

QUINS SÓN ELS FRAUS PER INTERNET MÉS COMUNS?

Cada dia, moltes persones reben intents de frau o estafa per internet.

Són molt freqüents i qualsevol pot caure-hi perquè semblen reals.

Per això, cal anar amb molta cura i tenir en compte tota la informació que t'expliquem a continuació.

Las 3 estafes més habituals tenen noms estranys, però aquí te'ls expliquem de manera senzilla.

1. *Phishing*: estafa per correu electrònic

Funciona de la manera següent:

- T'envien un correu electrònic que sembla del teu banc o d'una empresa que coneixes, però es fals.
- El missatge sol ser urgent, per exemple: «El teu compte serà bloquejat si no actualitzes les dades».
- Inclou un enllaç i, quan l'obres, et porta a una pàgina falsa que imita la real.
- En aquesta pàgina volen que posis les dades personals o bancàries per robar-te-les.

**Important:**

Si reps un correu així, no obris l'enllaç
ni introdueixis dades personals.

Si tens dubtes,
surt del missatge que t'han enviat
i entra tu mateix a la web oficial del banc o l'empresa
o truca al número de telèfon d'atenció al client.

2. *Smishing*: estafa per SMS al mòbil

Funciona de la manera següent:

- Reps un missatge de text (SMS) al mòbil.
- El missatge pot dir: «Tens un paquet pendent»
o «El teu compte serà suspès».
- També inclou un enllaç o un número fals
perquè l'obris i introdueixis les teves dades.
- Si ho fas, et poden robar diners del teu compte
o fer compres en nom teu.

**Important:**

Si reps un SMS així, no obris els enllaços.

Si tens dubtes,
entra tu mateix a la web oficial del banc o l'empresa
o truca al número de telèfon d'atenció al client.

3. *Vishing*: estafa per telèfon

Funciona de la manera següent:

- Et truquen fent-se passar per algú del banc, del servei tècnic d'una empresa o d'una institució oficial.
- Parlen de manera convincent perquè hi confiïs.
- Et demanen les dades personals o intenten que instal·lis programes que fan malbé el teu ordinador o el teu mòbil.

Important:

Si algú et truca demanant informació personal o accés al teu equip, penja.
És un intent d'estafa.

Si tens dubtes de si la trucada és real, entra tu mateix a la web oficial del banc o l'empresa o truca al número de telèfon d'atenció al client.



Com et pots protegir en tots els casos?

- No comparteixis les teves dades personals si no saps qui les demana.
- No responguis amb un «sí» quan despengis el telèfon.
- Revisa l'adreça del correu o el número des del qual t'escriuen o et truquen.
- No obris enllaços sospitosos ni descarreguis arxius de persones que no coneixes.

Què és la verificació en 2 passos (2FA)?

- La verificació en 2 passos és una seguretat extra per protegir els teus comptes.
- A més de la contrasenya, necessites un segon codi per entrar als teus comptes.
- Aquest codi t'arriba al mòbil o a una aplicació de seguretat.
- Així, encara que algú tingui la teva contrasenya, no hi podrà entrar sense el codi.

Recorda:

- Mantingues l'ordinador i el mòbil sempre actualitzats.
- Fes servir antivirus i actualitza'l.
- Si segueixes aquests consells, estaràs molt més protegit.
- I, si tens dubtes, mai comparteixis les teves dades.

Cuidar la teva informació personal és cuidar de la teva seguretat.

