Allianz Partners

Protégete del phishing

Allianz se enfrenta actualmente a un mayor número de intentos de fraude a través de certificados, cartas y mensajes falsos.

A continuación, encontrarás algunos consejos sobre cómo detectar mensajes de phishing y reaccionar correctamente.

¿Qué es phishing?

Los correos electrónicos de phishing son mensajes diseñados para que los destinatarios compartan información personal o instalen un malware (programa maligno) en la computadora sin darse cuenta. La mayoría de los intentos de Phishing son muy realistas y se esfuerzan por parecer oficiales, como si fueran de un banco, un sitio de pago, una tienda en línea o se esfuerzan por hacerse pasar por contactos conocidos.

Pueden tener diferentes temas, como restablecimiento de contraseña de cuenta de correo electrónico, documento compartido, noticias sobre un tema actual, notificación de factura o pago, entrega de un paquete, inicio de sesión en un sitio web o notificación de redes sociales.

Incluso la simple apertura de un correo electrónico de phishing proporciona la información al atacante, o le informa que hay alguien detrás de esta cuenta de correo electrónico que probablemente haga clic en los enlaces. **Por lo tanto, debemos evitar hacer clic en cualquier parte del mensaje hasta que determinemos si es real o falso.**

Consejos para identificar el phishing en los emails

Controla tus emociones: las estafas de phishing se basan en desencadenantes emocionales como la curiosidad, la urgencia, el miedo y la recompensa para llevarlo a la acción. Mantente atento a desencadenantes emocionales como titulares sorprendentes que hagan referencia a un evento actual, una oferta interesante, una recompensa, correos electrónicos de agradecimiento o avisos bancarios inesperados.

Busca señales de advertencia: escucha tu "intuición". ¿Algo en el correo electrónico parece extraño? ¿El correo electrónico fue enviado por un remitente desconocido? ¿Fue esperado o no solicitado? ¿Hay errores gramaticales o de ortografía? ¿Pide información personal? Si has respondido "sí" a cualquiera de estas preguntas, es posible que hayas recibido un correo electrónico de phishing.

Examina el nombre de dominio: algunos atacantes modifican los dominios para atrapar a los objetivos con la guardia baja. Por ejemplo, si el dominio correcto era allianz.com, los estafadores pueden registrar "alliaanz.com" o "allianz.co", con la esperanza de que no notes la sutil diferencia.

Siempre verifica al remitente: asegúrate de reconocer el nombre y el dominio del remitente. Para verificar, pasa el mouse sobre la dirección de correo electrónico; la mayoría de las organizaciones

enviarán mensajes desde una dirección de correo electrónico otorgada. Si reconoces al remitente, verifica que el mensaje sea legítimo con una llamada telefónica rápida o un mensaje de chat.

No hagas clic en ningún enlace; pasa el mouse sobre los enlaces **sin dar clic** para verificarlos; por lo general, un enlace tendrá una página alojada en una parte del dominio de la URL a la que se refiere el mensaje.

Verifica la ortografía: asegúrate de que el idioma utilizado sea correcto; en casos comunes, los atacantes usan una gramática poco profesional, términos o mayúsculas incorrectos. Sin embargo, están mejorando en esta área.

Verifica el saludo: los correos electrónicos de phishing a menudo usan un saludo genérico (por ejemplo, Estimado usuario) en lugar de un saludo personal.

Nunca proporciones tu información personal: Allianz NUNCA te pedirá tu contraseña o PIN.

No te dejes llevar por la urgencia: algunos correos electrónicos de phishing a veces pueden requerir una acción inmediata. Por lo tanto, analiza la situación antes de actuar.

Verifica la firma del correo electrónico: la mayoría de los remitentes legítimos tendrán una firma completa al final de sus correos electrónicos

Ten cuidado con los archivos adjuntos: los atacantes pueden engañarnos con archivos adjuntos atractivos e íconos de marcas falsas, documentos/certificados fraudulentos.
Considera un documento potencialmente sospechoso si:

- El documento contiene promesas poco realistas u ofertas inusuales, por ejemplo, pago de sumas muy elevadas.
- Se te pide que pagues una cierta cantidad antes de recibir algo de vuelta.
- El texto está mal redactado y/o contiene faltas de ortografía.
- El membrete, el sello, la firma y otros símbolos de la marca no son correctos.

Comprueba si el mensaje es demasiado bueno para ser verdad; algo simplemente no se ve bien.

En caso de duda, informa el mensaje a una oficina de Allianz Partners. Más vale prevenir que lamentar, sin importar la preocupación, ¡verifica antes de actuar!

En pocas palabras, ¿cómo protegerse?

- Elimina todos los correos electrónicos con direcciones de remitente desconocidas o de aspecto extraño sin controles ni vistas previas.
- Verifica cada correo electrónico entrante con los 3 principios de phishing explicados: si observas algo sospechoso, no abras ningún archivo adjunto (incluso los archivos de Word, Excel, PowerPoint o pdf pueden contener malware), no hagas clic en ningún enlace contenido en el correo electrónico (visible el texto del enlace y los enlaces reales pueden diferir) si el enlace parece ser una página web conocida, abre el navegador y escribe el enlace manualmente.