kontsumoBIDE
KONTSUMOKO EUSKAL INSTITUTUA
INSTITUTO VASCO DE CONSUMO

COMPROMISO CON LAS PERSONAS
EUSKO JAURLARITZA GOBIERNO VASCO

PHISHING

robo de datos personales

Protégete ante la ciberdelincuencia

INFORMACIÓN QUE OBTIENEN

- **Datos personales:** correo electrónico, DNI, nº teléfono, etc.
- **Nº de tarjetas de crédito y cuentas bancarias**
- **Contraseñas:** Redes Sociales, e-mail, etc.

MEDIOS QUE UTILIZAN

- Correo electrónico
- WhatsApp
- SMS
- Redes Sociales

CÓMO ACTÚAN

- Las personas que van a cometer un ciberdelito envían mensajes **haciéndose pasar** por entidades bancarias, organismos, comercios, personas conocidas...
- La víctima **recibe un mensaje** en el que se le pide que actualice o confirme datos personales, o en el que se le informa de que ha recibido algún premio (por ejemplo, un bono regalo). Para ello, debe pinchar un enlace que lleva a una web con **apariencia similar a la oficial**, donde deberá introducir sus datos.

CÓMO DETECTARLO

- El **contenido** del mensaje suele ser **inusual**. Por ejemplo, una entidad bancaria o una empresa nunca te pedirá la contraseña para obtener un premio o para recuperar la propia cuenta.
- Fíjate en la **redacción del mensaje**. Debe estar bien escrito y ser coherente.

CÓMO PROTEGERTE

- Si recibes un mensaje en el que te solicitan una actualización o confirmación de datos personales, **no respondas**. Y si hubiera algún **enlace, no lo pinches**. Si quieres entrar en la página web del supuesto remitente, teclea la dirección URL real en la barra de direcciones.
- No abras mensajes de **remitentes desconocidos**, elimínalos directamente.
- Introduce tus datos confidenciales únicamente en **páginas web seguras**: URLs que comiencen por https:// y en las que aparezca el símbolo del candado cerrado y/o una llave.
- **Utiliza un antivirus** para tus dispositivos y mantenlo actualizado.