CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

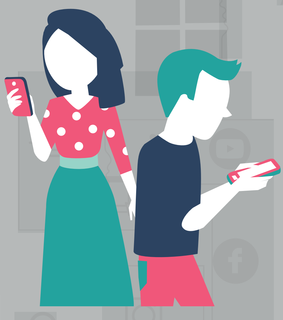
CIBERCONSEJOS PARA UNA NAVEGACIÓN MÁS SEGURA

Tener acceso a Internet tiene muchos beneficios. Podemos realizar trámites, trabajar, estudiar, jugar, etc., pero también existen riesgos asociados que pueden afectar tus dispositivos, el control de tu información, generar pérdidas económica e incluso una persona puede sufrir de acoso en línea o ser víctima de otro tipo de engaño.

Tanto adultos como niños pueden sufrir las consecuencias, por eso el 8 de febrero se celebra el Día Internacional de Internet Segura, una iniciativa que busca promo ver el uso seguro, respetuoso y responsable de las tecnologías digitales. El CSIRT de Gobierno junto a Entel entregan una serie de recomendaciones para navegar en Internet de forma más segura.

Para navegar seguro en redes sociales:

1. **Nunca** publiques datos personales como nombres, rut u otros, ya que pueden ser utilizados para descifrar contraseñas o suplantar identidad.
2. **Configura** tu perfil en modo privado y acepta sólo a personas que realmente conoces.
3. **Cuidado** con el envío de fotografías o videos. Otras personas pueden acceder a ellas y utilizarlas para extorsionar o acosar.

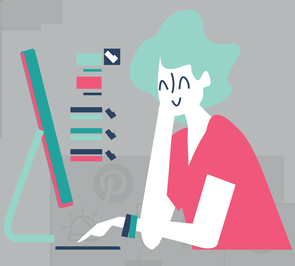


Navega seguro considerando:

1. **Bloquea** anuncios. Algunas ventanas emergentes pueden contener enlaces malicioso
2. **Borra** el caché y las cookies del navegador web para limitar el rastreo de datos.
3. **Usa** siempre antivirus y actualízalo.

En cada sitio web o red social que te registres:

1. **Utiliza** contraseñas robustas y diferentes. Si se filtra una clave, no todos los servicios se verán comprometidos.
2. **Cierra** la sesión cada vez que salgas.
3. **Nunca** guardes los datos de tus tarjetas bancarias o contraseñas.



Cuando navegues por internet:

1. Evita conectarte a redes públicas, especialmente a sitios donde ingreses información sensible.
2. Cambia constantemente las contraseñas y no las compartas.
3. Nunca dejes tus contraseñas en un papel y a vista de todos.
4. Evita ingresar tus contraseñas u otros datos sensibles en sitios web bancarios, correo electrónico, etc. en computadores ajenos.

Para evitar estafas:

1. **Sé crítico** con la información que recibes a través de correos electrónico, SMS o mensajes vía WhatsApp.
2. **Revisa** siempre la URL para confirmar que es el sitio al que quieres ingresar.
3. **Si no confías** en la página web, nunca ingreses tus datos personales
4. **Si crees** que recibiste un phishing, puedes reportarlo al **CSIRT llamando al 1510 o escribir a soc@interior.gob.cl**