Cuidado con las Estafas de Phishing

Los 5 métodos más usados por los estafadores para intentar robar su información

Los delincuentes cibernéticos están contando con que estemos distraídos y bajemos la guardia. Si lo hacemos pueden engañarnos para que les demos nuestra información personal o financiera usando una de sus tácticas favoritas: phishing.

Quizás esté familiarizado con el phishing por email pero no es el único tipo de phishing con el que podría encontrarse. Los delincuentes también recurren a llamadas telefónicas, mensajes de texto, sitios web y redes sociales para hacer estafas de phishing.

Estas son algunas formas comunes de phishing que podría encontrar y las señales de advertencia a las que debe estar atento.

Phishing por llamada telefónica

Señales de advertencia

1. Una llamada telefónica de **"su compañía de tarjeta de crédito"** o "institución financiera", en general de alguien que trabaja en el "Departamento de Fraude y Seguridad"
2. Le dicen que su tarjeta fue marcada por transacciones sospechosas y que tiene que **probar que tiene la tarjeta** en su poder
3. Le piden que **dé el código de seguridad de tres dígitos** que aparece en el dorso de su tarjeta de pago, y una clave de acceso temporal que le acaban de enviar, o su PIN

Phishing por email

Señales de advertencia

- **Errores** de ortografía o gramática en la línea de asunto o el cuerpo del email
- **Fecha límite.** A veces los estafadores incluyen una fecha límite y amenazan con suspender la cuenta para que la víctima no tenga la cautela que tendría normalmente por la urgencia
- La dirección de email **no coincide** con la organización (es decir, irs.net o amazon.mil)
- El email no se dirige a usted por su **nombre**
- **No hay información de contacto.** Si algo levanta su sospecha, comuníquese con su institución financiera directamente usando el número de teléfono que aparece en el dorso de su tarjeta
- **Solicitudes sospechosas.** Visa, al igual que otras instituciones financieras, no se comunica con los tarjetahabientes para solicitar su información de cuenta personal
- **Hipervínculos sospechosos.** Evite hacer click en hipervínculos si es posible. Un solo click es suficiente para que su computadora se infecte con malware

Phishing por mensaje de texto

Señales de advertencia

- Hay un **enlace** en vez de un número de teléfono para llamar
- Es posible que el mensaje de texto que reciba no contenga el **nombre del banco** ni ninguna otra información
- El mensaje de texto le pide que **ingrese** a su cuenta bancaria para verificar una transacción, ingrese su PIN o proporcione sucódigo CVV de 3 dígitos

Phishing en sitio web

Señales de advertencia

- Hay algo que **no está del todo bien** con la dirección del sitio web o la página en sí. Preste atención a palabras mal escritas, sustituciones o logotipos actualizados
- Una **ventana emergente inusual** en el sitio que le pide ingresar la información de su cuenta
- Hay **enlaces HTML** que no coinciden con su destino

Phishing en redes sociales

Señales de advertencia

- Una solicitud de amistad de alguien que no conoce
- Una publicación donde se le pide que haga clic en un enlace que solicita información personal