

PHISHING

El fraude que intenta robar nuestros datos personales y bancarios

“He recibido un e-mail pidiéndome que actualice los datos personales de mi cuenta corriente haciendo clic en un enlace, pero la URL de mi banco no es la misma de siempre”



¿Cómo actúan los ciberdelincuentes?

- Envían un e-mail, que abres pensando que es del banco.
- Te solicitan que accedas a una web y que facilites tus datos personales.
- La web parece legítima y facilitas toda la información.

Objetivos

- Apoderarse de la información personal que introducimos.
- Suplantarnos en redes sociales y otras webs de Internet.
- Robar nuestra información bancaria para conseguir dinero.



Consejos para evitar ser víctima de Phishing

- Sé precavido ante los correos que aparentan ser de entidades bancarias o servicios conocidos.
- Desconfía, los bancos nunca solicitan datos personales por e-mail.
- Sospecha si hay errores gramaticales en el texto.
- Si recibes comunicaciones anónimas dirigidas a “Estimado cliente”, “notificación a usuario” o “Querido amigo”.
- Si el mensaje te obliga a tomar una decisión en unas pocas horas, es mala señal.
- Asegúrate de que la URL que visitas es la que dice ser.
- No hagas clic en el enlace adjunto. Si quieres acceder a la web, hazlo a través de una búsqueda directa.
- Elimina siempre cualquier e-mail que te solicite datos.