GOBIERNO DEL PARAGUAY | MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GUÍA PARA APRENDER A IDENTIFICAR FRAUDES EN LÍNEA

INDICE

Introducción

En la actualidad, el uso cotidiano de internet para actividades como la comunicación, las compras, la búsqueda de empleo o la contratación de servicios ha incrementado considerablemente la exposición de los usuarios a diversos tipos de fraudes digitales. La facilidad con la que los ciberdelincuentes pueden suplantar identidades, crear sitios falsos o manipular emocionalmente a sus víctimas ha convertido a la estafa online en una de las amenazas más frecuentes y perjudiciales del entorno digital.

Esta guía, elaborada por el Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY), tiene como objetivo proporcionar al lector información práctica para reconocer y prevenir los fraudes más comunes en internet. Se presentan distintos escenarios fraudulentos organizados en diez categorías, junto con señales de alerta y recomendaciones de seguridad específicas para cada caso.

Conocer cómo operan los estafadores es el primer paso para evitar ser víctima de sus engaños. Por ello, esta guía busca fortalecer la cultura de ciberseguridad de los usuarios, promoviendo una navegación más segura, informada y responsable.

Guía para aprender a identificar fraudes en línea

La Guía para aprender a identificar fraudes en línea del Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY) ofrece información detallada sobre los fraudes más comunes en internet y cómo protegerse de ellos. A continuación, se resumen los principales tipos de fraudes abordados en la guía:

1. Phishing

Técnica utilizada para obtener información confidencial haciéndose pasar por entidades legítimas. Los atacantes envían correos electrónicos, mensajes de texto o enlaces fraudulentos que redirigen a sitios web falsificados para robar credenciales de acceso, datos bancarios o información personal.

Señales de alerta:

- Correos electrónicos con urgencia para actualizar información de cuentas.
- Mensajes con errores ortográficos o gramaticales.
- Enlaces sospechosos o remitentes desconocidos.

Recomendaciones de seguridad:

- No hacer clic en enlaces de correos electrónicos sospechosos.
- Verificar directamente con la entidad si una solicitud es legítima.
- Activar la autenticación en dos pasos en cuentas sensibles.

2. Falsos préstamos

Ofertas de préstamos con condiciones demasiado favorables que buscan engañar a las víctimas. Generalmente, los estafadores piden pagos por adelantado en concepto de comisiones o trámites administrativos.

Señales de alerta:

- Intereses muy bajos sin verificación de historial crediticio.
- Solicitud de pagos previos antes de otorgar el préstamo.
- Falta de información de contacto verificable.

Recomendaciones de seguridad:

- Investigar la reputación de la entidad financiera.
- No realizar pagos anticipados sin haber recibido el préstamo.
- Consultar con organismos oficiales sobre la legalidad de la empresa.

3. Tiendas online fraudulentas

Sitios web que venden productos inexistentes o de baja calidad, atrayendo a los consumidores con precios demasiado bajos.

Señales de alerta:

- Ofertas con descuentos irreales.
- Falta de datos de contacto o servicio al cliente.
- Métodos de pago sin garantías de seguridad.

Recomendaciones de seguridad:

- Comprar en sitios web reconocidos y revisar las opiniones de otros compradores.
- Verificar que el sitio tenga el protocolo de seguridad *HTTPS*.
- Usar métodos de pago seguros como tarjetas con protección antifraude.

4. Falsos alquileres

Anuncios de propiedades en alquiler que no existen o no están disponibles. Los estafadores suelen solicitar depósitos o pagos por adelantado sin mostrar la propiedad.

Señales de alerta:

- Propiedades a precios muy por debajo del mercado.
- Solicitud de pagos antes de firmar un contrato.
- Imposibilidad de visitar la propiedad antes de la transacción.

Recomendaciones de seguridad:

- Visitar la propiedad en persona o hacer videollamadas antes de pagar.
- Usar plataformas reconocidas para alquileres.
- No compartir información personal con desconocidos.

5. Falso soporte técnico

Los estafadores llaman o envían mensajes afirmando que han detectado un virus o problema en el dispositivo de la víctima. Su objetivo es obtener acceso remoto o información personal.

Señales de alerta:

- Llamadas inesperadas de "técnicos" de Microsoft, Apple u otras empresas.
- Solicitudes de instalación de programas de acceso remoto.
- Pedidos de información confidencial como contraseñas.

Recomendaciones de seguridad:

- No proporcionar acceso remoto a desconocidos.
- Contactar directamente al soporte oficial de la empresa.
- Instalar software de seguridad confiable y actualizar el sistema operativo.

6. Falsas ofertas de empleo

Propuestas laborales fraudulentas que buscan obtener dinero o información personal de los solicitantes.

Señales de alerta:

- Ofertas con sueldos muy altos sin requisitos de experiencia.
- Solicitud de pagos para capacitaciones o materiales de trabajo.
- Empresas sin presencia verificable en internet.

Recomendaciones de seguridad:

- Buscar referencias sobre la empresa antes de postularse.
- Nunca pagar por acceder a una oferta de trabajo.
- Revisar el correo del remitente y evitar enlaces sospechosos.

7. Sextorsión

Los delincuentes amenazan con divulgar imágenes o información íntima a menos que la víctima realice un pago.

Señales de alerta:

- Mensajes amenazantes de desconocidos con información personal.
- Correos indicando que han hackeado la computadora de la víctima.
- Solicitudes de dinero con urgencia para evitar la supuesta filtración de datos.

Recomendaciones de seguridad:

- No responder ni pagar a los extorsionadores.
- Denunciar el caso ante las autoridades correspondientes.
- Evitar compartir contenido sensible con personas que no sean de confianza.

8. Perfiles falsos

Creación de identidades falsas en redes sociales para engañar a los usuarios y obtener información o dinero.

Señales de alerta:

- Cuentas con pocos seguidores y sin publicaciones antiguas.
- Solicitudes de amistad o mensajes de desconocidos con historias trágicas o románticas.
- Peticiones de dinero o datos personales tras poco tiempo de interacción.

Recomendaciones de seguridad:

- Verificar la identidad de la persona antes de aceptar solicitudes.
- No compartir información personal con desconocidos.
- Configurar la privacidad de las redes sociales para limitar el acceso a los datos personales.

9. Fraudes en compraventa de productos

Estafas en transacciones de productos de segunda mano, donde el comprador o vendedor no cumplen con lo acordado.

Señales de alerta:

- Ofertas demasiado atractivas en comparación con el mercado.
- Vendedores que insisten en pagos inmediatos sin garantías.
- Compradores que envían cheques falsos o pagos fraudulentos.

Recomendaciones de seguridad:

- Usar plataformas de compraventa reconocidas.
- Evitar pagos por adelantado sin garantías.
- Realizar entregas en lugares públicos y verificar el dinero recibido.

10. Fraudes bancario

El fraude bancario es un conjunto de estafas dirigidas a usuarios de servicios financieros, cuyo objetivo es robar dinero o información confidencial relacionada con cuentas, tarjetas y accesos en línea. Los ciberdelincuentes emplean distintas modalidades, desde engaños digitales hasta manipulaciones físicas.

Modalidades frecuentes:

- **Phishing bancario:** correos, SMS o páginas falsas que imitan a entidades financieras para robar credenciales.
- **Smishing y vishing:** mensajes de texto o llamadas telefónicas que simulan provenir del banco para solicitar información sensible.
- **Skimming**: clonación de tarjetas a través de dispositivos instalados en cajeros automáticos o terminales de pago.
- **Robo de identidad:** uso de datos personales para abrir cuentas o solicitar créditos fraudulentos.
- **Transferencias no autorizadas:** manipulación de operaciones en banca online o aplicaciones móviles.

Señales de Alerta

- Comunicaciones con tono urgente que solicitan verificar o actualizar datos bancarios.
- Enlaces sospechosos en correos, SMS o chats que redirigen a sitios no oficiales.
- Solicitudes de PIN, token u otros datos confidenciales por canales no habituales.
- Movimientos o cargos desconocidos en las cuentas.

Recomendaciones de seguridad:

- Acceder siempre a la banca online escribiendo la dirección oficial del banco.
- No compartir claves ni datos sensibles por teléfono, correo o mensajería.
- Activar notificaciones de movimientos y la autenticación en dos pasos (2FA) cuando esté disponible.
- Revisar periódicamente estados de cuenta y reportar de inmediato cualquier irregularidad.
- Usar cajeros y terminales de pago en lugares seguros para reducir el riesgo de clonación de tarjetas.

Conclusión

La proliferación de fraudes online representa un desafío constante para la seguridad de los usuarios en el entorno digital. Los ciberdelincuentes emplean métodos cada vez más sofisticados y persuasivos para engañar a sus víctimas, aprovechándose muchas veces del desconocimiento o la falta de precaución. Por ello, estar informado es una de las herramientas más eficaces para prevenir este tipo de delitos.

A lo largo de esta guía se han descrito las principales modalidades de estafas digitales, sus señales de alerta y las recomendaciones clave para evitarlas. Desde correos de phishing hasta falsas ofertas de empleo o perfiles engañosos en redes sociales, todos estos fraudes comparten un mismo objetivo: obtener datos personales o dinero de forma ilícita.

La prevención comienza con una actitud crítica ante lo que recibimos o compartimos por internet. Validar la fuente, desconfiar de lo que parece demasiado bueno para ser cierto, proteger nuestros datos y denunciar cualquier intento de fraude son prácticas esenciales para resguardar nuestra seguridad en línea.

Promover una ciudadanía digital responsable y consciente no solo protege a cada individuo, sino que también contribuye a un entorno digital más seguro para todos.

Fuente:

- https://www.incibe.es/sites/default/files/docs/guia_fraudes/guia-fraudes-online.pdf
- https://www.ezarolegal.es/blog/como-identificar-una-estafa-online-guia-completa-evitar-fraudes-internet/