Ciberestafas y reclamos de consumo

Secretaría de Industria y Comercio
Ministerio de Economía

Subsecretaría de Defensa del Consumidor y Lealtad Comercial

Dirección Nacional de Defensa del Consumidor

Escuela Argentina de Educación en Consumo

Introducción

En la actualidad, el avance vertiginoso de la tecnología ha transformado nuestra manera de consumir productos y servicios, brindando numerosas ventajas pero también planteando nuevas problemáticas. Uno de los desafíos más preocupantes es el incremento significativo de estafas y fraudes virtuales que afectan a consumidores en todo el mundo.

Según datos recientes, en Argentina, el 76% de los usuarios de Internet ha experimentado algún tipo de fraude online, desde la suplantación de identidad hasta la compra de productos falsificados o la pérdida de datos personales sensibles (Fuente: CERT, 2023).

Esta tendencia alarmante no solo afecta a individuos, sino también a pequeñas y medianas empresas que enfrentan riesgos similares al realizar transacciones comerciales por medios electrónicos. La necesidad de educar a los consumidores sobre sus derechos y cómo protegerse en el entorno digital nunca ha sido más apremiante.

Este material tiene como objetivo proporcionar las herramientas necesarias para reconocer situaciones de riesgo, entender nuestros derechos como consumidores y adoptar prácticas seguras al realizar compras, transacciones online o proteger nuestra identidad e información digital.

Exploraremos casos prácticos, estrategias de prevención y recursos disponibles para promover un entorno digital más seguro y confiable para todos. Juntos podemos contribuir a una comunidad de consumidores informados y protegidos frente a los desafíos de la era digital.

Ciberestafas

Diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial.

- Se trata de ataques de **ingeniería social** donde se utiliza la información confidencial de los usuarios, obtenida de forma fraudulenta o mediante engaño, para apropiarse de la identidad de la persona y de sus claves personales, para provocar un daño patrimonial.

- **Hay distintos tipos de ciberestafas,** categorizadas por el modo de vulnerar y apropiarse de la identidad digital y claves de la persona. En este material veremos algunas de las más comunes.

¿QUÉ MÉTODOS PUEDEN UTILIZAR LOS **CIBERDELINCUENTES PARA COMETER SUS ATAQUES?**

1. **Hacerse pasar** por un familiar, un conocido o un compañero de trabajo.
2. **Ofrecer a la víctima premios o promociones** únicas y limitadas.
3. **Hacerse pasar** por el técnico de la empresa o por la persona responsable de sistemas.
4. **Invitar a completar formularios** para ganar un premio o un producto.
5. **Ofrecer actualizaciones** de navegadores o aplicaciones a través de páginas falsas.
6. **Se contactan** a través de diferentes medios (WhatsApp, mail, teléfono y redes sociales).

Tipos de ciberestafas más comunes

Algunos tipos de ciberestafas (pero no los únicos):

- ***Phishing*:** suplantación de identidad por correo electrónico.
- ***Vishing*:** suplantación de identidad por llamada.
- ***Smishing*:** suplantación de identidad por mensaje SMS.
- ***QRshing*:** suplantación de identidad por QR.
- ***Pharming*:** suplantación por un sitio web ilegítimo.

Son derivados del ***phishing***

OTROS TIPOS **NO DERIVADOS DEL PHISHING**

- ***Malware*:** es un programa malicioso que tiene como objetivo infectar el dispositivo de la víctima para así poder tomar control del mismo y extraer información confidencial u operar desde este.
- ***SIM swapping*:** es una técnica que consiste en engañar a la empresa de telefonía para tomar el control de la línea del cliente (SIM)

Phishing

Son ataques de ingeniería social donde se utilizan mails o sitios falsos como medio de contacto para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas, de su información sensible y de su patrimonio.

Una vez capturadas las credenciales del consumidor se procede a vulnerar los saldos disponibles en cuentas bancarias y/o explotar información personal para venta en la Deep Web.

