GUIA DE MESURES BÀSIQUES DE CIBERSEGURETAT 2026

Adaptat a la Intel·ligència Artificial

IL·LUSTRE COL·LEGI D'ADVOCATS DE GRANOLLERS

La Comissió de Tecnologia del Col·legi ha preparat aquest document amb diverses mesures bàsiques de ciberseguretat per protegir l'activitat profesional

IL·LUSTRE COL·LEGI D'ADVOCATS DE GRANOLLERS

GUIA DE MESURES BÀSIQUES DE CIBERSEGURETAT

Adaptat a la Intel·ligència Artificial

La Comissió de Tecnologia del Col·legi ha preparat aquest document amb diverses mesures bàsiques de ciberseguretat per protegir l'activitat professional.

Autor: Enric Mestre Ribera. Comissió de Tecnologia ICAVOR

Col·laboració: Genís Margarit i Contel. Centralip.

Versió 3.4 – 18 de març de 2026- www.icavor.cat

SUMARI

INTRODUCCIÓ

La Comissió de Tecnologia del Col·legi d'Advocats de Granollers, posa a la vostra disposició una "Guia de Mesures Bàsiques de Ciberseguretat" que ha elaborat per a tot tipus de nivell d'usuaris per ajudar a prevenir els riscos en ciberseguretat des d'un punt de vista professional i també personal.

Especialment, aquesta guia va dirigida els col·legiats de l'Il·lustre Col·legi d'Advocats de Granollers, com a eina fonamental de conscienciació, identificació dels problemes de seguretat que els advocats en l'ús de eines tecnològiques i de comunicació.

També està enfocada a les eines de **Google Workspace** que el Col·legi ofereix als seus col·legiats, amb l'objectiu de millorar-ne la seguretat en l'ús i aprofitar al màxim tots els seus avantatges..

La filosofia d'aquest manual i de la Comissió de Tecnologia del Col·legi d'Advocats de Granollers és **"no confiïs mai, verifica sempre"**

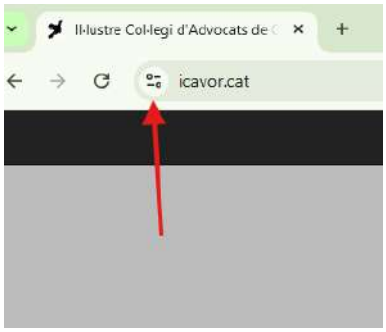
RECOMANCIONS DE SEGURETAT GENERALS

NAVEGACIÓ SEGURA

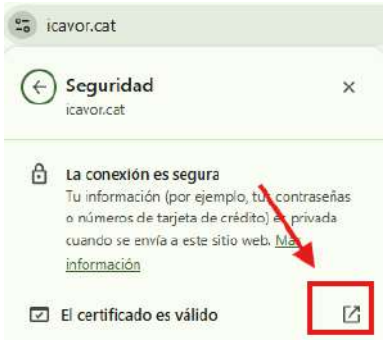
Alhora d'introduir, enviar o consultar dades en línia revisar que el **lloc web tingui certificat SSL** (Secure Sockets Layer), és a dir, que l'accés web comenci per HTTPS, ja que protegeix les dades transferides mitjançant el xifratge activat per un certificat SSL en un servidor.

Verificar el nom dels destins web als quals et connectis. No és suficient confiar amb el disseny i la interfície sigui el mateix de sempre, perquè els ciberdelinqüents la podrien replicar per enganyar, estafar o roba dades. **Hi ha certificats d'alta seguretat, certifiquen el nom de domini i de l'empresa, són els certificats EV SSL**, aquesta informació es pot consultar des del navegador i són molt útils per evitar la suplantació de web en serveis tant sensibles com bancs i correu electrònic.

Exemple navegador Chrome de certificat segur:



Com comprovar el certificat i propietari:



No ingressar a llocs que siguin potencialment perillosos o que hagen pogut ser compromesos. En aquest sentit, és molt recomanable la utilització de **programari antivirus que bloqui pàgines web que realitzen una activitat maliciosa.**

Bloquejar components de **Javascript** per defecte, solament habilitar aquells que confiem.

Important comprovar la **geolocalització el servidor de la web** (necessari a l'hora de valorar si un proveïdor ofereix garanties suficients de compliment RGPD):

- Introduir url web per saber la seva IP: https://www.wmtips.com/tools/info/
- Introduir núm. d'IP per saber a quin país s'allotja: https://www.ip2location.com/
  - **Si és país UE:** OK RGPD
  - **País no UE:** verificar si està sota sistema de nivell adequat de protecció que UE (Per exemple: AWS, Google, Microsoft Azure, etc...)

NOTA: la majoria d'antivirus, disposen d'opcions de vigilància i bloqueig de pàgines sospitoses.

NAVEGADORS D'INTERNET

És recomanable utilitzar navegació privada (Inprivate), sobretot si s'utilitza **un ordinador compartit**. La navegació privada, és la manera de utilitzar internet en mode d'incògnit, i és una funció de privacitat en alguns navegadors web per a desactivar l'historial de navegació i la caixeta web on s'introdueixen dades, com les contrasenyes. Això permet a una persona navegar per la web sense emmagatzemar dades locals en l'historial del navegador i que podrien ser recuperats més tard.

La majoria de navegadors disposen d'aquesta opció, com ara:

- Brave (la finalitat d'aquest navegador bloqueja cookies i dades de seguiment)
- Chrome
- Edge
- Explorer
- Firefox
- Opera
- Safari
- Tor (té la finalitat del navegador és protegir la privacitat dels usuaris. També s'utilitza per la navegació del Deep Web o internet profunda).
- ChatGPT Atlas (Basats en IA)
- Comet de Perplexity (basats en IA)

EL MODE INCÒGNIT NO GARANTEIX EN ABSOLUT L'ANONIMAT A INTERNET.

Recomanacions:

- Mantenir el navegador i les seves extensions actualitzades.
- No instal·lar complements innecessaris o poc de confiança.

ÚS DE CONTRASENYES SEGURES

Les contrasenyes que s'utilitzin a internet han de ser robustes i diferents entre els diversos recursos que utilitzes a Internet. Utilitza números, lletres majúscules o minúscules, signes (%,;- etc..) i mínim de 12 caràcters.

No és recomanable utilitzar una mateixa contrasenya per diversos serveis i aplicacions, per tant, pot ser útil un gestor de contrasenyes per emmagatzemar-les i utilitzar un patró per generar-ne diverses.

Obtenir una bona contrasenya pots utilitzar generadors com per exemple el següent: https://www.lastpass.com/es/password-generator

Tanmateix, la seguretat d'accés ja no es tracta només d'una contrasenya complexa, sinó garantir la confidencialitat d'accés, per exemple amb una eina de doble factor d'autenticació.

IMPORTANT:

La pàgina web https://haveibeenpwned.com/ ens permet saber si les teves contrasenyes s'han vist compromeses per una bretxa de seguretat.

Podem tenir la millor contrasenya del món, però si el servei on està vinculada s'ha filtrat per un atac, tindrem un problema de seguretat addicional, ja que podem donar pistes o patró d'una manera de crear les contrasenyes, que poden utilitzar per entrar en d'altres comptes. Per evitar-ho, es recomanable utilitzar un gestor de contrasenyes.

