

PHISHING



Es una técnica que utilizan los ciberdelincuentes para engañar y conseguir información sensible (*contraseñas, número de cuentas bancarias, datos de tarjetas de crédito, información de la organización...*)


Se considera un tipo de ataque de **ingeniería social** porque se basa en errores humanos.

CÓMO FUNCIONA

- Los ciberdelincuentes intentan suplantar a una entidad legítima (*organismo público, entidad financiera, servicio técnico...*)
- La mayoría de los ataques comienzan con la recepción de un correo electrónico o un mensaje directo.
- Los correos incluyen enlaces a sitios web preparados por los atacantes en los que se pide la información.
- Otros medios de propagación son: *mensajería instantánea, redes sociales, SMS, teléfono.*



PREVENCIÓN

- Comprueba que la dirección del correo remitente coincide con quien dice ser. *Presta atención a la sintaxis, una letra puede marcar la diferencia.*
- Cuidado con las urgencias que fuerzan a tomar decisiones rápidas para evitar supuestas consecuencias negativas:
 - *Tu cuenta ha sido o va a ser bloqueada.*
 - *Notificaciones de sanciones.*
 - *Confirmación de la identidad.*
 - *Mejoras en medidas de seguridad.*
- Desconfía de textos mal redactados o con faltas de ortografía.
- Desconfía de ofertas, loterías o premios de gran valor.
- Las webs seguras empiezan por **https://** y aparece en el navegador el icono de un pequeño candado cerrado. 
- Presta atención a la sintaxis de los enlaces a páginas web, en muchos casos la dirección web parece legítima, pero tiene algún cambio.
- Evita introducir datos en web cuyos enlaces lleguen acortados (**cort.as, bit.ly**)
- Si sospechas ser víctima de un phishing ponte en contacto con el soporte informático a usuarios de tu organización.



EJEMPLO

COVID-19

Usuarios no habituados a teletrabajar tienen que adaptarse a una nueva situación.

Los ciberdelincuentes pueden realizar campañas de “phishing” en las que haciéndose pasar por personal de la organización, en especial de atención a usuarios, pretendan obtener credenciales de acceso a los sistemas.