Phishing: La amenaza que entra por el correo

Una guía ejecutiva para reconocer, prevenir y proteger tu empresa frente al fraude digital.

¿Qué es el phishing?

El phishing es una técnica de fraude en la que los ciberdelincuentes **suplantan identidades legítimas** para obtener datos sensibles, credenciales corporativas o acceso a sistemas críticos.

> No es un ataque técnico sofisticado. Es manipulación psicológica disfrazada de confianza.

Cómo funciona un ataque

La mayoría de ataques siguen este patrón: urgencia, engaño y captura. Reconocer el patrón es el primer paso para detenerlo.

Tipos de phishing

Phishing tradicional

Correos masivos que imitan marcas o entidades conocidas para capturar datos.

Spear Phishing

Ataques personalizados dirigidos a una persona o empresa concreta.

Whaling

Variante dirigida específicamente a perfiles directivos y ejecutivos.

Un riesgo real para cualquier empresa

💸 Pérdidas económicas

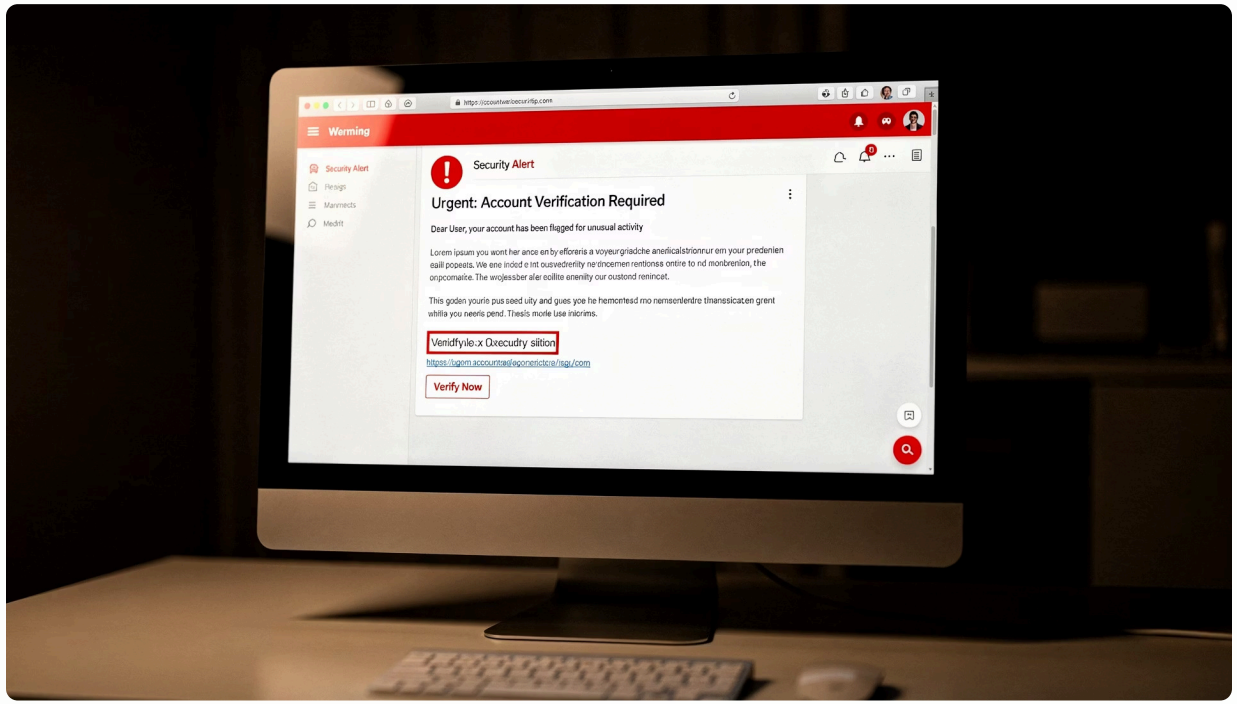
Transferencias fraudulentas y costes de recuperación.

🔓 Filtración de datos

Exposición de información confidencial de clientes y empleados.

📉 Daño reputacional

Pérdida de confianza difícil de recuperar.



Señales de alerta

- **Mensajes alarmistas** que exigen acción inmediata
- **Errores gramaticales** o redacción inusual
- **URLs sospechosas** que imitan dominios reales
- **Remitentes desconocidos** o ligeramente alterados

El principal riesgo: el error humano

> "La tecnología puede proteger sistemas, pero no puede sustituir el criterio de las personas."

La mayoría de brechas de seguridad comienzan con un **clic equivocado**. Un pequeño error puede generar consecuencias enormes: acceso a sistemas críticos, robo de credenciales o pérdidas millonarias.

La concienciación es la primera línea de defensa

Antes de actuar, **verifica siempre** el remitente, el enlace y el contexto del mensaje.

Buenas prácticas de prevención

Verificar remitentes

Comprueba siempre la dirección completa antes de responder o hacer clic.

Evitar enlaces sospechosos

Accede directamente a los sitios web en lugar de seguir enlaces en correos.

Formar a los empleados

La formación continua reduce drásticamente la exposición al riesgo.

Combinar tecnología

Filtros de correo, autenticación multifactor y protocolos de verificación.

Ciberseguridad como cultura empresarial

La ciberseguridad ya no es solo una cuestión tecnológica. Es parte de la **protección estratégica** de cualquier organización y debe integrarse en la cultura de empresa.

Tecnología	Formación	Cultura
Herramientas y sistemas de protección	Empleados informados y preparados	Hábitos digitales seguros en el día a día

Conclusiones clave

1 El phishing es una amenaza real y creciente

Ninguna empresa, grande o pequeña, está exenta del riesgo.

2 El error humano es el principal vector de ataque

Verificar antes de actuar es el hábito más valioso.

3 Prevención = tecnología + formación + cultura

Las tres dimensiones deben trabajarse de forma conjunta y continua.

Con concienciación y buenas prácticas, tu empresa puede estar un paso por delante de los atacantes.