



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CIBERGUÍA CONSEJOS PARA UNA TERCERA EDAD CIBERSEGURA





BLOQUEA TU CELULAR

Protege el acceso al celular con alguna medida de bloqueo como un PIN o la huella digital ayudará a evitar que terceros accedan a tu información personal, y eventualmente, seas víctima de un ciberdelito.

NO CAIGAS EN ESTAFAS POR WHATSAPP, SMS O LLAMADAS

Desconfía de mensajes de texto, audios o videos simulando a algún familiar, conocido o famoso, que solicite dinero o invite a invertir, aunque parezca que proviene de marcas o personas reconocidas.





EVITA WIFI PÚBLICAS PARA ACTIVIDADES SENSIBLES

Evita hacer transacciones
bancarias o ingresar contraseñas
importantes en redes wifi
públicas.

**Ejemplo: En una cafetería, no
accedas a tu banco en línea;
espera a estar en casa o usa una
red segura.**

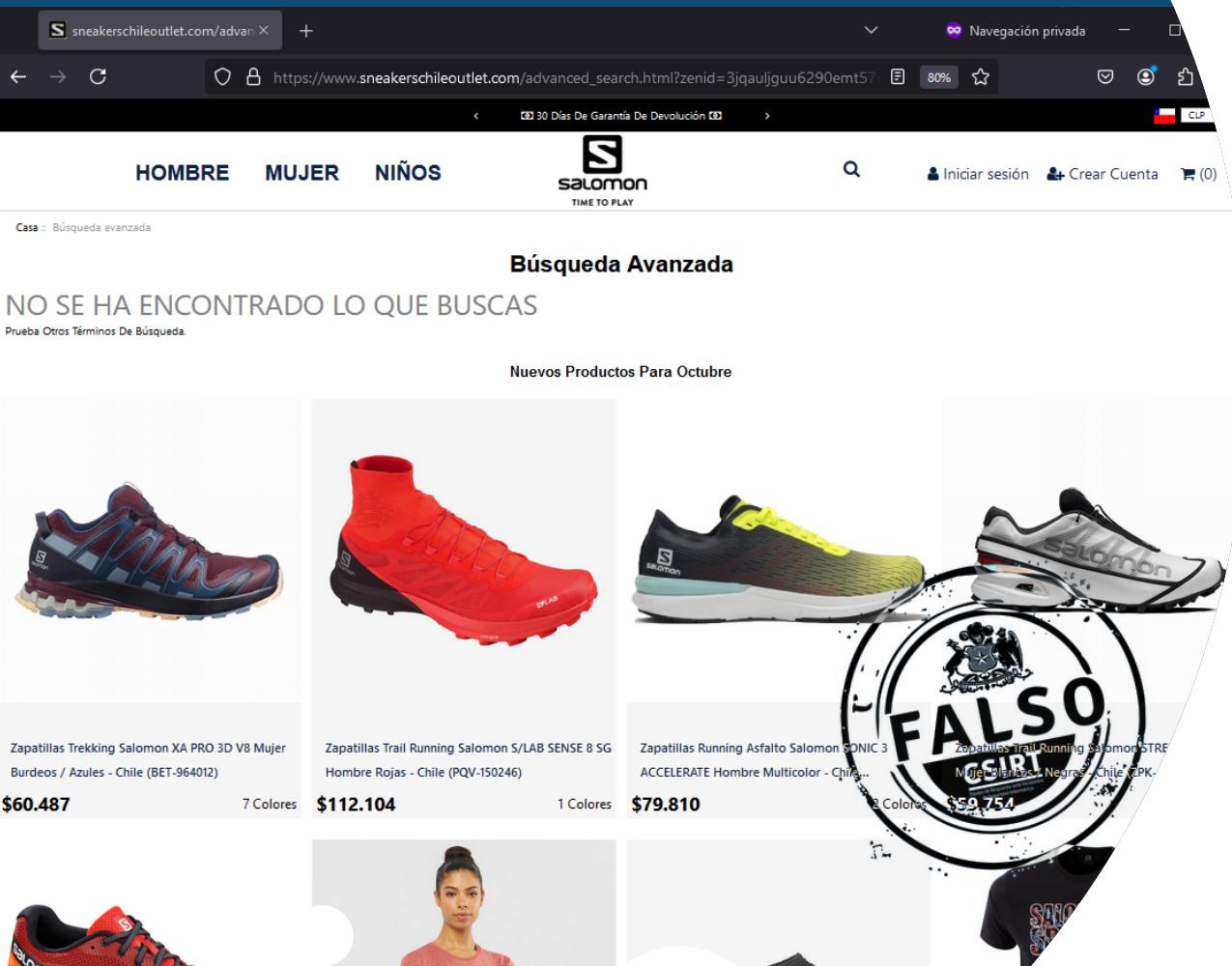
CUIDADO CON EL PHISHING

Una de las formas más usadas por los ciberdelincuentes es el phishing, el cual busca engañar a las personas a través de páginas web o correos electrónicos falsos, simulando ser las verdaderas con el objetivo de obtener información que permita por ejemplo, robar dinero de cuentas bancarias.

Compra sólo en sitios oficiales, reconocidos, con buena reputación o recomendados por conocidos y no hagas clic en enlaces ni descargas archivos sospechosos.



EJEMPLO PHISHING 1



PÁGINA WEB FALSA DE TIENDA

Un ejemplo reciente de phishing alertado por el CSIRT de Gobierno, es una página web que suplanta a la tienda de ropa deportiva Salomon, utilizando la dirección web (URL) falsa sneakerschileoutlet.com, cuando la URL real es <https://salomon.cl>

PÁGINA WEB FALSA DE SII

Otro ejemplo que fue alertado por el mismo Servicio de Impuestos Internos durante este 2024. En este caso se dio a conocer una página web que buscaba suplantar a la web de SII, en la imagen se puede ver que la dirección de la página, era zeusssiir.info, una dirección falsa, considerando que la URL real es <https://homer.sii.cl>

EJEMPLO PHISHING 2



CUIDA TU INFORMACIÓN PERSONAL

Cuidado con la información que compartas en internet o en las redes sociales. No entregues datos personales, financiera o claves de acceso, podrían ser utilizadas por los ciberdelincuentes.

Utiliza contraseñas diferentes para cada cuenta, que sean fáciles de recordar por ti pero difíciles de adivinar por otros..





CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática



<https://www.csirt.gob.cl/>

Síguenos en nuestras redes sociales:



Teatinos 92 piso 6. Santiago, Chile
2024