Ministerio del Interior y Seguridad Pública

CSIRT

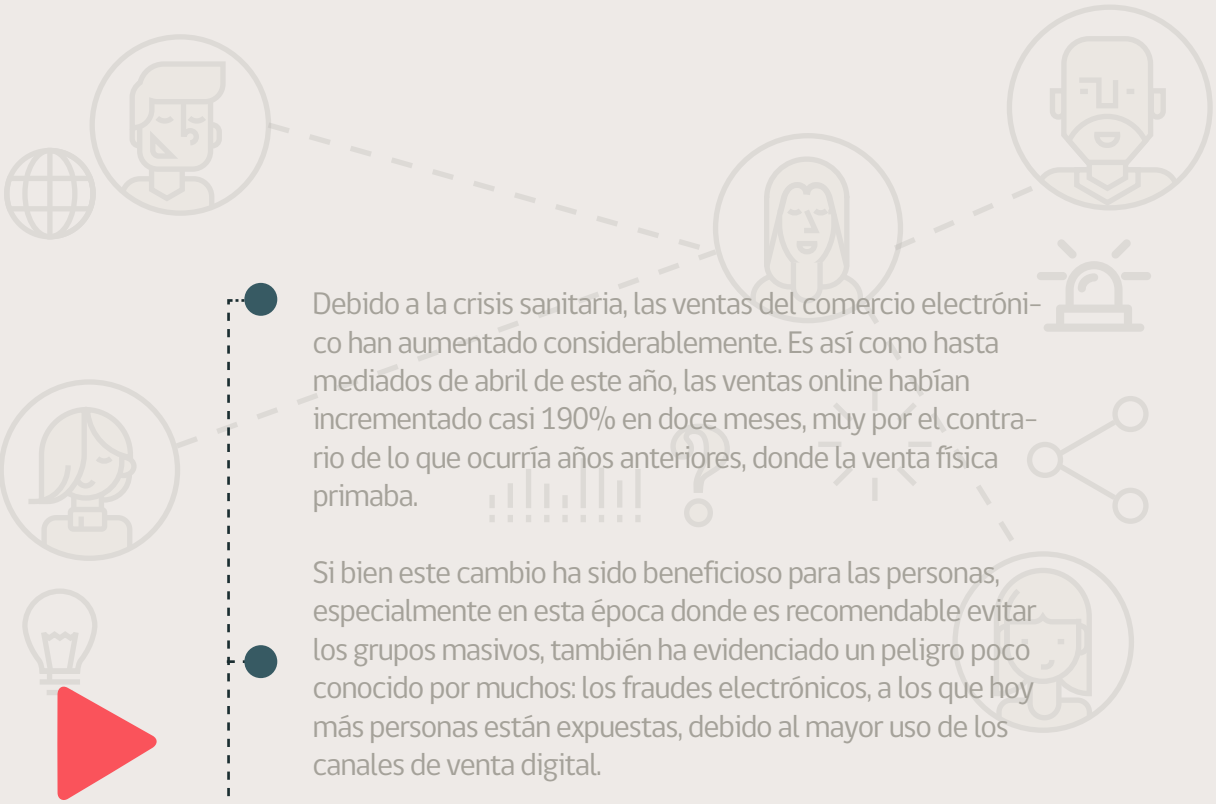
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS DE SEGURIDAD

Fraudes por e-commerce.
¿Cómo identificar una posible estafa electrónica en el comercio?

SERNAC

Servicio Nacional del Consumidor



Debido a la crisis sanitaria, las ventas del comercio electrónico han aumentado considerablemente. Es así como hasta mediados de abril de este año, las ventas online habían incrementado casi 190% en doce meses, muy por el contrario de lo que ocurría años anteriores, donde la venta física primaba.

Si bien este cambio ha sido beneficioso para las personas, especialmente en esta época donde es recomendable evitar los grupos masivos, también ha evidenciado un peligro poco conocido por muchos: los fraudes electrónicos, a los que hoy más personas están expuestas, debido al mayor uso de los canales de venta digital.

Para evitar ser víctima de una estafa es necesario informarse para conocer y aprender las formas de actuar de los ciberdelincuentes, quienes cada vez perfeccionan sus técnicas para convencer a sus futuras víctimas.

El Equipo de Respuesta Ante Incidentes de Seguridad Informática, **CSIRT** y el Servicio Nacional del Consumidor, **SERNAC**, elaboraron el siguiente documento, con la finalidad de explicar los tipos de fraudes que utilizan los delincuentes para robar datos personales u obtener ganancias económicas y cómo identificarlos rápidamente..

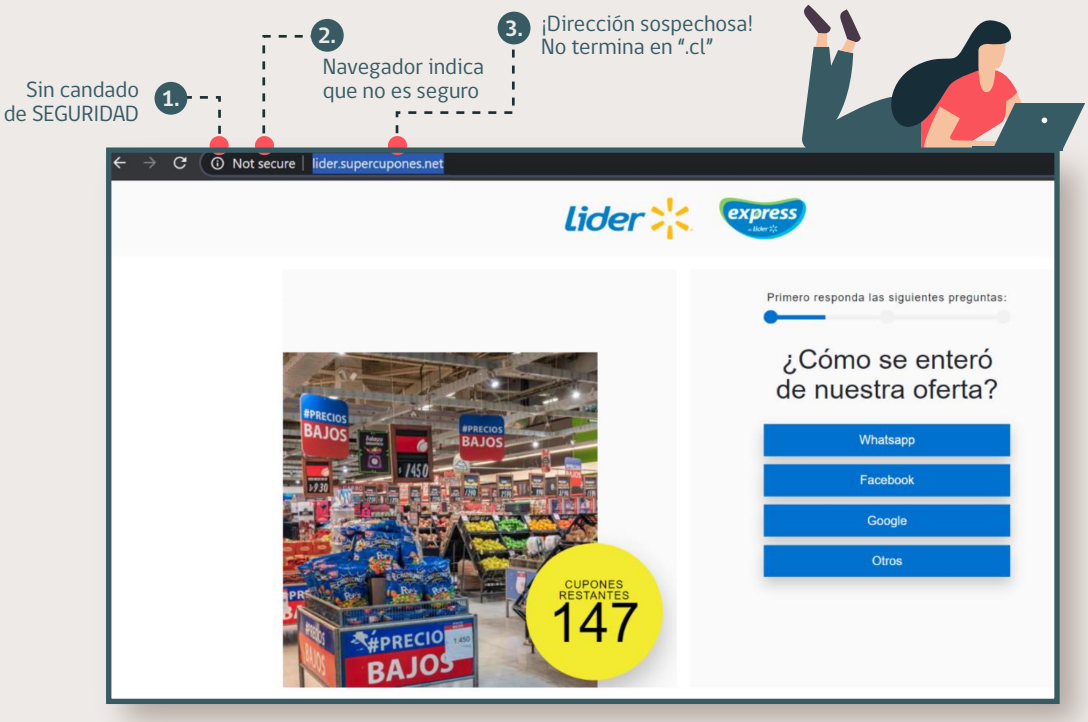
Algunos tipos de fraudes:

1. Sitios web fraudulentos

A través de la creación de páginas falsas, los delincuentes buscan robar las credenciales de las víctimas, obteniendo información bancaria, datos personales u otros. Por esto, es importante asegurarse de navegar en páginas seguras. ¿Cómo saber si es confiable?

- Revisa que el sitio web en el que quieres navegar sea el oficial.
- El navegador te avisará si esa página es segura o no.
- Se recomienda navegar por aquellos sitios con candado de seguridad.

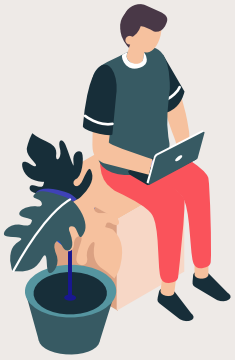
A continuación, un ejemplo de un sitio fraudulento:



En caso de navegar en una página con estas características, te recomendamos dejar de hacerlo, especialmente si el sitio te pide ingresar datos personales, bancarios o debes realizar algún tipo de transacción comercial.

Algunos tipos de fraudes:

2. Falsas ofertas por correo electrónico, SMS, mensaje de WhatsApp y campañas emergentes



Otra técnica que utilizan los estafadores es enviar, a través de distintos medios, supuestas ofertas por parte de una empresa reconocida para hacer más creíble el fraude.

A diferencia de una campaña real, las ofertas falsas se caracterizan por tener una promoción demasiado buena, algo que probablemente no pasaría de verdad. Si recibes un correo electrónico, mensaje de texto, WhatsApp, etc. con ese tipo de mensaje, te recomendamos estar atento a las siguientes señales:

Algunos tipos de fraudes:

3. Campañas de phishing

Este es el ataque más común. Mediante un correo electrónico, la persona es invitada a ingresar a un enlace adjunto en el correo o bajar un archivo, con el objetivo de dirigir a un sitio fraudulento donde la persona se expone a perder información personal, bancaria o comercial, o a descargar un malware en el equipo.

Existen diversos tipos de campañas de phishing que suplantan instituciones bancarias, retail, sitios de streaming, entre otros, y todas ellas tienen características comunes que las evidencian de ser un correo falso. Lo importante es leer con detención el contenido del mensaje, no apurarse a actuar de acuerdo a lo que invita el correo y estar atento a las siguientes señales:

Las campañas de phishing se caracterizan por adaptarse de acuerdo a la contingencia nacional. Este año, dentro de los temas usados para crear nuevas estafas se destacan el coronavirus y el retiro del 10% de la AFP.

De acuerdo a cifras de Kaspersky, entre febrero y marzo de este año se detectó un aumento de un 83% de phishing contra dispositivos móviles en Chile. Además, nuestro país aparece en el 7mo lugar de los lugares que más ataque recibe de este tipo.

Algunos tipos de fraudes:

4. Campañas de phishing

Otra modalidad conocida por los delincuentes para robar dinero es a través de una supuesta inversión con bitcoin. Para lograr su objetivo, los estafadores, en ocasiones, suplantan la identidad de una figura pública para persuadir a otras de imitarlo, logrando así armar una trama capaz de lograr que las personas realicen depósitos en bitcoins y obtener importantes sumas de dinero. En muchas ocasiones, estas pérdidas económicas son difíciles de cuantificar.

Este tipo de fraudes se promocionan a través de sitios web de noticias falsos, los que puedes identificar con el ejemplo que presentamos a continuación:

1. Revisa la URL. Por ejemplo, esta dirección es sospechosa al ser tan extensa

2. Medio en inglés, pero es una noticia local

3. Titular y noticia apuntan a un negocio de inversiones

Hasta febrero de este año, la PDI había recibido 64 denuncias en todo Chile por este tipo de estafas, las cuales llegan a la suma de $697 millones de pesos. Por eso, si quieres invertir, te recomendamos informarte y hacerlo a través de instituciones financieras formales.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS DE SEGURIDAD

Fraudes por e-commerce.
¿Cómo identificar una posible estafa electrónica en el comercio?

SERNAC
Servicio Nacional del Consumidor