imperiasti®
Liderar es Cumplir

Cómo evitar el Vishing.

El "vishing" (abreviación de "voice phishing") es una técnica utilizada por estafadores para engañar a las personas por teléfono, haciéndose pasar por una entidad legítima con el fin de obtener información confidencial, como números de tarjetas de crédito, contraseñas u otra información personal.

¿CUÁL ES LA DIFERENCIA ENTRE VISHING Y PHISHING?

El phishing y el vishing persiguen el mismo objetivo: obtener información confidencial de las personas que podría usarse para robo de identidad, obtener beneficios financieros o apoderarse de cuentas. La diferencia principal entre el phishing y el vishing es el medio que se emplea para identificar a las potenciales víctimas. Si bien el phishing es un ataque basado principalmente en correo electrónico, el vishing emplea la voz, típicamente mediante llamadas al móvil de un usuario.

En todos los casos los delincuentes y estafadores emplean tácticas de intimidación para convencer a los usuarios de que hagan una llamada telefónica o que respondan ante a la consulta de un IVR dando opciones para aceptar, por ejemplo un beneficio de ANSES, deudas con la AFIP, o el mensaje intimidante que “se instaló un agente en su computadora” y desde hace tiempo viene recogiendo información, tienen fotos comprometedoras, y que si no pagan un rescate en Bitcoins será publicadas en las redes y todos los contactos de la víctima.

Medidas para contrarrestar

Aquí tienes algunas medidas que puedes tomar para evitar caer en una estafa de vishing:

Desconfía de llamadas no solicitadas: Si recibes una llamada de alguien que afirma ser de un banco, empresa de tarjetas de crédito u otra entidad, y tú no esperabas esa llamada, mantén la guardia alta. Nunca proporciones información personal o financiera por teléfono a menos que estés seguro de la legitimidad de la llamada.

Verifica la identidad del llamante: Si alguien te llama y dice ser de una institución financiera o empresa, solicita su nombre y número de identificación. Luego, llama directamente a la empresa utilizando un número de teléfono oficial (no el que te proporcionaron en la llamada) para verificar la autenticidad del llamante.

No sigas enlaces ni proporciones información personal: Si te piden que ingreses información personal o financiera a través de una llamada telefónica automatizada o en vivo, no lo hagas. Los bancos y otras instituciones financieras rara vez solicitan información confidencial por teléfono.

Usa la autenticación de dos factores: Siempre que sea posible, habilita la autenticación de dos factores en tus cuentas. Esto proporciona una capa adicional de seguridad al requerir un segundo método de verificación, como un código enviado a tu teléfono móvil, además de tu contraseña.

Educa a los miembros de tu entorno: Asegúrate de que tus familiares, especialmente los más vulnerables como los ancianos, estén informados sobre el vishing y cómo detectarlo. Enseña a no proporcionar información personal por teléfono a menos que estén seguros de la legitimidad de la llamada.

Reporta las llamadas sospechosas: Si recibes una llamada que sospechas que es un intento de vishing, bloquea el número y repórtalo como SPAM a la empresa.

Al mantenerse alerta y siguiendo estos consejos, puedes ayudar a protegerte a ti mismo y a tus seres queridos del vishing y otras estafas telefónicas.

HMA

Héctor M. Amodeo
Socio
Gerente Comercial