QUÈ ÉS UN GESTOR DE CONTRASENYES?

Els gestors de contrasenyes són aplicacions que serveixen per a emmagatzemar les nostres credencials en una base de dades xifrada mitjançant una contrasenya mestra.

Mitjançant una extensió en el navegador, d'aquesta manera entrem en una web o aplicació que requereix contrasenya, la pròpia extensió ens la recordarà.

Però, com totes les mesures tenen els seus punts febles, **en l'any 2022 Lastpass va ser atacada**, i van filtrar molts contrasenyes dels usuaris. Això va posar de manifest el risc d'emmagatzematge centralitzat el núvol. Com avantatge d'aquest tipus de servei, és més fàcil cuidar i custodiar un sol lloc que totes els altres aplicacions i subscripcions per separat.

Gestors de Contrasenyes:

- https://www.lastpass.com/es
- https://1password.com/
- https://nordpass.com/es/

NOTA: destaquem els gestors de contrasenyes dels Navegadors com Chrome, poden ser útils per la seva gestió.

RECOMANACIÓ IMPORTANT:

En el cas d'haver-se infectat l'equip o dispositiu, recomanem canviar el més ràpid possible, totes les contrasenyes que tinguem emmagatzemades, com ara: Correu, bancs, xarxes socials, web, etc.

SEGONA AUTENTICACIÓ

Utilitzar com a mesura de seguretat una **segona d'autentificació per millorar el control d'accés remot**, per exemple en l'accés al correu electrònic o recursos de banca online, etc.

Amb aquest sistema t'assegures que malgrat t'encertin o et robin la contrasenya, també és necessari el teu dispositiu mòbil, targeta intel·ligent, clau USB, etc.

En algunes recursos web també recomanen utilitzar aplicacions per la doble autenticació, com per exemple:

- Google Authenticator
- Authy

GOOGLE PASSKEYS

Google disposa d'un sistema modern d'inici de sessió anomenat **Passkey** (o clau d'accés). Aquest sistema està dissenyat per substituir les contrasenyes de tota la vida i fer que entrar als teus comptes sigui molt més ràpid i segur.

Com es diferencia dels sistemes antics?

En els sistemes tradicionals de "doble verificació" (com quan reps un SMS o uses Google Authenticator), havies de fer dos passos lents i separats: Escriure la teva contrasenya i introduir un codi numèric que t'arribava al mòbil.

Amb les Passkeys, tot això s'unifica en un sol gest. No has de recordar cap contrasenya complexa; el sistema fa els dos passos de seguretat simultàniament en qüestió de segons.

Per què és tan segur si sembla més fàcil?

Tot i que per a tu només és un pas (posar el dit o mirar la càmera), en realitat el sistema està fent una **doble verificació** completa. Per entendre-ho, cal saber que per entrar de manera segura es demanen dues proves:

- **Una cosa que TENS (El dispositiu):** La clau digital està guardada dins del teu telèfon o ordinador. Ningú pot entrar al teu compte si no té el teu aparell físicament.
- **Una cosa que ETS o SAPS (El desbloqueig):** Perquè el telèfon utilitzi aquesta clau, tu has d'autoritzar-ho amb la teva empremta digital, la teva cara (FaceID) o el PIN de desbloqueig de pantalla.

Els 3 avantatges clau

1. **Adéu a les contrasenyes:** Funciona sense haver d'escriure res. S'acaba el problema d'oblidar la contrasenya o haver-la de canviar sovint.
2. **Molt més ràpid:** Inicies sessió fent servir el mateix mètode que uses per desbloquejar el mòbil (empremta, cara o patró).
3. **Anti-hackers (Anti-Phishing):** Com que no hi ha cap contrasenya escrita ni cap codi que t'enviïn per missatge, els hackers no poden enganyar-te perquè els hi donis. La clau digital mai surt del teu dispositiu.

Pas a pas per activar-ho?

1. **Accedeix al teu compte:** Entra a la web de gestió del teu compte de Google: myaccount.google.com.
2. **Ves a Seguretat:** Al menú de l'esquerra (o a la part superior si estàs al mòbil), busca i clica a l'opció **Seguretat**

WIFI

Evitar l'ús de xarxes wifi que no siguin confiança. Si no és imprescindible, no et connectis a xarxes públiques que no siguin conegudes ni autoritzades. El més recomanable és utilitzar la pròpia connexió 4G o 5G en el vostre dispositiu mòbil.

En el cas que no sigui possible i es necessiti una xarxa pública, connectar-se mitjançant **VPN**. Hi ha diverses opcions i serveis en el mercat.

Recomanem utilitzar una **contrasenya complexa i robusta en el vostre Wifi**, per evitar sabotatges externs.

VPN I XARXES

Connexió remota segura utilitzant una VPN (Virtual Private Network).

Què és la VPN? és una xarxa privada virtual, mitjançant túnel segur entre el dispositiu i Internet, que assegurar la privacitat de les nostres dades.

Si el programari maliciós ja ha aconseguit introduir-se al nostre dispositiu, l'ús d'una VPN pot permetre a l'atacant accedir directament a la xarxa interna. Per això, és imprescindible comptar amb mesures de seguretat addicionals, més, si tenim una infraestructura gran, com diverses seus de treball o un gran número de dispositius.

Mesures de seguretat per connexions en xarxa i VPN:

- **Firewall:** disposar d'un tallafoc que gestioni, filtri i controli tots els accessos entrants i sortints per evitar connexions no autoritzades dins la xarxa.
- **Control d'accés a la xarxa:** Segmentar la xarxa interna perquè, si un dispositiu es compromet, l'atacant no tingui accés global.
- **Monitoratge i avisos d'activitat sospitosa:** Ús d'eines EDR, SIEM o sistemes de monitoratge d'esdeveniments.
    - EDR — *Endpoint Detection and Response* **Què és?** Una solució instal·lada als dispositius finals (*endpoints*: ordinadors, servidors, portàtils…) **Funció principal:** Monitoritza
    - SIEM — Security Information and Event Management. **Què és?** Una plataforma centralitzada que recull i correlaciona logs i esdeveniments de diferents sistemes (servidors, firewalls, aplicacions…)
- **Política estricta d'instal·lació de programari:** Evitar instal·lar aplicacions desconegudes o no verificades.

Tipus VPN: softwares o mitjançant un aparell Firewall més programari.

És important protegir la nostra xarxa local amb connexió VPN, si **teletreballem i ens connectem remotament a un altre ordinador o servidor** (Per exemple connectar-se des de casa a terminal dels despatx).

Exemple de VPN en el mercat:

- Cyberghostvpn: https://www.cyberghostvpn.com/es_ES/
- Nordvpn: https://nordvpn.com/es/
- Google ONE https://one.google.com/
- Private internet access https://www.privateinternetaccess.com/es/
- Surfshark: https://surfshark.com/es/vpn

La majoria d'antivirus també inclouen de la possibilitat de contractar VPN.

FIREWALL

Un **Firewall és un sistema de seguretat de xarxa per ordinadors** que restringeix el trànsit d'Internet entrant, sortint o dins d'una xarxa privada. Aquest software o aquesta unitat de maquinari i programari dedicats opera bloquejant o permetent els paquets de dades de manera selectiva.