Utilizan mails o sitios que simulan ser verídicos y así "pescar" ('fishing' en ingles) **contraseñas y datos valiosos**

El consumidor ingresa en un sitio falso, que le pide ***datos de acceso*** al Home Banking (***usuario y clave***) y el segundo factor de autenticación (**Token**)

Con los datos recopilados, los estafadores **ingresan** al Home Banking.

Una vez dentro del canal **vacían las cuentas utilizando el Token** del consumidor para aprobar las operaciones.

De este modo logran **enviar dinero a cuentas fraudulentas** y sacarla del sistema.

Phishing

¿Qué son los correos electrónicos falsos?

Son correos electrónicos que contienen información falsa y enlaces que redirigen tus respuestas hacia páginas de internet falsas con formularios y preguntas para obtener datos personales.
Estos correos electrónicos pueden aparecer como comunicaciones cursadas por bancos, servicios de pago, mercados de compra en línea o proveedores de servicios públicos.

En general estos correos solicitan:

- Rellenar formularios o hacer clic en un enlace para obtener alguna información o archivo clave;
- Hacer clic en un enlace que redirigirte a una página de registro falsa;
- Descargar un archivo adjunto importante.

¿Qué datos desean obtener?

- Datos de contraseñas;
- Números de tarjetas de crédito;
- DNI, CUIT o CUIL;
- Nombres de usuario;
- Códigos PIN.

Datos sensibles

Cuando obtienen estos datos realizan compras, extracciones de dinero o toman créditos en nombre de la víctima.

Phishing

¿Cómo puedo saber si los mensajes o correos son un intento de phishing?

Es importar prestar atención a los detalles como por ejemplo:

- **Correos o mensajes de WhatsApp** enviados por remitentes desconocidos;
- El uso de **remitentes parecidos** (pero no iguales) a los de las páginas oficiales y legales;
- **Faltas de ortografía:** errores gramaticales u ortográficos, la falta de acentos o la presencia de caracteres en otros idiomas;
- La presencia de **enlaces y links dudosos**;
- **Solicitud de información:** ningún proveedor de servicios en línea le pide a sus clientes la introducción de datos por medio del correo electrónico;
- **Faltan o sobran letras en las direcciones URL:** no es lo mismo “argentina.gob.ar” que “argentina.io”, esta última dirección URL es falsa;
- La página **no tiene el candadito verde** o gris con su certificado de seguridad.
- **En caso de dudas, es recomendable no hacer clic sobre el enlace ni abrir ningún archivo.**

Phishing

¿Cómo se puede prevenir el phishing?

- **Chequeá el remitente:** antes de abrir cualquier correo electrónico es importante chequear que no sea falso. Observá cuál es la dirección completa del remitente.
- **Compará el remitente** con los mensajes anteriores de tu banco o servicio.
- **Comprobá la dirección de internet (URL)** que se muestra en la parte inferior izquierda en la ventana del navegador es igual a la de la empresa que te escribe. Podés hacer una búsqueda en internet de la empresa y comparar las URLs.
- **Verificá el certificado de seguridad** de la página de internet: es importante verificar que tenga el candado gris o verde y que sea una dirección HTTPS (con 's').
- **Si tenés dudas, comunicate con los servicios de atención al cliente** antes de contestar cualquier comunicación por correo electrónico.
- **No contestes formularios en línea enviados por destinatarios desconocidos.**
- **No respondas** a ningún correo electrónico, mensaje o llamado telefónico que te solicite divulgar información personal.
- **No envíes ni compartas ningún código de seguridad** como el código PIN por teléfono o por correo electrónico.
- **Desconfiá de los archivos adjuntos:** pueden causar la descarga de la clave de registro o instalar programas maliciosos (malware) en tu computadora.
- **Utilizá antivirus** y antimalware actualizado.
- **Actualizá tu sistema operativo** y el explorador de internet.

Algunos casos prácticos de ciberestafas

1

Consumidor navega desde sus dispositivos y se contacta, en búsqueda de asesoramiento, con un **perfil fraudulento** en redes sociales.

Recibe un **llamado telefónico o mensaje de WhatsApp** de un supuesto "asesor" de la empresa, quien lo va a ayudar con el inconveniente.

Consumidor engañado por el supuesto asesor, **comparte credenciales de acceso a HomeBanking, su Token y/o código de recupero**.

Con las claves de acceso, Token y/o código de recupero, el delincuente logra ingresar a HomeBanking y **fugar los fondos.**

2

El consumidor recibe **un llamado telefónico/mensaje de WhatsApp** de un origen desconocido, **indicándole que recibió un pago por error**.

El estafador envía un **comprobante de transferencia adulterado, solicitándole al consumidor que le devuelva los fondos** transferidos por "error".

El consumidor, habiendo sido engañado con un comprobante apócrifo, **transfiere los fondos voluntariamente al estafador,** produciendo así la fuga de los fondos.

3

A un allegado o familiar del consumidor **le vulneran su acceso a RR.SS** como Instragram, Facebook o WhatsApp.

El estafador, **haciéndose pasar por otra persona,** se contacta con este, **solicitándole una transferencia de forma urgente.**

El consumidor transfiere voluntariamente los fondos a la cuenta fraudulenta utilizada por los estafadores, permitiendo así la fuga de los fondos.

Métodos de protección: contraseñas

Las contraseñas son las primeras barreras de seguridad y protección de nuestra identidad virtual, así como de nuestros datos personales y fondos virtuales.

- **Utilizar contraseñas únicas** para cada cuenta o aplicación. De ser posible, cambiarlas con regularidad.
- **No utilizar contraseñas débiles** o predecibles como '123456' o 'password' o datos que podrían ser públicos como mi dirección legal o mi fecha de cumpleaños.
- **Las contraseñas deberían componerse de frases**, no palabras sueltas, y combinar alternadamente letras mayúsculas, minúsculas, números no consecutivos y caracteres especiales (como “!”, “@”, etc.).
- **No compartir contraseñas** con amigos, familiares o colegas ni como “texto plano” a través de aplicaciones de mensajería o correos electrónicos.
- **Evitar guardar contraseñas** en lugares inseguros como notas escritas o correos electrónicos no encriptados.
- **No aceptar la sugerencia** del navegador de guardar la contraseña.
- **Habilitar la autenticación** de dos factores siempre que sea posible.

Métodos de protección: malware

Malware es una aplicación o programa de software que, sin que lo sepas, permite que otra persona recopile o visualice toda la actividad de tu celular o computadora. Se instala sin pedirte permiso.

¿Cómo se puede infectar mi celular con un programa espía?

- Mientras bajás o ves una película de sitios no oficiales.
- Si navegás por un sitio web sospechoso que te obliga a:
  - suscribirte
  - descargar programas
  - completar encuestas
- Mientras instalás una aplicación no oficial en tu celular.
- Si compraste un celular en un negocio no oficial puede estar preinstalado.
- Alguna persona con acceso a tu celular lo instaló para tener tu información personal.

¿Qué medidas de seguridad puedo tomar?

- Instalar un antivirus y un antimalware.
- Conectarte a sitios seguros que tengan HTTPS.
- Evitar conectarte a sitios sospechosos.
- Descargar e instalar software y aplicaciones solo de sitios oficiales.
- No abrir correos electrónicos y archivos adjuntos de personas desconocidas.
- Activar las actualizaciones automáticas.
- Si sospechás que tu teléfono está infectado, podés restaurarlo a la configuración de fábrica.

Métodos de protección: SIM swapping

SIM swapping: es una técnica de ingeniería social que consiste en engañar a la empresa de telefonía o al usuario para tomar el control de la línea (SIM).

- **Mantener la tarjeta SIM segura** y fuera del alcance de personas no autorizadas.
- **Utiliza un código PIN** para proteger la tarjeta SIM.
- **No compartir tu número de tarjeta SIM** ni detalles de registro (ICCID: Integrated Circuit Card Identifier).
- **Reportar de inmediato la pérdida de tu SIM** o si sospechas que ha sido comprometida.
- Si recibimos un aviso de **reposición de tarjeta SIM** de nuestra compañía y no lo hemos solicitado, alertar a la empresa de inmediato.

Otros métodos de protección

- **Mantener el software actualizado**; sistema operativo, navegador y aplicaciones. Las ultimas versiones contienen las ultimas actualizaciones de seguridad.
- **Usar antivirus y antimalware;** realizar análisis de forma periódica.
- **Descargar aplicaciones solo de tiendas oficiales;** suelen realizar análisis sobre las aplicaciones disponibles, aunque no son infalibles.
- **Realizar copias de respaldo (back-up);** respaldar regularmente los datos importantes.
- **Evitar conexiones desde redes Wi-Fi públicas;** deshabilitar la opción cuando no la utilicemos, así como bluetooth y NFC.
- **Desactivar la ubicación, la cámara y el micrófono;** siempre que no sean necesarios.

Otros métodos de protección

- **Cuidado con los correos electrónicos y mensajes sospechosos;** Verificar que los remitentes de los correos electrónicos recibidos coincidan con el dominio oficial de las entidades o empresas.
- **No usar usuario administrador en el día a día;** en el sistema operativo podemos crear usuarios invitados o con permisos limitados para protegernos en caso de ataques.
- **No abrir enlaces que lleguen en mensajes de WhatsApp;** aunque el número tenga una descripción que diga “Mesa de ayuda” o similar, y la imagen de perfil sea la misma que identifica a la billetera digital, entidad bancaria o empresa conocida.
- **Atención al dar el celular a los niños;** pueden abrir correos y vínculos inseguros sin tener en cuenta estas precauciones.
- **No compartir códigos de verificación que se reciben por email, mensaje de texto o cualquier otra vía**; estos permiten blanquear la contraseña y tomar el control de la cuenta del usuario.

Ciberestafas vs. reclamos de consumo

Es importante diferenciar las ciberestafas o los fraudes, de los reclamos en el marco de las relaciones de consumo tradicionales.

Las ciberestafas o fraudes, que generalmente involucran engaños a través de medios electrónicos como correos electrónicos falsos, sitios web fraudulentos o aplicaciones maliciosas, están regidos por el Código Penal y leyes complementarias y son delitos.

Mientras que las relaciones de consumo, se refieren a los intercambios comerciales regulares entre proveedores y consumidores finales de bienes y servicios, estos se rigen por normativas específicas que protegen los derechos de los consumidores en términos de calidad, seguridad y cumplimiento de las condiciones pactadas.

Es fundamental que los consumidores comprendamos estas distinciones para saber cómo actuar y protegerse de manera efectiva en cada situación.

Veamos algunas características que nos permitan diferenciar estos conceptos mas fácilmente.

Ciberestafas vs. reclamos de consumo

Estafas	Reclamos de consumo
Generalmente hay una parte que engaña (el estafador) y otra que es engañada (la víctima).	Se establecen entre consumidores finales y proveedores. Son de naturaleza comercial.
Implican conductas engañosas o fraudulentas con la intención de obtener un beneficio económico ilícito a costa de otra persona.	Pueden surgir de incumplimientos contractuales o defectos en productos o servicios, sin necesariamente implicar una intención de provocar un daño.
Son necesariamente dolosas, es decir, con conocimiento y voluntad de producir un daño.	No es necesario que exista intención de causar daño para que una situación entre en el marco de una relación de consumo (aunque no es excluyente).
Son conductas tipificadas en el Código Penal y leyes complementarias.	Es aplicable la Ley de Defensa de Consumidor 24.240 (LDC).

Ciberestafas vs. reclamos de consumo

Ciberestafas

- Se tramitan como denuncias.
- Se deben denunciar ante la policía o la fiscalía especializada.
- Ver: donde hacer una denuncia por ciberdelitos; https://www.argentina.gob.ar/justicia/convosenlaweb/denuncia

Reclamos de consumo

- Se tramitan como reclamos.
- Se deben tramitar ante Ventanilla Única Federal (VUF) o dependencias locales.
- Ver: como cargar un reclamo en COPREC; https://www.argentina.gob.ar/servicio/iniciar-un-reclamo-ante-defensa-del-consumidor

AUNQUE SE TRATA DE CONCEPTOS DISTINTOS QUE SE TRAMITAN EN LUGARES DIFERENTES,
NO SON NECESARIAMENTE EXCLUYENTES.

Ejemplo: Si utilicé una plataforma apócrifa que simulaba ser otro sitio legitimo; puedo hacer la denuncia penal contra los organizadores del sitio web falso, pero también se puede gestionar un reclamo contra la empresa real si ésta no hubiera cumplido con su deber de información, seguridad o no hubiera dado la protección suficiente de los datos personales del Consumidor.

Ley de Defensa del Consumidor (LDC) 24.240 aplicada a ciberestafas

Como hemos visto, las estafas digitales son comportamientos tipificados en el código penal, pero no son excluyentes de aplicar la **LDC 24.240:**

- **Deber de información (art. 4):** Los proveedores deberán proveer a los consumidores toda la información relativa a seguridad, prevención de riesgos, posibles fraudes y canales de comunicación oficiales.
- **Deber de seguridad (art. 5):** En el ámbito financiero, máxime cuando se emplean canales digitales, los proveedores deberán velar que las operaciones que se realicen a través de sus plataformas, aplicaciones, dispositivos o canales de atención sean seguros y prevenir riesgos y peligros a los que puedan estar comprometidos la seguridad, los datos personales o los intereses económicos de los consumidores, cuestiones que se encuentran protegidas por el art. 42 de la CN.
- **Responsabilidad solidaria por daños (art. 40):** todos los proveedores involucrados en la cadena de comercialización son igualmente y solidariamente responsables frente al consumidor.
- **Trato digno y equitativo (art. 8 bis):** pesa sobre los proveedores que ofrecen sus productos o servicios a través de Internet o plataformas digitales la obligación de dispensar un trato digno y equitativo a los consumidores y usuarios, víctimas de ciberdelitos o delitos informáticos.

Denuncias y reclamos

¿Dónde realizar una denuncia por ciberestafa?

- **Fiscalía más cercana a tu domicilio**
  Podés buscarla en el *mapa de Fiscalías del Ministerio Público Fiscal*.
- **Ministerio Público Fiscal. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)**
  - **Dirección: Sarmiento 663, Piso 6, Ciudad Autónoma de Buenos Aires.**
  - **Teléfono: (54-11) 5071-0040**
  - **Correo:** *denunciasufeci@mpf.gov.ar.*
  - **Sitio web:** *https://www.mpf.gob.ar/ufeci/*

¿Dónde realizar un reclamo de consumo de consumo?

- **Defensa del Consumidor:** por *Ventanilla Única Federal (VUF)*.
- ***OMICs y delegaciones locales***
- También podés asesorarte llamando a la línea gratuita **0800-666-1518**, de **lunes a viernes de 10 a 16 hs.**

Fuentes

- CERT.ar; Informe anual de incidentes informáticos 2023.
- Ministerio de Justicia; https://www.argentina.gob.ar/justicia/convosenlaweb
- “Cómo prevenir estafas”, sitio web BCRA.
- Última revisión: agosto 2024.

¡Gracias!