

ZEINTZUK DIRA INTERNET BIDEZKO IRUZURRIK OHIKOENAK?

Egunero, jende askok iruzur saiakerak jasotzen ditu internet bidez. Oso ohikoak dira, eta edonor eror daiteke horietan benetakoak diruditelako.

Horregatik, kontu handiz joan behar da eta informazio guztia kontuan hartzea Jarraian azalduko dizugu.

3 iruzur ohikoenek izen arraroak dituzte, baina hemen modu errazean azalduko dizkizugu.

1. **Phishing:** posta elektronikoko bidezko iruzurra

Honela funtzionatzen du:

- Zure bankuarena edo ezagutzen duzun enpresa batena dirudien mezu elektronikoko bat bidaltzen dizute, baina gezurra da.
- Mezua presazkoa izan ohi da, adibidez: «Zure kontua blokeatu egingo da zure datuak eguneratzen ez badituzu».
- Esteka bat du, eta, irekitzean, benetakoa imitatzen duen orrialde faltsu batera eramaten zaitu.
- Orri horretan zure datu pertsonalak edo bankuko datuak jartzea nahi dute, lapurtzeko.

**Garrantzitsua:**

Horrelako mezu bat jasotzen baduzu, ez ireki esteka ez sartu datu pertsonalik.

Zalantzarik baduzu,
bidali dizuten mezuaren gatz
eta sartu zeu bankuaren edo enpresaren web ofizialean
edo deitu bezeroaren arretarako telefono-zenbakira.

2. *Smishing*: SMS bidezko iruzurra mugikorrera

Honela funtzionatzen du:

- Testu-mezu bat (SMS) jasotzen duzu mugikorrean.
- Mezuak hau esan dezake: «Pakete bat daukazu zintzilik» edo «Zure kontua bertan behera geratuko da».
- Esteka edo zenbaki faltsu bat ere badu, ireki eta zure datuak sar ditzazun.
- Egiten baduzu, zure kontutik dirua lapurtu edo zure izenean erosketak egin ditzakete.

**Garrantzitsua:**

Horrelako SMS bat jasotzen baduzu, ez ireki estekak.

Zalantzarik baduzu,
sar zaitez zu zeu bankuaren edo enpresaren webgune ofizialean
edo deitu bezeroaren arretarako telefono-zenbakira.

3. *Vishing*: telefono bidezko iruzurra

Honela funtzionatzen du:

- Bankuko, enpresa bateko edo erakunde ofizial bateko zerbitzu teknikoko norbaiten plantak eginez deitzen dizute.
- Modu sinesgarrian hitz egiten dute, haiengan konfiantza izan dezazun.
- Zure datu pertsonalak eskatzen dizkizute edo ordenagailua edo mugikorra kaltetzen duten programak instalatzea nahi dute.

Garrantzitsua:

Norbaitek deitzen badizu informazio pertsonala eskatzeko edo zure ekiporako sarbidea, eseki.

Maula saiakera bat da.

Deia benetakoa den ala ez zalantzak badituzu, Sar zaitez zeu bankuaren edo enpresaren web ofizialean edo deitu bezeroaren arretarako telefono-zenbakira.



Nola babes zaitezke kasu guztietan?

- Ez partekatu zure datu pertsonalak ez badakizu nork eskatzen dituen.
- Ez erantzun «bai» batekin telefonoa hartzen duzunean.
- Begiratu zer helbide edo zenbakitatik idazten edo deitzen dizuten.
- Ez ireki esteka susmagarriak eta ez deskargatu ezagutzen ez dituzun pertsonen fitxategirik.

Zer da aparteko segurtasuna: 2 urratseko egiaztapena (2FA)?

- Bi urratseko egiaztapena segurtasun estra zure kontuak babesteko.
- Horrez gain pasahitza, behar duzu bigarren kodea zure kontuetan sartzeko.
- Kode hau hona iritsiko zaizu: mugikorra edo bat segurtasun-aplikazio.
- Horrela, norbaitek zure pasahitza izan arren, ezingo da sartu koderik gabe.

Gogoan izan:

- Eduki beti eguneratuta ordenagailua eta mugikorra.
- Erabili antibirusa eta eguneratu.
- Aholku hauek jarraitzen badituzu, askoz ere babestuago egongo zara.
- Eta, zalantzarik baduzu, ez partekatu inoiz zure datuak.

Zure informazio pertsonala zaintzea zure segurtasuna zaintzea da.

