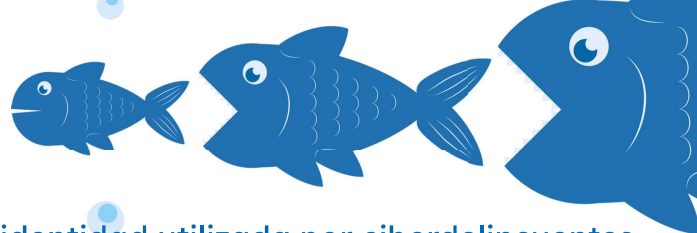


# PHISHING



El phishing es una técnica común de suplantación de identidad utilizada por ciberdelincuentes para engañar a las víctimas y obtener sus datos personales. Funciona de la siguiente manera:

1. Los atacantes se hacen pasar por un remitente de confianza.
  2. Envían correos, SMS o mensajes en redes sociales con enlaces a páginas web fraudulentas.
- Si los usuarios ingresan información en estas páginas, los ciberdelincuentes obtienen sus datos.

## GENERALIZADO

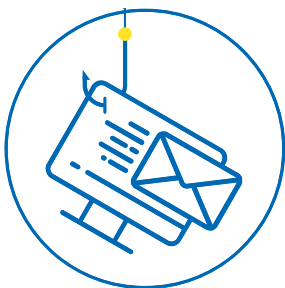
*a muchas personas,  
usando como anzuelo  
falsos concursos o  
premios, por ejemplo.*



## DIRIGIDO

*a una sola víctima para  
lograr un objetivo  
concreto.*

## TIPOS DE PHISHING



### Phishing

Se hace pasar por un tercero de confianza para extraer información personal y/o credenciales de acceso.



### Spray and pray

Envío masivo de correos que suplantán la identidad de una empresa o servicio. Buscan generar una sensación de urgencia o euforia.



### Malware-Based Phishing

El mensaje fraudulento incluye un archivo adjunto que contiene malware o un enlace para descargar un archivo malicioso.



### Spear phishing

Ataque personalizado a personas concretas de la empresa con acceso a información confidencial.



### Smishing

Es similar al phishing tradicional, sin embargo, los mensajes fraudulentos se envían a través de SMS.

## Medidas para evitarlo:

1. Verifica que el mensaje, el emisor y los enlaces estén libres de errores.
2. Desconfía de mensajes que causen urgencia o euforia.
3. Pasa el cursor sobre un enlace antes de hacer clic para verificar su destino.
4. Las empresas legítimas no piden datos personales por email, SMS o teléfono sin aviso previo.
5. Si tienes dudas, contacta a la empresa a través de sus canales oficiales.
6. ¿Y si eres víctima? Cambia todas tus contraseñas de inmediato.

