CaixaEnginyers
BANCA COOPERATIVA

*Humanitzem les teves finances*

# EVITA LA TRAMPA!

## 10 consells bàsics de ciberseguretat

Amb la col·laboració de Selva Orejón



Els fraus digitals són cada vegada més sofisticats
i qualsevol persona pot ser víctima dels ciberdelinqüents
en algun moment. Conèixer com actuen i saber
**identificar els senyals d'alerta**
és el primer pas per protegir les nostres dades
i els nostres diners.

**Com aconsegueixen guanyar-se la nostra confiança?**
**Quins senyals ens haurien de fer sospitar?**

Des de Caixa Enginyers, **amb la col·laboració**
**de Selva Orejón**, consultora experta en ciberseguretat
i identitat digital, volem ajudar-te a conèixer les trampes
digitals més habituals, aprendre a identificar-les i,
sobretot, **saber com evitar-les**.

Perquè, tot i que tenen noms tan curiosos
com *phishing, smishing, vishing o quishing*,
aquestes estafes són, malauradament, molt més
habituals del que ens pensem.

**Tingues sempre presents aquests 10 consells**
**i no abaixis mai la guàrdia!**



## 1 Correus electrònics i *phishing*: no et deixis enganyar

El *phishing* consisteix en **correus electrònics que imiten la imatge d'una entitat bancària** per aconseguir les teves claus d'accés, dades de la targeta o codis de verificació. Sovint utilitzen **missatges urgents**, com ara «El teu compte serà bloquejat», amb enllaços a pàgines web falses que semblen autèntiques.

No accedeixis a la banca a través d'enllaços de correus sospitosos. Entra directament al web oficial o a l'aplicació de Caixa Enginyers. I recorda que mai no et demanarem la contrasenya completa, el PIN o els codis de verificació per correu electrònic.

## 2 SMS i *smishing*: compte amb els missatges que semblen del teu banc

El *smishing* utilitza **SMS fraudulents que suplanten una entitat bancària**. Poden incloure dades personals reals per resultar més creïbles i demanar-te que cliquis un enllaç per resoldre una incidència urgent.

Desconfia dels missatges que et demanin dades personals, claus o codis. No cliquis els enllaços i comprova qualsevol avís directament a través dels canals oficials de Caixa Enginyers.

## 3 Trucades i *vishing*: no et refiïs de qui et truca

El *vishing* és una estafa telefònica mitjançant la qual **algú es fa passar per una persona professional del banc**, amb un to urgent i convincent, per aconseguir dades confidencials o fer que autoritzis una operació.

No facilitis mai per telèfon contrasenyes, PIN ni codis d'un sol ús. Si tens dubtes, penja immediatament i truca a Caixa Enginyers a través dels nostres canals oficials.

## 4 Codis QR i *quishing*: no tots et porten on esperes

El *quishing* consisteix a utilitzar **codis QR manipulats, sovint enganxats sobre codis legítims** en cartells, aparcaments o establiments, que et dirigeixen a pàgines fraudulentes.

Abans d'obrir un enllaç, comprova l'adreça web que apareix en escanejar el codi. Desconfia dels QR manipulats o que et demanin dades bancàries inesperadament.

## 5 Intel·ligència artificial: no tot el que veus o sents és real

Amb la intel·ligència artificial es poden **clonar veus, manipular vídeos** (*deepfakes*) i **crear perfils o converses que semblen autèntics**. Els estafadors poden simular la veu d'un familiar que necessita diners urgentment o utilitzar persones conegudes per promocionar inversions falses.

Si reps una petició urgent, encara que reconeguis la veu o la imatge, no actuïs immediatament. Contacta amb la persona per un número que ja tinguis guardat i confirma que la petició és real. O pregunta-li per alguna cosa que només vosaltres conegueu.

