DIRECTRIUS DE CIBERSEGURETAT EN ELS SISTEMES CORPORATIUS DE LA DIPUTACIÓ DE BARCELONA

ÍNDEX

Ciberseguretat 3
Credencials d'accés 4
Protegim les nostres contrasenyes 4
Com fer una contrasenya segura i recordar-la 4
Segon factor d'autentificació 5
Canvi de contrasenya a la Diputació de Barcelona 5
Correu brossa 6
Phishing 6
Detectem i combatem el *phishing* 7
Correu brossa i phishing a la Diputació de Barcelona 7
Programari maliciós (*malware*) 8
Punts d'entrada típics del *malware* 8
Segrest d'informació *(ransomware)* 8
Com combatem el programari maliciós? 8
Dispositius mòbils 10
Aplicacions (apps) 10
Dispositius mòbils a la Diputació de Barcelona 10
Xarxes socials 12
Sextorsió o xantatge amb gravacions sexuals 12
Missatgeria instantània 14
Notícies falses i enganys (*hoax*) 14
Missatgeria instantània a la Diputació de Barcelona 14
Navegació segura 16
Com podem saber si un web és segur? 16
Altres recomanacions 16
Galetes (*cookies*) 16
Certificats digitals a la Diputació de Barcelona 17
El lloc de treball 18
Estacions de treball a la Diputació de Barcelona 18
Estacions de treball en remot a la Diputació de Barcelona 18

Ciberseguretat

A mesura que creix l'ús de la tecnologia a la feina i en l'àmbit personal, estem sotmesos a més riscos dels entorns digitals i a ciberamenaces com ara el robatori de dades personals, la usurpació de personalitat i altres fraus.

En aquest document hi trobareu informació i consells per fer un **ús més segur dels recursos tecnològics** tant al vostre lloc de treball com en l'àmbit personal, ja que aquests dos entorns sovint poden estar connectats i tenir repercussió l'un sobre l'altre.

La Direcció de Serveis de Tecnologies i Sistemes Corporatius posa tots els **mitjans tècnics disponibles** (antivirus, tallafocs, antispam...) per protegir els usos poc segurs de les tecnologies de la informació i la comunicació (TIC). Però sabem que vosaltres, **els empleats, sou la peça clau per garantir la seguretat** a la Diputació. Perquè sou vosaltres qui gestioneu la **informació**, la modifiqueu, transmeteu, elimineu i processeu.

La **conscienciació i col·laboració de tots** és clau per avançar en la seguretat en l'ús de les eines informàtiques. Aquí us proporcionem els recursos necessaris i les recomanacions per vetllar per un **ús òptim i segur de tots els recursos TIC**.

Credencials d'accés

- En el món digital **les persones ens hem d'identificar** per **accedir amb seguretat als recursos** que s'hi ofereixen.
- La identificació més utilitzada és la combinació de **nom d'usuari** i **contrasenya**, aquesta combinació rep el nom de **credencials d'accés**.
- L'augment de recursos digitals (ordinador, correu electrònic, webs bancàries, webs de compra, blogs, aplicacions de mòbil...) fa que les persones cada cop tinguem més **credencials d'accés** diferents.
- És important tenir en compte que aquestes credencials són la **única barrera** per accedir a les nostres dades,

Protegim les nostres contrasenyes

- No utilitzis mai les mateixes credencials per a recursos diferents i no utilitzis la mateixa contrasenya en llocs diferents.
- Com més valuós sigui el recurs al qual accedeixis més cura cal tenir amb les credencials.
- La contrasenya ha de ser personal i intransferible, mai s'ha de compartir o cedir a terceres persones.
- No anotis enlloc la teva contrasenya, ni l'enviïs mai per correu electrònic.
- És molt recomanable canviar periòdicament les contrasenyes.
- És important utilitzar contrasenyes segures. Les contrasenyes s'emmagatzemen i viatgen per les xarxes de forma encriptada. Ara bé, si la contrasenya va a parar a mans inadequades, la desxifrat d'una contrasenya poc segura pot ser cosa de segons.
- Hi ha dues normes a seguir per fer una contrasenya segura:

  Fer-la llarga. Com a mínim hauria de tenir 8 caràcters.

