EUROPOL EC3 European Cybercrime Centre

AMENAZAS EN WEB

MIRA DOS VECES ANTES DE PINCHAR.

Puedes perder dinero, información personal y los datos que tengas almacenados si el dispositivo deja de funcionar. ¡No piques!

¿CÓMO PUEDE PASAR?

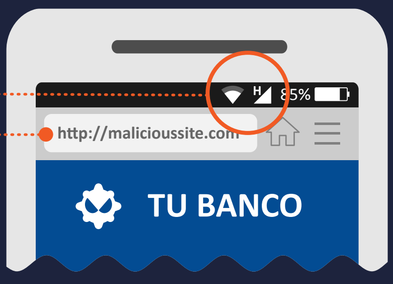
ATAQUES DE PHISHING: Engañan al usuario para que les dé información personal haciéndose pasar por alguien fiable. Se contagian a través de correos electrónicos, mensajes de texto o redes sociales.

NAVEGACIÓN WEB: Tu dispositivo móvil puede infectarse solo con visitar una página no segura.

DESCARGA DE ARCHIVOS: En un correo se pueden incluir enlaces y adjuntos maliciosos.

¿POR QUÉ FUNCIONA?

Los dispositivos móviles están **CONSTANTEMENTE CONECTADOS** a internet.



EL TAMAÑO REDUCIDO DE LA PANTALLA DEL DISPOSITIVO suele suponer una restricción. Los navegadores móviles muestran las URL en una pantalla con espacio limitado, poniéndonoslo difícil a la hora de comprobar la legitimidad de un dominio.

CONFIANZA IMPLÍCITA DEL USUARIO en la naturaleza personal de un dispositivo móvil.

¿QUÉ SE PUEDE HACER?

Desconfía si recibes una llamada o SMS de una empresa para solicitarte información personal. Puedes comprobar la legitimidad de la llamada o el mensaje contactando con el número oficial de la empresa.

Nunca pinches en enlaces ni descargues adjuntos de correos o SMS que no hayas solicitado. Bórralos inmediatamente.

Desconfía de los sitios con faltas de ortografía y gramática o baja resolución.

Al navegar por internet con tu dispositivo móvil, asegúrate de que tu conexión está protegida con HTTPS. Siempre puedes comprobarlo al principio de la URL.

Si puedes, instala una app de seguridad móvil que te avise de las actividades sospechosas.

GUARDIA CIVIL · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · OSI Oficina de Seguridad del Internauta · Norton by Symantec · TREND MICRO · KASPERSKY lab

#MobileMalware