

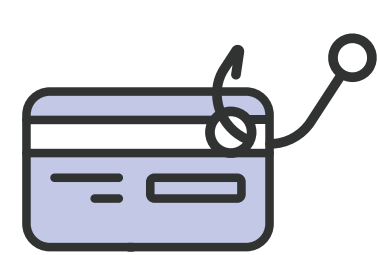
# ZIBERERASO OHIKOENAK BLACK FRIDAY ETA CYBER MONDAY EGUNETAN

Egun horietan Gabonetako erosketaren denboraldia inauguratzen da eta denda askotan beharpen handiak jartzen dituzte. Erabiltzaile asko baliatzen dira oparietarako preziorik onenak aurkitzeko eta hacker edo pirata informatikoen helburu ohikoenetako bat iruzurra izaten da.

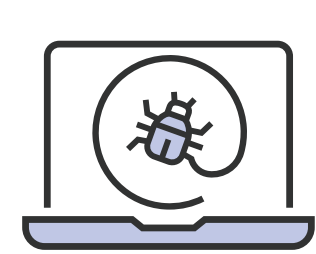
**Denboraldi horren gorakadarekin**, Gabonetako erosketaren denboraldia inauguratuko da. **Denda askotan beharpen handiak izango ditu**, eta Europan gero eta errotuago dagoen tradizio amerikarra du. **Erabiltzaile asko baliatzen dira oparietarako preziorik onenak aurkitzeko. Hacker edo pirata informatikoen helburu ohikoenetako bat iruzurra da.**



## BADAKIZU ZER ONDORIO IZAN DITZAKEZUN ZENTZUMEN GUZTIAK AKTIBATUTA EZ BADITUZU?



**Phishing:** Mezu elektronikoak helbide-zerrenda batera bidaltzeari egiten dio erreferentzia, hartzaile jakinik gabe. Horren adibidea izan daiteke azken smartphone modeloa prezio oso baxuetan eskaintzen duen kanpaina



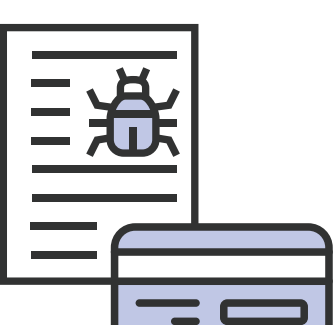
**Typosquatting:** Gure nabigatzailearen barran web helbideak idaztean egiten ditugun akatsak arakaten dituen zibereraso-mota bat da. Horrela, nahi gabe, normalean iruzurrezko helburuak dituzten orrialde alternatiboak bisitatuko ditugu.



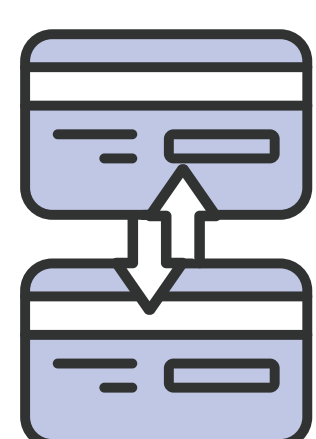
**Spam:** Masiboki bidali gabeko posta elektroniko gisa definitzen da, baina terminoa askoz zabalagoa da. Spam mezu desegokia, gogaikarria eta desiratua da, eta erabiltzaile askori bidaltzen zaio, posta elektronikoz, WhatsApp bidez, SMS bidez, sare sozialetan edo telefonoz deituta.



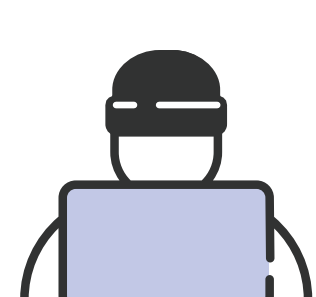
**Adware:** Software mota honen helburua da erabiltzaileak gailu batean publizitatea ikustera behartzea, nahi ez duen eta kontrolik gabe. Hori lortzeko, ausaz atera ditzakezu iragarkiak, eta, horretarako, adwarearen bidez izango ez liratekeen publizitate-webguneetara bideratu.



**Chargeback edo nahitaezko itzulketa:** Zure bankuak edo ordainketa-hornitzaileak jasotako kobrantza bat kentzen dizunean gertatzen da, normalean iruzurrezko txartel bat onartu izanaren ondorioz.



**E-skimming:** Kreditu-txartelen skimming-aren bertsio digitala da. Mundu fisikoan, skimmer-ak kreditu-txartelen irakurgailuen gainean jartzen dira kreditu-txartelei buruzko informazioa irakurtzeko; e-skimmer-ak, berriz, kode maltzuraren zatiak dira, eta bezero baten kreditu-txarteleko datuak lapurtzen dituzte lineako transakzio batean.



**Datu pertsonalak, bankuko datuak edo gakoak lapurtzea.** Zibergaizkileek bidean jartzen dizkiguten tranpetan erortzen garenean, beren borondatez eta buru-belarri eman diezazkiekegu gure datu pertsonalak, eta, hartara, gure banku-datuak eman diezazkiekegu.

## ZIBERERASOTZAILEEN JOKOAN ERORI NAHI EZ BADUZU, AKTIBATU ZURE ZENTZUMENAK, PENTSATU KLIK EGIN AURRETIK ETA JARRAITU AHOLKU HAUEI:



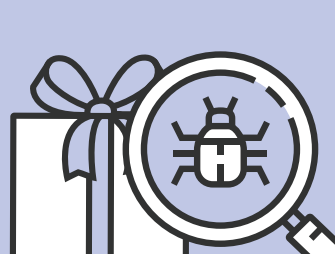
**1.Egiaztatu zure konexioa.** Babestu WiFi publikoak VPN baten bidez erabiltzean.



**2.Egiaztatu dendaren URLa zuzena dela.** Askotan, webgunearen itxura eta giltzarrapoa baino ez ditugu kontuan hartzen. Web-orri baterako ziurtagiria jaulkitzea nahiko erraza eta kostu txikikoa denez, garrantzitsua da URLa egiaztatzea ere.



**3.Berretsi online denda fidagarria dela.** Egin erosketak soilik merkataritza elektroniko fidagarri, ezagun edo pribatutasun-politika eta erosketa-baldintza seguruak dituzten produktuetan.



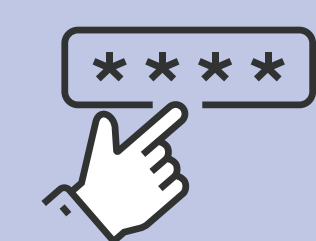
**4.Kontuz bereziki baxuak diren prezioekin.** Eskaintza oso ikusgarrien edo ohi baino merkeenen inguruko zalantza.



**5.Ez erabili kreditu-txartelarik.** Txartel birtualak erabil ditzakezu.



**6.Babestu zure banku-kontua.** Ez gorde banku-kontuaren zenbakia inongo web orritan.



**7.Erabili pasahitz sendoak edo aldatu maiz.**



**8.Eguneratu zure gailuak.** Ziurtatu malwarerik eta infekziorik gabe daudela, eta erabili birusen aurkako sistema bat.



Iruzur edo zibereraso saiakeraren bat antzeman baduzu, eman abisua guri, gertakariei erantzuna emateko talde teknikoak zabalkundea saihesteko neurriak hartzeko eta arriskuen berri emateko.

**MALWARE EDO PHISHING KANPAINA AKTIBO BAT IDENTIFIKATZEN BADUZU, JAKINARAZ IEZAGUZU:**



Doako telefono zenbakia: 900 104 891



Helbide elektronikoak: [incidencias@besc.es](mailto:incidencias@besc.es)