Phishing

Un ataque en el que un hacker se hace pasar por una entidad de confianza para robar información, difundir malware o engañar a las víctimas.

Tipos de phishing

Correo electrónico	Crear urgencia para engañar a las víctimas y que proporcionen información, inicien sesión o envíen dinero.
Vishing (por teléfono)	Estafa telefónica en la que los atacantes se hacen pasar por entidades de confianza para robar información.
Smishing (por mensaje de texto)	Estafa por mensaje de texto en la que se fingen ser una entidad de confianza para robar datos o dinero.

Señales a tener en cuenta en ataques de phishing

Dirección de correo electrónico del remitente	Busca errores ortográficos, cambios sutiles o remitentes desconocidos.
Lenguaje urgente o alarmista	Ten cuidado con frases urgentes como "acción inmediata" o "cuenta suspendida".
Enlaces y archivos adjuntos sospechosos	Pasa el cursor sobre los enlaces y verifica las extensiones de los archivos para detectar amenazas.
Gramática y ortografía deficientes	Errores tipográficos y gramaticales pueden ser señales de phishing; las empresas legítimas revisan sus mensajes.
Solicitudes de información personal/financiera	Ten cuidado con correos electrónicos inesperados que soliciten información sensible.
Contenido inusual	Observa saludos genéricos, contenido extraño o un tono inusual.

Medidas para enfrentar ataques de phishing / spam

1. Reportar correos electrónicos/llamadas/mensajes de texto de phishing al departamento de TI o supervisor.
2. Proporcionar capacitación en ciberseguridad a los empleados.
3. Verificar la legitimidad del correo electrónico/mensaje de texto del remitente.
4. Verificar la información de contacto en sitios web oficiales antes de continuar con llamadas telefónicas.

Elementos de los ataques de phishing

Suplantación de identidad	Parece legítimo con logotipos oficiales, formato y lenguaje apropiado.
Lenguaje persuasivo	Utiliza emociones, amenazas o recompensas para incitar a la acción.
Sentido de urgencia	Presiona a las víctimas con amenazas de seguridad urgentes o problemas con la cuenta.
Enlaces maliciosos	Envía a las víctimas a sitios web falsos o números para robar datos.
Archivos adjuntos peligrosos	Pueden ocultar malware en facturas o recibos falsos.

Correos electrónicos de spam

Los correos electrónicos de spam roban datos, recogen direcciones o propagan malware.
Ejemplos
1) Promociones (descuentos falsos, sorteos)
2) Estafas de empleo (ofertas de empleo fraudulentas)
3) Estafas de lotería (ganancias falsas, reclamaciones de premios)
4) Intentos de phishing (mensajes engañosos para robar información)
Características clave
I. No solicitados e indeseados (también conocidos como correos electrónicos no deseados)
II. Distribuidos en masa a muchos destinatarios
III. Pueden formar parte de campañas de phishing
IV. A menudo vinculados a publicidad o fraude