## 6 Inversions fraudulentes: massa bones per ser veritat

Els anomenats ***xiringuitos financers*** són **entitats que ofereixen serveis d'inversió sense l'autorització corresponent**. Sovint contacten per WhatsApp, Telegram o xarxes socials i prometen rendibilitats molt elevades, ràpides i sense risc. Evidentment, falses.

Identifica aquests **senyals d'alerta**: contactes inesperats amb ofertes d'inversió, rendibilitats molt altes i «garantides», pressió per invertir o reinvertir ràpidament, plataformes amb guanys aparentment creixents, però impossibles de verificar... Abans d'invertir, comprova si l'entitat està autoritzada a través de la CNMV (cnmv.es). I, si tens dubtes, consulta amb Caixa Enginyers.







## 7 **Banca digital i compres:** opera sempre amb seguretat

Operar des de webs poc fiables, utilitzar xarxes Wi-Fi públiques o comprar en botigues en línia fraudulentes **pot posar en perill les teves dades bancàries i els teus diners.**




Quan operis amb els teus diners a Internet, pren algunes precaucions bàsiques.

- Accedeix a BancaONLINE només des del web oficial o de l'app de Caixa Enginyers.
- Evita les xarxes Wi-Fi públiques per fer operacions bancàries.
- Revisa periòdicament els moviments dels teus comptes.
- Tanca la sessió quan acabis d'operar.
- Compra només en webs de confiança, consulta les opinions sobre el venedor i utilitza mètodes de pagament segurs.

## 8 **Falses identitats i enginyeria social:** quan la confiança és la trampa

L'enginyeria social és una tècnica que utilitzen els ciberdelinqüents per **manipular la teva confiança**. Poden fer-se passar per un venedor, un assessor financer o fins i tot un familiar per aconseguir diners o informació personal.

Desconfia de les peticions inesperades de diners o dades, **especialment si van acompanyades de pressió o urgència**. Abans de fer res, verifica sempre la identitat de qui t'ho demana trucant a la persona directament.

## 9 **Contrasenyes i dispositius:** posa barreres als ciberdelinqüents

Les **contrasenyes poc segures, els dispositius desprotegits o les aplicacions desactualitzades** poden facilitar que els ciberdelinqüents accedeixin a les teves dades personals i als teus comptes.






Protegir els teus comptes i dispositius és essencial per **evitar accessos no autoritzats.**

- Utilitza contrasenyes llargues, robustes i diferents per a cada servei.
- Activa la verificació en dos passos, especialment al correu electrònic.
- Bloqueja el mòbil amb PIN, patró o identificació biomètrica.
- Mantén els dispositius i les aplicacions actualitzats.
- No descarreguis arxius de fonts desconegudes.
- Activa el Face ID a l'app de Caixa Enginyers, si el dispositiu ho permet.
- No comparteixis les contrasenyes amb ningú.

## 10 **I en tots els casos:** si sospites d'un frau, actua ràpidament

Quan es produeix un frau digital, els ciberdelinqüents **poden actuar en qüestió de minuts.** Per això, detectar qualsevol moviment sospitós i reaccionar ràpidament és fonamental per limitar-ne les conseqüències.




Davant d'una operació sospitosa, el **temps és clau**.

- Contacta immediatament amb Caixa Enginyers si detectes una operació que no reconeixes.
- Si sospites que han utilitzat la teva targeta, desactiva-la des de BancaONLINE o BancaMOBILE.
- Si creus que algú ha accedit als teus comptes, comunica-ho a l'entitat perquè pugui aplicar les mesures de protecció adequades.
- Truca al 017 d'INCIBE, el servei gratuït d'ajuda en ciberseguretat.
- Consulta periòdicament els avisos i les recomanacions de seguretat de Caixa Enginyers.



GRUP CaixaEnginyers BANCA COOPERATIVA

*Humanitzem les teves finances*

**Vols conèixer les últimes tendències en frau i estafes?**

Visita el nostre espai de seguretat al web de Caixa Enginyers i descobreix més consells i recomanacions per protegir-te dels fraus digitals.

Informa't sobre la nostra Assegurança Protecció Digital.