Tu guía para frenar el Cibercrimen

¿Por qué esta guía?

Los ciberataques son una nueva forma de delincuencia online. Gracias al desarrollo de las nuevas tecnologías y a la gran penetración de las mismas en los hogares, han evolucionado y adquirido niveles de peligrosidad inauditos. Los delincuentes han encontrado un auténtico filón en esta modalidad ya que todos los usuarios de Internet somos víctimas potenciales.

El objetivo de esta guía es proporcionar unas pautas básicas para protegerse de los ciberdelincuentes y facilitar al lector una "enciclopedia básica" sobre las última modalidades de riesgo online.

Índice

Cualquier término marcado en negrita está explicado en el glosario que encontrarás al final de esta guía.

1. ¿Cuál es el riesgo?

Al conectar tu PC a Internet, te conviertes automáticamente es un target para los cibercriminales. Así como una casa desprotegida supone un jugoso botín para los ladrones, un PC desprotegido pasa a ser una buena oportunidad para los creadores de malware y para los cibercriminales.

Los ciberataques incluyen virus, gusanos, troyanos, ataques de hackers, *phishing* y mucho más. Todos ellos han alcanzado un nivel de sofisticación nunca visto, y se han duplicado en cantidad. La mayoría de ellos se diseñan para robarte la identidad, utilizar tus datos personales y estafar dinero.

A pesar de esto, y mientras el riesgo de ataques online continúa creciendo, siguiendo las sencillas pautas que te mostramos en esta guía, no hay razón alguna para no disfrutar navegando en Internet de manera completamente segura.

Cibercriminales

Pocos años atrás, los programas malignos se limitaban al "ciber-vandalismo", una forma de expresión antisocial que irrumpía en los PCs causando diversos daños. Pocos de ellos, no obstante, estaban diseñados con este fin, aunque inevitablemente se producían daños colaterales en los archivos o dejaban el equipo inservible. La mayoría de las amenazas en esta época consistían en virus y gusanos.

Hoy en día, por el contrario, la amenaza más grave proviene del llamado cibercrimen. Los criminales se sirven del anonimato que la red otorga para, mediante códigos maliciosos, acceder a los equipos y robar dinero o datos confidenciales como contraseñas, logins, códigos PIN, etc.

Las amenazas del cibercrimen incluyen virus, gusanos, troyanos, ataques de *hackers*, *phishing* y un largo etcétera. Estas amenazas no sólo son cada día más sofisticadas, es que además su número crece exponencialmente. Nuestro laboratorio de virus identifica cada día unas 30.000 nuevas amenazas.

2. Programas maliciosos: consecuencias y tipos

Al igual que cualquier otro software, los programas maliciosos (también conocidos como malware) están diseñados para comportarse de determinada manera y para cumplir con ciertas funciones específicas pero, cómo no, también tienen limitaciones y fallos de programación. Los efectos de estos programas dependen directamente de la intención de su creador.

Algunos virus antiguos estaban diseñados simplemente para expandirse, pero no acarreaban ningún efecto devastador ni "carga explosiva" alguna. Resultaban un incordio o podían suponer cierta pérdida de información, pero ninguno de ellos trataba de robar datos para usos ilegales posteriores.

Hoy en día, las cosas han cambiado: el objetivo más común en todos los programas maliciosos es el robo de información. Hoy en día, la información equivale a dinero y, afortunadamente para los criminales, la red está rebosante de datos e información de todo tipo.

La mayoría de programas maliciosos son instalados en el ordenador sin que el usuario se percate. Por ejemplo, muchos troyanos son designados como *spyware*; son instalados sin que el usuario se percate, y así controlan todos sus movimientos diarios, al tiempo que borran cuidadosamente su rastro con la ayuda de programas llamados *rootkits*. De esta forma, todo parece funcionar correctamente en el ordenador y no hay motivos de sospecha. Una vez alcanzado el ordenador de la víctima, el criminal puede utilizar la información que encuentra como más le convenga. Así, puede por ejemplo robar la personalidad de la víctima y cometer delitos en su nombre, puede robarle dinero de sus cuentas o puede vender sus datos personales a empresas especializadas en Spam. Por supuesto, supone también una forma de tener acceso libre a la lista de contactos de la víctima.

Los programas *spyware* son instalados sin que el usuario se percate y así controlan todos sus movimientos diarios.

Principales tipos de malware:
Ataques Hacker, ataques Phishing, ataques ransomware, rogue dialer, spam

3. Ataques de Hackers

Las aplicaciones actuales son muy complejas y se componen de cientos de líneas de códigos. Están, al fin y al cabo, diseñados por humanos y, por lo tanto, no son infalibles. Los *hackers* aprovechan estos agujeros en los sistemas de seguridad para introducirse en los equipos y lanzar así sus programas maliciosos.

El término "*hacker*" se utilizaba antiguamente para describir a un excelente programador. Actualmente, se aplica a aquellos que quiebran los sistemas de seguridad para introducirse y adueñarse de ellos. Serían comparables con un ladrón electrónico.

Habitualmente los hackers se introducen tanto en los ordenadores personales como en las grandes redes para instalar allí programas maliciosos que les sirven para robar información o expandir spam. También podrían inundar el servidor web de otra compañía con tráfico de red. Por ejemplo, los ataques *DoS* (denegación de servicio) que son diseñados para inutilizar las páginas Web y dañar el negocio de las compañías.

Está claro que los cibercriminales aspiran a rentabilizar el tiempo que dedican y el esfuerzo que ponen en sus actividades delictivas, por lo que intentan hacer blanco en los sistemas más grandes y extendidos. Así, por ejemplo, los hackers se centran sobre todo en los sistemas Windows®, ya que son los más utilizados en todo el mundo.

Los hackers son como ladrones electrónicos; utilizan cualquier agujero o debilidad en los programas para introducirse en tu ordenador.

¿Cómo puedo protegerme de los códigos maliciosos y de los ataques de los hackers?
Existen varios pasos que puedes dar para protegerte tu ordenador de las amenazas cibernéticas actuales. Siguiendo estas simples guías lograrás minimizar los riesgos de ataque:

- Protege tu ordenador instalando un programa de seguridad en Internet.
- Actualízalo regularmente (al menos una vez al día)

- Instala refuerzos de seguridad en tus aplicaciones y en tu sistema operativo. Si utilizas Windows® , simplemente activa la opción de actualización automática. Y no olvides actualizar también tus aplicaciones Microsoft® Office.
- No abras e-mails con archivos adjuntos (documentos Word, hojas Excel, archivos EXE, etc.). En caso de no conocer al remitente o no esperar el correo, no abras este tipo de archivos, y no abras NUNCA los archivos adjuntos de los e-mails no solicitados ni los *links* de los mensajes instantáneos.
- Utiliza la cuenta de administrador en tu ordenador sólo en caso de que necesites instalar un software o hacer cambios en el sistema. Para el uso diario, crea una cuenta separada con derechos de acceso limitados (esto se puede ejecutar en el panel de control). Así limitarás el acceso a tu sistema de datos a todos los programas maliciosos.
- Almacena tus datos de manera regular en un CD, DVD o en un USB externo. En caso de que tus archivos hayan sido dañados, siempre podrás recuperarlos a través de estos dispositivos.

4. ¿Qué es el phishing?

El phishing está diseñado para robar tu identidad, adueñarse de tus datos personales y estafar tu propio dinero o el de terceras personas.

Muy a menudo, los cibercriminales envían a sus víctimas e-mails que contienen *links*. Estos links redirigen a las víctimas a sitios web falsos o trucados en los que, habitualmente, el usuario necesita y rellenar distintos campos con información personal. La víctima confía en que la página web es legal y no tiene intenciones fraudulentas y, sin embargo, está facilitando sus datos personales a expertos informáticos que sabrán sacar muy buen provecho de esta oportunidad que la victima les ofrece.

Un tipo de ataque phishing muy habitual ocurre cuando, a través de estos links falsos, se le redirige a la víctima a una página Web que imita la Web de su entidad bancaria (reproduce fielmente el aspecto físico de la Web de la entidad bancaria, haciendo uso de su mismo logo y su estilo, y utilizando un URL que se asemeja a la dirección real del banco). Una vez que la víctima introduce su contraseña y sus datos para acceder a su cuenta bancaria, el cibercriminal recoge esta información para, acto seguido, robar dinero y realizar otros actos delictivos.

Los cibercriminales envían una cantidad masiva de e-mails a direcciones de correo aleatorias. Lógicamente, no todos los destinatarios de estos email son clientes del banco en cuestión o se ven interesados por la información que ofrece el correo. Sin embargo, un pequeño porcentaje de los mismos cae en la trampa. Es aquí donde estos criminales encuentran su nicho perfecto para delinquir.

Habitualmente, los delincuentes inventan una razón falsa para enviar el email y para preguntar por tus datos personales. Puede que aleguen una inspección de seguridad del banco, o que el banco ha realizado cambios en el sistema y necesita que cada cliente confirme su identidad…

Normalmente, los cibercriminales van retirando cantidades pequeñas de dinero que no levantan sospechas. No obstante, dado que, lamentablemente, juegan con muchas víctimas al mismo tiempo, las cantidades que finalmente consiguen estafar suelen ser cuantiosas.

Los e-mail de *phishing* pretenden hacer creer a la víctima que son mensajes procedentes de su entidad bancaria. Por norma general, incluyen un link que remite directamente a una página Web falsa del banco e intentan hacer que, mediante engaños, la víctima introduzca sus datos personales.

¿Cómo puedo auto protegerme del phishing?

- Es altamente improbable que tu banco te pida información personal a través de un email. Por lo tanto, nunca reveles información confidencial mediante por esa vía.
- No hagas clic en los links que te lleguen a través de correo electrónico, ya que los criminales pueden esconder una dirección URL falsa tras la apariencia de una dirección legítima. La opción más segura es escribir tú mismo la dirección del link en tu navegador, aunque también puedes optar por configurar tu correo para leer simplemente texto corriente y rechazar los links.
- No rellenes nunca un formulario que haya llegado a tus manos a través de un e-mail. Asegúrate que procuras esta información en páginas seguras. Comprueba que la dirección URL comienza con un "https" y fíjate que en la parte inferior derecha de la página hay un símbolo de un candado cerrado. Al pinchar en este candado, aparecerá una dirección de URL que tiene que coincidir con la dirección en la que estás. Si tienes alguna duda al respecto, ponte en contacto con tu banco para asegurarte.
- Revisa de manera regular todas tus cuentas bancarias para comprobar que puedes responder de todas y cada una de las transacciones especificadas. En caso de sospecha, ponte inmediatamente en contacto con tu banco.
- Sospecha de todos los correos que lleguen a tu buzón desde una supuesta entidad bancaria.
- Sospecha de todos los correos que lleguen a tu buzón y que estén dirigidos a más destinatarios.
- Sospecha de todos los correos que lleguen a tu buzón y que contengan faltas de ortografía, sintaxis o gramática.

Para protegerte de los ataques de *phishing*

- No hagas clic en los *links* de los e-mails
- Introduce información sólo en páginas Web seguras
- Revisa tus cuentas bancarias con regularidad
- Ten en mente las características típicas de los email phishing
  - No ser el único destinatario.
  - Faltas de ortografía o fallos gramaticales.
- Sigue las instrucciones mencionadas sobre cómo evitar ataques de *hackers* y sobre cómo protegerte de códigos maliciosos.

5. Ataques ransomware

Algunos cibercriminales utilizan programas ***ransomware*** para robar dinero a sus víctimas. Mediante estos programas, los criminales encriptan los datos de las víctimas y, más tarde,

muestran a la víctima una manera de contactar con ellos para pedir un rescate a cambio de la normalización de su sistema. Es decir, la víctima sufre un chantaje clásico.

Algunos cibercriminales utilizan programas *ransomware* encripter tus datos y, más tarde, pedir un rescate a cambio de la normalización de tu sistema.

¿Cómo puedo auto protegerme de los programas *ransomware*?

- Guarda tu información en distintos dispositivos. Kaspersky Lab ha diseñado sus programas *anti-malware* para desencriptar información y desmantelar así los planes de los cibercriminales. Pero los criminales están haciendo sus programas cada vez más sofisticados y difíciles de desarmar. La opción más segura será siempre ser precavido y guardar tu información en dispositivos seguros.
- No pagues NUNCA un rescate a los cibercriminales. Si no tienes tu información guardada a salvo, contacta con tu empresa de antivirus para que ellos te asesoren.

Para protegerte de los ransomware

- Copia tu información en dispositivos seguros
- No pagues nunca los rescates que te pidan
- Sigue los consejos especificados arriba para protegerte

6. Ataques Rogue Dialer

Rogue dialer son programas maliciosos que, a la hora de conectarte a internet, transfieren la llamada y, en vez de utilizar tu número de teléfono habitual, te conectan a través de un número de teléfono de pago.

Estos programas se instalan sin tu consentimiento y operan de forma oculta. Así, la primera noticia de que algo extraño ocurre llega con una factura de teléfono más grande de lo normal. Esta factura incluirá números “Premium" a los que tú, obviamente, no recordarás haber llamado nunca.

Pero los *rogue dialer* tan sólo tienen como víctimas a la gente que utiliza la línea de teléfono para conectarse a Internet. Si decides cambiar tu línea de teléfono por la banda ancha, comprueba que desconectas el cable del módem y que eliminas de tu escritorio cualquier icono referente a la conexión telefónica.

Si en el futuro necesitaras de nuevo una conexión telefónica, bastará con conectar de nuevo el cable del módem al teléfono.

Los *rogue dialers* “hackean” el modem de tu ordenador para cambiar el número de teléfono desde el que te conectas a Internet.

¿Cómo puedo autoprotegerme de los *rogue dialers*?

Deberías seguir los consejos para protegerte de los códigos y programas maliciosos y de los ataques de *hackers*. Por otro lado, contacta con tu proveedor de línea telefónica y pide que prohíba llamadas desde tu teléfono a números de que comiencen por “90x”, “80x”... los típicos teléfonos de alto coste.

Para protegerte de los *rogue dialers*

- Prohíbe las llamadas a números que comienzan por “90x”, “80x”, etc.
- Desconecta tu módem si te pasas a una línea ancha

7. ¿Qué es el Spam?

