Cuáles son las estafas virtuales más comunes y cómo evitarlas

12/06/2023

Los dispositivos conectados a Internet son parte del día a día de la mayoría de las personas del mundo. Es por eso que la **ciberseguridad debe ser primordial** a la hora de realizar trámites o simplemente navegar en al web. Y es que la facilidad y comodidad para realizar transacciones en línea o acceder a datos personales **acarrea un creciente número de amenazas**.

Las **estafas por Internet** suelen combinar elementos comunes en los mecanismos de fraude y que son utilizados por los delincuentes para robar datos, información y dinero. El principal es la **suplantación de identidad,** que tiene como consecuencia la urgencia, desesperación o poca información de la víctima. Es por ello que hay que cuidarse de ciertos engaños virtuales.

Estafas virtuales. Foto: NA.

Phishing

Quizás **la estafa más utilizada**. En ella, los ciberdelincuentes **se hacen pasar por un tercero de confianza** para que las víctimas brinden información o descarguen programas maliciosos. Suele llevarse a cabo mediante correo electrónico, mensajes de texto o vía WhatsApp, por donde se envía un enlace que dirige a una página falsa que simula ser la oficial de una empresa u organismo. Al ingresar los datos personales, los delincuentes **los habrán capturado y podrán acceder a la cuenta de la persona y cambiar las claves**. Los ataques de phishing están en su nivel más alto en 3 años.

Cuentas falsas y perfiles clonados

Este fraude consiste en **simular ser una persona conocida de la víctima y pedirle transacciones por diferentes motivos.** Esto se da luego de que el delincuente obtiene acceso a una cuenta de WhatsApp, desde donde comienza a comunicarse con todos los contactos de la agenda, haciéndose pasar por el dueño del perfil.

Estafas «románticas»

Los ciberdelincuentes también se aprovechan de las personas que buscan pareja o un encuentro romántico a través de internet. Esto no solamente sucede en aplicaciones de citas, como **Tinder,** sino que también aparecen en las redes sociales. En estos casos, el estafador se gana la confianza de la víctima y **luego de promesas de encuentros, le solicita dinero**. En otras oportunidades, se incluye la amenaza de **publicar fotos íntimas** del damnificado a menos que se les haga un depósito.

Estafa virutal. Foto: Unsplash.

Estafas desde cuentas verificadas

En manos de delincuentes, la verificación en redes sociales como Instagram o Twitter puede ser aprovechada para **engañar a usuarios y conseguir datos privados** o solicitar transferencias por la compra de un producto que nunca llega.

Scareware

Se trata de **programas maliciosos que tienen el objetivo de engañar a los usuarios para que visiten sitios web infectados con virus**. Estos suelen aparecer en ventanas emergentes, con mensajes o advertencias que simulan a publicidades de empresas legítimas. Ante estas situaciones, muchas personas terminan comprando software inútil, descargan un virus verdadero o visitan sitios infectados, desde donde les pueden robar datos personales.

Ofertas y ventas falsas

Estas estafas ocurren en torno a las **compraventas,** y principalmente se dan en el Marketplace de Facebook. Muchas veces, luego de enviar una transferencia, el producto no llega nunca y el vendedor **desaparece de la plataforma**. En ocasiones más graves, **la víctima es interceptada por ladrones en el lugar pactado para el intercambio.**

Hackers. Foto: Unsplash.

Cómo prevenir estas estafas virtuales

El **sentido común,** la **información** y mantener la **calma** son las tres vías de prevención fundamentales ante este tipo de

estafas virtuales. Además, existe una serie de consejos para evitar caer en estas cibertrampas.

- Prestar atención a la URL (la dirección) de la página donde vas a ingresar tus datos. Corroborar que tenga el candado a la izquierda y que comience con https://.
- Recordar que los bancos, los organismos gubernamentales y otras entidades nunca piden claves por teléfono, correo electrónico o redes sociales.
- Desactivar la descarga de archivos automática en los dispositivos.
- En caso de recibir un mensaje desesperado de una persona cercana, contactarla por otro medio y confirmar que se trata de un pedido genuino.
- No abrir archivos adjuntos en correos de remitentes desconocidos o sospechosos.

Fuente: Diario 26