PHISHING
LA CIBERESTAFA MÁS COMÚN

¿QUÉ ES?

Es una de las técnicas de ingeniería social más comunes y peligrosas, debido a su bajo coste y la alta efectividad.
Proviene del termino “fishing” ya que intenta que los usuarios piquen el anzuelo.

¿EN QUÉ CONSISTE?

Los atacantes utilizan correos electrónicos y sitios web fraudulentos para engañar a sus victimas y robarles información sensible, como contraseñas o información bancaria.

CÓMO DETECTARLO

Enlaces sospechosos. URL distintas a las oficiales, aunque lo parezcan.

Solicitud de datos. Requieren proporcionar **datos sensibles**.

Urgencia. Generan emociones como el **miedo** o la **curiosidad** para que actuemos rápido y sin pensar.

No personalizados. Se dirigen a “Cliente” o “Usuario”.

Fallos de redacción. Suelen tener **errores de ortografía y gramática.**

COFM

GOVERTIS
Part of Telefónica Tech

PHISHING
LA CIBERESTAFA MÁS COMÚN

¡CUIDADO! Existen técnicas más sofisticadas para engañarnos:

- Utilizan datos reales o detalles específicos que han recopilado.
- Suplantan perfiles conocidos (entidades legitimas o amigos y familiares), para transmitir confianza.
- Utilizan web clonadas con URLs similares a los sitios originales.
- El candado y https solo indican que el trafico es cifrado, pero el sitio puede seguir siendo malicioso o fraudulento.
- No solo son peligrosos los enlaces, un archivo puede servir para instalar malware en tu dispositivo.

¿COMO NOS DEFENDEMOS?

- Verificar que la **URL** o el dominio del remitente son **oficiales**.
- Desconfiar de solicitudes urgentes o promesas demasiado buenas.
- Validar la identidad del remitente por otro canal de confianza.
- No hagas click en enlaces, navega manualmente al sitio web.
- No proporcionar información sensible en en lugares sospechosos.
- Presta atención a la redacción y la ortografía.

¡LA SEGURIDAD DIGITAL COMIENZA CONTIGO!

COFM

GOYERTIS
Part of Telefónica Tech