

# PHISHING-AREN KLASIKOAK

**Phishing**-aren bidez, zibergaizkileek erakunde ezberdinen identitatea ordeztan dituzten mezu elektronikoak bidaltzen dizkigute. Mezu horietan, premiazko ekintzaren bat eskatzen digute, besteak beste esteka bat sakatzea edo informazio jakin bat bidaltzea. Helburua **alarma sortzea** da, gure informazio pertsonala eta bankukoa lortzeko.



## EZAGUNAK EGITEN ZAIZKIZU?



**Zure kontua egiaztatzen ez baduzu, 48 ordutan kontua blokeatuko dizun pertsona hori.**

**Ezeren truke ematen dizuten oparitxo hori.**



**Kodea sartu ezean, ezabatu egingo dizkizuten argazkiak eta bideoak.**

**Parte hartu gabe zauden zozketa.**



**Inoiz egin ez duzun kontu iraungitu hori.**

**Inoiz eskatu ez duzun pakete baten birprogamatutako entrega.**



## EZ UTZI ZIRIA SARTZEN!

Hain premiazkoak diren mezu elektroniko horiek guztiek beti dute zerbait komunean. Horregatik, gomendio hauek jarraitzea garrantzitsua da:

**URL helbidea egiaztatu:** legezkoa dela ziurtatu eta ez sakatu aurretik. Halakorik ezean, webgunera helbidea eskuz sartuta sar zaitetz.

**Ortografia eta gramatika aztertu:** mezu horiek askotan akatsak izaten dituzte.

**Pertsona zuzenari zuzentzen direla** eta egitura orokorrik erabiltzen ez dela egiaztatu.

**Kontuz presekin:** askotan mehatxuak edo premiak erabiltzen dituzte azkar jardun dezazun.

**Igorleari erreparatu:** emaila arraroa dirudien helbide batetik badator, kontuz ibili.

**Identitatea beste bide batzuetatik egiaztatu:** enpresa edo erakundearekin telefonoz harremanetan jarri emaila legitimoa dela egiaztatzeko.

**Kontuz erantsitako fitxategiekin eta estekekin:** fitxategi edo esteka horiek malwarea izan dezakete, eta URL laburtagailua erabili ohi dira birbideratzeak ezkutatzeko.

Phishing saiakeraren bat detektatzen baduzu, [incidencias@cyberzaintza.eus](mailto:incidencias@cyberzaintza.eus) helbidean jakinarazi iezaguzu.

