kontsumoBIDE
KONTSUMOKO EUSKAL INSTITUTUA
INSTITUTO VASCO DE CONSUMO

PERTSONA HELBURU
ELISKO JAURLARITZA
GOBIERNO VASCO

PHISHING

datu pertsonalen lapurreta

Ziberdelinkuentziatik babestu zaitez

LORTZEN DUTEN INFORMAZIOA

- Datu pertsonalak: helbide elektronikoa, NAN, telefono zenbakia, etab.
- Kreditu-txartelen eta banku-kontuen zenbakiak
- Pasahitzak: Sare sozialak, e-mail, etab.

ERABILTZEN DITUZTEN BIDEAK

- Helbide elektronikoa
- WhatsApp
- SMS
- Sare sozialak

NOLA JOKATZEN DUTE?

- Ziberdelitu bat egingo duten pertsonek mezuak bidaltzen dituzte **nortasun faltsuak erabiliz:** banketxeak, erakundeak, saltokiak edota pertsona ezagunen izenean.
- Biktimak datu pertsonalak eguneratu edo egiaztatzeko eskatzen dion **mezu bat jaso** dezake. Baita sari bat irabazi duela esaten dioten mezu faltsuak ere (adibidez, opari-txartela). Edozein kasutan, lotura bat klikatzea eskatzen zaio. Esteka horren bidez, biktima **benetako web orriaren antza** duen webgune faltsu batera heltzen da, eta bertan bere datuak ematea eskatuko zaio.

NOLA DETEKTATU?

- Normalean, mezuaren **edukia ezohikoa** da. Adibidez, banketxe edo enpresa batek ez dizu inoiz pasahitza eskatuko sari bat lortzeko edo kontua berreskuratzeko.
- Erreparatu **mezuaren erredakzioari**: modu egokian eta koherentziaz idatzita egon behar du.

NOLA BABESTU?

- Datu pertsonalak eguneratzea edo egiaztatzea eskatzen dizun mezu bat jasotzen baduzu, **ez erantzun**. **Estekaren** bat agertuz gero, **ez klikatu**. Ustezko igorlearen webgunean sartu nahi baduzu, URL helbide erreala helbide-barran idatz ezazu.
- Ez zabaldu **igorle ezezagunen** mezurik, zuzenean ezabatu itzazu.
- Zure datu konfidentzialak **webgune seguruetan** soilik sar itzazu: URL helbidearen hasierak https:// izan dadila, eta giltzarrapo itxi bat edota giltza bat ager daitezela.
- **Antibirus bat instalatu zure** gailuetan, eta eguneratuta mantendu.