Ciberguía familiar

Hábitos para navegar en Internet

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Introducción

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Llevar una vida digital segura y sana es tarea de todos, y los padres y cuidadores tienen un rol fundamental.

Desde el momento en que los niños, niñas y adolescentes tienen acceso a un teléfono inteligente o juegan conectados, deben estar informados y conscientes de que en el mundo online también deben cuidar su PRIVACIDAD, estar atentos a los ENGAÑOS, mantenerse PROTEGIDOS, ser EMPÁTICOS con quienes se rodean y CONVERSAR con un adulto frente a situaciones difíciles.

PRIVACIDAD

Todo lo que publicamos y compartimos en redes sociales viaja rápido, queda para siempre en Internet y deja una huella. Antes de publicar debemos ser conscientes de las consecuencias de una foto, un video e incluso los comentarios.

Antes de publicar, piensa qué puede pasar si...

¿Publicas dónde vives, tu ubicación actual, tu teléfono o cualquier otro dato personal?

Esta información puede ser utilizada por delincuentes para suplantar tu identidad o descubrir tus contraseñas. En el mundo físico, no entregamos estos datos a cualquier persona. Sin embargo, al hacerlo por Internet, quedan expuestos y cualquiera los puede usar para bien o para mal.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Revisemos otro ejemplo:

-Qué puede pasar si... ¿tu hijo o hija comparte fotos o videos de connotación sexual?

Una imagen se puede hacer viral rápidamente y una vez compartida nunca se sabe dónde terminará. Si bien puede ser enviada a una persona o publicada en su perfil, alguien la puede tomar y reenviar muchas veces.

El riesgo es ser víctima de ciberbullying (acoso, hostigamiento y humillación mediante alguna plataforma o dispositivo digital) o sextorsión (chantaje con difundir imágenes, videos o mensajes de contenido sexual).

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Otros peligros asociados a la pérdida de la privacidad en línea son:

Grooming: Engaño por parte de un adulto hacia los menores para crear lazos emocionales y poder abusar de ellos sexualmente u obtener contenido pornográfico.

Desafíos en línea: A través de distintas pruebas, difundidas por redes sociales, se invita a niños y/o adolescentes a realizar retos que pueden poner en peligro su vida.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

¿Cómo cuidar tu privacidad en Internet?

- **Configura** tus redes sociales en modo privado para que solamente las personas que conoces tengan acceso a tu información.
- **Evita** publicar información personal y tu ubicación. Puedes desactivar la geolocalización.
- **Desconfía** de quienes solicitan tu amistad. Hay quienes mienten sobre su identidad para crear estafas o usar tus datos con otros fines.
- **Cuida** la privacidad de tus hijos y su sobreexposición en Internet. Evita, por ejemplo, subir imágenes de ellos con poca ropa.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

ENGAÑOS

No todo lo que circula en Internet es verdadero, real o confiable. La masificación y popularidad del uso de las redes sociales (RRSS) ha permitido que los delincuentes utilicen estas plataformas para crear nuevos tipos de estafas.

Además, las redes sociales se han convertido en un canal de producción, difusión y consumo de noticias, lo que gracias a su inmediatez y amplio alcance, se han transformado también en un medio para propagar desinformación (o “fake news”).

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Para que tanto adultos como niños no sean víctimas de un fraude, es necesario ser crítico con la información que se recibe y siempre dudar antes de actuar.

En redes sociales ojo con...

Donaciones: A través de RRSS circulan falsas donaciones de dinero para causas sociales o campañas de apoyo, pero los fondos realmente llegan a estafadores.

Encuestas y concursos: Los delincuentes buscan robar datos bancarios u obtener información y así crear futuras campañas de phishing.

¿Qué es phishing?

Mediante un correo electrónico, SMS o apps de mensajería, delincuentes invitan a las personas a ingresar a un enlace adjunto en el correo o bajar un archivo, con el objetivo de robar información personal, bancaria o comercial, o a descargar un programa malicioso (malware).

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Publicidad: En redes sociales abunda publicidad con falsas inversiones relacionadas con criptomonedas, prometiendo grandes utilidades o sitios web donde invitan a la víctima a llenar formularios con datos personales en donde, en algunos casos, incluso se puede acceder a las credenciales de sus billeteras de criptomonedas.

Solicitud de amistad: Para robar dinero, los delincuentes crean perfiles falsos para comercializar productos que realmente no existen, acercarse con fines amorosos para luego pedir plata o extorsionar a la persona con compartir videos o fotos con contenido sexual. También puede pasar que los delincuentes suplanten la identidad de algún amigo(a) para pedir ayuda económica.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Atento también con las “fake news”...

Es decir, aquella “información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población y que puede causar un perjuicio público”.

Características de las “fake news”:

- Imprecisos, con escasa calidad informacional, pero que se pueden malinterpretar.
- Descontextualizados o sesgados con intención de influir en la opinión pública.
- Fabricados intencionalmente para engañar y manipular.

Antes de compartir cualquier información:

DUDA, CUESTIONA y VERIFICA.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Algunas preguntas que te pueden ayudar a identificar una “fake news”:

¿Quién creó la información?

¿La noticia la publicó un medio de comunicación de confianza?

El titular, ¿se ajusta al contenido, es creíble?

¿Cuándo se creó la noticia o esa foto es reciente?

¿Está bien escrito o tiene faltas de ortografía y gramática?

¡Los padres pueden educar desde pequeños a sus hijos!

- Acompáñalos desde temprana edad en su aprendizaje digital.

- Promueve el respeto, la empatía, la tolerancia y a valorar diferentes puntos de vista.

- Fomenta el pensamiento crítico frente a lo que leen y a usar fuentes seguras y confiables de información.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

PROTECCIÓN

Si cierras tu casa con llave al salir para que nadie ingrese, lo mismo debes hacer con tu información. Protégela con una contraseña segura para resguardar tus datos, dispositivos, cuentas bancarias, redes sociales, etc.

¿Cómo crear una contraseña segura y robusta?

Combina mayúsculas, minúsculas, usa símbolos y números, con mínimo 9 caracteres. Por ejemplo:

- Si la frase es: CREANDO MI CLAVE SEGURA
- Agrego números: CR3ANDO MI CL4VE SEGURA
- Incluyo símbolos: CR3ANDO_M1.CL4VE/SEGURA
- Combino mayúsculas con minúsculas: CR3ANdO_M1.Cl4VE$eGurA

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Para estar aún más seguros, evita:

1. Usar nombres tuyos, de tus familiares o incluso de tus mascotas.
2. Crear la misma contraseña en cada sitio web o red social que te registras.
3. Utilizar direcciones u otros datos personales como teléfonos, RUT o fechas de cumpleaños.

Y siempre...

4. Bloquea la pantalla de tus dispositivos.
5. Activa el doble factor de autentificación en la medida que sea posible.

Ahora que ya sabes cómo crear una contraseña segura, enséñales a tus hijos.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

EMPATÍA

Para tener una sana convivencia digital es necesario que adultos y niños sean respetuosos y amables, aunque no veamos a las personas.

Cifras...

El último estudio realizado por la Fundación Katy Summer y publicado en enero de este año, evidenció que:

47%

de los jóvenes entre 15 y 29 años declara haber sido **acosado virtualmente.**

El ciberacoso se relaciona principalmente a:

43% apariencia personal

33% opinión política

30% violencia de pareja

28% pertenecer a una etnia originaria

27% orientación sexual

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Los padres y cuidadores deben ser un ejemplo para los menores y enseñar a cuidarse y a respetar a los demás.
Conversar es una buena alternativa para saber cómo se comportan y qué harían frente a una situación de violencia o acoso que les afecte a ellos o a un conocido.

Puedes hablar con ellos sobre:

1. ¿Cómo quieres ser tratado en redes sociales?

2. Sus gustos, los riesgos y cómo se deben cuidar, qué hacer si tienen un problema.

3. El tipo de contenido. Guía a los menores para que compartan contenido con precaución, sobre todo si es privado.

4. El respeto a otros pidiendo autorización antes de publicar para que nadie se vea afectado.

¡RECUERDA! Hay redes sociales para cada edad.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CONVERSA

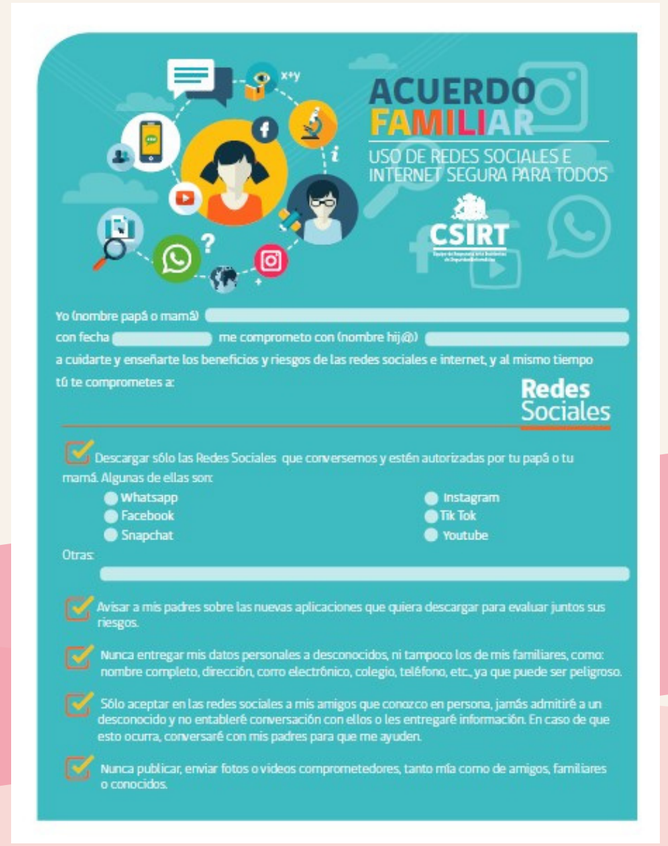
Un último aspecto que se debe tener en cuenta para una vida digital sana y segura es establecer acuerdos con los hijos, por ejemplo, sobre el tiempo que permanecerán conectados o qué sitios web podrán visitar.

Si consideramos que el **90% de los adolescentes mayores de 13 años tiene un celular y el 51% de los niños, niñas y adolescentes tienen un computador propio***, es necesario asegurarse que esos niños no estén solos y que permanezcan conectados el tiempo adecuado según su edad y que accedan a contenido apropiado.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

*Estudio Radiografía Digital de VTR año 2022

Establecer una relación de confianza puede ayudar a que tus hijos recurran a ti frente a un problema.



Una forma puede ser firmando un acuerdo familiar que establezca ciertas reglas de privacidad, el uso de redes sociales y/o juegos en línea.

Para esto, te presentamos una propuesta de ACUERDO que elaboró el CSIRT de Gobierno y que puedes descargar en el siguiente link: https://www.csirt.gob.cl/recomendaciones/acuerdo-familiar/

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática