

Los beneficios que brinda el internet son muchos, pero también los riesgos. Infórmate y sigue los consejos que te ofrecemos para asegurar tu información.

AMENAZAS DE SEGURIDAD EN INTERNET EN 2013¹

Identidades expuestas por ataques cibernéticos
552 millones
261 % más que en 2012



Tipo de información expuesta

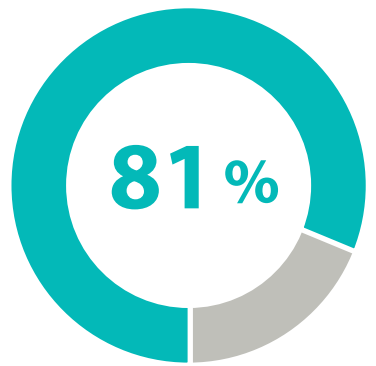
1. Nombres reales
2. Fechas de nacimiento
3. Claves de identidad
4. Domicilios
5. Registros médicos
6. Números telefónicos
7. Información financiera
8. Direcciones de correo electrónico
9. Nombres de usuario y contraseñas
10. Datos de seguros

Virus en 1 de cada 196 correos electrónicos

Robo de datos en 1 de cada 392 correos electrónicos

71% de los robos de datos (*phishing*) se dieron mediante la imitación de organizaciones bancarias

Principales engaños en redes sociales



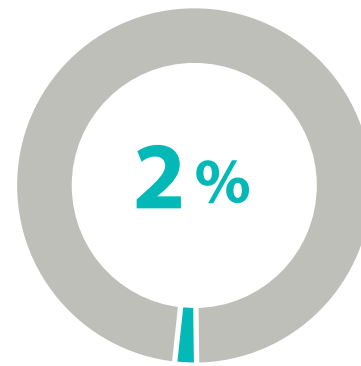
Solicitudes
Invitaciones a grupos o eventos falsos donde se solicita información personal.



"Me gusta"
Simulación de botones "Me gusta" que instalan *software* viral al dar clic.



Extensiones (*plug-in*)
Complementos para el navegador que roban información.



Aplicaciones
Suscripción o descarga de programas falsos que roban datos personales.



Compartir manualmente
Materiales tramposos que son enviados a todos los contactos.

PROTEGE TU CELULAR²

- 1 Actualiza siempre tu sistema operativo.
- 2 Agrega contraseña y no la compartas.
- 3 No publiques tu ubicación exacta ni tus rutas o actividades.



PROTEGE TU COMPUTADORA³

- 1 Instala antivirus en tu equipo.
- 2 Mantén actualizados todos tus programas.
- 3 Usa contraseña en tu pantalla de inicio.
- 4 Ten precaución al compartir recursos.
- 5 No compartas la contraseña de administrador.
- 6 Evita guardar contraseñas en el navegador.

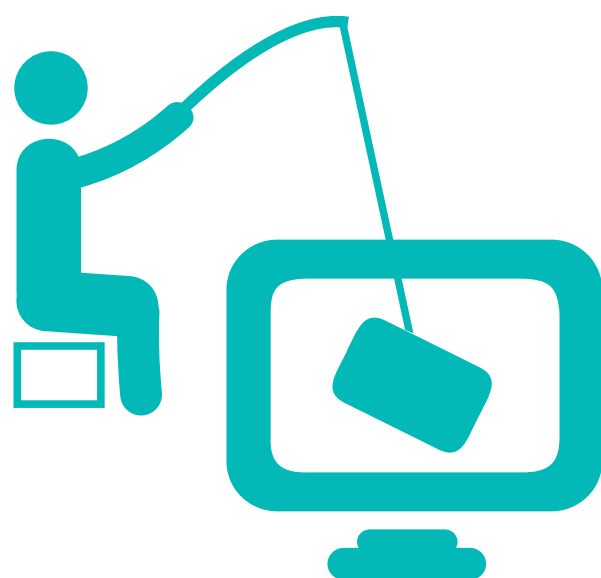


CUÍDATE EN LAS REDES SOCIALES⁴

- No aceptes solicitudes de personas desconocidas.
- Mantente alerta ante mensajes fraudulentos, aun si aparentan ser contactos confiables.
- Investiga antes de cualquier encuentro personal.
- Comprueba la privacidad de las aplicaciones que descargas.
- Recuerda cerrar las sesiones que inicies en equipos ajenos.
- Selecciona la información que compartirás en la red.
- Ten precaución con los vínculos a los que accedes.

RESGUARDA TU INFORMACIÓN FINANCIERA⁵

El *phishing* es un método de robo de datos personales y financieros. Quienes cometen la estafa obtienen la información a través de correos electrónicos fraudulentos.



- Ignora correos electrónicos y anuncios que te soliciten información personal o financiera.
- No confíes en mensajes que amenazan con cerrar tu cuenta o tomar alguna otra medida si no los respondes.
- Si dudas del contenido de un archivo, no lo descargues.
- Para aclarar dudas financieras, comunícate al número que aparece en tu tarjeta bancaria.
- No compartas números de cuenta, tarjeta o NIP en sitios no certificados.

LIGAS DE INTERÉS

- Detectar y reportar software malicioso
- Mejorar la seguridad en tus dispositivos
- Reportar sospechas de *phishing*

FUENTES

1. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
2. <http://www.nocaigasenlared.bo/contrasenas.html>
3. <https://www.takebackthetech.net/es/be-safe/herramientas-de-seguridad>
4. <http://www.cjex.org/redes/6-1-conductas.html>
5. <http://www.consumidor.ftc.gov/articulos/s0003-phishing>