INCREMENTO EN ATAQUES CIBERNÉTICOS EN LÍNEA
Nadie está exento de estos intentos engañosos

No tienes que ser proficiente en la tecnología para adoptar buenas prácticas e identificar si un mensaje de texto o correo electrónico es de alto riesgo.

Igual que en la calle existe el crimen, también existen delincuentes que le hacen mucho daño a la gente usando tácticas de engaño a través del Internet.

Los cibercriminales, o *hackers*, tienen tiempo e interés en lograr su objetivo: robar tu información personal y generar ingresos por la venta de ella. Todos somos posibles víctimas de recibir un correo fraudulento porque los hackers obtienen listas de contactos y emails para realizar envíos masivos.

Para el hacker, el resultado de éxito es uno matemático. Ellos identifican las probabilidades de éxito por la cantidad de envíos realizados y determinan el por ciento de probabilidad en que varias personas de esa lista de contactos van a caer en la trampa. Nadie está exento de estos mecanismos de robo de información porque tu información tiene valor en este mundo digital.

Mi intención en compartir esta información es ayudar a crear buenos hábitos y, sí, hasta un poco de malicia en el manejo de correos electrónicos y mensajes de textos. Así que, tómate esos segundos adicionales para validar el comunicado que te llega. Recuerda, que la precaución que uno toma en las calles aplica en línea. **Protégete**.

El ataque más común es conocido como *phishing* y *smishing*. Ocurren a través de correos electrónicos y mensajes de texto. A continuación, comparto unos pasos simples y rápidos que puedes aplicar para reducir el riesgo de caer victima a una estafa en línea.

3 TIPS DE CÓMO VALIDAR SI UN CORREO ELECTRÓNICO ES UN POSIBLE FRAUDE

1. **Valida el Nombre**: El paso primordial es validar de dónde proviene el mensaje y quién lo envió. Confirma que el mensaje recibido es de una empresa o persona que conoces.
2. **Valida el Dominio**: Cuando es un correo electrónico, verifica si el dominio de la empresa o persona es legítimo. Presta atención a cada letra de la dirección electrónica. En muchas ocasiones, el dominio cambia números por una letra (3 en vez de E); le faltan letras (hotmal.com); o mal escrito (*hotmial* en vez de *hotmail*).
3. **Valida el Mensaje Escrito**: Frecuentemente, el mensaje escrito contiene errores ortográficos, mensajes impersonales, o tienen saludos son genéricos. Cuando uno pone todo junto – *mensaje de alguien desconocido, hablando de un servicio o problema genérico, pidiéndote información personal, y posiblemente con errores ortográficos* - son señales de un posible fraude.

www.vpnet.net | (787)620-5950 | info@vpnet.net

Un mecanismo muy común es el correo que se hace pasar por una empresa legitima. Por ejemplo, recibes un correo del banco. El mismo parece ser auténtico ya que tiene el logotipo oficial del banco, está dirigido a ti por nombre, el escrito parece ser profesional y bien escrito. Pero tome precaución, porque si el comunicado pide que accedas a un enlace, descargar o abrir un archivo, o te redirige a un portal para ingresar tus credenciales **¡OJO!** ya que puede ser una estafa. **Los Bancos NO piden información personal sobre tu cuenta o credenciales mediante un correo electrónico**.

5 TIPS DE CÓMO VALIDAR SI UN TEXTO ES UN POSIBLE FRAUDE

1. **¿El mensaje es relevante a ti**? Confirma que el mensaje recibido es de una empresa o persona que conoces. Cuestiona el mensaje y confirma si realmente participaste de una rifa o recientemente pediste un paquete que viene por DHL/FedEx o el correo postal.
2. **Valida el Mensaje Escrito**: Frecuentemente, el texto es enviado por delincuentes de países extranjeros donde el inglés o español NO es su idioma principal. El escrito pudiera contener errores ortográficos, saludos impersonales, y oraciones incompletas.
3. **No ingreses al enlace del texto**
4. **Si seleccionas el enlace:** Si el enlace del texto te redirige a una página web, **no ingreses tu información**. Puede ser que el *hacker* creó una página web parecido a una empresa legitima.
5. **Cuando en duda:** contacte a la institución directamente y valida si el mensaje es legítimo. *Mejor tomarse un momento para validar que lamentar*.

DEFINICIONES IMPORTANTES:

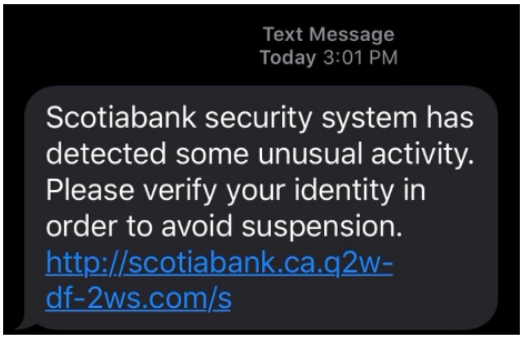
Ciberseguridad es el trabajo realizado por técnicos especialistas mediante el uso de aplicaciones tecnológicas en la infraestructura para reducir los riesgos de ataques, intrusión en la red, y/o incidentes a través de la buena aplicación de políticas y monitoreo de seguridad.

Ingenería Social es un conjunto de técnicas que usan los cibercriminales para engañar a las personas para compartir datos confidenciales. Hay varios motivos para los hackers realizar este tipo de ataques. Una de ellas es confirmar su información personal para robar su identidad. Otra razón es para infectar las computadoras con *malware* para robar datos del dispositivo y enviárselo por el Internet sin que te des cuenta.

Phishing es cuando alguien actúa como un representatnte legítimo de una empresa o institución con el fin de robar tu información personal como detalles de la tarjeta de crédito, datos de la cuenta bancaria, el número de seguro social, dirección postal, fecha de nacimiento, y nombre completo. Todos estos datos juntos permiten el robo de información o dinero.

Smishing es un fraude realizado por mensajes de texto para levantar información personal. Típicamente, usan mensajes que llevan a la persona verificar su cuenta *para robar las credenciales*, confirmar un pago *para obtener información de su cuenta bancaria*, o reclamar un premio *para obtener su información de contacto*. Abajo, unos ejemplos de textos fraudulentos.

Spear Phishing es un ataque sofisticado donde el *hacker* se hace pasar por un alto Gerente, Director, VP, o Presidente de una empresa o institución. El mensaje, usualmente, es dirigido a un empleado o consultor terciario, para completar una acción fraudulenta. Por ejemplo, el hacker se hace pasar por el Presidente de la empresa dirigiendo el correo a un empleado de Contabilidad pidiendo que complete una transacción bancaria. ¿Cómo logra que el empleado no se percate que es una solicitud fraudulenta? Porque el hacker invierte muchísimo tiempo estudiando a la empresa. Hacen organigramas, identificar las personas de la empresa, su departamento, y su rol. ¡Hasta estudian el tono y lenguaje típico de la empresa para lograr hacer el mensaje sentirse lo más auténtico posible!



Distintos Ataques Phishing

Se pueden realizar mediante correos electrónicos, mensajería (chats), y mensajes de texto (SMS).

- Spam/Bulk Emails
- Business Email Compromise (BEC)
- Email Account Compromise (EAC)
- DNS Hijacking (Compromised Home Router)
- USB / Thumb Drive (Endpoint, Data Loss)
- Smishing (Text SMS)
- Phishing
- Spear Phishing
- Whaling