Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación

con vos en la web

GUÍA DE AMENAZAS

Las diez amenazas más peligrosas de Internet

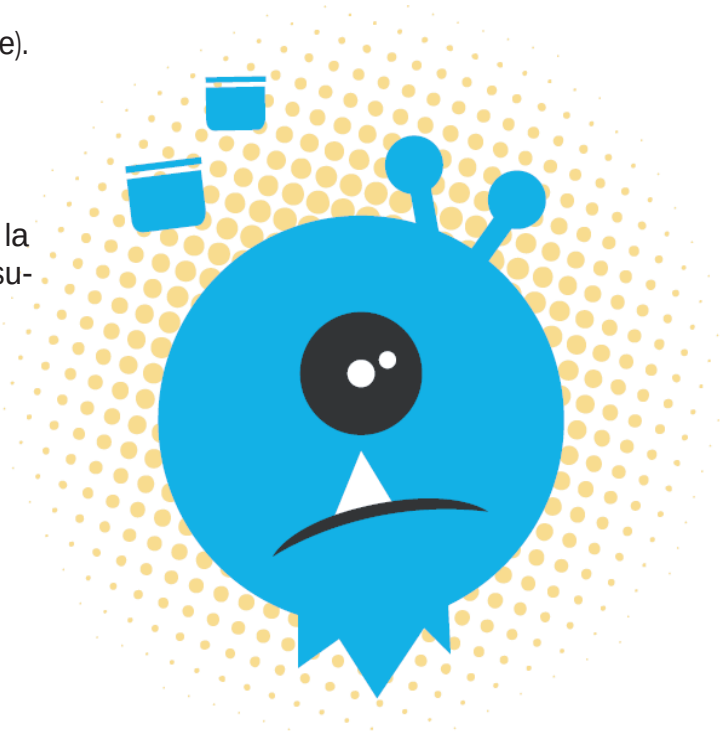
con vos en la web

Las diez amenazas más peligrosas de Internet

Botnet

Su accionar consiste en formar una red o grupo de computadoras zombis (infectados con malware), que son controlados por el propietario de los bots (atacante). Es decir, toman control de equipos y los convierten en zombis, pudiendo así propagar virus y generar spam.

Ésta última práctica es la más habitual de un botnet (enviar spam a direcciones de correo electrónico para la descarga de ficheros que ocupan gran espacio y consumen gran ancho de banda).



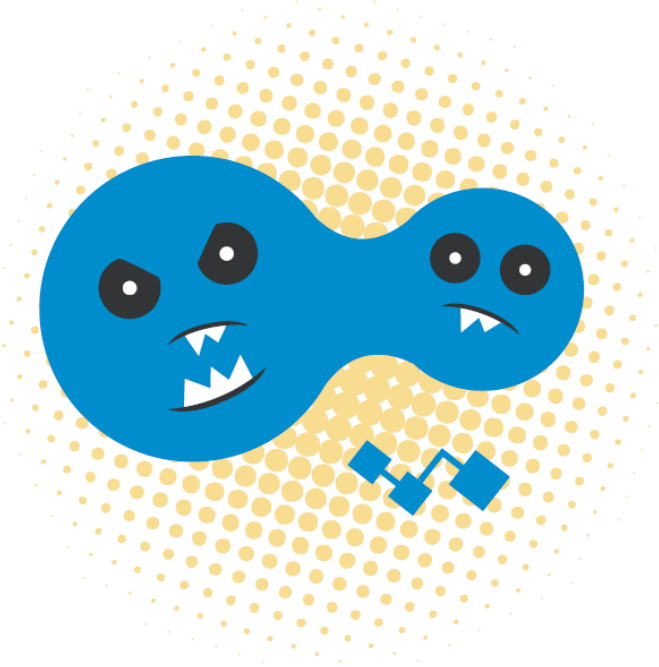
Consejos para prevenir la amenaza:

1. Mantener las actualizaciones
2. Disponer de un firewall y un antivirus
3. Instalar programas que sólo provengan de fuentes fiables
4. Ocultar nuestra IP (Navegar de forma anónima)

con vos en la web

Las diez amenazas más peligrosas de Internet

Gusanos



Un gusano (o Worms en inglés) es un malware que tiene la propiedad de duplicarse a sí mismo. Utiliza las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Los Gusanos son capaces de trasladarse a través de redes de computadores con el fin de realizar una actividad concreta incorporada en su código. Aunque su finalidad no tiene en principio generar daños en la PC, estos programas pueden instalar un virus, instalar un programa que actúe en segundo plano sin conocimiento del usuario.

Consejos para prevenir la amenaza:

1. Es importante que el usuario no instale un software que no proceda de una fuente fiable, así debe solamente utilizar los servicios de descarga del fabricante o los sitios autorizados por el mismo para la obtención de nuevas versiones y actualizaciones.

2. Actualizar el antivirus, software de seguridad y Sistemas Operativos periódicamente.

3. No abrir correos electrónicos de desconocidos. Podrían contener enlaces o archivos nocivos para la PC.

con vos en la web

Las diez amenazas más peligrosas de Internet

Keyloggers

Es un tipo de software que registra cada tecla que presionamos en el teclado, para posteriormente guardarlas en un archivo y/o enviarlas a través internet.

Permite a quien utiliza esta herramienta tener acceso a información importante de otros usuarios (como ser contraseñas, números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener).

Aplicaciones que realizan keylogging pueden ser distribuidas a través de un troyano o como parte de un virus o gusano informático.

Consejos para prevenir la amenaza:

1. Instalar un programa anti-spyware. Los programas Anti-spyware pueden detectar diversos keyloggers y limpiarlos.

2. Habilitar un cortafuegos o firewall puede resguardar el sistema del usuario, no solo del ataque de keyloggers, sino que también puede prevenir la descarga de archivos sospechosos, troyanos, virus, y otros tipos de malware.

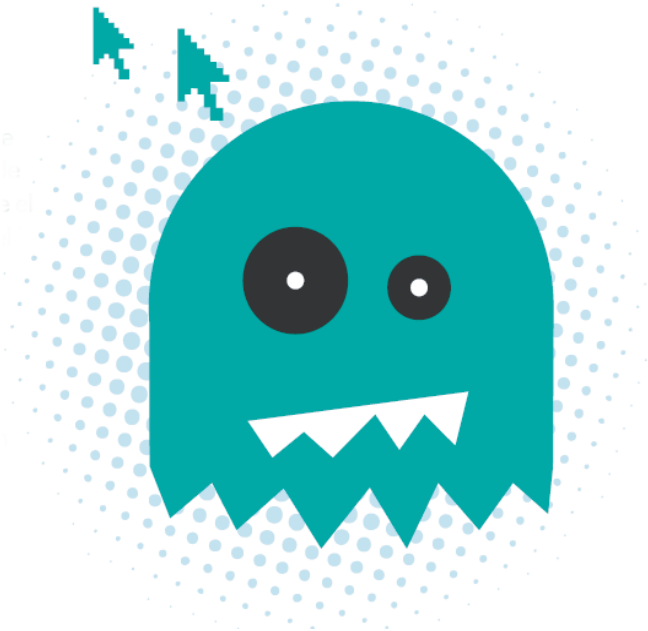
3. Los monitores de red (llamados también cortafuegos inversos) se pueden utilizar para alertar al usuario cuando el keylogger use una conexión de red. Esto da al usuario la posibilidad de evitar que el keylogger envíe la información obtenida a terceros

4. Software anti-keylogging. El software para la detección de keyloggers está también disponible. Graba una lista de todos los keyloggers conocidos. Los usuarios legítimos de la PC pueden entonces hacer, periódicamente, una exploración de esta lista, y el programa busca los artículos de la lista en el disco duro.

con vos en la web

Las diez amenazas más peligrosas de Internet

Pharming



Es el aprovechamiento de una vulnerabilidad en el software de los equipos de los usuarios, que permite redirigir un nombre de dominio a otra máquina distinta haciendo creer al usuario que el sitio visitado es el original cuando en realidad es una copia del mismo.

De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

Consejos para prevenir la amenaza:

1. Cuando quiera ingresar al sitio web de su banco, digite la url en el navegador, no la copie y pegue de algún mail.

2. Controlar los íconos de seguridad: suele ser un candado en la barra del navegador o en que la url comience con https.

3. Algunos de los métodos tradicionales para combatirlo son la utilización de software especializado para la protección DNS (suele utilizarse en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing) y el uso de complementos para los exploradores web que permite a los usuarios domésticos protegerse de esta técnica.

con vos en la web

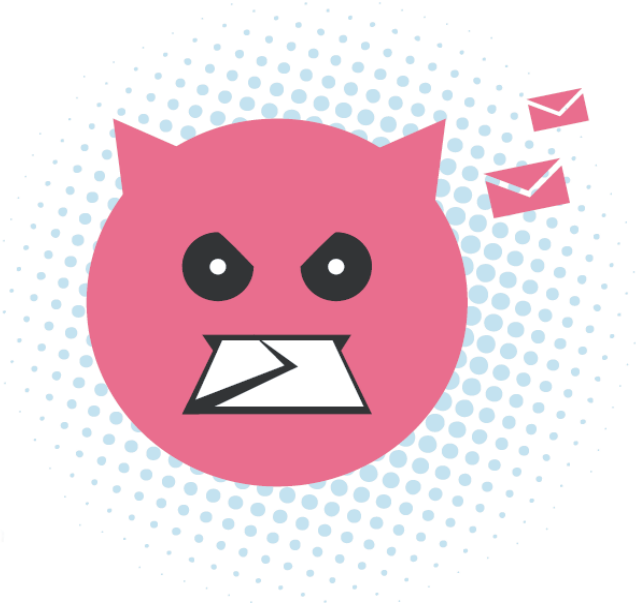
Las diez amenazas más peligrosas de Internet

Phishing

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. Lo que se extrae puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantáneao incluso utilizando también llamadas telefónicas.

Al recibir un email o un mensaje a través de un chat en el cual se nos solicite información personal financiera o de cualquier índole, es importante que jamás respondamos, pero además tampoco debemos clickear en los enlaces que puedan aparecer en el mensaje.



Consejos para prevenir la amenaza:

1. Las empresas y organizaciones que trabajan dentro del marco legal jamás solicitan datos personales, claves o números de cuenta de sus clientes o miembros a través de correos electrónicos o mensajes.

2. Nunca acceder a páginas web comerciales, financieras o bancarias desde un enlace que venga en un correo electrónico, siempre es preferible si se conoce la dirección web escribirla directamente en el navegador.

3. No es recomendable copiar y pegar la dirección de un sitio, ya que las redes de phishing operan generando sitios webs falsos, que poseen una apariencia similar a las páginas oficiales de las organización, precisamente para engañarnos.

4. Verificar la legitimidad de un correo que solicite información confidencial, estableciendo contacto con la entidad, a través de información previamente conocida, como números de teléfono o personal de la organización.

con vos en la web

Las diez amenazas más peligrosas de Internet

Rootkits

Un rootkit es un programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

Por lo general un atacante instala un rootkit en una PC después de haber obtenido un acceso al nivel raíz, ya sea por haberse aprovechado de una vulnerabilidad conocida o por haber obtenido una contraseña (ya sea por crackeo de la encriptación o por ingeniería social).

Una vez que el rootkit ha sido instalado, permite que el atacante oculte la siguiente intrusión y mantenga el acceso privilegiado a la computadora.

Pese a que los rootkits pueden servir con muchos fines, han ganado notoriedad fundamentalmente como malware, escondiendo programas que se apropian de los recursos de las computadoras o que roban contraseñas sin el conocimiento de los administradores y de los usuarios de los sistemas afectados.

Consejos para prevenir la amenaza:

1. La mejor defensa contra los rootkits consiste en prevenir que el atacante acceda a la PC. Para esto, es necesario que se instale un firewall que le proteja de accesos no autorizados a su ordenador.

2. Instalar una buena solución antimalware en la computadora y mantenerla permanentemente activa y actualizada.

3. Mantener las aplicaciones instaladas en su ordenador siempre actualizadas, instalando los parches de seguridad proporcionados por los fabricantes.

con vos en la web

Las diez amenazas más peligrosas de Internet

Sidejacking

La técnica considerada Sidejacking sucede cuando se copia la información contenida en las cookies de una máquina conectada a una misma red (generalmente sucede en redes Wi-Fi públicas) para poder acceder a cuentas de la víctima y robar su información.

Esta modalidad de ciber ataque, suele darse en aeropuertos, confiterías, bares, restaurants, etc. Y todo lugar público en donde haya redes Wi-fi, y donde se comparta la misma red de conexión a Internet. Al compartir la red, el atacante se introduce en la computadora de la víctima, para tomar posesión de sus cookies y así poder tomar información sobre cuentas, claves, etc.

El atacante escanea y reemplaza las cookies de la víctima con otro sitio web, suplantando así la identidad. El usuario sigue usando su sesión sin darse cuenta de que otro usuario está también usando la misma.

Consejos para prevenir la amenaza:

1. Evitar entrar a cualquiera de tus cuentas de correo electrónico, sitios de compra online, redes sociales, a través de un navegador web en una red pública.

2. Asegúrate de ver HTTPS en la barra de direcciones. Cuando estés conectado a una red Wi-Fi pública y tengas que ingresar datos personales a un sitio, observa la barra del navegador para ver si hay varios símbolos que denoten que estás con conexión segura. Símbolos como por ejemplo un candado, seguido de las letras HTTPS (siglas de HyperText Transfer ProtocolSecure, Protocolo seguro de transferencia de datos) te indican que no habrá fuga de datos cuando tengas que utilizarlos.

con vos en la web

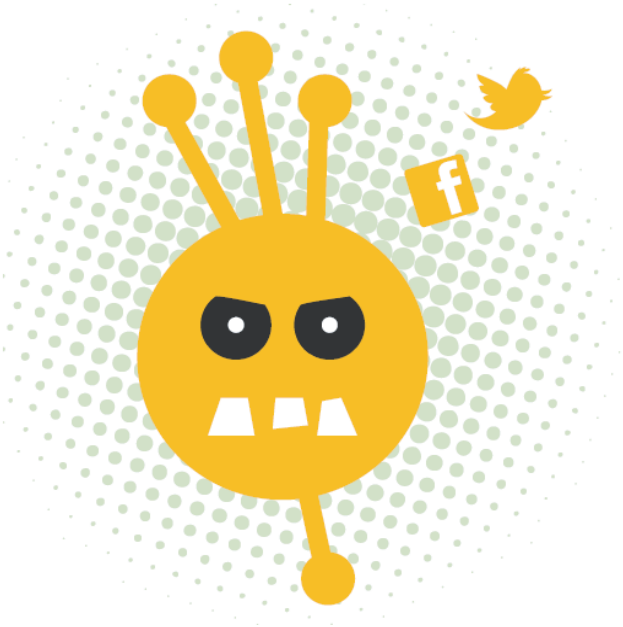
Las diez amenazas más peligrosas de Internet

Tabjacking

El Tabjacking opera sobre las pestañas de los navegadores web, espera a que pase un tiempo de inactividad sobre una pestaña que se queda abierta y cambia ésta, más el icono, por otra página falsa con apariencia de la web que se está utilizando como Facebook, Twitter, Gmail, etc.

En esta amenaza mientras el usuario está concentrado en otro sitio web un código escrito en JavaScript detecta ese intervalo y cambia el ícono y el contenido por uno de otro sitio, con la intención de robar información confidencial de los usuarios. El sitio cambia, pero se ve idéntico a uno popular que el usuario seguramente usa.

Así, el usuario no se da cuenta que el sitio donde continúa navegando no es ya el original, que está siendo utilizado por el atacante.



Consejos para prevenir la amenaza:

1. No abrir mensajes sospechosos, con remitentes desconocidos o servicios en los que no estás dado de alta.

2. Verificar la veracidad de los remitentes de cualquier tipo de mensaje, sea por email, red social o mensajero instantáneo. Pregunta a tu amigo si realmente fue él que te mandó ese link o al gerente de tu banco sobre cualquier notificación de problema con tu cuenta.

3. Controlar que el software de seguridad actualizado periódicamente (firewall, antivirus, anti-spyware, etc.) lo mismo que el navegador, con las últimas actualizaciones instaladas.

4. En sitios web que requieran el ingreso de usuario y contraseña, siempre verifica que la dirección de la página es auténtica. Los candados mostrados a la derecha de la barra de direcciones o en el borde inferior del navegador son una simple y práctica manera de realizar esa verificación.

con vos en la web

Las diez amenazas más peligrosas de Internet

Troyanos

Los troyanos están diseñados para permitir a un individuo el acceso remoto a un sistema. Una vez ejecutado el troyano, se puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar permiso.

Se presenta como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños severos.

Una de sus principales características es que no son visibles para el usuario. Un troyano puede estar ejecutándose en una computadora durante meses sin que el usuario lo perciba.

Algunas de las operaciones que se pueden llevar a cabo en la pc remota son:

Utilizar la máquina como parte de una botnet (por ejemplo para realizar ataques de denegación de servicio o envío de spam).

Instalación de otros programas (incluyendo malware - otros programas maliciosos).

Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
Borrado, modificación o transferencia de archivos (descarga o subida).

La mayoría de infecciones con troyanos ocurren cuando se ejecuta un programa infectado con un troyano. Estos programas pueden ser de cualquier tipo, desde archivos ejecutables hasta presentaciones de fotos. Al ejecutar el programa, este se muestra y realiza las tareas de forma normal, pero en un segundo plano y al mismo tiempo se instala el troyano. El proceso de infección no es visible para el usuario ya que no se muestran ventanas ni alertas de ningún tipo.

Consejos para prevenir la amenaza:

1. Disponer de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas.
2. Disponer de un firewall correctamente configurado, algunos antivirus lo traen integrado.
3. Tener instalados los últimos parches y actualizaciones de seguridad del sistema operativo.
4. Descargar los programas siempre de las páginas web oficiales o de páginas web de confianza.
5. No abrir los datos adjuntos de un correo electrónico si no conoces al remitente.

con vos en la web

Las diez amenazas más peligrosas de Internet

Virus

Los Virus se presentan como un programa aparentemente legítimo e inofensivo que al ejecutarlo ocasiona daños severos.

Los virus tienen por objeto alterar el normal funcionamiento de una computadora, sin el permiso o el conocimiento del usuario. Habitualmente reemplazan archivos ejecutables por otros infectados con el código de este. Así pueden destruir, de manera intencionada, los datos almacenados en una computadora aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

El nivel de peligrosidad de los virus se establece en función de los daños que es capaz de producir en el sistema - desde la aparición de mensajes hasta la total destrucción de la información de los equipos infectados - y de su velocidad y facilidad de propagación. Su desarrollo y creación tienen mucho que ver con las vulnerabilidades existentes en el software de uso común, por lo que una primera barrera de prevención la encontraremos en mantener actualizado y al día nuestro sistema, además de utilizar herramientas de detección y desinfección.

Además, en la actualidad existen numerosos servicios públicos donde podremos encontrar cumplida información sobre cualquier virus, además de información sobre cómo prevenir sus ataques.

Consejos para prevenir la amenaza:

1. No ingresar tu dispositivo de almacenamiento (Pendrive, Disco Externo, etc) en computadoras que posean indicios de virus.

2. No abrir correos electrónicos de desconocidos. Podrían contener enlaces o archivos nocivos para la PC.

3. Es esencial tener actualizado el Sistema operativo, antivirus y software de seguridad.

Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación

con
vos
en la
web

buscanos también **convosenlaweb** en: twitter facebook Google+ YouTube