El Spam es un conjunto de e-mails anónimos. Es el equivalente electrónico de la propaganda clásica que llega a través del correo ordinario. El Spam supone aproximadamente entre el 70% y 80% de todo el volumen de e-mails enviados.

El spam se utiliza para anunciar productos y servicios. Los *spammers* envían e-mails de manera masiva y consiguen dinero a través de la gente que se pone en contacto con ellos interesándose por sus productos o servicios. A pesar de que el porcentaje de personas que contestan es muy bajo, suponen un número suficiente para obtener beneficios.

Resulta una tarea farragosa buscar entre el spam los correos que realmente te interesan. Además, existe otro punto a tener en cuenta; el spam puede acarrear programas maliciosos que perjudiquen tu sistema, o links que te remitan a páginas falsas con la intención de cometer una estafa.

Los *spammers* utilizan programas de tipo botnet para distribuir sus e-mails. Estos “botnets” son programas maliciosos que sirven para robar direcciones, de forma que las víctimas no son conscientes de que los hackers pueden controlar su sistema a distancia para utilizarlo como plataforma para enviar spam a otros usuarios. Utilizando un software de seguridad adecuado, estos riesgos pueden ser minimizados.

El spam supone una pérdida de tiempo y satura tu buzón de correo. Además, puede distribuir códigos maliciosos.

¿Cómo puedo autoprotegerme del spam?

- No respondas a los e-mails spam. Los *spammers* verifican quién ha respondido en alguna ocasión a este tipo de correos, por lo que contestar, aunque sea una sola vez, tan sólo hace aumentar el riesgo de recibir más spam.
- No hagas clic en los links que se adjuntan en este tipo de correos. Esto confirmaría que tu cuenta de correo es una cuenta activa, e incrementaría el riesgo de recibir más spam en el futuro.
- Utiliza más de una dirección de correo. Mantén una cuenta para tu correo personal y otra cuenta distinta para los foros públicos, los chats y otras Webs públicas. De esta forma, si empezaras a recibir mucho correo spam, podrías eliminar la cuenta sin perder tus contactos personales.
- Crea una dirección de correo privada difícil de deducir. Los *spammers* hacen combinaciones de nombres y números comunes para lograr deducir las direcciones. Sé creativo y evita utilizar tu nombre y apellido.
- Evita publicar tu dirección en cualquier página pública. Si no te queda más remedio, escríbela de la siguiente manera; ‘juan-punto-perez-arroba–midominio-punto-com’, en vez de ‘juan.perez@midominio.com’-

Para reducir la cantidad de spam que recibes

- No respondas a los e-mails spam
- No hagas clic en los links adjuntos
- Utiliza distintas cuentas de correo
- No escribas tu dirección de correo en páginas públicas
- Sigue las instrucciones de arriba sobre cómo protegerte de los programas maliciosos

8. ¿Cómo puedo proteger mi red inalámbrica?

La mayoría de los ordenadores actuales permiten la conexión internet por *WiFi* (sin cables), de manera que puedes utilizar tu ordenador en cualquier lugar de la casa o de la oficina. Sin embargo, este método acarrea numerosos riesgos de los que debes protegerte.

1. Un *hacker* podría interceptar cualquier información que recibas o envíes.
2. Un *hacker* podría tener acceso a tu red *wireless*.
3. Otra persona podría *hackear* tu acceso a Internet.

Si tu red inalámbrica no es segura, un *hacker* puede interceptar tus datos, acceder a tu red y utilizar tu conexión para conectarse a Internet

Existen unos simples pasos para asegurar tu dispositivo *wireless* y minimizar los riesgos.

- Cambia la contraseña del administrador de tu router. Es muy sencillo para un hacker localizar los routers sin contraseña y utilizarlos para acceder a Internet. Procura elegir una contraseña difícil de deducir (más abajo encontrarás una guía sobre cómo escoger contraseña).
- Utiliza la encriptación: la encriptación WPA es la mejor opción.
- Desactiva la línea de banda ancha SSID y evita así que tu dispositivo “anuncie” su existencia.
- Cambia el nombre de tu dispositivo SSID, ya que resulta sencillo de deducir el nombre asignado desde fábrica.
- A la hora de comprar un router, escoge uno que admita NAT. Esto ocultará tu presencia y hará más difícil el ataque a los hackers.

Para proteger tu red inalámbrica
- Cambia la contraseña del administrador
- Activa la encriptación
- Desactiva el SSID y cambia el nombre de tu router
- Sigue las instrucciones que se explican más arriba sobre cómo evitar ataques *hacker*.

9. ¿Por qué resultan importantes las contraseñas?

Una manera importante de salvaguardar información confidencial es a través del uso de contraseñas de acceso.

A medida que el uso de Internet va extendiéndose, estas medidas van cobrando importancia. Cada día el número de usuarios de Internet va creciendo y, lógicamente, se utiliza para diferentes actividades incluyendo banca online, compra online y búsquedas online. Asimismo, cada vez más utilizamos la red para socializarnos. En los últimos años, ha habido un crecimiento

masivo de páginas sociales como Facebook, MySpace, etc. Aquí compartimos todo tipo de información personal como fotos, afinidades, vídeos y mucho más.

Lamentablemente, cuanta más información personal facilitemos, más expuestos quedaremos ante los ladrones de identidad, que roban tu información personal y cometen actos delictivos en tu nombre. Un cibercriminal podría abrir una cuenta bancaria en tu nombre, obtener una tarjeta de crédito o un carné de conducir. O, simplemente, podría robar dinero de tu cuenta.

Por todo ello, es muy importante proteger tus cuentas online con contraseñas seguras.

Las contraseñas te ayudan a mantenerte a salvo de los ladrones de identidad. Las contraseñas han de servir para impedir a los hackers acceder a tu cuenta bancaria y defraudar dinero.

¿Cómo escoger una buena contraseña?

Al escoger una contraseña "débil" (muy elemental o fácil de averiguar), el riesgo de convertirse en víctima del cibercrimen se incrementa.

- Escoge una contraseña fácil de recordar para que no te resulte necesario escribirla en alguna de tus carpetas del PC (recuerda que estas carpetas pueden ser robadas por los cibercriminales).
- No digas tu contraseña a nadie. En caso de que alguna organización se ponga en contacto contigo mediante una llamada, no reveles tu contraseña ni siquiera en caso de que te la pidan. Recuerda que no sabes quién se encuentra al otro lado del teléfono.
- Si una Web te envía por e-mail una contraseña para entrar en su sistema por primera vez, no olvides cambiarla una vez que hayas entrado.
- No utilicen contraseñas obvias como tu nombre, el nombre de tu pareja, de tus hijos...
- No utilices palabras reales que un hacker podría encontrar en el diccionario.
- Combina letras mayúsculas y minúsculas, números y letras.
- En caso de que se te permita, utiliza una frase como contraseña en vez de una sola palabra.
- No utilices la misma contraseña para varias cuentas.
- No utilices la palabra contraseña (por ejemplo, "contraseña1", "contraseña2", etc.)
- Comprueba que tu software de seguridad en Internet bloquea los intentos de robo de contraseña.

Para escoger contraseña

- Crea contraseñas fáciles de recordar, para no tener que escribirlas
- Mantenlas en secreto
- Mezcla minúsculas, mayúsculas, números y letras
- No utilices la misma contraseña para distintas cuentas
- No utilices la palabra "contraseña" como contraseña
- Sigue las instrucciones especificadas arriba sobre cómo evitar ataques hackers y códigos maliciosos.

10. ¿Cómo puedo ayudar a mis hijos a navegar por la red de manera segura?

Primero, reflexiona sobre los posibles riesgos a los que se exponen. Incluyendo los siguientes:

1. Virus que se instalan en el equipo a través de las descargas.
2. Los riesgos de infección a través de peer-to-peer (P2P). Programas en los que se comparten archivos y que permiten a otros usuarios acceder a tu ordenador.
3. Publicidad no deseada (*pop ups*, programas adware que se instalan automáticamente a través de programas sin protección disponibles en la red).
4. Contenidos de sexo explícito u otros contenidos no apropiados
5. Los niños pueden caer en la trampa y revelar información confidencial
6. Los niños pueden bajar de la red material pirateado
7. Los niños pueden caer en la trampa y revelar información confidencial de los padres
8. Los niños pueden contactar con pedófilos en la red.

Los niños son tan vulnerables en la red como en la vida real. Es importante comprender los riesgos y protegerles de la mejor forma.

Aquí se muestran unas pautas que pueden seguirse para minimizar los peligros.

- Explica a tus hijos los peligros de la red
- Instala tu PC en un lugar de la casa común a todos los miembros de la familia
- Habla con tus hijos sobre las experiencias que obtienen de la red
- Llegar a un acuerdo común y establecer una guía de normas de uso de Internet. Aquí encontrarás una serie de factores que cabría tener en cuenta
- Restringe el acceso a determinados contenidos desde el ordenador.
    - ¿Pueden tus hijos registrarse en redes sociales o en otras websites?
    - ¿Pueden hacer compras *on line*?
    - ¿Pueden utilizar programas de mensajes instantáneos? Si la respuesta es afirmativa, asegúrate de que tengan claro que no pueden hablar con desconocidos.
    - ¿Pueden visitar *chats*?
    - ¿Pueden bajar música, vídeos u otros programas?
- Restringe el acceso a determinados contenidos desde el ordenador. Muchas soluciones de seguridad en Internet permite esta opción.
- Sigue las instrucciones explicadas arriba para protegerte a ti mismo y a tus hijos de programas maliciosos y ataques hackers.

Para proteger a tus hijos en la red

- Explícales los peligros de la red
- Mantén el ordenador en un lugar común de la casa
- Anima a tu hijos a hablar de sus experiencias en la red
- Establece unas normas de uso de Internet
- Restringe los contenidos a los que tus hijos no pueden tener acceso

11. ¿Qué debo hacer si mi ordenador ha sido comprometido?

No es siempre fácil saber si tu ordenador ha sido comprometido. Ahora más que nunca, los autores de virus, de gusanos, de troyanos y de *spyware* están especializados para ocultar su rastro. Por este motivo es esencial seguir los consejos que se especifican en esta guía. Resulta fundamental instalar un software de seguridad, instalar los parches de refuerzo a tu sistema operativo y guardar tu información en dispositivos diferentes.

Es complicado mostrar una lista de símbolos característicos que ayudan a distinguir un ordenador comprometido, ya que los mismos símbolos pueden producirse por problemas en el hardware o en el software. Aquí mostramos algunos ejemplos:

- Tu ordenador se comporta de manera extraña haciendo cosas nunca vistas antes
- Encuentras mensajes o imágenes inesperadas
- El programa se inicia de forma inesperada
- Tu *firewall* te avisa de que una de tus aplicaciones ha intentado conectarse a Internet sin tu consentimiento
- Tus amigos te comentan que han recibido desde tu dirección mensajes que tú no has enviado
- Tu ordenador se "cuelga" habitualmente o los programas se ralentizan constantemente.
- Encuentras muchos mensajes de error del sistema
- Tus archivos y carpetas cambian o se eliminan
- Encuentras un acceso del disco duro cuando no hay ningún programa trabajando
- Tu buscador se comporta de forma errática; por ejemplo no te deja cerrar la pantalla

Puede que estés ante un problema de hardware o software, más que ante un virus o programa maligno. Esto es lo que te aconsejamos que hagas.

- Desconecta tu ordenador de Internet.
- Si tu ordenador está conectado a una red de área local, desconéctalo de la red.
- Si tu sistema operativo no se carga, enciende el ordenado de manera segura (enciende el ordenador, presiona la tecla F8 y selecciona la opción "modo seguro" del menú), o utiliza un CD de recuperación.
- Guarda tu información en un dispositivo seguro.
- Asegúrate de que tus antivirus estén actualizados. A ser posible, no actualices el antivirus desde el equipo que crees podría estar comprometido. Esto es importante ya que si tu ordenador está infectado y te conectas a la red, el código maligno podría enviar información privada desde tu ordenador a un criminal localizado en otro lugar.
- Escanea todo el ordenador.
- Si encuentras un programa malicioso, sigue los pasos que se indican en la guía que te facilita tu proveedor. Los buenos programas de seguridad dan la opción de desinfectar los objetos infectados y poner en cuarentena los objetos que podrían estar infectados. Además, suelen crear también un informe de daños.
- Si tu software de seguridad en la red no detecta ninguna infección, probablemente tendrás tu equipo a salvo.
- Si tienes cualquier problema a la hora de borrar programas maliciosos, consulta la página Web de tu vendedor.
- En caso de que sea necesario, contacta con el soporte técnico de tu vendedor para que te aconsejen. También puedes enviarles una muestra para que analicen tu problema.

Si crees que podrías estar infectado

- Que no cunda el pánico
- Desconecta tu ordenador de la red
- Haz una copia de seguridad de tu información
- Actualiza tu antivirus
- Escanea tu ordenador
- Si no se detecta ninguna infección, comprueba tu hardware y tu software
- Si aún sigues teniendo problemas, contacta con tu proveedor

Nota final sobre los robos de identidad

Recuerda que la seguridad offline es también importante. Los datos físicos pueden ser usados por los criminales para acceder a tus cuentas. Destruye los documentos que contengan información personal antes de deshacerte de ellos.

Glosario de términos

ADWARE
Término aplicado a los programas que envían publicidad (*pop-ups* o banners) o que redirigen búsquedas específicas a páginas Web promocionales. Los *adware* se construyen a menudo en programas sin protección como el freeware o el shareware. Si descargas un programa freeware, el adware se instala en tu sistema sin tu consentimiento. En ocasiones, un troyano podría descargarse oculto en un adware e instalarse en tu ordenador. Si tu navegador no está actualizado y contiene debilidades, los hackers (en este caso, conocidos como *browser hijackers*) podrían instalar un adware en tu ordenador sin que te des cuenta, así como formatear tu buscador para redirigirte a otras páginas como, por ejemplo, Webs de pago o pornográficas.

Normalmente, los programas adware no son fácilmente visibles en el sistema, y rara vez disponen de un procedimiento de desinstalación. Intentar quitarlos manualmente, podría provocar fallos en el sistema.

BOTNET
Este término se refiere a las network controladas por los cibercriminales utilizando Troyanos o programas maliciosos.

CHAT ROOM
Esta es una manera de comunicación online a tiempo real. Lo único que necesitas hacer es teclear tu mensaje. Tal y como indica su propio nombre, cualquiera puede introducirse en la conversación.

CRIMEWARE
Cualquier programa malicioso utilizado por los cibercriminales para robar dinero.

CIBERCRIMEN
El término “Crimen” se refiere a todo acto ilegal. El cibercrimen es todo acto ilegal que implique el uso de un ordenador.

DoS (*DENIAL-OF-SERVICE*)
El ataque de un Denial-of-Service (DoS) se diseña para dificultar o eliminar el normal funcionamiento de una Web o de un servidor. Existen varios métodos utilizados por los hackers para conseguir esto. Un método común es inundar el servidor de envíos, de manera que no pueda procesarlos todos y termine quebrando el sistema.

El ataque de un Denial-of-Service se realiza a través de varias máquinas. Los *hackers* utilizan una máquina central llamada “master” que coordina el ataque a través de otras máquinas llamadas “zombie”. Tanto los master como los zombies trabajan para quebrar la seguridad del ordenador e instalar en él troyanos o códigos maliciosos.

DRIVE-BY DOWNLOAD
Con un drive-by download serás infectado visitando una simple página Web. Los cibercriminales buscan por toda la red las páginas más vulnerables para insertar en ellas sus códigos maliciosos. Si tu sistema operativo o una de tus aplicaciones no están debidamente protegidos,

al entrar en una de estas páginas infectadas se descargará un programa malicioso directamente a tu ordenador.

GUSANO
Los gusanos son considerados derivados de los virus, pero con algunas importantes diferencias. Un gusano es un programa maligno que se replica y se expande a otros ordenadores, pero que no infecta otros archivos. En su lugar, se instala en un ordenador y busca la vía para extenderse a otros equipos. En el caso de los virus, cuanto más tiempo resista oculto, más daños causará en los archivos del ordenador. Sin embargo, los gusanos crean un solo ejemplo de su código que no se extiende a archivos en el mismo ordenador.

HACKER
Este término se solía utilizar para describir los programadores de talento. Hoy en día, hace referencia a personas que trabajan para quebrar la seguridad de los sistemas y adueñarse de los mismos.

INSTANT MESSAGING (MENSAJERÍA INSTANTÁNEA)
Los programas de mensajería instantánea ofrecen un sistema de comunicación a tiempo real con personas que se encuentran en tu lista de contactos.

INTERNET
Internet es un sistema global que conecta ordenadores alrededor del mundo. Internet desbordó su red de origen ARPANET. Esta fue construida en 1969 por la Agencia Gubernamental de los Estado Unidos ARPA para conectar ordenadores con fines de investigación. Hoy en día, Internet está compuesto por una cantidad incontable de ordenadores alrededor del mundo que se conectan utilizando una infraestructura pública de telecomunicaciones. La estructura conjunta es TCP/IP (Transmission Control Protocol/Internet Protocol): el TCP divide la información en dos partes para transmitirlo a través de Internet y volver a reconstruirlo al otro lado de la línea. La IP direcciona la información a la dirección correcta.

IDENTITY THEFT (ROBO DE IDENTIDAD)
El robo de identidad se da cuando un criminal roba información privada y confidencial y la utiliza para cometer crímenes en nombre de otra persona. El criminal podría abrir una cuenta bancaria, obtener una tarjeta de crédito, licencia de conducción o un pasaporte. O podrían simplemente robar dinero de tu cuenta bancaria.

ISP
Un ISP (Internet Service Provider) proporciona acceso a Internet a empresas y particulares. El ISP posee lo que conoce como “punto de presencia” en Internet. Todos los ISP tienen la infraestructura necesaria para proporcionar a distintos usuarios acceso a Internet y una dirección IP. Algunos ISP dependen en la estructura de algún proveedor de telefonía, aunque, otros, tienen sus propias líneas.

KEYLOGGER
Son programas que graban contraseñas y que son utilizados por los hackers para obtener información confidencial (códigos PIN, contraseñas, números de tarjetas de crédito…) Los troyanos, habitualmente tienen un *keylogger* integrado.

MALWARE
Es la abreviatura de "*malicious software*". El término describe cualquier programa creado para realizar una acción ilegal y, casi siempre, dañina. Virus, troyanos y gusanos, son todos ellos ejemplos de malware.

PEER-TO-PEER
Hace referencia a una conexión temporal entre diferentes personas con la misma aplicación. Esto les permite compartir la información que cada uno tenga en su ordenador (música, fotos, vídeos…)

PHISHING
Es un tipo muy específico de cibercrimen, diseñado para robar información financiera personal. Los criminales crean una Web falsa reproduciendo la imagen de la de un banco o de cualquier otra página en la que se realicen transacciones económicas. Mediante engaños, hacen que la víctima llegue hasta la Web falsa y que introduzca su contraseña o su PIN. Por norma general, los cibercriminales envían una gran cantidad de e-mails a fin de aumentar la posibilidad de éxito en su estafa.

RANSOMWARE
Código malicioso usado por los criminales para robar dinero mediante la extorsión. Los virus, troyanos o los gusanos encriptan la información haciéndola inservible. Después, los criminales muestran a la víctima cómo ponerse en contacto con ellos para pedir un rescate.

ROGUE DIALER
Programas maliciosos que, a la hora de conectarte a internet, transfieren la llamada y, en vez de utilizar tu número de teléfono habitual, se conectan mediante un número de teléfono de pago. Estos programas se instalan sin tu consentimiento y operan de forma oculta. Así, la primera noticia de que algo extraño ocurre llega con una factura de teléfono más grande de lo normal.

ROOTKIT
Programas que ayudan a los hackers a evadir los sistemas de seguridad de los ordenadores que quieren hackear. Los *rootkits* son utilizados para ocultar las actividades de los troyanos. El hecho de que muchos usuarios entren en sus sistemas directamente desde la cuenta de administrador, sin crear una cuenta privada propia, facilita mucho el trabajo a los criminales.

SPAM
Es un correo masivo anónimo. El equivalente a la propaganda en el correo ordinario.

SPYWARE
Es un software diseñado recoger tus datos personales y enviarlos a terceras personas sin tu consentimiento o conocimiento. Además de robarte información privada, el spyware afecta inevitablemente al correcto funcionamiento de tu ordenador.

TROYANO
Este término hace referencia al caballo de madera que los griegos utilizaron para entrar en la ciudad de Troya y conquistarla. En el mundo informático, hace referencia a un programa con apariencia legítima que, sin embargo, tiene fines dañinos. Los troyanos, a diferencia de los virus y los gusanos, pueden extenderse por sí solos. Existen distintos tipos de troyanos aunque los

más comunes son los *backdoor*, *Trojan Spies*, ladrones de contraseñas y *Troyanos Proxies* (que convierten tu ordenador en una base de distribución de spam).

VIRUS
Un término utilizado para hacer referencia a cualquier tipo de programa malicioso.
Estrictamente, el virus es un programa malicioso que puede autocopiarse tanto en el ordenador como en otros dispositivos.
VULNERABILIDAD
El término se utiliza para describir un fallo e seguridad en el sistema que permite a los hackers introducirse en tu ordenador. Una vez que se identifica la vulnerabilidad del sistema, el creador del sistema procura crear un refuerzo para paliar esa debilidad. De esta manera, los creadores de sistemas lícitos y los hackers están en constante competición para ver quién puede encontrar las debilidades antes.

WORLD WIDE WEB
La World Wide Web (WWW, en su forma abreviada) es el sistema que facilita el acceso a toda la información disponible en Internet. Expone los datos de forma gráfica y permite buscarlos de manera más sencilla y rápida.

La World Wide Web fue desarrollada por Tim Berners-Lee, un consultor de software británico con cuya idea se desarrollaron los estándares que permitían compartir datos a través de Internet. Berners-Lee diseño, por ejemplo, el sistema de direcciones (URL, o Universal Resource Locator) para ubicar y hacer accessible el contenido, y creó el protocolo de hipertexto (HTTP, Hypertext Transfer Protocol) como el estándar para desarrollar y transferir los contenidos.

La Word Wide Web apareció, tal y como lo conocemos hoy, en 1991, y ha continuado creciendo de manera masiva desde entonces hasta la actualidad.

Enlaces de interés

www.kaspersky.es
www.viruslist.com/sp
www.getsafeonline.org
www.identitytheft.org.uk
www.banksafeonline.org.uk
www.cardwatch.org.uk
www.antiphishing.org

Acerca de Kaspersky Lab:
Kaspersky Lab desarrolla la protección más inmediata contra amenazas a la seguridad informática, incluyendo virus, programas espía, fraudes cibernéticos, ataques de hackers, robo de información confidencial y correo spam. Los productos de Kaspersky Lab ofrecen a usuarios particulares, PYMES, grandes corporaciones y al entorno de la informática móvil, los más altos niveles de detección y el tiempo más rápido de respuesta a brotes maliciosos.

La tecnología de Kaspersky ® también se integra también como parte de otros productos y servicios de proveedores líderes de soluciones informáticas de seguridad.
Para obtener más información, visite www.kaspersky.es . Para obtener información más reciente sobre antivirus, antiespías, antispam y otras amenazas informáticas, además de las últimas tendencias, visite http://www.viruslist.com/es

Para más información, contactar con:

PRISMA Comunicación
Marga Suárez
Tel. +34 91 357 19 84
Fax +34 91 357 19 85
marga.suarez@prismacomunicacion.com

Kaspersky Lab Iberia
Vanessa González
Directora de Marketing
Tel. +34 91 398 37 52
vanessa.gonzalez@kaspersky.es