Disposar d'un Firewall es recomanable quan tenim diversos equips connectats en xarxa, ja que és una barrera de seguretat essencial juga un paper crític en protegir els sistemes informàtics contra amenaces en línia, filtrant activament les comunicacions per assegurar-se que només les connexions segures siguin establertes. El Firewall pot ser configurat per adaptar-se a les necessitats específiques de la xarxa, oferint un control detallat sobre quins tipus de tràfic són autoritzats i quins són bloquejats. Això ajuda a prevenir atacs externs malintencionats i a mantenir la integritat i la confidencialitat de les dades. També ens proporciona com un control d'accessos a la xarxa (important per esbrinar possibles origens d'atacs o problemes de segureat).

Els Firewall ha d'estar constatant actualitzant-se, en cas contrari perdent molt eficàcia. Normalment, els es connecten després del Router.

També es poden utilitzar firewalls per crear una VPN entre oficines situades en diferents llocs.

ANTIVIRUS

Limita l'accés a Internet per prevenir contingut perillós. Això implica tenir un sistema **d'antivirus** activat i les aplicacions actualitzades a les darreres versions. **És recomanable disposar d'antivirus a tots els dispositius, tant ordinadors, telèfons mòbils i tablets.**

Els **antivirus gratuïts ofereixen una versió molt bàsica i nivells de protecció més baixos que els de pagament**, a més de contrarestar només amenaces ja conegudes. Els antivirus de pagament estan dissenyats per respondre contra Malware que ha estat generat recentment.

Serveis addicionals: actualment, algunes versions d'antivirus inclou serveis complementaris molt interessants no només per la seguretat dels nostres equips, sinó també per la **protecció de la nostres dades a Internet**. Per exemple:

- Alertes en temps real sobre bretxa de seguretat del correu electrònic
- Alertes immediates quan les teves targetes de crèdit o identificacions personals formen part d'una bretxa de dades
- Informes periòdics de la seguretat de les teves dades personals actualitzat qualsevol possible violació que podria haver-te afectat.

Aquesta informació es permetrà actuar ràpidament i prendre les mesures adients per protegir les nostres dades.

Mantenir actualitzat els equips, dispositius i aplicacions. Assegurat que el sistema d'actualització d'aplicacions i programes sigui l'habitual. La majoria d'aquestes actualitzacions són per millorar o corregir errors de seguretat.

> ⚠️ **AVÍS:** Darrerament, s'han detectat atacs de ciberseguretat amb **actualitzacions falses de programari**. En cas de dubte esbrinar si les novetats proposades són correctes i legítimes. També en cas de dubte, es recomana posar-se en contacte amb el proveïdor per confirmar-ho la legitimitat de l'actualització.

CÒPIES DE SEGURETAT

És molt important realitzar periòdicament còpies de seguretat. Guardar-les en una ubicació diferent i alguna fora de la connexió a xarxa i verifica que es realitzen correctament. D'aquesta forma, en el cas de veure'ns afectats per algun incident de seguretat, podrem recuperar la informació i activitat d'una manera més àgil.

Cal tenir clar el temps de retenció de la informació, és a dir, durant quant temps es poden recuperar les dades perdudes o fins a quina data es conserven les còpies de seguretat.

En el cas de Google Drive, els arxius creats amb aplicacions de Google (Docs, Sheets, Slides…) disposen d'un historial de versions il·limitat, cosa que permet recuperar versions anteriors de manera senzilla. Altres serveis al núvol també ofereixen funcionalitats similars.

És molt important disposar de còpies de seguretat externes als dispositius locals per protegir-se de ransomware i d'altres incidents. És recomanable utilitzar aplicacions o serveis específics de backup que garanteixin una recuperació ràpida i segura de les dades.

SERVEIS CLOUD O NÚVOL D'ARXIUS

Antigament recomanàvem utilitzar serveis al núvol com OneDrive (Microsoft 365), Google Drive (Workspace), Dropbox, iCloud, etc. com a sistema de còpia de seguretat, sincronitzant els fitxers amb diferents dispositius, i poder accedir a la documentació des de qualsevol ubicació, mitjançant connexió a Internet.

Ara per seguretat, recomanem treballar directament al núvol, ja que això ajuda a reduir el risc d'infeccions per ransomware. Quan els fitxers no es desen localment, s'evita que es puguin infectar o encriptar i que, en conseqüència, la infecció es sincronitzi també amb el servei al núvol. A més, els servidors dels proveïdors de cloud disposen de mesures de seguretat més avançades que els equips locals.

Actualment, el sistema de sincronització, segueix sent útil per comoditat i productivitat: treballar des de diferents dispositius, compartir documents i tenir-los sempre accessibles.

Cal tenir present que, encara que plataformes com Google estan incorporant noves proteccions contra ransomware i altres amenaces, no poden garantir la recuperació total de tots els fitxers en cas d'incident. Per aquest motiu, és imprescindible mantenir una estratègia de còpies de seguretat addicional, independent del núvol, per assegurar la recuperació completa de la informació.

Les condicions d'ús del servei al núvol, han de garantir de disponibilitat i confidencialitat de la informació, i apostar per serveis dirigits a professionals.

L'advocat/da és responsable del tractament d'aquestes dades, està obligat a escollir proveïdors cloud que ofereixen garanties de compliment de la normativa de protecció de dades o inclús, que hagin estat validades i analitzades prèviament per l'autoritat de control (Per exemple: Drive dins el paquet de Google Workspace).

MESURES DE SEGURETAT GENERALS PEL CORREU ELECTRÒNIC

L'enviament de correus fraudulents és un dels problemes més greus en ciberseguretat, aquests pretenen que el receptor del missatge descarregui un document adjunt maliciós que podria infectar el seu equip o xarxa amb algun tipus de Malware per robar informació (contrasenyes, credencials bancaries, contactes, adreces, etc...) o bé utilitzar els contactes per enviar correu Spam o fins i tot amb la finalitat d'infectar-los.

Els missatges intenten enganyar-nos instant a revisar pressupostos, ofertes o ens demanen directament dades pròpies.

El funcionament del correu electrònic, quan es va dissenyar, no preveia que es pogués utilitzar per enganyar. Per aquest motiu, és força **senzill fer-ne un ús fraudulent**, sobretot pel que fa al nom del remitent, ja que s'hi pot posar qualsevol cosa. **Fins i tot es pot indicar com a nom una altra adreça de correu per confondre i enganyar sobre qui envia realment el missatge.**

Amb la **intel·ligència artificial**, encara és més fàcil crear correus fraudulents, ja que poden imitar la nostra manera de redactar i comunicar-nos.

Dels correus maliciosos més perillosos són els ens poden infectar amb un **Ransonware.** Aquests encripten l'ordinador o ordinadors que estiguin connectats en una mateixa xarxa, demanat un rescat econòmic per poder-ho desencriptar. Normalment es realitzen en criptomònades i és impossible de rastrejar el pagament.

