



Guía práctica de Navegación segura para adultos



¿Cuáles son los principales riesgos en Internet?

> Phishing

Los ciberdelincuentes utilizan mensajes de correo electrónico con información falsa para engañar y robar datos de tarjetas de crédito, claves y números de cuentas.

> Robo de identidad

Tu información personal puede ser blanco de los ciberdelincuentes, con el objetivo de suplantar tu identidad o cometer algún acto ilegal.

> Malware

Infectarse con virus informático (u otro código malicioso como gusanos o troyanos) que borre o dañe la información de tu computadora puede ser muy fácil si no tenés cuidado dónde hacés clic.

> Fuga de información

En los dispositivos personales alguna vez se guarda información sensible del trabajo, por lo tanto hay que ser precavidos en su manejo.



No todo lo que está en Internet es verdad

Obtener información privada utilizando el engaño y la manipulación de los usuarios es una técnica conocida como Ingeniería Social y si sos víctima de ella puede quedar expuesta tu información personal. Por eso:

- Tené mucho cuidado con páginas y mensajes que te dicen "mirá quién te ha bloqueado", "conocé quién mira tu perfil" o similares y luego te piden el usuario y la contraseña, pueden ser falsas y robarte tus datos.
- Páginas que ofrezcan regalos o premios por algo a lo que nunca te suscribiste son un claro ejemplo de un engaño para robarte tu información personal o infectar tu PC con un virus.
- Los archivos adjuntos en correos electrónicos ofreciendo fotos "íntimas" de alguna persona famosa, algún programa "gratis" o cosas similares son un ejemplo de un ataque de Ingeniería Social.

Algunos consejos para tener en cuenta

🔒 Es necesario mantener actualizado el anti-virus con el que protegés tu computadora ya que los ciberdelincuentes continuamente desarrollan nuevas maneras de ataque.

🔒 Cuando necesité descargar algún programa, hazelo siempre desde las páginas oficiales, o al menos desde páginas de confianza. Todo lo que descargues, analízalo con un antivirus antes de abrirlo o ejecutarlo.

🔒 Si hacés compras o trámites bancarios en internet, hazelo únicamente en sitios confiables y que protejan tu información codificándola mientras viaja desde tu computadora hasta sus servidores (https).

🔒 Cuanto más extensa sea tu contraseña más difícil será descifrarla. Usá como mínimo entre 8 y 10 caracteres. Combiná letras, números y símbolos, tratando de no utilizar palabras de uso corriente. Además, recordá

las compañías que operan legítimamente no envían mensajes para pedir contraseñas, con lo cual no des tus contraseñas por teléfono, en mensajes de texto o por email.

🔒 No hay ningún sistema que sea totalmente seguro. Copiá los archivos importantes en un disco removible o disco duro externo, y guardalo en un lugar seguro. De esta manera, si tenés algún problema con tu computadora, podrás acceder a tus archivos.

🔒 Al abrir una cuenta en una red social configurá muy bien los niveles de privacidad para que tu información personal sea vista solamente por quienes deban verla.

🔒 Al igual que usas el sentido común cuando utilizás tu equipo, no olvides usarlo cuando utilices tu teléfono móvil. Sobretodo debes tener en cuenta el tipo de información que guardás en él: las fotos.

ANTE SITUACIONES NO DESEADAS

- En las redes sociales el contenido malicioso o mal intencionado puede ser reportado para que éste sea bloqueado.
- Si sentís que has sido víctima de algún delito informático comunicate con las autoridades, ellos sabrán orientarte sobre lo que debés hacer.

www.argentinacibersegura.org | info@argentinacibersegura.org

 /argentinacibersegura  /argentinacibersegura  /company/argentina-cibersegura
 @arg_cibersegura  /argentinacibersegura

Gracias al apoyo de



ENJOY SAFER TECHNOLOGY™

