SecPro

7 CONSEJOS DE SEGURIDAD EN INTERNET

CIBERSEGURIDAD PARA TODOS

1 No facilites Información personal

Evita los intentos de phishing, la suplantación de identidad y la adivinación de contraseñas manteniendo la privacidad de tus datos personales. No des tu número de teléfono, documento de identidad, información bancaria o de tu familia a alguien que no conozcas.

2 Crear contraseñas complejas

Crea contraseñas con una combinación de palabras, que contengan letras, números y símbolos ejemplo:

C0lomb1@esP@ss1on

Considera la posibilidad de utilizar gestores de contraseñas (por ejemplo, LastPass) y utiliza siempre la autenticación multifactor (2FA).

3 Comprobar la fiabilidad del sitio web

Antes de comprar nada en un sitio web, asegúrate de que es seguro. Puedes validar la credibilidad con herramientas como la barra de herramientas Netcraft. Atención: tener un "https" no siempre significa "sitio real"; los sitios de actores maliciosos también utilizan "https".
Si es posible, utilice una tarjeta de crédito de prepago (Virtual) para comprar en línea.

4 Evite enlaces en línea y códigos QR sospechosos

Tenga cuidado con los sitios web, correos electrónicos o QR que contengan enlaces sospechosos. Algunos sitios web pueden utilizar concursos, obsequios o historias atractivas para que hagas clic en ellos y luego robar tu información personal.

5 Utilice un navegador seguro

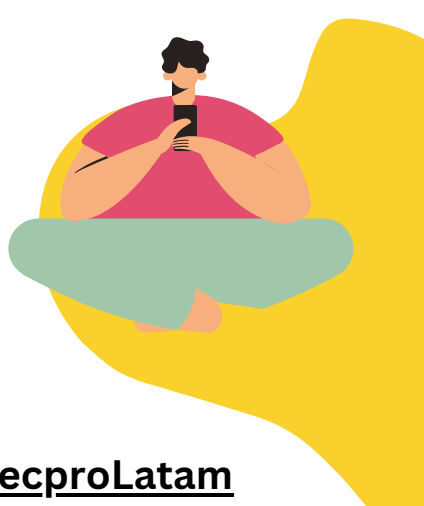
Empezar a usar navegadores seguros es uno de los pasos más importantes para mejorar tu ciberseguridad. Los navegadores como Firefox, Brave o Epic bloquean las acciones de terceros en tu dispositivo mediante el bloqueo de cookies, por ejemplo, y no comparten tu identidad.

6 Mantenga su dispositivo actualizado y tenga un antimalware

Los desarrolladores sw aplicaciones lanzan actualizaciones para mantener los productos más seguros. Mantén actualizado el software de tu dispositivo para que sea menos vulnerable a malware o ataques, e instala un antimalware, ¡aunque sea gratuito!.

7 Evite las redes WiFi públicas

Si es posible evita conectarte a WiFi públicas; actores maliciosos pueden crear redes WiFi falsas, disfrazarlas y robar tu información cuando te conectas a la red o infectar tus dispositivos; Además desactiva los servicios WiFi y Bluetooth en tus dispositivos si no los estás utilizando.



linktr.ee/SecproLatam