# Protege tu empresa: lo que debes saber sobre el Whaling


El Whaling es un ataque cibernético en el que los delincuentes suplantan la identidad de altos ejecutivos o comúnmente llamados “peces gordos” para engañar a empleados y robar información sensible o dinero.

Todo comienza con un correo malicioso que parece haber sido enviado por un superior, induciendo al empleado a prestarle atención y a cumplir sus instrucciones, como compartir información confidencial de la empresa o descargar archivos maliciosos en la computadora.

Sin embargo, existen formas de evitar caer en este tipo de estafas. Entre ellas se encuentran:

1. **Implementa un programa de capacitación en ciberseguridad para todos los empleados:** Educarlos sobre los métodos

del Whaling, incluyendo cómo identificar correos electrónicos sospechosos y solicitudes inusuales, es esencial. Establece la cultura de «verificar antes de actuar», incentivando a confirmar solicitudes a través de un canal de comunicación diferente al correo electrónico.

2. **Refuerza las configuraciones de privacidad en redes sociales:** Aconseja a los ejecutivos y empleados a mantener privados sus perfiles en redes sociales. Menos información pública sobre la empresa y sus altos mandos reducen la oportunidad de que los cibercriminales recopilen datos para personalizar sus ataques.
3. **Adopta protocolos de autenticación de correo electrónico como SPF, DKIM y DMARC:** Esto protege a la organización y sus empleados de mensajes falsificados, evitando así que mensajes maliciosos lleguen a la bandeja de entrada.

***Fuente:***

*https://easydmarc.com/blog/es/whaling-como-funciona-este-ataque-y-como-podemos-evitarlo/*

*https://www.primicias.ec/ciencia-tecnologia/whaling-nueva-tactica-ciberdelincuentes-empresas-empleados-82407/*