Tipos de fraude digital: ¿Cómo funcionan y cómo proteger tus cuentas digitales?

Recopilado por Amalia Beltrán

El fraude digital continúa siendo uno de los principales vectores de ataque utilizados por delincuentes, en el cual buscan engañar y/o manipular para obtener información, dinero o acceso no autorizado a recursos.

Durante los últimos años, los esquemas de fraudes han evolucionado significativamente derivado del uso de tecnología, redes sociales y, con ello, nacen nuevas técnicas de ingeniería social permitiendo a los delincuentes operar con mayor alcance y sofisticación.

Debido a los eventos masivos que se aproximan en los siguientes meses, desde Hot Sale hasta el Mundial de Fútbol, se anticipa un incremento en la publicación de anuncios y ofertas sospechosas, lo que podría resultar en un aumento de intentos de fraude relacionados con dichos eventos.

¿Cuáles son los tipos de fraude digital más comunes?

Fraudes por Phishing (correo electrónico falso). El atacante envía correos electrónicos que aparentan provenir de instituciones o personas legítimas, buscando que la víctima:

Ingrese a un sitio falso.
Descargue archivos maliciosos.
Proporcione información confidencial o haga alguna acción "con urgencia".
Mensajes que generan presión o urgencia para que el usuario actúe rápidamente.
En este tipo de fraudes, los atacantes suelen copiar logotipos, formatos y lenguaje institucional para hacer el mensaje creíble.
¿Cómo prevenirlo?
Verifica siempre el remitente del correo electrónico.
Ingresa a sitios web escribiendo la dirección directamente en el navegador.
No hagas clic en enlaces sospechosos.
No descargues archivos adjuntos inesperados.
Reporta correos electrónicos sospechosos.
De igual manera, existen otros tipos de fraudes digitales similares como: Vishing y Smishing. Conoce más sobre cómo funcionan y cómo protegerte.

Fraude por Soporte Técnico

En este tipo de fraude los delincuentes se hacen pasar por personal de soporte técnico de empresas de tecnología o instituciones financieras.
El contacto suele ocurrir por: llamadas telefónicas, mensajes de texto, ventanas emergentes de páginas web.
Los mensajes de este tipo suelen indicar que el dispositivo o cuenta digital del usuario presenta algún problema sobre presencia de virus, actividad sospechosa en su equipo o cuentas digitales o detectan supuestas fallas de seguridad.
En estos escenarios, el supuesto técnico solicita a la víctima algunas de las siguientes acciones:
Instalación de software de acceso remoto.
Proporcionar contraseñas o claves de acceso.
Realizar pagos por servicios.
Una vez que el delincuente tiene acceso al equipo o dispositivo, pueden robar información, instalar software malicioso (malware) o exigir pagos adicionales.
¿Cómo prevenirlo?
No permitir acceso remoto de personas desconocidas a tu equipo.
Ignorar alertas de seguridad que aparezcan dentro de sitios web.
No instalar software recomendado por fuentes no validadas.
Contactar directamente al proveedor oficial del soporte técnico para reportar o validar.

Fraude Financiero

El fraude financiero busca obtener dinero directamente de tu banca en línea o cuentas digitales. Los atacantes pueden intentar acceder a tus cuentas digitales mediante:
Robo de datos bancarios, como tarjetas de crédito y débito.
Clonación de tarjetas mediante dispositivos instalados en cajeros.
Acceso no autorizado a cuentas bancarias o banca en línea.
Manipulación para convencer a la víctima de realizar transferencias