Recomanacions:

El correu d'ICAVOR utilitza la plataforma Google Workspace, que és una de les més grans del món amb milions d'usuaris, on s'inverteix molts recursos fer frenar i evitar aquest tipus de correu. Tanmateix, és important si tenim el més mínim dubte que analitzem bé el correu. Per això, us recomanem el següent:

Aquests consells serveixen per a qualsevol tipus de dispositiu o sistema operatiu.

a. **No obris correus d'usuaris desconeguts o que no hagis sol·licitat**: elimina'ls directament. No contestis en cap cas a aquests correus.
b. **Revisa els enllaços** abans de fer clic encara que siguin de contactes coneguts.
c. **Desconfia dels enllaços escurçats**.
d. **Desconfia dels fitxers adjunts** encara que siguin de contactes coneguts.

Recomanem el recurs https://www.virustotal.com/ que escanejar un document o URL amb més de 80 antivirus simultàniament.

e. **Tingues sempre actualitzat el sistema operatiu i l'antivirus**. En el cas de l'antivirus, comprova que està actiu.
f. En cas que **dubtis de la veracitat d'un correu**, posar-se en contacte amb el remitent per verificar que sigui autèntic. Us recomanem la Guia de "el Instituto Nacional de Seguirdad" per ajudar a identificar i verificar correus electrònics: https://www.incibe.es/protege-tu-empresa/blog/dudas-legitimidad-correo-aprende-identificarlos
g. **Verifica que el nom del remitent correspongui amb l'adreça de correu**. És un sistema bastant utilitzat per enganyar el receptor. Per exemple: remitent és el Col·legi Advocats Granollers però s'envia des de l'adreça: baldimir.7.7@ermail.ru

   És molt fàcil atribuir qualsevol nom a un correu electrònic, no confiar-se només identificant-lo.

h. **Si el correu l'envia més d'un remitent o amb còpia vista, revisar que les adreces siguin correctes** i que no n'hagi cap d'estranya. Per exemple: col·legi@icavor.com ; baldimir.7.7@ermail.ru En aquest cas desconfia del missatge.
i. Sempre que sigui possible, utilitzar el correu en versió cloud, Exchange o Imap, en cas de virus o Ransonware en un dels nostres dispositius, que no afecti bústia correu que està en el servidor cloud, si més no, hi ha tindrem menys possibilitats que això passi.
j. **Filtres spam:** cada dia s'envien de 300 millons de correus SPAM a tot el món, alguns d'aquest amb virus. Per millorar la gestió del correu i ajudar els filtres antispam, els correus SPAM cal etiquetar-los com no desitjat. També es pot utilitzar els filtres dels gestors de correu per evitar aquells missatges molt repetitius s'enviïn a brossa directament. També es recomanable afegir els remitents més habituals o més important per nosaltres a com a correus segurs o llistes blanques. Així ens assegurem que sempre entrin en la safata d'entrada i no com a correu SPAM.

CORREUS TEMPORALS

Els correus electrònics temporals s'utilitzen principalment per protegir la privacitat i reduir riscos digitals en situacions concretes, com ara quan ens registrem en llocs web on no volem facilitar cap dada personal però se'ns exigeix un correu electrònic per completar el procés. Aquests correus no substitueixen el correu personal, sinó que el complementen per a usos puntuals.

A més, és important conèixer aquest tipus de serveis per prendre consciència que poden ser utilitzats per tercers en comunicacions, fins i tot en entorns professionals. Conèixer la seva existència ens permet identificar possibles usos inadequats i entendre tant els seus avantatges com els seus riscos, amb l'objectiu de millorar la nostra seguretat digital.

💡 **IMPORTANT; No serveixen per coses importants**

No utilitzis un correu temporal per:

Recuperar el compte d'un servei important (Banc, correu principal, feina).

Autenticacions que requereixen seguretat (2FA, contrasenyes, notificacions sensibles).
Si el correu temporal caduca, perdràs l'accés.

⚠️ **Quins són els perills i limitacions de fer servir correus temporals**

Tot i que poden ser útils, no són una solució segura per a tot:

- **No són privats ni molt segurs:** Molt serveis de correu temporal no tenen clau ni xifrat fort, i algunes bústies poden ser públics o accessibles per altres que coneguin la mateixa adreça.
- **Poden ser bloquejats:** Molts llocs web no accepten registres amb correus temporals perquè saben que poden ser usats per fraus o abús.
- **Generen un risc per a serveis**: Si fas servir correus temporals massiu per crear comptes falsos o escalar recursos, els proveïdors ho poden considerar abús i podrien bloquejar-te.

Servei	URL	Notes breus
10 Minute Mail	https://10minutemail.com	Correu que expira després de 10 min (es pot ampliar).
Temp Mail	https://temp-mail.org	Un dels més populars per registrar-se ràpidament.
Guerrilla Mail	https://www.guerrillamail.com	Adreces temporals que duren una hora aproximadament.
Internxt Temporary Email	https://internxt.com/temporary-email	Permet crear correus per una estona i evitar exposar el teu real.

CORREU EN LÍNIA VERSUS CORREU GESTOR D'ESCRIPTORI

Gmail d'ICAVOR, dins de Google Workspace és un servei per a professionals, de correu electrònic dissenyat per operar íntegrament en línea, ja sigui mitjançant el **navegador web** o les **aplicacions mòbils**. La seva major fortalesa resideix en ser una solució totalment basada en el núvol (*cloud-native*).

Els serveis el núvol com Gmail, tenen un munt de sistemes de seguretat avançada, que milloren les que puguem disposar en els nostres equips si utilitzem gestors de correu IMAP, com ara Outlook a Thunderbird.

En qualsevol cas, no és recomanable utilitzar configuracions POP3, és molt antiga i desfasada, ja que aquest protocol descarrega els correus al dispositiu local i impedeix consultar-los fàcilment des d'altres equips o ubicacions. A més, els missatges queden emmagatzemats exclusivament a l'ordinador, cosa que obliga a fer còpies de seguretat manuals i a realitzar exportacions si es canvia d'equip. També és necessari un programa per la seva gestió com Outlook.

A banda d'això, és imprescindible comptar amb un bon sistema de seguretat antivirus per evitar riscos afegits.

Avantatges enfront correu Web respecte a programes de gestor de correus d'Escriptori (com ara Outlook):

Accessibilitat Global: Pots accedir a tots els teus correus i arxius des de qualsevol dispositiu i lloc, sense dependre d'una instal·lació d'escriptori ni de sincronitzacions manuals.

Seguretat Centralitzada: La seguretat, incloent-hi la protecció contra *phishing* i *spam*, es gestiona i s'actualitza constantment des dels servidors de Google, superant sovint les defenses locals.

MODE CONFIDENCIALITAT DE GMAIL

El Mode Confidencial de Gmail permet als usuaris enviar correus amb proteccions addicionals per a la informació sensible. La seva funció principal és evitar que els destinataris copiïn, imprimissin, reexpedeixin o descarreguin el contingut del missatge i els fitxers adjunts.

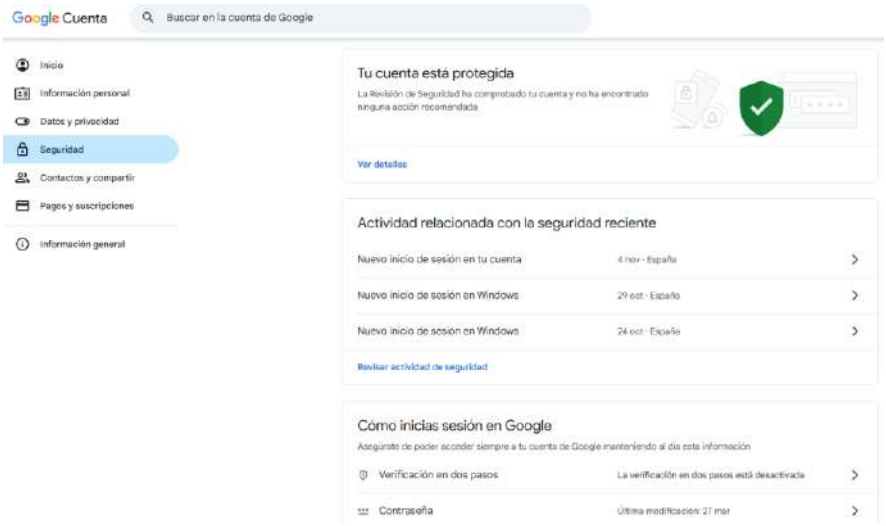
Aquest mode estableix una data de caducitat per al missatge (des d'un dia fins a cinc anys). Un cop passat el termini, el correu desapareix de la safata d'entrada del destinatari. A més, l'emissor pot revocar l'accés al missatge en qualsevol moment abans de la caducitat. Per a una seguretat màxima, es pot requerir una contrasenya d'accés per SMS abans que el destinatari pugui obrir el contingut. Aquesta funció és ideal per compartir dades privades temporalment.

CONSELLS PER UTILITZAR EL DISPOSITIU MÒBIL

Sempre que sigui possible, els dispositius d'ús professional utilitzar-los només per tasques relacionades amb el treball i per usuaris autoritzats. **La instal·lació d'aplicacions personals podrien comprometre la confidencialitat d'informació de l'empresa.**

Recomanacions per a qualsevol sistema operatiu:

- Una correcta protecció i **bloqueig del dispositiu** amb mesures d'accés, com ara: utilitzar contrasenya, PIN, accés biomètric (empremta digital, etc). També bloquejar automàticament la pantalla del dispositiu passat uns segons sense utilitzar-lo.
- **Actualitzar** el sistema operatiu i aplicacions sempre que es requereixi. El propi mòbil i les aplicacions solen notificar que hi ha actualitzacions pendents. Sovint aquestes són millores i correccions de seguretat.
- **Evitar l'ús de xarxes Wifi que no siguin confiança.** Utilitzar la pròpia connexió 4G o 5G en el vostre dispositiu mòbil. En el cas que no sigui possible, es recomanable utilitzar una VPN
- **Disposar d'antivirus.**
- **Disposar d'un sistema de protecció en cas de pèrdua o robatori del dispositiu mòbil:** geolocalitzar el mòbil, bloquejar-lo remotament i eliminar totes les dades. Aquest opció està disponible en els sistemes operatius com iOS i Android.
    - En Android disposa de les opcions: localització, bloqueig, eliminació de dades i fer sonar el mòbil encara que estigui en silenci. Més informació: https://myaccount.google.com/find-your-phone
- En la **compte del nostre Google (My Account**), disposem de **l'apartat de Seguretat** és el centre de control per a totes les mesures de protecció i us proporciona una visió completa de l'estat de seguretat del vostre compte. Per exemple:
    - Estat de Seguretat i Alertes
    - Comprovació de Seguretat (Security Check-up): Us ofereix un resum ràpid de l'estat actual de la vostra seguretat, amb recomanacions personalitzades per reforçar-la (per exemple, si la vostra contrasenya és antiga o si heu de revisar algun dispositiu).
    - Activitat de Seguretat Recent: Una llista dels esdeveniments de seguretat importants, com ara nous inicis de sessió en dispositius desconeguts, canvis de contrasenya, o intents de bloqueig, per tal que pugueu actuar immediatament si detecteu alguna cosa sospitosa.
    - Inici de Sessió i Verificació
    - Dispositius i Aplicacions: Els vostres dispositius: Una llista de tots els dispositius (ordinadors, mòbils, tauletes) on teniu la sessió iniciada actualment. Us permet revisar si reconeixeu tots els equips i tancar la sessió en aquells que ja no feu servir o que us han robat.
    - Gestió d'accés d'aplicacions de tercers: Us mostra quines aplicacions o serveis de tercers tenen permís per accedir a dades del vostre Compte de Google (com ara Gmail o Drive) i us permet revocar l'accés si cal.



Opcions de seguretat també estan disponibles en sistema operatiu iOS d'Apple.

UTILITZAR EL RECURSOS, SERVEIS WEB O APLICACIONS CONEGUDES I VERIFICADES

Vigilar i comprovar que les aplicacions que s'instal·len, siguin fiables i oficials. Per a disminuir la possibilitat de descarregar aplicacions falses o malicioses, us recomanem els següent:

- Què l'aplicació estigui verificada per la plataforma o market de les aplicacions
- Valoracions i comentaris dels usuaris
- Revisar els permisos de seguretat

  Alhora d'instal·lar un aplicació vigilar els permisos d'accés i seguretat que ens demanen, i només autoritzar les que serveixen per l'ús de l'aplicació en concret. Per exemple: no té sentit que una aplicació de calculadora ens demani autorització per accedir els nostres contactes i geolocalització.

DISCS DURS EXTERNS

Sempre que sigui possible, si necessitem mobilitat d'arxius, utilitzar plataformes cloud o de disc dur virtual, per evitar la possibilitat extraviar el dispositiu amb les conseqüències que poden esdevenir en pèrdua de dades, afectació i infracció en la privacitat dels clients. Recordeu que els advocats gestionen dades molt sensibles.

També evitem possibles infeccions de Virus i Malware si utilitzem el disc en dispositius que no són els nostres.

En el cas d'utilitzar discs durs externs es recomana encriptar-lo.

ENCRIPTACIÓ DE DOCUMENTS

Xifrar una informació significa ocultar el contingut d'un missatge d'un document a simple vista. Això es fa mitjançant un algorisme matemàtic que modifica el text. Aquest només es pot desxifrà mitjançant una clau.

El contingut del document només el podran consultar els usuaris autoritzats.

És recomanable per informació que es comuniqui i contingui dades personals i/o amb contingut sensible (Per exemple: dades de categoria especial o de condemnes i infraccions penals).

El sistema operatiu Windows en versions Pro incorpora el programa **Bitlocker** per encriptar el disc dur.

Exemples d'altres serveis o aplicacions d'encriptació:

- Veracrypt: https://veracrypt.fr/en/Home.html
- Enigmail (desenvolupat per Mozilla Thunderbird) https://www.enigmail.net/index.php/en
- WinRAR

SMS

SMS és un sistema de notificacions i avisos que utilitzem en el dia a dia i que també s'usen per enviar missatges maliciosos, on el remitent es fa passar per diferents empreses d'enviament i recepció de paqueteria i també d'entitats bancàries.

L'objectiu d'aquests SMS és que els seus destinataris facin clic en l'enllaç per executar una aplicació mòbil (Malware o troià) que es descarrega en el terminal mòbil facilitant d'aquesta manera l'accés a les dades de l'usuari, entre els quals es poder robar dades i claus bancàries. També s'enganya amb enllaços que suplanten webs verdaderes per que l'usuari escrigui les seves dades personals. Aquest engany és molt comú en missatges d'entitats bancàries.

Aquest sistema de SMS fraudulents es basa en la probabilitat, és a dir, en encertar amb situacions i serveis reals del destinatari, com ara el seu Banc o que estiguin esperant un paquet.

Mesures de protecció:

- Desconfiar del missatges genèrics. Les dades normalment són personalitzades amb informació del receptor. Per exemple: hem detectat que la targeta acabada 0000 ha fet un càrrec.
- Desconfiar dels missatges que demanen dades personals o fer login. Aquest tipus d'informació no es demana mai.
- Busquen enganyar la víctima amb missatges d'alerta. Per exemple: hem detectat que han utilitzat la seva targeta de crèdit de forma fraudulenta. Els missatge verdaders, sempre indican alguna dada personal, com la terminació de la targeta de crèdit.
- Molta atenció amb els missatges que s'acompanyen amb enllaços URL que s'assemblen a les reals per confondre i enganyar. Per exemple: bancosantande**rr**.com. També es recomanable verificar la web consultant el certificat SSL del HTTPS (https://www.nomweb.com). En el cas que la web inici l'adreça web inicia amb HTTP desconfiar, segurament estaran suplantant una web verdadera.
- Desconfiar dels enllaços escurçats.
- ⚠ **IMPORTANT:** En cas de dubte trucar al remitent i preguntar si el missatge és autèntic.

APLICACIONS DE MISSATGERIA INSTANTÀNIA O XAT

És un mitjà de comunicació molt estès i utilitzat en l'àmbit personal com professional. Els serveis de missatgeria més coneguts són:

- Whatsapp
- Telegram
- Signal
- Messenger
- Hangouts
- Teams, etc.

És recomanable utilitzar les aplicacions de missatgeria com a canal de comunicació a nivell informatiu, i no com a mitjà per a compartir dades personals o informació confidencial.

Quan utilitzem per finalitats professionals, cal informar prèviament sobre com es tractaran les dades (amb especial atenció als riscos derivats d'aquest tractament de dades) i sol·licitar el consentiment per poder dur a terme aquesta comunicació electrònica d'acord amb la normativa sobre comerç electrònic (LSSICE 34/2002) i, posar a disposició un sistema gratuït i fàcil per oposar-se a seguir rebent missatges i oposar-se al tractament de dades en sí. **També és recomanable fer còpies de seguretat dels missatges.**

Protegir l'accés aquestes aplicacions de missatgeria amb una contrasenya, PIN o mitjançant accés biomètric i també amb **activar notificacions per correu electrònic** quan s'accedeixi des d'un altre dispositiu.

Important: amb les noves eines d'intel·ligència artificial l'engany o suplantació d'identitat és més senzill que mai, hem d'estar atents i no contestar cap missatge mínimament sospitós.

TRUCADES DE VEU

Amb les noves aplicacions d'intel·ligència artificial, cal estar més amatents a les converses i disposar d'estratègies per evitar enganys, com ara paraules clau consensuades.

Cal vigilar els números als quals contestem i tenir mesures de seguretat al telèfon mòbil. Tanmateix, també es poden suplantar números telefònics i serveis de missatgeria, com les trucades i missatges de WhatsApp.

Podeu ampliar la informació a l'apartat d'intel·ligència artificial.

VIRUS, MALWARE I ESTAFES

En les aplicacions de missatgeria com Whatsapp, també podem rebre missatges maliciosos amb l'objectiu d'estafar, infectar amb Virus o Malware per hackejar el telèfon mòbil. **Modus operandi:**

- Rebre un missatge per Whatsapp amb un codi de verificació, rebut suposadament per error des d'algun dels nostres contactes, ja que els criminals es valen del compte d'un número conegut per a suscitar la confiança de la seva víctima. Això vol dir que segurament el teu contacte l'han hackejat el seu compte. En aquest cas avisar ràpidament al remitent ja que li estan **suplantant la seva identitat**. Aquest sistema d'engany és molt utilitzat en **Grups de Whatsapp.** Aquest tipus de missatges simulen la verificació de dos passos demanen un codi de 4 a 6 xifres.
- Desconfiar de Whatsapp amb promocions i publicitat, sobretot si demanen dades personals o fer login.
- Desconfiar de enllaços escurçats
- Rebre missatges de contactes coneguts amb números de telèfon amb un prefix estranger.

CIBERSEGURETAT VERSUS INTEL·LIGÈNCIA ARTIFICIAL

La intel·ligència artificial ens aporta grans avantatges —automatització, precisió i productivitat—, però també introdueix riscos creixents en l'àmbit de la ciberseguretat. Un dels més rellevants i emergents és la proliferació de **deepfakes**, continguts falsos generats amb IA que poden afectar greument la confiança digital, la seguretat jurídica i a la suplantació d'identitat.

QUÈ SÓN ELS DEEPFAKES?

Els deepfakes són imatges, vídeos o àudios creats amb IA generativa que imiten persones o situacions que mai no han existit. Permeten recrear cares, veus o discursos falsos amb un realisme que fa difícil detectar la manipulació.

Aquest fenomen no només serveix per enganyar, sinó que també pot utilitzar-se per **posar en dubte proves reals**, el conegut **Liar's Dividend**: qualsevol persona pot afirmar que un contingut verídic és un deepfake.

PER QUÈ SÓN UN RISC CREIXENT?

La seva creació s'ha democratitzat: abans era una tasca tècnica i costosa; ara qualsevol persona pot generar vídeos falsos amb pocs clics.

Això obre la porta a usos maliciosos com:

- Manipulació informativa i política
- Difamació personal o professional
- Pornografia no consentida i falsa.
- Estafes econòmiques (veus o imatges clonades en trucades)
- Suplantació d'identitat
- Compromís de proves judicials

En paral·lel, la seva detecció és cada vegada més difícil i requerirà eines forenses més sofisticades o experts especialitzats.

RECOMANACIÓ DE SEGURETAT

Per evitar suplantacions d'identitat per veu, text o vídeo generades amb intel·ligència artificial, és recomanable acordar amb les persones més properes —tant a la família com a la feina— una paraula clau o "contrasenya subliminal" que permeti verificar ràpidament si qui es posa en contacte amb nosaltres és real o si pot ser una IA suplantant la identitat.

Si rebem una trucada, podríem intentar demanar quin és el seu **system prompt**, ja que una IA no hauria de poder revelar aquesta informació. Tot i això, aquest mètode no és fiable ni segur. Les IA avançades poden evitar respondre o generar una excusa convincent, i fins i tot, enganyar.

Per aquest motiu, és molt més recomanable utilitzar **una paraula clau acordada prèviament per verificar la identitat, tant en entorns familiars com de treball.**

Un dels enganys més habituals és la **modificació de tiquets o comprovants de compra**. Actualment, és bastant fàcil manipular aquest tipus de documents amb eines d'intel·ligència artificial.

IMPACTE EN L'ÀMBIT JUDICIAL

Els deepfakes representen un desafiament crític per als professionals del dret:

- Com podem garantir que una foto, un vídeo o un àudio són autèntics?
- Els peritatges tècnics i la verificació d'origen seran essencials per assegurar la fiabilitat de les proves en un procediment judicial.

PROTECCIÓ DE DADES en la IA

Moltes eines d'intel·ligència artificial utilitzen les dades que proporcionem per entrenar-se i millorar les seves respostes. Per aquest motiu, és important revisar la política de privacitat de cada eina que fem servir, especialment si hi introduïm dades personals, i encara més si es tracta d'informació especialment protegida, com la que poden gestionar els advocats: dades sobre delictes, informes mèdics, etc.

Les nostres imatges penjades a la IA, poden ser utilitzades per generar nous continguts.

⚠️ **És recomanable utilitzar informació anonimitzada.**

EINES ÚTILS PER ENTENDRE I COMBATRE ELS DEEPFAKES

Eines per crear Deepfakes (per comprendre la facilitat del risc)

- **HeyGen – Deepfake Maker:** https://www.heygen.com/tool/deepfake-maker
- **HeyGen – AI Video Avatar:** https://www.heygen.com/avatars/ai-video-avatar
- **Runway Gen-4:** https://runwayml.com
- **Resemble AI / Voice Cloning:** https://www.resemble.ai
- **ElevenLabs:** https://elevenlabs.io
- **Kling Motion Control:** https://app.klingai.com/

MOTION CHAT A TEMPS REAL

Un motion chat amb deepfakes és un sistema de xat amb IA que utilitza imatges o vídeos manipulats (deepfake) per crear un avatar realista en moviment que parla i interactua amb tu en **temps real**. És dir, es pot suplantar una persona en temps real, per exemple en un videoconferència. Aquesta tecnologia existeix, és nova, però segur que anirà millorant. Exemple d'aplicació:

- **Lucy 2.0:** https://lucy.decart.ai/

EINES PER DETECTAR DEEPFAKES

UTILITZAR MODELS RAONATS D'IA

Una de les mesures generals per verificar qualsevol document, imatge o vídeo que sospitem que pot haver estat generat per intel·ligència artificial és consultar models d'IA amb capacitat de raonament, com ChatGPT, Gemini o Claude. Només cal pujar el document, imatge o vídeo. On de moment això no serveix de gaire és en els àudios.

Aquestes eines estan dissenyades per analitzar la informació de manera lògica i ajudar-nos a determinar si un contingut podria haver estat creat per una IA. Tot i que la seva resposta no és definitiva ni completament fiable, ens pot oferir indicis útils per orientar-nos.

VÍDEO I IMATGE:

- Deepware Scanner — https://deepware.ai
- Reality Defender — https://www.realitydefender.com
- Sensity AI — https://sensity.ai
- Detect Fakes (MIT) — https://www.media.mit.edu/projects/detect-fakes/overview/

ÀUDIO:

- IDLive Voice Clone Detection — https://www.idrnd.ai/idlive-voice-clone-detection
- TruthScan / AI Voice Detector — https://truthscan.com/ai-voice-detector

ANÀLISI DE METADADES

Les metadades d'un fitxer poden ajudar a identificar-ne l'origen, el dispositiu, el programari o la data de creació, però poden ser manipulades. Per això cal combinar-les amb anàlisi forense i verificació de context.

DETECCIÓ DE TEXT GENERAT AMB IA

Fonamental en entorns acadèmics i de recerca, on l'autoria i l'autenticitat són clau:

- Copyleaks — https://copyleaks.com/es
- TextDetector.ai — https://textdetector.ai
- Compilatio AI Detector — https://www.compilatio.net/en/ai-detector-info
- QuillBot AI Detector — https://quillbot.com/ai-content-detector

Scribbr AI Detector — https://www.scribbr.com/ai-detector/

QUÈ ÉS L'ESTAFA DEL "BIZUM INVERS"?

L'estafa del "Bizum invers" és un frau molt comú, dissenyat per enganyar els **venedors de plataformes d'articles de segona mà o vehicles**. L'objectiu de l'estafador és aprofitar-se de la teva il·lusió per vendre i de la rapidesa amb què utilitzem el mòbil perquè, en lloc de cobrar per un article que vens, l'acabis pagant tu.

On actuen els estafadors?

Aquests delinqüents busquen les seves víctimes a aplicacions com **Vinted**, **Wallapop**, **Milanuncios** o en portals de venda de cotxes. Saben que en aquestes webs hi ha usuaris disposats a tancar un tracte ràpidament i s'apliquen a fons per trobar persones que actuïn per impuls o distracció.

El mètode pas a pas: Com intenten enganyar-te?

- **El contacte inicial i l'evasió:** Un suposat comprador et contacta mostrant un interès cec i immediat pel teu article. No fa preguntes sobre el seu estat ni intenta regatejar. El primer que fa és demanar-te el número de telèfon per portar la conversa a WhatsApp i evitar els sistemes de seguretat de l'aplicació.
- **L'excusa del pagament i la pressa:** Et pressiona argumentant que ho necessita de manera urgent. Rebutja utilitzar els mètodes de pagament segurs de la plataforma (com el sistema de Wallapop Envíos o la cartera de Vinted) i proposa fer-te un Bizum a l'instant, amb l'excusa que és "més directe i no cobra comissions".
- **L'enviament de la trampa:** En el moment del pagament, en lloc d'utilitzar l'opció "Enviar diners" a la seva aplicació bancària, l'estafador selecciona **"Sol·licitar diners"**.
- **La confusió fatal:** T'arriba una notificació de Bizum al mòbil. Com que estàs esperant rebre els diners i actues de pressa, llegeixes el missatge per sobre i prems "Acceptar" o

introdueixes el teu codi de confirmació. En fer-ho, el que estàs autoritzant realment és l'enviament dels teus propis fons al compte de l'estafador.

Com detectar-ho i evitar-ho?

⚠️ **LA REGLA D'OR DE BIZUM:** Per rebre diners a Bizum **MAI** és necessari acceptar cap sol·licitud, introduir contrasenyes ni confirmar res. L'ingrés es fa de manera totalment automàtica i el banc només t'envia una notificació informativa indicant que has rebut els fons.

Si l'aplicació del teu banc et demana una confirmació o un codi PIN, atura't immediatament. Aquesta acció només es requereix quan els diners han de sortir del teu compte. **Si et demana confirmació, és un frau.**

Consells bàsics de seguretat

- **Mantingues la conversa a l'app:** El teu principal escut és no facilitar el teu número de telèfon a desconeguts. Les plataformes oficials bloquegen ràpidament els perfils fraudulents.
- **Fes servir els mètodes de pagament oficials:** Les aplicacions de compravenda tenen passarel·les de pagament dissenyades precisament per retenir els diners i protegir tant el comprador com el venedor fins que l'operació es tanca amb èxit.
- **Desconfia de les facilitats extremes:** Si un comprador d'un cotxe o un article car no vol veure el producte, l'accepta a cegues i té una urgència inusual per pagar per Bizum, sospita immediatament.

VIDEOCONFERÈNCIES SEGURES

Potser l'engany o les falsificacions en les videoconferències mitjançant IA, no estan tan avançades com en els àudios, però precisament per aquest motiu és més fàcil que ens confiem i ens puguin enganyar. Amb les imatges, si ens les creiem, ens poden colar enganys encara més grans. També cal tenir en compte que la tecnologia està avançant molt ràpid i, per tant, **cada vegada serà més difícil saber què és real i què no.**

Cal tenir en compte, que els advocats tracten amb els seus clients dades personals especialment sensibles, i cada vegada més, s'utilitzen les videoconferències per atendre els clients, per aquest motiu, hem cregut necessari crea un apartat específic sobre aquest tema.

RECOMANACIONS DE SEGURETAT

- Apostar per versions professionals
- Convidar els participants per correu electrònic i activar la sala d'espera a la reunió, que és un entorn previ a la reunió, per controla els assistents i per poder bloquejar les persones que no han estat convidades.
- Protegir l'accés a reunions amb un contrasenya, per evitar que terceres persones no autoritzades tinguin accés.
- Verificar que la plataforma de videoconferències s'adapti a la RGPD.

NOVES MESURES EN LES VIDEOCONFERÈNCIES: COM DETECTAR DEEPFAKES EN VIDEOCONFERÈNCIES

1. Moviments facials i expressió no natural

Els deepfakes en temps real encara tenen dificultats per sincronitzar perfectament:

- Parpelleig massa uniforme o molt poc freqüent
- Moviments de la boca que no encaixen del tot amb l'àudio
- Expressions facials rígides o que canvien de manera estranya
- Mala sincronització entre veu i llavis (liptiming)
- Senyal d'alerta: somriures "gelats", microexpressions repetitives o poc variades.

2. Anomalies al contorn de la cara i la il·luminació

Un deepfake en temps real sovint falla en:

- Franges o vibracions lleus al contorn de la cara
- Canvis de llum no coherents amb l'entorn
- Zones borroses o deformacions quan el cap es mou ràpid
- Qualitat de pell massa "perfecta" o amb textura inconsistent
- Truc: demana a la persona que giri el cap de costat: és un dels punts més difícils de falsificar.

3. Moviments corporals limitats

En deepfakes en temps real, la cara és el que millor funciona, però:

- El coll i les espatlles sovint no segueixen el moviment natural
- El cos no "acompanya" l'emoció de la cara
- Sovint es veuen només de cintura cap amunt i gairebé immòbils

4. Problemes amb el fons

- Els deepfakes sovint utilitzen fons fixes o borrosos:
- El fons no reacciona de manera natural al moviment
- Ombres incoherents

- Sorolls digitals a les vores del cap o orelles

5. Peticions sospitoses o comportament anòmal

Independentment del vídeo, fixa't en:

- Pressions per actuar ràpid ("Necessito que em facis una transferència ara mateix")
- Dades o ordres que la persona *real* no acostuma a donar
- Manca de paciència o respostes mecàniques a coses personals

Mesures preventives que podeu implementar en videoconferències

1. Paraula clau de verificació (el més important)

Igual que comentàvem abans: Una paraula o frase de verificació acordada prèviament és la millor defensa.

2. Preguntes personalitzades difícils de predir

Si sospites d'una suplantació, pregunta:

- "Quin va ser l'últim projecte que vam fer junts?"
- "Quina és la frase que sempre dius quan…?"
- "Amb quin nom tens guardat el meu contacte?"

Les IA poden inventar respostes, però sol ser evident la inconsistència.

3. Activar serveis de detecció d'activitat sospitosa

Algunes plataformes com Google Workspace tenen:

- Alertes d'inicis de sessió inusuals
- Protecció avançada de comptes
- Verificacions de seguretat automàtiques

Encara no detecten deepfakes directament, però redueixen vectors d'atac.

4. Demanar una acció física a temps real

Els deepfakes en temps real fallen amb moviments improvisats:

- "Pots aixecar la mà esquerra?"
- "Pots ensenyar el teu entorn girant la càmera?"
- "Toca't l'orella dreta."

Aquest tipus d'acció és difícil de falsificar sense retard o errors.

5. Comprovar l'àudio

La veu també pot ser falsificada, però:

- Les IA tenen dificultats amb sons espontanis
- Tos, riure, balbucejar, interrupcions…

- Variacions emocionals reals

Un deepfake pot sonar massa "net" i homogeni.

És possible detectar un deepfake automàticament avui?

Encara no existeix cap eina fiable integrada a Meet o Zoom que ho detecti automàticament en temps real.

WEBS D'INTERÉS

Agència de Ciberseguretat de Catalunya. (s. f.). *Actualitat de l'Agència Catalana de Ciberseguretat*. Recuperat de https://ciberseguretat.gencat.cat/ca/actualitat/

Instituto Nacional de Ciberseguridad (INCIBE). (s. f.). *Guía de ciberseguridad "La ciberseguridad al alcance de todos"*.2022 Recuperat de https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberseguridad-la-ciberseguridad-al-alcance-de-todos

Agència de Ciberseguretat de Catalunya (ACC). (2021). *Ciberseguretat: Increment dels incidents per Ransomware dirigit a ajuntaments*. Consorci Administració Oberta de Catalunya (AOC). Recuperat de https://www.aoc.cat/blog/2021/ciberseguretat-ransomware/

Agència de Ciberseguretat de Catalunya (ACC). *Recursos Educatius: Ciutadania*. Recuperat de https://ciberseguretat.gencat.cat/ca/ciutadania/recursos-educatius

Universitat Politècnica de Catalunya (UPC). *Documentació de ciberseguretat*. Servei IRT. Recuperat de https://serveistic.upc.edu/ca/irt/documentacio/ciberseguretat

Associació Catalana per a la Ciberseguretat (ASCICAT). *Portal principal*. Recuperat de https://www.ascicat.cat/

Centro Criptológico Nacional (CCN-CERT). Portal principal. Recuperat de https://www.ccn-cert.cni.es/es/

Centro Criptológico Nacional (CCN-CERT). Novedades CCN-CERT. Recuperat de https://www.ccn-cert.cni.es/es/seguridad-al-dia/novedades-ccn-cert.html

Instituto Nacional de Ciberseguridad (INCIBE). Guías para empresas. Recuperat de https://www.incibe.es/empresas/guias

Instituto Nacional de Ciberseguridad (INCIBE). Guías para ciudadanía. Recuperat de https://www.incibe.es/ciudadania/formacion/guias

Agencia Española de Protección de Datos (AEPD). (2022). Guía de Privacidad y Seguridad en Internet. Portal de Transparencia. Recuperat de https://transparencia.gob.es/transparencia/transparencia_Home/index/MasInformacion/Informes-de-interes/Seguridad/GuiaPrivacidadSeguridadInternet.html

European Union Agency for Cybersecurity (ENISA). (2025). ENISA Sectorial Threat Landscape - Public Administration. Recuperat de https://www.enisa.europa.eu/publications/enisa-sectorial-threat-landscape-public-administration

European Union Agency for Cybersecurity (ENISA). ENISA's security guide and online tool for SMEs when going Cloud. Recuperat de https://www.enisa.europa.eu/news/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud

Cybersecurity and Infrastructure Security Agency (CISA). Product Security Bad Practices. Recuperat de https://www.cisa.gov/resources-tools/resources/product-security-bad-practices

Cybersecurity and Infrastructure Security Agency (CISA). ICS Advisories. Recuperat de https://www.cisa.gov/news-events/ics-advisories/icsa-25-322-03