5 CONSEJOS PARA NO CAER EN PHISING

El phishing es un método que los ciberdelincuentes utilizan para engañarte y conseguir que reveles información personal, como contraseñas, datos de tarjetas de crédito, de seguridad social y números de cuenta bancarias. Si no se toman las medidas necesarias, una compañía podría sucumbir a un ataque dirigido

Protege tu información de los atacantes, siguiendo estos consejos prácticos que te ayudarán a reducir las posibilidades de caer en Phishing..

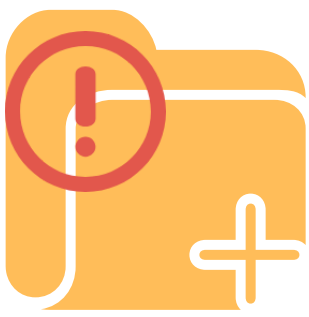
1. PRESTA ATENCIÓN A LOS ERRORES DE ORTOGRAFÍA Y MALA GRAMÁTICA

Detecta un correo electrónico de suplantación de identidad (phishing) verificando **si hay errores gramaticales y ortográficos** ELIMÍNALO.

2. REVISA QUE EL NOMBRE DE DOMINIO Y DIRECCIÓN DE CORREO COINCIDAN

Es muy común que en los correos de phishing **el nombre de dominio y la dirección de correo electrónico NO COINCIDEN, si pasa esto** ELIMÍNALO.

3. TEN CUIDADO CON LOS ARCHIVOS ADJUNTOS



Recibimos miles de correos a diario que contienen archivos adjuntos para el registro, suscripción, comentarios, etc. Recuerda que, los **correos que salen de la nada pueden contener archivos adjuntos sospechosos.** NO ABRAS LOS ARCHIVOS ADJUNTOS **si no conoces el remitente.**

4. SOSPECHA DE LOS CORREOS QUE TE SOLICITAN INFORMACIÓN PERSONAL

Independientemente de lo "auténtico" u "oficial" que parezca un correo, **siempre es una bandera roja.** Si el mensaje te pide que compartas información personal IGNÓRALO.

5. EVITA ABRIR CORREOS CON OFERTAS DEMASIADO BUENAS PARA SER VERDAD

Muchas veces recibimos correos que nos anuncian como el gran ganador de una lotería o con ofertas poco creíbles; Antes de hacer clic en cualquiera de estos enlaces ¡ESPERA! **puede ser una trampa.**

HABLA CON UN CONSULTOR EXPERTO Y COMIENZA TU CAMPAÑA ANTI PHISHING

Grupo Smartekh