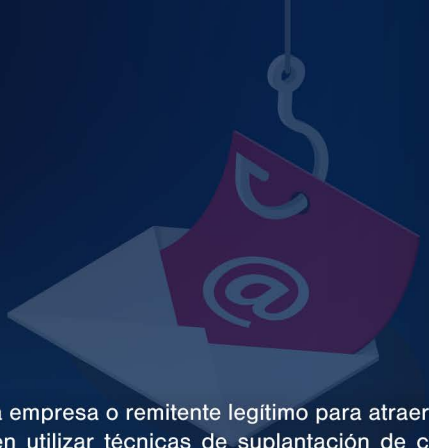
Phishing

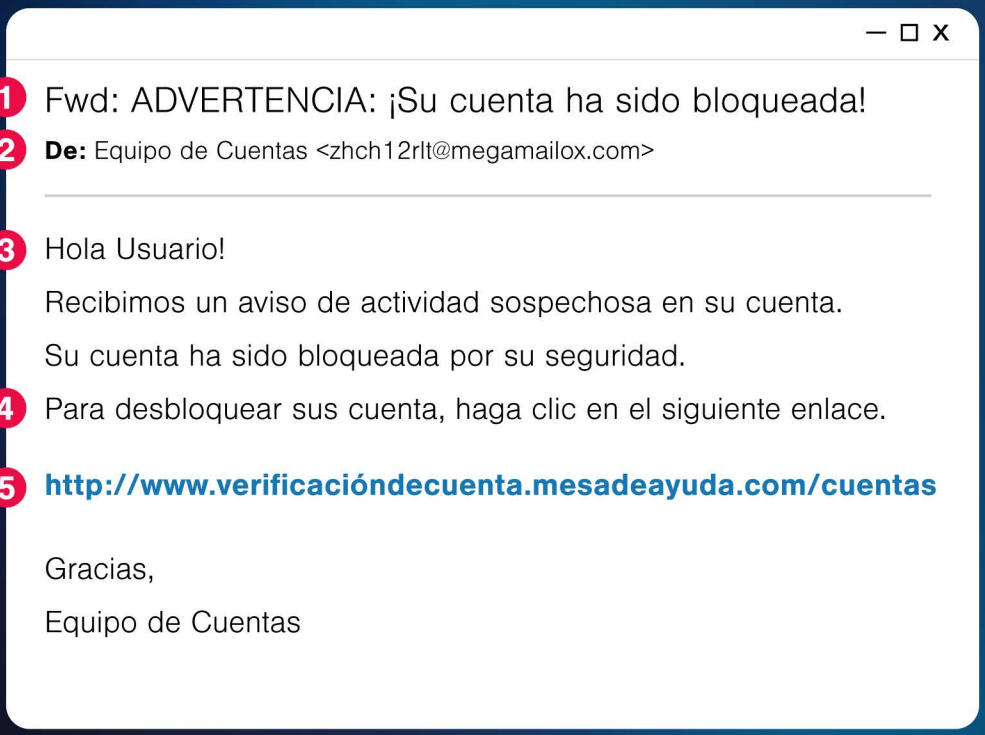
Lo Que Necesitas Saber



¿Qué es el Phishing?

El phishing es un delito cibernético en el que un atacante se hace pasar falsamente por una empresa o remitente legítimo para atraer a las víctimas a compartir información personal o confidencial. Los ataques de phishing suelen utilizar técnicas de suplantación de correo electrónico diseñadas para engañar a las víctimas pidiéndoles que actualicen o verifiquen su información personal respondiendo el correo electrónico o visitando un sitio web. Los sitios web falsificados pueden parecer casi idénticos a los reales, como su banco o el sitio de su tarjeta de crédito, y solicitar al usuario que ingrese información confidencial como contraseñas, números de tarjetas de crédito, PIN bancarios, etc. Estos sitios web falsos se utilizan únicamente para robar su información.

SIGNOS DE PHISHING POR CORREO ELECTRÓNICO



1. **LÍNEA DE ASUNTO** — Sensación de urgencia o alarma
2. **REMITENTE** — Remitente legítimo y confiable
3. **SALUDO** — Saludo genérico y no personalizado
4. **SOLICITUD DE CIERRE** — Un llamado a la acción inmediata
5. **HIPERVÍNCULO** — Declaración solicitando su enlace

ESTADÍSTICAS DE PHISHING

96% de los ataques de phishing llegan por correo electrónico

76% de las organizaciones estadounidenses han sufrido un ataque de phishing

30% de los correos electrónicos de phishing se abren

80% de los incidentes de seguridad reportados fueron ataques de phishing en 2022

Cada día se crean **1,5** millones de nuevos sitios de phishing

ATSG

Si sospecha que ha sido víctima de un ataque de phishing, informe el incidente inmediatamente a Seguridad. Si cree que un correo electrónico es una estafa de phishing, comuníquese con el Departamento de TI. No haga clic en ningún enlace de terceros.