PREVENCIÓN DE ESTAFAS DIGITALES

Secretaría de Modernización | LA PLATA CAPITAL
Secretaría de Justicia | LA PLATA CAPITAL

PREVENCIÓN DE ESTAFAS DIGITALES

Indice

¿Qué son las estafas digitales?

Entendemos por estafas digitales a aquellos engaños perpetrados mediante el uso de tecnologías digitales o medios electrónicos, con el objetivo de apropiarse de dinero ajeno, realizar compras no autorizadas, obtener créditos, amenazar, robar datos personales o información sensible de individuos u organizaciones, vulnerando su privacidad. Estas acciones pueden incluir, además, la suplantación de identidad, el acoso digital y sexual, o la comisión de delitos contra la integridad sexual.

Estas prácticas ilícitas se basan en la obtención ilegal de datos personales, como usuarios, contraseñas, tokens, números de tarjetas de crédito y débito, accesos a homebanking, billeteras virtuales y cuentas de aplicaciones o redes sociales, con el fin de llevar a cabo operaciones fraudulentas.

Marco Legal

Las ciberestafas como delito

La estafa está tipificada en el artículo 172 del Código Penal, que establece: “Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño”.

La **Ley Nacional N° 26.388** incorpora y tipifica los Delitos Informáticos en el Código Penal Argentino, con el fin de regular el uso de las nuevas tecnologías como medios para la comisión de delitos. Esta normativa modifica, reemplaza y actualiza varios artículos del Código Penal, con el objetivo de clasificar, detallar y enunciar las distintas modalidades de ciberestafas, así como las sanciones y penas que les corresponderán.

¿Cuáles son los tipos más comunes de ciberestafas?

La ingeniería social consiste en un conjunto de técnicas utilizadas para manipular o engañar a las personas con el fin de obtener información personal, acceder a datos confidenciales de individuos u organizaciones, o incluso suplantar identidades. Estas prácticas pueden incluir amenazas, extorsión, fraude, acoso digital o sexual, y en muchos casos buscan obtener un beneficio económico de manera ilícita.

Existen también programas maliciosos, diseñados específicamente para dañar, destruir o modificar datos informáticos sin el consentimiento del usuario. Estos programas pueden hacer que la información sea inaccesible, alterada o suprimida, y generalmente se desarrollan con fines económicos o para causar perjuicios a las personas u organizaciones afectadas.

PHISHING

Es una técnica maliciosa utilizada para obtener información confidencial o datos personales mediante **correos electrónicos y/o sitios web falsos**. Los estafadores emplean logos y diseños oficiales para engañar a las víctimas y lograr que revelen sus datos personales. Estas comunicaciones suelen contener enlaces que redirigen a páginas web fraudulentas con el objetivo de captar información sensible. No abra enlaces sospechosos.

SPEAR PHISHING

Es un tipo de phishing dirigido a un objetivo específico, con el fin de obtener información específica de la víctima, y así personalizar los ataques y aumentar su efectividad.

SMISHING

Este método de fraude consiste en el envío de **mensajes de texto, WhatsApp o a través de redes sociales** para engañar a los usuarios. Los mensajes simulan provenir de instituciones bancarias u otras entidades, y tienen como objetivo inducir a las víctimas a acceder a sitios web fraudulentos, proporcionar información confidencial o realizar transferencias y pagos. Nunca comparta códigos ni claves.

WHATSAPP

Una de las estafas más comunes en WhatsApp es la **conocida como estafa de los 6 dígitos**, que consiste en engañar a la víctima para que comparta un código de verificación enviado a su número de contacto. Con este código, los estafadores acceden a la cuenta de WhatsApp y, mediante el uso de identidades fraudulentas, solicitan dinero a los contactos de la víctima.

VISHING

Se lleva a cabo mediante **llamadas telefónicas**, en las que los estafadores se presentan como representantes de bancos u otras instituciones con el fin de solicitar información personal. A veces utilizan simulaciones de contestadores automáticos para engañar a las víctimas. Recientemente, el uso de inteligencia artificial (IA) ha dado lugar a nuevas estafas mediante voces clonadas. Es fundamental no proporcionar datos personales a menos que se tenga plena certeza sobre la autenticidad de la llamada. Evite atender a desconocidos.

VIDEOLLAMADAS

Este tipo de fraude corresponde a la modalidad conocida como **vishing**, en la que los estafadores, a través de videollamadas en las que permanecen ocultos, engañan a las víctimas para que revelen información confidencial. Durante la llamada, comparten su pantalla con el fin de obtener datos sensibles y operar de manera ilícita.

SKIMMING

Es un riesgo al que podemos estar expuestos al **utilizar cajeros automáticos o terminales de pago (POS)**. Este fraude consiste en la obtención no autorizada de la información de la tarjeta mediante dispositivos ocultos instalados en estos equipos.

ESTAFAS EN LÍNEA

Técnica que implica el uso de **sitios web o aplicaciones de compraventa** para engañar a las personas actuando como falsos compradores o falsos vendedores.

HACKEO

A través del **hackeo o acceso ilegítimo a cuentas ajenas** de redes sociales o aplicaciones de mensajería, buscan suplantar la identidad de la persona para solicitar dinero a conocidos de la víctima refiriendo una urgencia, realizar **ventas falsas** o **estafar** a otras personas.

BLUESNARFING

Fraude mediante el cuál se aprovechan vulnerabilidades en la conexión Bluetooth para acceder de manera no autorizada a datos personales almacenados en dispositivos cercanos, como contactos, calendarios, correos electrónicos o incluso fotos. Este ataque puede ocurrir sin que el usuario sea consciente de que su dispositivo está siendo accedido. Es recomendable **desactivar el Bluetooth** cuando no se utilice, mantenerlo en modo "no visible", emparejar solo con dispositivos confiables, utilizar contraseñas seguras, actualizar regularmente el software y evitar usarlo en lugares públicos.

¿Cómo nos cuidamos de las estafas digitales?

Recomendaciones generales

Para protegerse de posibles intentos de phishing, le sugerimos tener en cuenta las siguientes medidas de seguridad:

- **Nunca ingrese información confidencial en correos electrónicos sospechosos ni en sitios a los que haya accedido mediante enlaces adjuntos.**
- **Antes de proporcionar cualquier dato o interactuar en un sitio web, asegúrese de que se trata de una página oficial verificando la dirección URL.** Los sitios legítimos utilizan 'https://', lo que indica que la transmisión de datos se encuentra protegida mediante cifrado. Este protocolo, respaldado por un certificado SSL/TLS, autentica la identidad del sitio y garantiza que está visitando una página confiable.
- **En caso de que la URL no cuente con 'https://', es fundamental verificar la legitimidad del sitio o la dirección de correo electrónico.** Para ello, revise cuidadosamente la parte del dominio que sigue al símbolo '@' en las direcciones de correo electrónico o examine la URL completa, ya que estos elementos permiten identificar si se trata de una fuente legítima o sospechosa.
- **Se sugiere prestar atención a la extensión del dominio de un sitio web.** Es importante tener en cuenta que los dominios con extensión .com son de uso abierto y pueden ser registrados por cualquier persona o entidad, lo que facilita su uso fraudulento. En cambio, .gob.ar es un dominio de nivel superior reservado exclusivamente para entidades gubernamentales en Argentina, lo que asegura la autenticidad del sitio. De manera similar, existen otros dominios específicos como .org, destinado a organizaciones sin fines de lucro, o .edu, utilizado por instituciones educativas, que también pueden ayudar a identificar sitios web confiables.

- **Las claves bancarias, los datos de usuario y la información de tarjetas de crédito o débito** constituyen datos personales que **deben mantenerse en estricta confidencialidad.** No deben ser compartidos con desconocidos, incluso si se presentan como personal de entidades oficiales. Asimismo, es importante evitar la publicación de esta información en redes sociales, donde puede quedar expuesta a terceros.

- **Conservar un registro:** Es recomendable guardar un historial de las transacciones financieras y revisar regularmente los estados de cuenta para identificar actividades sospechosas a tiempo. En caso de detectar alguna, se debe informar de inmediato a la entidad bancaria o billetera virtual correspondiente.

- Ningún banco ni organismo del Estado solicitará datos personales a través de teléfono, correo electrónico o redes sociales. **En ningún caso se deben proporcionar datos sensibles**, como usuarios y claves bancarias, en respuesta a llamadas telefónicas.

- **Validar siempre que el número de teléfono desde el cual se realiza el contacto sea el oficial.** Si se tiene duda sobre su veracidad, es recomendable finalizar la comunicación, buscar los números habilitados por el organismo o entidad, y contactar directamente para verificar la autenticidad del llamado.

- Al acceder a las redes sociales del banco o billetera virtual, **confirme que la cuenta sea oficial mediante el ícono de verificación junto al nombre de usuario**. Si ingresa a través de un sitio web, asegúrese de que la dirección comience con "https://" y que muestre un candado cerrado en la barra de direcciones, lo cual garantiza la seguridad y autenticidad del sitio.

- Evite realizar reclamos o solicitar ayuda y asesoramiento a través de comentarios en publicaciones en redes sociales, ya que esto puede habilitar contactos con perfiles falsos que se ofrecen como ayuda. **Siempre utilice los canales de contacto oficiales y de referencia para comunicarse.**

- Las personas representantes y empleadas de entidades bancarias y del Estado **nunca solicitan claves y/o contraseñas de las y los usuarios** para asesorarlas/os o resolver un inconveniente por teléfono, Whatsapp, correo electrónico o redes sociales.
  Si recibe una solicitud de este tipo, manténgase alerta, ya que podría tratarse de un intento de estafa. **En tal caso, se recomienda no responder y, si la comunicación es telefónica, finalizarla de inmediato.**

- En los servicios de mensajería, es fundamental **verificar la identidad de la persona** con la que se está interactuando antes de compartir información personal o acceder a enlaces.

- En lo posible utilizar métodos de pago seguros, como tarjetas de crédito o plataformas de pago en línea con protección al comprador.

Otros consejos importantes en relación al uso de tarjetas:

- Nunca pierdas de vista tus tarjetas en el proceso de cobro.
- Verifica que la tarjeta no haya sido utilizada en más de un dispositivo de lectura.
- Evita entregar la tarjeta a terceros para que realicen el pago en otra área del establecimiento.
- Evita recibir ayuda de personas desconocidas y jamás reveles datos sensibles como tu clave de acceso al cajero.

- Al realizar un pago por transferencia, **verificar el comprobante** para asegurarse de que sea legítimo y confirme que el dinero haya impactado en la cuenta correspondiente. Además, es recomendable **revisar periódicamente** los movimientos en el Home Banking o billetera virtual.

- Antes de realizar una compra o venta en línea, es fundamental **corroborar la identidad del vendedor o comprador**. Lea reseñas, verifique su historial de ventas y busque posibles reclamos o denuncias en línea.

- Se recomienda **utilizar plataformas de confianza** que sean reconocidas y con medidas de seguridad establecidas para realizar compras en internet. **Leer las políticas de seguridad y privacidad** de la plataforma antes de realizar cualquier transacción.

- Al realizar compras o ventas en línea, **verifique cuidadosamente la información del producto y evite comunicarse fuera de la plataforma**. No comparta su correo electrónico ni número de teléfono hasta verificar la legitimidad del comprador o vendedor.

PREVENCIÓN DE ESTAFAS DIGITALES

recomendaciones

página 12

- **Mantener el software actualizado:** Instalar actualizaciones de seguridad en todos los dispositivos, incluyendo sistemas operativos, navegadores web y aplicaciones.

- **Utilizar contraseñas seguras:** Es recomendable emplear contraseñas únicas para cada cuenta, que sean difíciles de adivinar pero fáciles de recordar, combinando letras, números y caracteres especiales.

- **Proteger dispositivos:** Se recomienda utilizar soluciones de seguridad como antivirus y firewalls en los dispositivos, para salvaguardarlos contra malware y otras amenazas.

- **Mantener precaución al utilizar redes Wi-Fi públicas:** Es aconsejable no acceder a información sensible ni realizar transacciones financieras mientras se esté conectado a redes Wi-Fi públicas, especialmente si no se tiene la certeza sobre la autenticidad del dominio de la misma, ya que estas pueden ser vulnerables a posibles ataques.

- **Habilitar la verificación en dos pasos** en las aplicaciones que lo permitan, proporcionando una capa adicional de seguridad. Además, es fundamental mantener el dispositivo actualizado, ya que las nuevas versiones de las aplicaciones incluyen parches de seguridad que refuerzan la protección contra posibles amenazas.

- **Bloquear y reportar como spam** mensajes o enlaces sospechosos para ayudar a proteger a otros usuarios.

- No descargar aplicaciones de sitios inseguros o archivos adjuntos si se desconoce al remitente. **Siempre verificar qué tipo de programa o aplicación se está instalando**.

- **Desactivar la función de autocompletar formularios** con datos sensibles en el navegador web de los dispositivos electrónicos.

- Se sugiere **ingresar a las páginas web tipeando la dirección** en la barra de direcciones. Seleccionando en buscadores web se corre el riesgo de ingresar a páginas falsas, es importante revisar siempre el nombre de la página.

Denuncias y reclamos

- Para **realizar denuncias**, diríjase a la **Comisaría** o **Fiscalía** de turno más cercana.
- Para recibir **asesoramiento** o iniciar un reclamo, contacte con la **Dirección General de Defensa al Consumidor de la Municipalidad de La Plata**

> DIRECCIÓN: Calle 11 nro 1079
> DÍAS Y HORARIOS DE ATENCIÓN AL PÚBLICO: lunes a viernes de 8:00 a 14:00 horas
> Para iniciar tu reclamo online y/u obtener más información *https://defensaconsumidor.laplata.gob.ar/*