Seguridad digital

Si bien la era digital ha facilitado muchas ámbitos de la vida de las personas (trabajo, educación, entretenimiento), también ha provocado que sean más vulnerables a los ataques de ciberseguridad, especialmente en un entorno en el que la mayor parte de nuestras acciones cotidianas las realizamos en línea.

En este sentido, la seguridad digital es de suma importancia. Un ciberataque puede causar enormes daños a organizaciones, instituciones y personas, especialmente si no se cuenta con ningún tipo de protección contra ellos.

A continuación conocerás las amenazas, riesgos y consecuencias de la falta de seguridad digital:

Amenazas, riesgos y consecuencias

Al hacer uso de la tecnología tenemos que ser conscientes de las reglas que debemos seguir, así como de situaciones que debemos evitar por nuestra seguridad. Cuando utilizas el ciberespacio debes tener

cuidado con la información que compartes, como ubicaciones, fotografías o números telefónicos, ya que esta puede ser utilizada para fines delictivos.

Riesgos

Algunos de los riesgos a los que se está expuesto en el ciberespacio son:

- **Grooming:** consiste en el acoso por parte de adultos que a través de engaños mantienen conversaciones con los menores por medio de contactos online, por ejemplo, vía mensajería instantánea (chats), a través de la cual intentan conseguir imágenes de contenido erótico para extorsionar y posteriormente amenazar y exigir un encuentro físico que podría terminar en violación.

- **Sexting:** consiste en el envío de contenidos de tipo sexual en formato de imágenes o videos producidos generalmente por la propia persona para enviar a otra que puede ser conocida o desconocida, a través de dispositivos móviles, incluso sistemas de chat o correo electrónico.

- **Phishing:** hacerse pasar por otro para obtener contraseñas, información, mensajes de bancos, redirección a webs similares a las oficiales.

Amenazas a la seguridad digital

En cuanto a las amenazas, encontramos las siguientes:

- **Spam:** también conocido como “correo basura”, son mensajes no solicitados, en ocasiones de remitentes desconocidos.

- **Malware:** se refiere al software hostil, intrusivo y malicioso, que tiene por objetivo dañar o infiltrarse en las computadoras o sistemas de información.
- **Adware:** es un software que despliega publicidad de distintos servicios o productos.

- **Hoax:** bulo, en español, es un correo electrónico distribuido en cadena, cuyo objetivo es hacer creer a los usuarios que algo falso es real.

- **Keyloggers:** son aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado.

Consecuencias

Las consecuencias que pueden derivarse de los riesgos y amenazas a la seguridad son:

- **Sextorsión:** Acto de obligar a personas a realizar acciones que no desea por medio del chantaje a través de imágenes o fotos provocativas personales

- **Pornovenganza:** Colocar imágenes o videos impropios en cuentas de redes sociales de una persona por resentimiento para que sus contactos y familiares lo vean.

- **Ciberacoso (ciberbullying):** se refiere al acoso de una o varias personas a otra, utilizando como herramientas las redes sociales, foros, blogs, mensajería instantánea, correos electrónicos, juegos en línea, WhatsApp, grupos cerrados, etc.

- **Secuestro de información:** Se deriva del phishing. Se trata de personas que toman o bloquean información de otras de manera ilegal y piden el pago de importantes sumas de dinero a cambio de regresarla o dar acceso a la misma.

Resguardo de la identidad digital

Identidad digital

Por identidad entendemos al conjunto de rasgos distintivos, el carácter, los valores, la personalidad y los gustos que aprendemos y asimilamos a lo largo de la vida. Todo este conjunto va formando a un

individuo único y diferente de los demás. La **identidad digital** es el conjunto de información sobre una persona o una organización expuesta en Internet: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc. que conforma una descripción de dicha persona en el plano digital

Consejos para una buena identidad digital

1. Apoyarse en Antivirus actualizados, que prevengan acceso de información maliciosa.
2. Creación responsable de perfiles en las redes sociales.
3. Configuración adecuada de la seguridad y privacidad.
4. Participación agradable en la red.
5. Medidas de seguridad en la navegación.
6. Revisión periódica de la identidad.

¿Cómo evitar el robo de identidad?

La **seguridad digital** es un término amplio que se refiere a todas las diferentes formas de protección de datos e información en línea para que no sean robados, dañados o comprometidos.

Esto incluye diferentes tipos de herramientas para proteger los datos e información, desde la instalación de firewalls y software antivirus en los computadores y diferentes hardwares, hasta el cifrado de los discos duros y el uso de contraseñas seguras.

Es decir, la seguridad digital es la protección del contenido de los dispositivos conectados a Internet de intrusos, que podrían caer en piratería, phishing y más, por lo que es una práctica fundamental de protección de información personal, como los datos privados y datos sensibles.

A continuación, se presentan algunos tips para protegerse contra el robo de identidad:

Revisar el informe de crédito: Obtenga una copia de su informe de crédito cada año y verifique aquellos elementos que le parezcan extraños, por ejemplo, compras, traspasos o retiros que no recuerda haber realizado.

Contraseñas robustas: Es importante utilizar contraseñas que no guarden relación obvia con el propio usuario, por ejemplo: no utilizar fechas de cumpleaños, números telefónicos, nombres de familiares, etc., en las contraseñas de bancos, teléfonos y cuentas de tarjetas de crédito. Además, es importante cambiar las contraseñas que sean asignadas al tramitar algún tipo de cuenta bancaria.

Eliminación de información: Cuando se disponga a eliminar cualquier tipo de documento, sobre todo los personales como copias de actas de nacimiento, identificaciones personales, cualquier tipo de comprobante de domicilio, documentos escolares o trabajo; es muy recomendable destruir perfectamente cualquier indicio de información legible en estos. Lo ideal es contar con una trituradora de papel que permita cortar en partes muy pequeñas estos documentos, de tal manera que su reproducción a partir de los desechos de la trituradora sea imposible.

Resguardo de información: Los documentos personales deben ser resguardados en un lugar seguro, además de reportar aquellos que hayan sido extraviados o robados.

El siguiente video nos explica un poco más sobre este tema: