CONSELLS PER A CONVERTIR-TE EN UN/A IAI@ CONNECTAT

Protegeix la teua informació i la dels teus equips

Tingues precaució i **no et fies de ningú** que et demane informació personal o et propose la instal·lació d'una aplicació en el teu PC o mòbil. Els bancs mai demanaran informació confidencial per telèfon, correu o SMS.

Mantingues les teues aplicacions i dispositius actualitzats, activa les actualitzacions automàtiques del teu ordinador, la teua tauleta i el teu mòbil.

Evita instal·lar-te aplicacions de dubtosa procedència o reputació i utilitza sempre els repositoris oficials.

Utilitza algun tipus d'antivirus en el teu PC, així com les opcions de seguretat per defecte que t'oferisca el teu equip.

Precaució en línia i en públic

Sigues conscient que **al publicar informació en Internet** (Facebook, LinkedIn, Instagram, Twitter, etc.), **qualsevol pot accedir a ella** i utilitzar-la per a intentar enganyar-te.

Revisa les configuracions de privacitat de les xarxes socials. Per exemple, que només els teus contactes directes puguen veure informació personal.

Mai publiques contrasenyes, ubicacions, temps de vacances on estigues absent, números de telèfon, informació sobre targetes bancàries, etc. En general, tot allò que no comptaries mai a un desconegut pel carrer.

Tingues molt **compte amb els desconeguts que inicien una conversa** en línia o telefònica amb tu, planteja't quina és la seua motivació i fins a quin punt pots verificar la seua identitat real. Mantingues les teues contrasenyes segures

Crea contrasenyes robustes, que no siguen fàcils d'endevinar. Evita utilitzar la teua data de naixement, la teua ciutat, nom d'un familiar, del gos, 1234, etc.

Mai les anotes en paper ni les compartisques. I, sobretot, no li les proporciones a ningú que contacte amb tu en línia ni per telèfon.

Pensa sempre abans de fer clic o respondre

Davant el dubte, el millor és no respondre al correu, penjar el telèfon o esborrar el missatge de text, així evitem que ens enganyen.

No existeixen gangues, ni tenim el dia de sort

No existeixen les ofertes massa bones, solen ser enganys. Si sospites, cerca el contacte oficial de la suposada botiga i cerciora't que el que has rebut per correu és real, cerca el telèfon de la marca i flama o visita l'establiment per a verificar-lo.

No existeixen les inversions hiper-rendibles

No hi ha inversions amb altes rendibilitats. Dubte de les inversions que prometen grans rendibilitats, especialment amb criptomonedes, i de "quiosquets" poc fiables o no coneguts. Darrere sol haver-hi una estafa on, una vegada invertit els diners, desapareixerà.

Les ofertes de treball no cauen del cel

No existeixen ofertes de treball tan fabuloses. Dubte dels anuncis que prometen fantàstiques ofertes de treball que et facen pensar que podrien ser per als teus fills o nets. Darrere sol haver-hi una estafa on se'ns demana diners i l'oferta de treball no existeix.

Si dubtes, assessora't

Les estafes estan molt ben dissenyades. Si dubtes sobre si és o no una estafa, abans de parlar amb un desconegut o entrar en un enllaç, **parla amb els teus fills, els teus familiars o persones de confiança i explica'ls els teus dubtes.**

El món digital no és molt diferent del món real. Pot semblar-te perillós, però amb aquestes senzilles precaucions pot resultar més segur i fiable que el presencial i amb molts més avantatges.

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic
TOTS A UNA veu
IVF* INSTITUT VALENCIÀ DE FINANCES
iai@ connectat

iai@ connectat

Consells per a utilitzar internet de manera segura

Vivim en l'era digital. L'ús de les **noves tecnologies** per a comprar en línia, interactuar amb la banca o amb l'administració **ens poden ser de molta utilitat** en permetre'ns fer gestions còmodament, des de qualsevol lloc, a qualsevol hora, sense esperar cues i estalviant-nos temps.

Malgrat els seus avantatges, moltes persones no fan el pas perquè encara tenen **por d'usar internet.**

No obstant això, amb unes **precaucions bàsiques**, les compres en línia o la banca per internet poden ser fins i tot **més fiables que la interacció presencial**, i els teus diners estarà molt més segur que quan el portes damunt o els tens a casa.

10 ESTAFES USADES PELS CIBERDELINQÜENTS I COM PROTEGIR-TE

TELEFONADES DE DESCONEGUTS (Vishing)

Si reps una **telefonada d'un número desconegut** en la qual t'ofereixen un servei o producte o t'avisen d'un problema amb el teu compte bancari **HAS DE PENJAR SENSE DONAR CONVERSA.**

Encara que t'intenten alertar o fer por deus desconfiar i penjar, sense tindre objeccions a ser poc educat/a amb l'interlocutor. Mai has d'entaular conversa ni donar informació. El teu banc MAI et demanarà informació per internet.

TELEFONADES DE FALSOS TÈCNICS (VISHING)

Si reps una **telefonada d'un número desconegut** en la qual t'avisen d'un problema en el teu ordinador **HAS DE PENJAR SENSE DONAR CONVERSA.**

Els serveis tècnics no criden si no els has anomenat prèviament o no tens contractat un suport tècnic per al teu ordinador. MAI has d'entaular conversa, ni seguir cap instrucció que et donen, ni donar informació.

MISSATGES DE TEXT (SMISHING)

Si reps un SMS amb la recepció d'un paquet que no has demanat, o un problema en el compte bancari o un pagament que no esperes **HAS D'ESBORRAR-LO.**

Encara que el SMS siga "aparentment" de Correus o del nostre banc. Ni Correus, ni el nostre banc ens demanaran MAI informació per internet.

CORREUS ELECTRÒNICS (PISHING)

Si reps un correu electrònic en el qual et demanen dades personals o et porta a visitar una pàgina web o a descarregar una aplicació **HAS D'ESBORRAR-LO.**

Encara que el correu siga "aparentment" de Correus o del nostre banc habitual. Ni Correus, ni el nostre banc ens demanaran MAI informació per internet.

OFERTES FANTÀSTIQUES O REGALS PER INTERNET

Si navegant per internet veus una oferta molt bona d'un producte, oferta de treball o se't notifica que has sigut agraciat/a amb un premi **NO HAS DE FER CAS.**

Evita entrar en l'enllaç. Si dubtes, cerciora't a través del contacte oficial amb el comerç per a veure si és real o és un engany. Si així i tot dubtes, abans de fer res comenta-ho amb familiars o persones de la teua confiança.

FALSOS BIZUM

Si reps un missatge de Bizum en el qual sembla que rebràs diners NO HAS DE FER CAS.

Has de llegir bé el missatge que ens arriba perquè, en lloc de rebre, podria ser una petició de diners. En tot cas, els organismes oficials no utilitzen Bizum.

NOTIFICACIONS DE PROBLEMES AMB EL COMPTE DEL BANC

Si es posen en contacte per SMS/correu per a dir-nos que hi ha un problema en el nostre compte NO HAS DE FER CAS.

Sospita sempre dels SMS o de correus electrònics que porten a un enllaç o et demanen dades de qualsevol mena. To banc MAI et demanarà informació per internet.

ESCANEIG DE CODIS QR (QRjacking)

Si et demanen que escaneges un codi QR des del teu telèfon mòbil NO HAS DE FER CAS.

Evita l'escaneig de codis QR i/o desactiva en el mòbil l'opció d'obrir automàticament els enllaços en escanejar un codi QR.

DISCOS USB (Baiting)

Si una persona desconeguda et demana introduir una memòria USB en el teu ordinador o connectar el teu mòbil a un ordinador **NO DEUS PERMETRE-LI-HO.**

Sospita de dispositius de desconeguts, evita connectar-nos i mantingues actualitzat l'antivirus de l'ordinador.

COMPRES PER INTERNET

Si veus pàgines web de botigues en línia amb ofertes increïblement bones NO HAS DE FER CAS.

També pots buscar informació sobre l'empresa o consultar amb les teues persones de confiança.

No hi ha "duros a quatre pessetes" i tampoc penses que és el teu dia de sort. Evita entrar en l'enllaç. Si dubtes, cerciora't a través del contacte oficial amb el comerç per a veure si és real o és un engany. Si així i tot dubtes, abans de fer res comenta-ho amb familiars o persones de la teua confiança.