Amenazas en Internet

Guía práctica para adultos

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

CONTENIDO

Esta guía es para las familias y docentes que quieran ayudar, acompañar e informar a los niños, niñas y adolescentes sobre las amenazas en Internet y las redes sociales.

¿Qué es la seguridad informática?

La **seguridad informática** es la protección de los sistemas que se utilizan para trabajar con redes de computadoras conectadas.

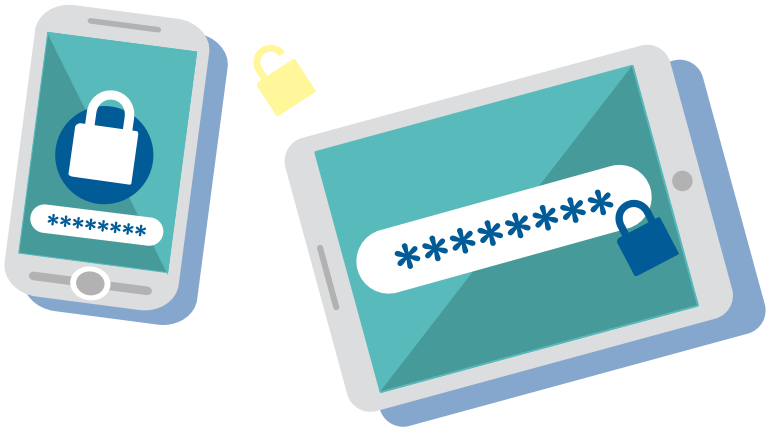
¿Qué es la seguridad de la información?

La **seguridad de la información** es la protección de toda información confidencial que se encuentra en medios informáticos o en forma física, por ejemplo archivos o documentos de trabajo.

¿Por qué son importantes la seguridad informática y la seguridad de la información?

Son importantes porque garantizan:

1. **Que los datos sean confidenciales.** Esto quiere decir que solo podrán acceder a nuestros datos las personas que autorizamos.
2. **Que los mensajes, documentación o archivos que intercambiamos por correos electrónicos o aplicaciones de mensajerías de texto no sean modificados por otras personas.** Esto quiere decir que ninguna persona puede cambiar nuestra información, salvo que la autoricemos.
3. **Que las bases de datos o sitios web estén disponibles y se pueda acceder a ellos.** Por ejemplo, que un sitio web no esté fuera de línea en el momento que hay que acceder al sistema.



¿Qué son las amenazas en Internet?

Es todo lo que atenta contra la seguridad de la información de las personas. Los usuarios están expuestos a las amenazas cuando navegan por Internet, usan servicios, hacen compras u otras actividades por medio de Internet.

¿Qué amenazas puedo encontrar en Internet?

Podes encontrar, entre otras:

1. Malware.
2. Ataques informáticos.
3. Robo de identidad y de datos personales.
4. Delitos informáticos.

¿Qué es el Malware?

El malware es un programa malicioso que busca dañar a las computadoras y dispositivos móviles. Malware también se usa para nombrar distintos softwares hostiles, intrusivos o molestos que abren ventanas con publicidad o expulsan el CD.

Tienen como objetivo:

- Robar información personal.
- Robar tarjetas de crédito y contraseñas.

- Espiar.
- Cobrar rescate en criptomonedas (monedas digitales como el Bitcoin).
- Bloquear equipos.
- Destruir información.
- Utilizar tu computadora o celular para minería de criptomonedas.
- Usar tu computadora para impedir el acceso a sitios web.
- Mostrar publicidad no deseada.

¿Cómo circula el malware?

Por medio de:

- Computadoras y dispositivos móviles.
- Correo electrónico.
- Redes sociales.

¿Qué tipos de malware existen?

- Virus
- Troyanos
- Gusanos
- Ramsonware
- Cryptojacking
- Spyware
- Scareware
- Adware
- Botnet
- Keyloggers
- Rootkits

¿Qué es un ataque informático?

Es un un ataque a computadoras, dispositivos y usuarios realizado por un individuo o varios para dañar o robar.

¿Qué es un phishing?

Es un ataque informático que se hace por medio de un correo electrónico, mensajería instantánea o por teléfono para obtener información personal, contraseñas o tarjetas de créditos de la víctima.

¿Qué es un delito informático?

Es un tipo de delito que se comete utilizando medios o sistemas informáticos. La Ley 26.388 incorporó al código penal los delitos informáticos. Los temas que incluye son:

- Violación de secretos y de la privacidad
- Acceso a sistemas de manera no autorizada
- Acceso a bases de datos personales en forma ilegal
- Alteración y destrucción de datos
- Distribución de datos
- Introducción de programas en sistemas para causar daños
- Interrupción de las comunicaciones
- Distribución y tenencia de pornografía infantil

¿Qué buscan las amenazas?

Algunos ataques pueden utilizar un malware para lograr sus objetivos que son:

MALWARE	PUBLICIDAD NO DESEADA	ROBAR INFORMACIÓN PERSONAL	ROBAR TARJETAS DE CRÉDITO Y CONTRASEÑAS	ESPIAR	COBRAR RESCATE EN CRIPTO-MONEDAS	BLOQUEAR EQUIPOS	DESTRUIR INFORMA-CIÓN	UTILIZAR TU COMPUTADORA O CELULAR PARA MINERIA DE CRIPTOMONEDAS	USAR TU COMPUTA-DORA PARA IMPEDIR ACCEDER A SITIOS WEB
Virus				X		X	X	X	X
Troyano		X	X	X			X	X	X
Gusano						X		X	X
Keylogger		X	X	X					
Rootkits		X	X	X		X	X		X
Adware	X			X					
Scareware		X							
Botnet		X	X	X		X			X
Ramsonware					X	X			
Cryptojacking								X	
Spyware				X					

TIPOS DE PHISHING	PUBLICIDAD NO DESEADA	ROBAR INFORMACIÓN PERSONAL	ROBAR TARJETAS DE CRÉDITO Y CONTRASEÑAS	ESPIAR	COBRAR RESCATE EN CRIPTO-MONEDAS	BLOQUEAR EQUIPOS	DESTRUIR INFORMA-CIÓN	UTILIZAR TU COMPUTADORA O CELULAR PARA MINERIA DE CRIPTOMONEDAS	USAR TU COMPUTA-DORA PARA IMPEDIR ACCEDER A SITIOS WEB
Phishing		X	X	X			X		
Ingeniería Social	X	X	X	X			X		
Tabnabbing		X	X	X			X		
Sidejacking		X	X				X		
PHarming		X	X				X		

¿Cómo se pueden prevenir las amenazas en Internet?

Te recomendamos seguir estos pasos:

Protegé tu computadora y tus dispositivos. Seguí los siguientes consejos:

- Descargá e instalá software de sitios oficiales.
- No abras mails y archivos adjuntos de correos de personas desconocidas.
- Activá las actualizaciones automáticas de:
    a) sistemas operativos
    b) antivirus
    c) antimalware
    d) antiramsomware
- Habilitá un cortafuegos o firewall para evitar el acceso no autorizado a tus equipos.
- Realizá una copia de respaldo de toda la información 1 vez por semana.
- Usá contraseñas seguras con mayúsculas, minúsculas, números y símbolos. Cambialas cada 30, 60 o 90 días.

Protegé la privacidad y la seguridad

- Activá el “no me rastrees” del navegador.
- Usá buscadores alternativos que protegen la privacidad.
- Usá navegadores para utilizar Internet en forma anónima
- Usá el modo incógnito para navegar en equipos públicos. De esta forma no se guarda el historial ni las contraseñas.
- No guardes contraseñas en lugares públicos.
- No ingreses datos personales en sitios desconocidos.
- Prestá atención a los permisos que das cuando instalás aplicaciones.
- Accedé a las páginas web comerciales, financieras o bancarias escribiendo la dirección directamente en el navegador.
- Leé las condiciones de uso de redes sociales o aplicaciones antes de aceptarlas.

Protegé las comunicaciones

• Chequeá si estás navegando seguro con el “candadito verde”. Cuando estés conectado a una red Wi-Fi pública y tengas que ingresar datos personales a un sitio o hacer alguna compra con tarjeta de crédito, mirá la barra del navegador y fijate si en la barra de direcciones aparece el “candadito verde” y las letras “https”(siglas de HyperText Transfer Protocol Secure, Protocolo seguro de transferencia de datos) para estar seguro de que nadie verá tus datos.

• Si vas a utilizar una red pública es recomendable que utilices una Red Privada Virtual o Virtual Private Network (VPN). Este tipo de servicio impide que la información que viaje por ese túnel sea vista por terceros. Estas redes pueden ser gratuitas o pagas.

• En sitios web que requieren el ingreso de usuario y contraseña, verificá siempre que la dirección de la página sea 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 controlar este punto.

Editado por la DNSAIJ del Ministerio de Justicia y Derechos Humanos en el marco del Programa Con Vos en la Web.

Estos textos tienen carácter divulgativo, orientativo e informativo.

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación