Ministerio del Interior y Seguridad Pública

En el Mes de la Ciberseguridad **2021**

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA GUIAR A LAS PERSONAS MAYORES EN EL MUNDO DIGITAL

INTRODUCCIÓN

¿Navegar por Internet?, ¿enviar un archivo adjunto?, ¿un virus en un computador?, ¿bloquear? Éstas y muchas otras preguntas pueden surgir en aquellos que no nacieron con tecnología en sus manos, y que han debido adaptarse para poder ser parte de una sociedad que cada día está más digitalizada.

Si tener un smartphone o teléfono inteligente puede ser desafiante para las personas mayores, más aún lo es entender todo aquello que gira en torno al mundo digital: nuevas tecnologías, tendencias, riesgos cibernéticos, conceptos, etc.

Por esta razón, el CSIRT de Gobierno desarrolló esta ciberguía que busca educar sobre los diversos aspectos que emergen desde la tecnología y el uso de internet, para que la experiencia de quienes las utilizan sea lo más segura posible, gracias a una serie de recomendaciones y buenas prácticas.

Capítulo **1**

INTRODUCCIÓN AL **MUNDO DIGITAL**

Para comenzar, es importante entender algunas definiciones que permiten comprender el lenguaje digital que se utiliza actualmente, ya sea para conectarse a Internet o usar nuestros equipos de forma más segura.

Diccionario

Conceptos **Generales**

Buscador web: Un buscador nos permite encontrar información en internet. Uno de los más conocidos es Google.

Bluetooth: Consiste en una conexión inalámbrica que permite intercambiar información, ya sea entre dos teléfonos inteligentes o conectar dos dispositivos para que interactúen, por ejemplo, la música del celular a un parlante.

Ciberseguridad: También conocida como seguridad informática hace referencia a las distintas herramientas que se utilizan para proteger la información desde los computadores, teléfonos, redes, etc.

Dispositivos: Son todos aquellos aparatos tecnológicos que utilizamos: computador, celular (Smartphone), tablet, impresora, reloj inteligente (Smartwatch), etc.

Link o enlace: Texto o imagen que dirige hacia una página web al hacer clic sobre él.

Navegador web: Google Chrome, Mozilla Firefox o Safari son navegadores. Gracias a ellos es posible ingresar a cualquier sitio web.

Router: Dispositivo que permite la conexión a Internet.

URL: Consiste en una dirección única y específica para acceder a un sitio web. Por ejemplo: www.csirt.gob.cl

Wi-Fi: Tipo de conexión inalámbrica que se utiliza para conectar los dispositivos a Internet.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Diccionario
Conceptos de Seguridad

Antivirus: Programa que se debe instalar en los dispositivos, con el fin de proteger y eliminar virus informáticos.

Apps: Programas que podemos instalar en nuestros teléfonos para acceder a redes sociales, juegos, etc.

Biometría: Tecnología que identifica a una persona con alguna parte de su cuerpo para ingresar a un dispositivo, por ejemplo, la huella dactilar.

Bloqueo de pantalla: Opción que entregan los dispositivos para impedir que una persona, sin autorización, acceda a nuestro celular o computador.

Información sensible: Son nuestros datos privados o confidenciales, como el nombre, apellidos, fecha de nacimiento, ubicación, datos bancarios, etc.

Spam: Correo electrónico malicioso o no deseado que llega a nuestros e-mail, con la finalidad de infectar con un virus nuestros dispositivos o cometer una estafa.

Malware: Es un programa diseñado intencionalmente para causar daño a cualquier clase de dispositivo. Existen distintos tipos con características diferentes. Algunos de ellos son los virus, gusanos, ransomware, entre otros.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Capítulo 2
EL MUNDO DEL INTERNET

Conexión segura a Internet

Vivir en el mundo digital implica que todo aquello que nos mantiene conectados a internet y al uso de las tecnologías tiene beneficios y también riesgos. Todo lo que hacemos, desde que nos conectamos a una red wifi hasta la forma en que nos comportamos al navegar por Internet, puede tener consecuencias negativas si no tomamos las medidas de seguridad necesarias.

¿Cómo te conectas a internet?

Generalmente se utiliza una red wifi que puede ser privada (nuestra casa) o pública (supermercado, Metro, etc.). En este último caso debemos tener mucho cuidado, puesto que en ocasiones estas redes no son confiables ni tampoco seguras, ya que detrás de éstas puede haber ciberdelincuentes que buscan:

- Robar nuestras contraseñas, datos e información sensible.
- Redireccionarnos a páginas fraudulentas.
- Infectar el dispositivo con malware.

¿Cuándo vuelves al lugar, sigues conectado?

Sí, es posible. Esto, porque nuestros dispositivos pueden guardar los datos de conexión, por lo tanto, si nos conectamos a la red wifi pública de un supermercado, cada vez que estemos ahí se conectará automáticamente. El problema es que, si no nos acordamos y realizamos alguna transacción comercial, ponemos en riesgo nuestros datos. Por este motivo, te recomendamos:

- En lo posible, evitar conectarte a internet en redes públicas.
- Nunca realizar transacciones bancarias o comprar por internet cuando estés conectado a redes públicas.
- Desconectar la función del dispositivo móvil para conectarse automáticamente a redes públicas.

Ministerio del Interior y Seguridad Pública

NAVEGAR EN UN MUNDO DESCONOCIDO

Cuando se habla de navegar por Internet, se hace referencia a ir de un sitio web a otro, gracias al software que se utiliza, más conocido como navegador web. Realizar esta navegación implica que podemos encontrar publicidad, avisos, promociones, invitaciones a suscripciones, las políticas de cookies, etc. Y si bien en muchos casos tienen fines positivos, también hay algunas notificaciones que son maliciosas y que buscan, principalmente, robar nuestra información o descargar algún malware. Una notificación maliciosa se caracteriza por aparecer sin haberlas solicitado e invita a comprar un producto o a descargar algún programa.

Recomendaciones

Descarga desde la tienda oficial de tu dispositivo un bloqueador de anuncios para tu navegador.

Navega siempre por páginas web seguras y confiables.

Evita ingresar a los anuncios que aparecen en páginas web y redes sociales.

Desconfía de la publicidad que invita a invertir tu dinero, aunque provenga de marcas o personas reconocidas.

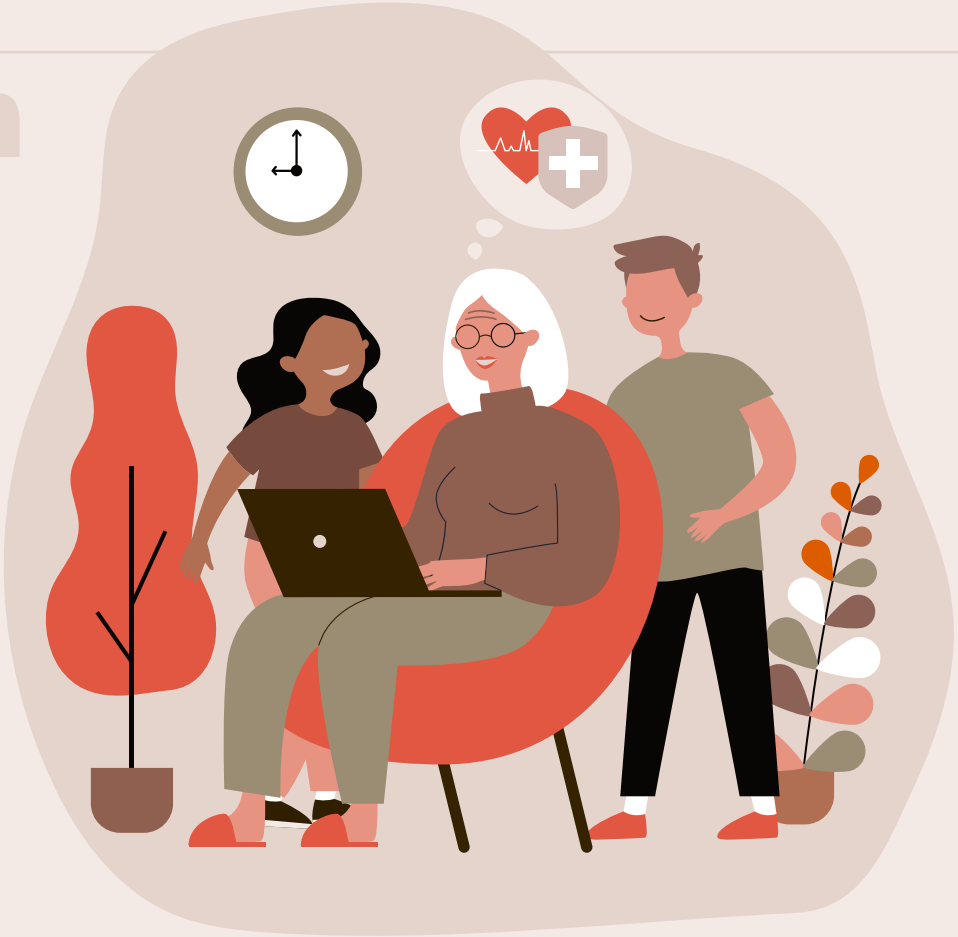
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Huella digital

Todo lo que hacemos en Internet va dejando una huella: las páginas que visitamos, los productos que compramos, si nos registramos en un sitio, nuestras contraseñas y usuarios, etc. Esto se debe a que el navegador registra y almacena toda esta información, con el fin de mejorar nuestra experiencia en Internet. ¿El problema? Es un riesgo para nuestra privacidad y, si no contamos con la debida protección, nos pueden robar nuestra información. Para evitar que esto ocurra, aquí encontrarás una guía con buenas prácticas:

- Borra regularmente los datos de navegación: historial y cookies.
- Evita guardar contraseñas y datos de tus tarjetas de pago. De hacerlo, revisa si tus datos están almacenados y elimínalos.
- Navega en lo posible en "modo incógnito". De esta manera, no dejas rastro en tu navegador de lo que haces en Internet.
- Siempre cierra tu sesión, ya sea en tu correo, banco o cualquier sitio en que estés registrado.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Capítulo 3
UTILIZA TUS DISPOSITIVOS DE **FORMA SEGURA**

Tener un computador o smartphone requiere de ciertos cuidados, ya que los ciberdelincuentes logran sus objetivos gracias al descuido de las personas. Por eso, es fundamental contar con los elementos básicos de protección y aplicar las recomendaciones y buenas prácticas para el cuidado de cualquier dispositivo, con el fin de mantener la información más segura y resguardada.

Antivirus
Elemento básico de protección

Es una herramienta esencial para cualquier tipo de dispositivo (computadores, tablet, smartphone, etc.), ya que un antivirus tiene como objetivo detectar, eliminar y prevenir lo virus informáticos (malware) que circulan en internet o que, sin darnos cuenta, descargamos desde un correo electrónico o una página web.

En algunos computadores y teléfonos inteligentes este programa viene instalado de forma predefinida, por lo que se recomienda revisar si se cuenta con este elemento de protección, de lo contrario te invitamos a adquirir uno lo antes posible.

Actualización de programas
Previene amenazas y corrige fallas

Para algunos, este término podrá ser nuevo o desconocido, pero es una forma de protección necesaria para evitar que nuestros dispositivos estén expuestos a ciertos riesgos cibernéticos. Todos los dispositivos, programas o aplicaciones cuentan, cada cierto tiempo, con una actualización, que agrega nuevas funcionalidades o en la que el creador corrija alguna falla de seguridad.

En la mayoría de los casos, esta actualización se descarga automáticamente, pero en ocasiones este proceso debemos hacerlo nosotros mismos, por ello te invitamos a revisar constantemente las notificaciones de tus dispositivos que te informan de las actualizaciones disponibles.

Bloquea tu dispositivo

Protege siempre tu información

¿Qué guardas en tus dispositivos? La mayoría de las personas usan sus teléfonos y computadores para almacenar fotografías y videos, realizar transferencias bancarias, revisar sus redes sociales y correo electrónico, en fin. Todo esto puede ser de interés para los ciberdelincuentes.

Por esta razón, un tercer elemento de protección que debemos considerar para nuestros dispositivos es el sistema de bloqueo, el cual tiene como fin evitar que cualquier persona pueda acceder a nuestro teléfono o computador, y a la información que tenemos ahí. Debemos configurar esta opción en los dispositivos, los que solicitarán una contraseña, huella dactilar, un PIN o patrón para poder ingresar una vez encendido el dispositivo.

¿Puedo bloquear **mi smartphone**?

Todos los teléfonos inteligentes tienen esta opción, pero la forma de acceder a esta alternativa dependerá de la versión y el modelo del teléfono.

Android:

1. Dirígete a "Ajustes"
2. Selecciona "Contraseña y seguridad"
3. Busca la opción "Seguridad"
4. Encontrarás "Bloqueo de pantalla"
5. Podrás seleccionar el tipo de contraseña que quieras utilizar para desbloquear: patrón, PIN, contraseña, huella dactilar, desbloqueo facial o con dispositivo Bluetooth.

IPhone:

1. Ingresa a "Configuración"
2. Elije la opción "Pantalla y brillo"
2. Selecciona "Bloqueo automático" y en cuánto tiempo que se bloquee el dispositivo.

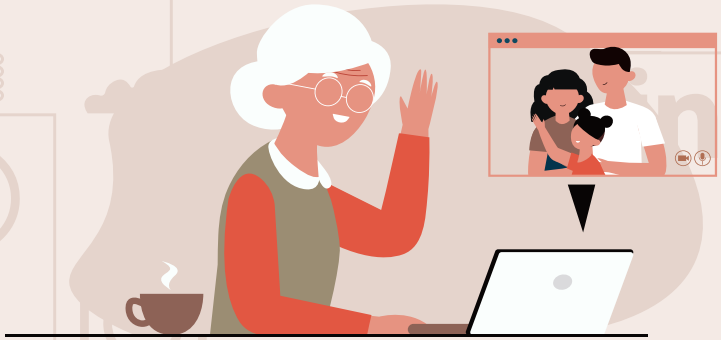
¡Recuerda!
También puedes utilizar esta herramienta en un tablet y computador.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Tips para identificar una aplicación segura

Si utilizas WhatsApp, lees algún medio de comunicación o juegas en tu teléfono o tablet es porque ya descargaste una aplicación. Y si bien es un proceso simple, es importante considerar que no todo lo que está en Internet es seguro y confiable. Por esto, si no tomamos las precauciones necesarias, es posible exponerse a:



1. Descargar un malware en nuestros dispositivos, lo que puede imposibilitar su uso o correcto funcionamiento.
2. Descargar aplicaciones piratas, es decir, programas no oficiales, lo que impide actualizar la app, quedamos expuestos a hackeos por alguna falla de seguridad.

Por esto, ya sea en tu smartphone o tablet, antes de descargar cualquier aplicación, considera más de alguna de las siguientes recomendaciones para confirmar que estás bajando una app confiable:

a. **Descarga las aplicaciones sólo de tiendas oficiales:** Play Store -Android- y App Store -iOS- cuentan con filtros de seguridad para disminuir los riesgos de descargar una aplicación maliciosa.

b. **Revisa el número de descargas de la app:** Si tiene muchas descargas, probablemente es una aplicación conocida y utilizada por otras personas, de lo contrario, desconfía.

c. **Lee los comentarios y valoraciones de la aplicación:** Sé crítico a la hora de revisarlos. Puede ser útil para saber si es o no confiable, pero también pueden ser falsos. Si desconfías, mejor no la descargues

d. **Verifica quién desarrolló la app:** Así evitarás descargar aplicaciones falsas o con contenido malicioso. Si fue una empresa reconocida es más confiable, de lo contrario investiga más sobre su creador.

e. **Verifica los permisos:** En ocasiones, algunas apps piden autorizaciones que no son necesarias para su funcionamiento. Por ejemplo, una aplicación de linterna no necesita acceder a tus contactos o tu ubicación.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Capítulo **4**

¿CÓMO IDENTIFICAR **UN FRAUDE O ESTAFA EN INTERNET?**

Una de las técnicas más utilizadas por los cibercriminales es la "ingeniería social", la cual consiste en manipular a las personas para obtener información personal y así acceder de forma ilícita a los dispositivos de las víctimas.
A través del engaño, los delincuentes logran que las personas hagan lo que ellos quieren, de manera de robar sus contraseñas y usuarios, infectar su dispositivo con algún malware, robar dinero e incluso suplantar su identidad.

Tipos de estafas que usan ingeniería social

1. Phishing: Técnica de ataque por excelencia, ocurre cuando una persona recibe un email que trata de persuadirlo de visitar un link o abrir algún archivo adjunto, el que conduce a un sitio fraudulento o descarga malware en el equipo.
Por lo general, estos correos provienen supuestamente de una fuente confiable, por lo que la víctima no duda. Podemos identificar esta estafa si estamos atentos a:

1. Llaman nuestro interés con ofertas u ofreciendo premios si hacemos lo que se solicita en el correo.
2. Nos pide actualizar nuestra información al ingresar a un link, en donde nos pedirán el usuario y contraseña, por ejemplo, de un sitio bancario.
3. Recibimos un e-mail con un documento adjunto que, supuestamente, habíamos solicitado.
4. Ofrecen beneficios económicos o reprogramar deudas bancarias. Durante el año 2020, este tipo de phishing fue uno de los más comunes, con motivo de la crisis sanitaria provocada por el COVID-19.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Recomendaciones

Revisar la gramática y redacción. Si el contenido del correo tiene errores gramaticales u ortográficos significativos, tómalo inmediatamente como falso.

Nunca entregues información personal o financiera. Si te piden estos datos, es mejor dudar y llamar a la entidad que supuestamente envía el correo.

Nunca ingreses tus contraseñas, ya que puede ser un sitio falso. Es mejor escribir la dirección directamente en el navegador.

Revisa el contenido. Si es alarmante, desconfía.

Nunca descargues archivos adjuntos, especialmente si no los solicitaste. Pueden contener un malware e infectar tu equipo.

2. Falsas ofertas y/o ventas de productos: En Internet abunda todo tipo de información y también la venta de falsos productos. La creación de páginas fraudulentas es su principal canal de ventas atrayendo víctimas con supuestas promociones. Por eso, siempre ten cuidado si:

1. La oferta o valor del producto es demasiado bueno, en comparación al comercio establecido.
2. El sitio web está mal construido, con faltas de ortografía, etc., ya que podría ser un sitio falso.
3. Al momento de pagar, el sitio web te pide las coordenadas de tus tarjetas bancarias. Asegúrate que la página en la que realizarás el pago sea de confianza.

Recomendaciones

Utiliza canales de pago formales y cuidado con la información que solicitan si lo haces directamente desde el sitio de la tienda.

Nunca compartas la información de tus tarjetas de crédito, claves dinámicas o cuentas bancarias.

Evita comprar a través de enlaces que te lleguen en un correo electrónico, ya que se podría tratar de un phishing.

¡Atención! Si revelaste tu información bancaria, contacta rápidamente a tu banco y cambia tus contraseñas inmediatamente. En caso de tener más de una cuenta bancaria y usar la misma clave, debes cambiarla también.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

3. Suplantación de identidad: En el último tiempo ha sido tendencia este tipo de estafa, consistente en usurpar la identidad de un usuario de redes sociales para cometer actos ilícitos, como el robo de datos personales o de dinero. La suplantación se puede realizar de forma sencilla, ya que sólo se debe crear una cuenta con el nombre de la persona. En algunos casos, se utiliza la misma fotografía que la cuenta real y en otros no hay foto de perfil.
Para prevenir ser víctima de una estafa de este tipo y evitar ser suplantado, te recomendamos:

1. Configura tu perfil en modo privado para que sólo la gente que conoces y decides aceptar pueda acceder a tu información.
2. Sólo acepta como amigos a quienes conoces.
3. Nunca publiques información personal y sensible en las redes sociales.
4. Utiliza contraseñas robustas y doble factor de identificación.
5. Si un amigo te escribe un mensaje a través de una red social pidiendo ayuda o dinero, lo mejor es contactarlo por otro canal para confirmar la información.

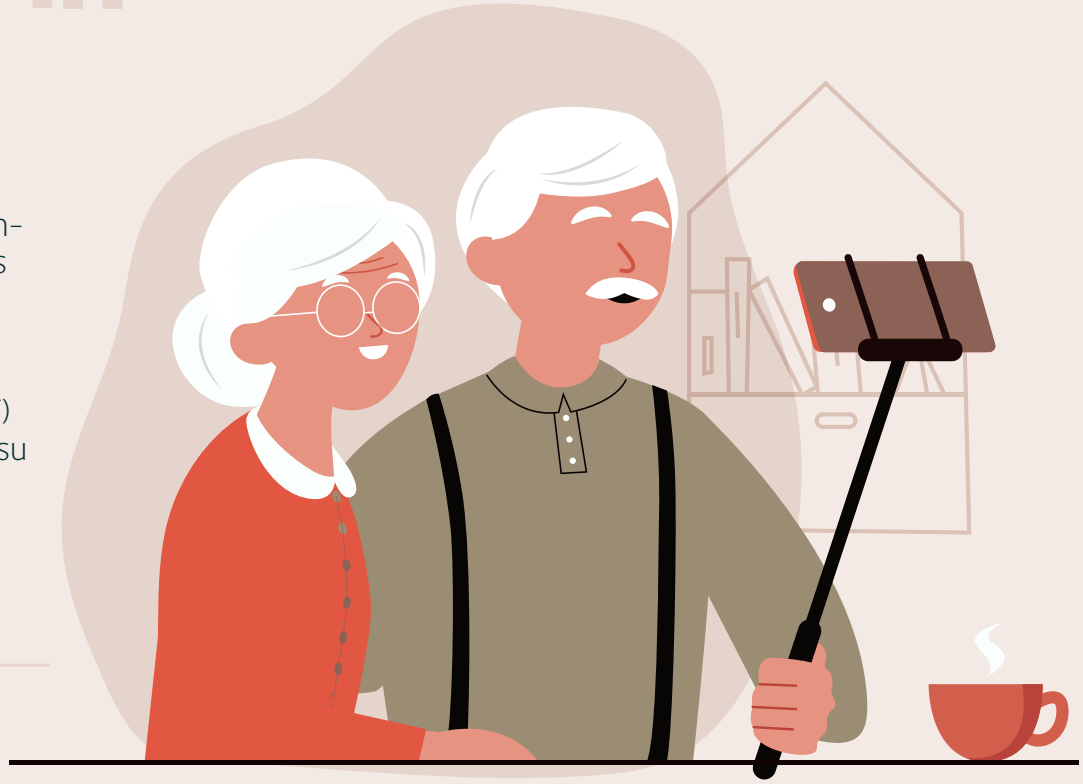
4.Cuidado también con... la suplantación de una imagen pública o de empresas
Una técnica muy utilizada por los ciberdelincuentes es usar la imagen de un rostro de televisión o el nombre de una empresa reconocida para invitar a invertir.
Así se han visto falsas empresas de asesorías que llaman a las víctimas para pedirles los datos de sus cuentas y, como supuestamente un famoso había invertido con ellos, la persona cae en la estafa y su cuenta bancaria termina con $0.

Recomendaciones

Verifica si el sitio web es verdadero. Revisa la URL y si la encuentras sospechosa, desconfía.

Nunca entregues los datos de tus cuentas bancarias. Una empresa seria jamás te pedirá esa información.

Infórmate a través del sitio web de la Comisión del Mercado Financiero (CMF) si la empresa de inversiones está bajo su supervisión.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Capítulo **5**

REDES SOCIALES Y CORREO ELECTRÓNICO: **MÁS CONECTADOS, MÁS EXPUESTOS**

En la actualidad, existen diversas plataformas que nos permiten estar conectados, saber más sobre la vida de los amigos, conocer gente, compartir videos, enviar información, entre otras bondades. Uno de estos canales son las redes sociales, sitios web o aplicaciones diseñadas para compartir contenido de forma rápida y en tiempo real. Algunas de las redes sociales más conocidas son: Facebook, Instagram, WhatsApp, Youtube, Tik Tok, Linkedin, Snapchat, Twitter, etc. Y si bien la información que compartimos puede ser muy entretenida e interesante, también es un blanco muy atractivo para los ciberdelincuentes, quienes usan esa información para cometer distintos tipos de estafas, como:

REDES SOCIALES

1. Suplantación de identidad
2. Préstamos falsos
3. Concursos fraudulentos
4. Descuentos en productos de lujo
5. Phishing
6. Secuestro de cuentas de WhatsApp

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

EN SU MAYORÍA

los fraudes a través de las redes sociales tienen como objetivo robar información o dinero. Evita ser una víctima siguiendo estas recomendaciones:

a. **No aceptar** sugerencias de amistad de personas que no conoces o de famosos.

b. **Desconfiar** de los links que te envían, especialmente si es de un desconocido o, supuestamente, del equipo de soporte de la red social.

c. **Nunca** aceptes préstamos de dinero, aunque ofrezcan tazas de interés muy bajas.

d. **Nunca** entregues tu información sensible: cuentas bancarias, tarjetas de coordenadas, contraseñas.

e. **No compartas** códigos que te envían por WhatsApp.

f. **Desconfía** de los mensajes directos de quienes no conoces, sobre todo si tiene errores gramaticales, se dirigen de forma genérica o su mensaje es alarmante.

g. **Nunca** transfieras dinero a desconocidos, especialmente si lo solicitan como requisito para ganar algún premio.

h. **Sé crítico** con la información que recibes. Si venden productos a muy bajo precio en comparación con el mercado, o si ofrecen premios en dinero sólo con entregar tus datos, desconfía.

i. **Nunca** confíes 100%. Lo mejor siempre es investigar y verificar la información.

j. **Configura** tus redes sociales en modo privado para que sólo tus verdaderos amigos y conocidos puedan ver tu información.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CORREO ELECTRÓNICO

El correo electrónico o e-mail ha ido evolucionando en sus distintas funcionalidades. Si bien se caracteriza por ser una herramienta de comunicación, para enviar y recibir mensajes, hoy también se utiliza para crear cuentas en las distintas aplicaciones y sitios web, ya sea de una red social como también para contar con una plataforma de streaming, como Netflix, e incluso realizar compras a través de Internet.

Así también, si no recordamos la contraseña de un sitio web en el que estamos registrados, es posible recuperarla si ingresamos el correo electrónico. Debido a la cantidad de funcionalidades que hoy tienen nuestras cuentas, es fundamental contar con medidas de protección para cuidar la información y evitar que alguien tenga acceso a todos nuestros datos y servicios.

1. Utiliza contraseñas seguras, nunca uses tus datos personales.
2. Nunca compartas tus contraseñas.
3. Crea una contraseña exclusiva para tu correo electrónico.
4. Desconfía de los correos que provienen de desconocidos y nunca realices alguna acción que te soliciten.
5. Utiliza el doble factor de autentificación para asegurar tu cuenta.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Capítulo 6
CONTRASEÑAS SEGURAS, DATOS MÁS PROTEGIDOS

Una contraseña o clave es una palabra, frase, números o una cadena de caracteres que sirven para verificar la identidad de un usuario en cualquier proceso de autenticación, ya sea en un sitio web, aplicación o al usar tarjetas bancarias.

Gracias a la contraseña podemos mantener nuestra información segura y protegida. Para esto, es importante crear claves robustas, ya que de lo contrario el riesgo es que los delincuentes accedan a tus cuentas, usen tus plataformas y servicios, roben tu información, tus datos, tu dinero e incluso puedan suplantar tu identidad. Es decir, una contraseña débil afecta tu privacidad y seguridad.

Para crear una clave segura necesitas:

1. Utilizar mínimo 9 caracteres.
2. Usa letras mayúsculas y minúsculas, símbolos y números.
3. Utiliza frases de canciones, poemas, libros, etc.
4. Usa claves diferentes en cada sitio o aplicación en la que estés registrado.
5. Cambia la contraseña periódicamente

Nunca crees una contraseña con:

1. Datos personales como RUT, fechas de nacimiento, direcciones, etc.
2. El nombre de algún familiar.
3. El número de teléfono o fechas de cumpleaños.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

DOBLE FACTOR DE AUTENTIFICACIÓN

Además de tener una contraseña robusta, hoy es posible implementar en nuestras aplicaciones y correo electrónico el doble factor de autentificación, un sistema que agrega un nivel adicional de seguridad, reduciendo cualquier tipo de riesgo. La verificación en dos pasos significa que para acceder a un sitio online, la persona se deberá identificar de dos formas diferentes. Primero, ingresando la contraseña y, segundo, la aplicación solicitará un código o enviará un mensaje de texto. Pasos para implementar doble factor de autentificación en Gmail:

1. Ingresar a tu cuenta de Gmail
2. En el navegador, arriba a la derecha, dirígete a "Configuración"
3. Selecciona "Verificación en dos pasos" y "Comenzar"
4. Sigue los pasos que aparecerán

Pasos para implementa doble factor de autentificación en WhatsApp:

1. En la app ingresa a "Ajustes"
2. Luego, selecciona "Cuenta"
3. Dirígete a "Verificación en dos pasos" y selecciona "Activar"
4. Ingresa un código de 6 dígitos

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

En el Mes de la Ciberseguridad **2021**

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA GUIAR A LAS PERSONAS MAYORES EN EL MUNDO DIGITAL

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Director: Carlos Landeros Cartes

Jefa de contenidos y edición: Katherina Canales Madrid

Colaboradores equipo CSIRT: Carolina Covarrubias

Diseño y diagramación: Jaime Millán

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile