CaixaBank
PAYMENTS & CONSUMER

CALES SON AS FRAUDES POR INTERNET MÁIS COMÚNS?

Cada día, moitas persoas reciben intentos de estafa por Internet.
Son moi frecuentes e calquera pode caer nelas
porque parecen reais.

Por iso, hai que ir con moito coidado
e ter en conta toda a información
que che explicamos a continuación.

As 3 estafas máis habituais teñen nomes raros,
pero aquí explicámoschos de maneira sinxela.

1. *Phishing*: estafa por correo electrónico

Funciona da seguinte maneira:

- Mándanche un correo electrónico
  que parece do teu banco
  ou dunha empresa que coñeces, pero é falso.
- A mensaxe adoita ser urxente, por exemplo:
  «A túa conta será bloqueada se non actualizas os teus datos».
- Inclúe unha ligazón e, ao abrila,
  lévate a unha páxina falsa que imita a real.
- Nesa páxina queren que poñas os teus datos persoais
  ou bancarios para roubarchos.

Importante:
Se recibes un correo así, non abras a ligazón
nin introduzas datos persoais.

Se tes dúbidas,
sal da mensaxe que che enviaron
e entra ti mesmo na web oficial do banco ou a empresa
ou chama o número de teléfono de atención ao cliente.

2. *Smishing*: estafa por SMS ao móbil

Funciona da seguinte maneira:

- Recibes unha mensaxe de texto (SMS) no teu móbil.
- A mensaxe pode dicir: «Tes un paquete pendente»
  ou «A túa conta será suspendida».
- Tamén inclúe unha ligazón ou un número falso
  para que o abras e introduzas os teus datos.
- Se o fas, poden roubarche diñeiro da túa conta
  ou facer compras ao teu nome.

Importante:
Se recibes unha SMS así, non abras as ligazóns.

Se tes dúbidas,
entra ti mesmo na web oficial do banco ou a empresa
ou chama o número de teléfono de atención ao cliente.

3. *Vishing*: estafa por teléfono

Funciona da seguinte maneira:

- Chámante facéndose pasar por alguén do banco,
  do servizo técnico dunha empresa
  ou dunha institución oficial.
- Falan de maneira convincente para que confíes neles.
- Pídenche os teus datos persoais
  ou tentan que instales programas
  que danan o teu computador ou o teu móbil.

Importante:
Se alguén te chama pedindo información persoal
ou acceso ao teu equipo, colga.
É un intento de estafa.

Se tes dúbidas de se a chamada é real,
entra ti mesmo na web oficial do banco ou a empresa
ou chama o número de teléfono de atención ao cliente.

Como podes protexerte en todos os casos?

- Non compartas os teus datos persoais
  se non sabes quen os pide.
- Non respondas cun «si» cando descolgues o teléfono.
- Revisa o enderezo do correo ou o número
  desde o que che escriben ou te chaman.
- Non abras ligazóns sospeitosas
  nin descargues arquivos de persoas que non coñezas.

Que é a seguridade extra: verificación en 2 pasos (2FA)?

- A verificación en 2 pasos é unha seguridade extra
  para protexer as túas contas.
- Ademais do contrasinal,
  necesitas un segundo código para entrar nas túas contas.
- Este código chégache ao móbil
  ou a unha aplicación de seguridade.
- Así, aínda que alguén teña o teu contrasinal,
  non poderá entrar sen o código.

Lembra:

- Mantén o teu computador e o teu móbil sempre actualizados.
- Usa antivirus e actualízao.
- Se segues estes consellos, estarás moito máis protexido.
- E, se tes dúbidas, nunca compartas os teus datos.

Coidar a túa información persoal é coidar da túa seguridade.