ZIBERSEGURTASUN GIDA PRAKTIKOA

... EROSKETAK EGITEKO

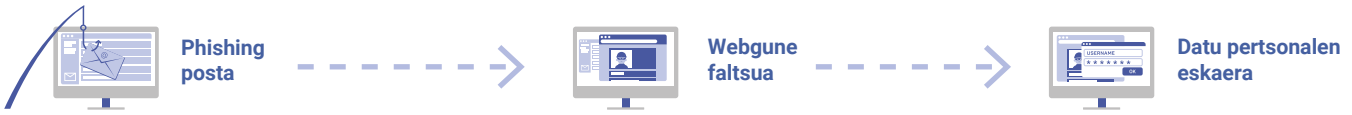
Zibergaizkileek baliatu egiten dituzte *Single Day*, *Black Friday*, *Cyber Monday* Eguberrietako kanpaina eta halako data bereziak, eta phishing posta masiboak bidali eta gune faltsuekin lotzen dituzte, dendak imitatuz, datu pertsonalak lortzeko helburuarekin..

"Amazon, 'Phishing'-eko sareen biktima Black Friday jaialdian" Iturria: Crónica Global. 30/11/2019.

"Phishing'-aren gorakadak Single Day eta Black Friday egunen ospakizuna arriskuan jartzen ditu: 803.000 eraso saiakera egun batean" Iturria: Europa Press. 11/11/2020.

"Phishing-ak gora egin du Black Friday eta Gabonetako online erosketekin" Iturria: Redes Zone. 26/11/2019.

PROZEDURA



AHOLKUAK

1. Pentsatu klik egin baino lehen

Kontuz ibili esteketan klik egitera animatzen zaituzten iragarkiekin. Ez egin klik eta webgunera jo zuzenean, eskaintza zilegi dela egiaztatzeko.

2. Babestu zeure burua WiFi publikoak erabiltzean

Webgunea segurua izan arren, hirugarrengoen jardueraren eragina jasateko arriskua duzu.

3. Egiaztatu helbide-barra

Ziurtatu erosketa egin nahi duzun webguneofizialean zaudela.

4. Begiratu eCommerce-aren web-helbidea segurua ote den

URLaren hasierak "https://" edo "shttp://" izan behar du.

5. Egiaztatu ziurtagiri baliagarria ote duzun

SSL (Secure Sockets Layer) ziurtagiriek webgune baten identitatea egiaztatzen dute.

6. Egiaztatu domeinuaren existentziari buruzko informazioa

Domeinua oso berria bada eta entitate misteriotsu baten izenean erregistratuta badago, zure susmoak oinarri sendoa du.

7. Baieztatu online-denda fidagarria dela

Erosi baino lehen, fidagarritasunari buruzko online-iritziak bilatu. Denda fidagarria bada, harremanetarako bidea, helbide fisikoa eta abar emango ditu.

8. Itzulpen-politika berrikusi

Adi letra txikiari.

9. Zure kreditu-txartela erabili gabe erosi online

Erabili txartel birtualak, paypal edo beste diru-zorro birtual bat.

10. Kontuz ibili zure banku-kontuarekin

Mugimenduak berrikusi, jarduera susmagarririk ote dagoen ikusteko

11. Pasahitz-kudeatzaile bat instalatu

Ausazko pasahitz sendoak sortu eCommerce bakoitzerako, eta faktore anitzeko egiaztapena erabili aukera duzun guztietan.

12. Zure gailuak eguneratuta izan

Ziurtatu malwarerik eta infekziorik ez dutela, eta erabili antibirus bat.

Lagundu mehatxuak gutxitzen...

atzematen dituzun iruzurren berri emanez, 900 104 891 telefonora deituz edo incidencias@bcsc.eus helbidera mezua bidaliz. Beharrezko neurriak hartuko ditugu.

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza