CaixaBank
PAYMENTS & CONSUMER

¿CUÁLES SON LOS FRAUDES POR INTERNET MÁS COMUNES?

Cada día, muchas personas reciben intentos
de fraude o estafa por internet.
Son muy frecuentes y cualquiera puede caer en ellos
porque parecen reales.

Por eso, hay que ir con mucho cuidado
y tener en cuenta toda la información
que te explicamos a continuación.

Las 3 estafas más habituales tienen nombres raros,
pero aquí te los explicamos de manera sencilla.

1. *Phishing*: estafa por correo electrónico

Funciona de la siguiente manera:

- Te mandan un correo electrónico
  que parece de tu banco
  o de una empresa que conoces, pero es falso.
- El mensaje suele ser urgente, por ejemplo:
  «Tu cuenta será bloqueada si no actualizas tus datos».
- Incluye un enlace y, al abrirlo,
  te lleva a una página falsa que imita a la real.
- En esa página quieren que pongas tus datos personales
  o bancarios para robártelos.

Importante:
Si recibes un correo así, no abras el enlace
ni introduzcas datos personales.

Si tienes dudas,
sal del mensaje que te han enviado
y entra tú mismo en la web oficial del banco o la empresa
o llama al número de teléfono de atención al cliente.

2. *Smishing*: estafa por SMS al móvil

Funciona de la siguiente manera:

- Recibes un mensaje de texto (SMS) en tu móvil.
- El mensaje puede decir: «Tienes un paquete pendiente» o «Tu cuenta será suspendida».
- También incluye un enlace o un número falso para que lo abras e introduzcas tus datos.
- Si lo haces, pueden robarte dinero de tu cuenta o hacer compras a tu nombre.

Importante:
Si recibes un SMS así, no abras los enlaces.

Si tienes dudas,
entra tú mismo en la web oficial del banco o la empresa
o llama al número de teléfono de atención al cliente.

3. *Vishing*: estafa por teléfono

Funciona de la siguiente manera:

- Te llaman haciéndose pasar por alguien del banco, del servicio técnico de una empresa o de una institución oficial.
- Hablan de manera convincente para que confíes en ellos.
- Te piden tus datos personales o intentan que instales programas que dañan tu ordenador o tu móvil.

Importante:
Si alguien te llama pidiendo información personal o acceso a tu equipo, cuelga.
Es un intento de estafa.

Si tienes dudas de si la llamada es real, entra tú mismo en la web oficial del banco o la empresa o llama al número de teléfono de atención al cliente.

¿Cómo puedes protegerte en todos los casos?

- No compartas tus datos personales
  si no sabes quién los pide.
- No respondas con un «sí» cuando descuelgues el teléfono.
- Revisa la dirección del correo o el número
  desde el que te escriben o te llaman.
- No abras enlaces sospechosos
  ni descargues archivos de personas que no conozcas.

¿Qué es la verificación en 2 pasos (2FA)?

- La verificación en 2 pasos es una seguridad extra
  para proteger tus cuentas.
- Además de la contraseña,
  necesitas un segundo código para entrar en tus cuentas.
- Este código te llega al móvil
  o a una aplicación de seguridad.
- Así, aunque alguien tenga tu contraseña,
  no podrá entrar sin el código.

Recuerda:

- Mantén tu ordenador y tu móvil siempre actualizados.
- Usa antivirus y actualízalo.
- Si sigues estos consejos, estarás mucho más protegido.
- Y, si tienes dudas, nunca compartas tus datos.

Cuidar tu información personal es cuidar de tu seguridad.