono. Por ejemplo haciéndose pasar por una obra de caridad famosa o comunicándole que ha recibido un premio buscan una excusa para que les dé su número de tarjeta de crédito u otra información personal que pueden usar para el beneficio económico de los criminales.

Comprando a Empresas por Internet

Tenemos dos casos distintos cuando quiere comerciar en Internet. Primero sería el caso de buscar o ir a un

sitio web de una empresa para hacer una compra y el segundo caso sería la compra-venta entre particulares que trataremos más adelante.

Cuando está buscando comprar un objecto o servicio a una empresa por Internet (especialmente la primera vez) tenga en cuenta estos consejos generales:

- Investigue la reputación de la empresa a la que compra: busque en Internet el nombre de la empresa o página web junto con las palabras “timo” o “revisión”, “crítica”, “servicio” o similares.
- Revise la garantía del producto y la política de devolución del sitio en el que quiere comprar.
- Signos positivos que indican que un sitio web es serio son por ejemplo: tienen número de teléfono de atención al cliente, señalan su dirección postal real (no una casilla de correos), reseñan la directiva de la empresa con nombres y apellidos, tienen un foro o boletín de mensajes públicos donde puede ver los comentarios de usuarios de los productos que venden. Y al contrario, un sitio web sospechoso es uno que no incluye dirección física, ni teléfono ni nombres de personas.
- Una manera de comprobar que detrás de un sitio web hay una empresa real que responde es llamarles o mandarles un email con cualquier consulta como excusa. De esta forma usted comprueba cómo es su servicio al cliente, por ejemplo cuánto tardan en contestar en el caso de email.
- Use la tarjeta de crédito en vez de una tarjeta

de débito. Muchas tarjetas de crédito ofrecen algún tipo de protección contra compras fraudulentas.

- Tenga en cuenta que dependiendo de la ley en su país, puede ser ilegal hacer efectivo el cargo a su tarjeta de crédito si el producto que compró no ha sido enviado.
- Desconfíe completamente de sitios web que venden cierto tipo de productos que están plagados de timadores, como presuntos "productos milagrosos" para adelgazar o mejorar la salud, páginas que venden productos o libros con "secretos" para hacerse rico de forma rápida o sitios que prometen hacerle ganar mucho dinero trabajando desde casa y similares.

Compra-Venta entre Particulares en Internet

Probablemente desde que ha existido bienes, dinero o economía han existido timadores y timos. Internet no solamente añade un nuevo vehículo para estos timadores para encontrar a sus víctimas sino que es un medio ideal para estos criminales ya que:

- Internet ofrece un gran anonimato a los timadores.
- Muchos de los timadores están basados en países donde es muy difícil perseguir este tipo de delitos desde el país de la víctima.
- Internet ofrece un gran volumen de posibles víctimas a un precio muy bajo (hospedar una página pagina web o abrir una cuenta de email

es muy barato o gratuito).

Muchos timos dependen de las costumbres del país de las víctimas. Un ejemplo típico es un país en el que el uso de cheques de banco personales es común. Un timo que explota esto es cuando la víctima ofrece un servicio a través de Internet como la renta de una casa por ejemplo y el timador manda un email muy interesado haciéndose pasar por una profesión "respetable" como un doctor o profesor universitario residiendo en otro país y ofreciendo todo tipo de facilidades. El timador envía un cheque con más dinero del pactado y entonces pide a la víctima que lo cobre y le envíe la diferencia. Por supuesto el cheque es falso y la víctima pierde el dinero que manda.

Características de timos o señales de peligro:

- Le piden que mande dinero usando Western Union, Moneygram u otro servicio similar de envío de fondos. Los timadores usan estos servicios porque son fáciles para recibir dinero sin tener que dejar un rastro real que les pueda identificar.
- El supuesto vendedor o el producto está en otro país; le ofrecen entrega a domicilio desde otro país.
- Le piden usar un servicio intermediario de pago o le dan garantías de la transacción.
- Le piden un adelanto o parte de pago inicial antes de recibir el producto que compra.
- Le dan un cheque por más valor de lo que usted vende o alquila (arrienda) y le piden que mande la diferencia.

Cómo protegerse:

- Nunca envíe fondos a desconocidos de forma electrónica con Western Union, Moneygram o similar, y menos aún a otros países.
- Realice las transacciones viendo al vendedor y al producto en persona. Desconfíe incluso si habla con el vendedor por teléfono.
- Tenga en cuenta que la página web de anuncios o avisos es simplemente una publicación y no garantiza y no se hace responsable de las transacciones.
- Sepa que si recibe un cheque éste puede ser falso e incluso si lo deposita cuando se descubra que es falso varios días después el banco en muchos casos (dependiendo de la legislación de su país) le hará devolver el dinero.
- No mande nunca información confidencial como números de cuenta bancarias etc.

Use el sentido común para protegerse de timos.
Esté alerta y sea muy escéptico de fantásticas ofertas o sistemas para ganar dinero rápidamente o desde casa que reciba por correos electrónicos; recuerde que si parece demasiado bueno para ser verdad seguramente lo sea.

Medios Sociales

Ha habido un auge reciente de redes sociales como Facebook y Twitter y a medida que un área tecnológica nueva alcanza mayor popularidad lo que ocurre es que se convierte en un objetivo mayor para los ciber-criminales.

Como preocupaciones que introducen los medios sociales podemos señalar:

- Cierta pérdida de privacidad.
- Nuevo punto de entrada para spam, malware y phishing (por ejemplo: los gusanos Koobface y Mikeyy Mooney).
- Peligro de escape de información no autorizada de la empresa o exposición de datos.
- Timos dirigidos (haciéndose pasar por otro etc) y ámbito favorable a la ingeniería social.

Indice