Conoce más sobre el Phishing

El Phishing es un término informático que persigue el engaño a una víctima haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad) mediante correo electrónico o mensajes de texto con la finalidad de obtener información confidencial como: credenciales de acceso, números de tarjeta, etc.

¿Cómo funciona?

El contenido del mensaje intenta infundir miedo en la víctima, con la intención de debilitar su buen juicio al plantear situaciones extremas que algo ocurrirá. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

¿Cómo Identificar si es Phishing?

Reconoces al remitente pero es alguien con quien no tratas. Sospecha si es alguien con quien normalmente no te comunicas o apareces en una copia de correo con personas que no conoces.

La cuenta de correo del remitente es de un dominio parecido a los de instituciones reconocidas.

El mensaje tiene un lenguaje alarmista para crear un sentido de urgencia, incitándote a que hagas clic y “actúes ahora”.

El mensaje contiene archivos adjuntos inesperados o extraños. Estos adjuntos pueden contener malware.

Enlaces disfrazados que te dirigen a un sitio falso (urls extrañas), o imágenes sobre las cuales puedes hacer clic y te dirigen al sitio fraudulento.

Solicitan información confidencial que incluye usuarios contraseñas, datos de tarjetas de crédito, cuentas bancarias, datos personales, etc.

Contiene errores de ortografía y de redacción por ser traducidos con herramientas automáticas.

La firma no brinda detalles de la empresa o contiene información limitada.

Riesgos que puede ocasionar un ataque de Phishing:

- Suplantación de Identidad
- Acceso a información confidencial
- Robo de dinero en cuentas bancarias, uso indebido de tarjetas de crédito
- Estafas

¡Juntos creamos una cultura de seguridad!

Produbanco
Grupo Promerica