MODALIDADES DE ROBO ELECTRÓNICAS

MY® Edison Urriago Cerquera

SMISHING
Mensajes de texto maliciosos

Los criminales buscan tener toda la información confidencial de su víctima y el medio para lograrlo es a través de mensajes de texto

VISHING
Llamadas telefónicas para extraer información confidencial

Intentan ganar la confianza de la víctima llamándola y haciéndose pasar por funcionarios de una entidad financiera

PHISHING
Correo electrónico con enlace a sitios fraudulentos

Es una táctica en la que los criminales suplantan entidades confiables como empresas de pagos en línea, agencias gubernamentales o entidades financieras

SIM SWAPPING
Hurto tarjeta SIM de celular

- A través de llamadas telefónicas los delincuentes engañan a sus víctimas recabando su información personal
- Posteriormente se ponen en contacto con las compañías de telefonía celular solicitando reposición de la tarjeta SIM

WEB SCRAPING
Robo de datos en sitios web

- A través de un programa informático, extraen contenido y datos de un sitio web, logrando almacenar de manera automatizada grandes cantidades de bases de datos encontradas en los diversos motores de navegación
- Posteriormente usa dicha información en contra de los incautos

RECOMENDACIONES PARA NO CAER EN EL ENGAÑO

1. **Utilizar dispositivos de confianza**
   Una de las formas más sencillas de prevenir un ciberataque es haciendo uso de dispositivos propios o de confianza al momento de hacer una transacción y/o compra
2. **Usted es la mejor contraseña**
   Si su celular lo permite, active biometría, desbloqueo y protección de aplicaciones mediante huella digital o reconocimiento de rostro; así, solo usted podrá autorizar transacciones
3. **No abrir correos electrónicos ni mensajes desconocidos**
   Existe toda una estrategia para enviar enlaces fraudulentos a partir de correos electrónicos o mensajes de texto con asuntos llamativos como: "espectaculares descuentos", "sólo por hoy", "has ganado".
   ¡Preste atención! estos mensajes pueden incluir archivos adjuntos maliciosos
4. **Asegurarse de entrar siempre a las páginas oficiales**
   Descargar las Apps de las tiendas oficiales (App Store y Play Store) y asegurarse de que el enlace donde se están haciendo las compras corresponde al sitio de la tienda digital
5. **Tener cuidado con la ingeniería social**
   Desconfíe de cualquiera que le solicite datos personales y bancarios, ya que estos no se deberán proporcionar a nadie
6. **Utilizar claves de seguridad diferentes**
   Es conveniente que se utilicen varias claves, ya que cuantas más capas de seguridad haya, más difícil será acceder a nuestra información sensible

¿CÓMO HACER MÁS SEGURAS LAS PASARELAS DE PAGOS?

1. **Seguridad**
   - Certificación PCI-DSS Nivel 1 vigente
     Objetivo: reducir el uso fraudulento de los métodos de pago
   - 3D Secure
     Objetivo: prevenir el fraude por uso de tarjetas en plataformas online
   - Tokenización
     Objetivo: el fraude al reemplazar los datos de la tarjeta de crédito
2. **Integraciones fáciles y en las 2 vías**
   - Con la plataforma web
   - Con otros proveedores
3. **Cobertura extendida**
   Empresas con experiencia internacional, que tengan operación local y cuya tecnología sea respaldada en todos los mercados