  Combinar diferents tipus de caràcters: lletres (majúscules i minúscules), números i altres caràcters no alfanumèrics.

Com fer una contrasenya segura i recordar-la

- Cal descartar, per més llarg que sigui, paraules existents o combinacions únicament de números.
- La millor manera d'aconseguir recordar una contrasenya llarga que combini lletres (minúscules i majúscules), números i caràcters no alfanumèrics és si la podem associar a una frase. Per exemple, si utilitzem la frase **"Els empleats som clau per garantir la seguretat"** podem agafar les inicials i utilitzar **Eescpgls**. A partir d'aquí podem aplicar algun canvi per afegir seguretat:

  Substituir alguna lletra per números. La l per un 1, la e per un 3 o la p per un 9. Quedaria: **33sc9g1s**

  Posar els verbs en majúscules. Quedaria: **EeScpGls**

  Afegir caràcters no alfanumèrics. Quedaria: **E"e"scpgls!**
- Pots utilitzar frases que ja incloguin números, majúscules i caràcters no alfanumèrics.

  DBaMhh40q? "De Barcelona a Mataró hi ha 40 quilòmetres?"

  Vne1.970aM "Vaig néixer el 1.970 a Manresa"

  Van32dc/PC "Visc al número 32 del c/ Pau Claris"

  EPvne6ilMe18 "El Pau va néixer el 6 i la Marta el 18"

- Un cop tinguis una contrasenya forta la pots utilitzar per diferents recursos afegint una diferència.

  e2Sc!pglS:Fcb --> Per a Facebook

  e2Sc!pglS:YTb --> Per a YouTube
- No es recomana fer servir els navegadors per emmagatzemar les claus d'accés a les diferents adreces internet.
- Existeixen eines conegudes com a gestors de contrasenyes que faciliten emmagatzemar i recordar la totalitat de les nostres contrasenyes . Es basen en crear i recordar una única contrasenya robusta, la del gestor de claus, aquest pot emmagatzemar o crear de noves claus robustes per tots els llocs web que emmagatzemem. Un exemple d'eina d'aquestes característiques és *Keepass*.

Segon factor d'autentificació

- Quan en l'autentificació involucrem una confirmació a través d'un canal diferent (el més habitual és una confirmació amb un sms al nostre número de mòbil) augmentem molt la seguretat. Això es coneix com segon factor d'autenticació (2FA) i progressivament la **Direcció de Serveis de Tecnologies i Sistemes Corporatius** (DSTSC) anirà adoptant aquets tipus de solució per la majoria dels serveis.

Canvi de contrasenya a la Diputació de Barcelona

- La majoria de recursos de la Diputació de Barcelona (correu, xarxa, menú d'aplicacions, wifi,...) utilitzen les mateixes credencials.
- Cal ser especialment curós en la protecció d'aquestes credencials, utilitzant una contrasenya segura i canviant-la periòdicament.
- Davant de la sospita de que el teu usuari o contrasenya han estat capturats per un tercer tenim l'obligació legal d'informar immediatament al telèfon 22007 o al correu sgot.22007@diba.cat.

Correu brossa

- El correu brossa (*spam*, en anglès) són aquells missatges enviats **sense el consentiment del receptor** a adreces de correu obtingudes de forma fraudulenta. És a dir, missatges no desitjats.
- Per quins motius rebem missatges d'aquest tipus?
  - **Per fer-nos publicitat** - Fer un ús indegut de llistes de correus electrònics és una forma fàcil de fer arribar publicitat d'un producte a molta gent.
  - **Per obtenir dades personals** - Aquesta pràctica coneguda com a *phishing* (pesca en anglès) pretén obtenir dades del destinatari.
  - **Per transmetre algun tipus de programari maliciós** - El programari maliciós s'instal·larà al nostre ordinador si obrim un fitxer adjunt o accedim a una plana web a través d'un link que ens proposen.
- Hi ha dos tipus de remitents:
  - Algú ha creat una adreça de correu des d'on enviar correu brossa. Aquests correus són fàcils de detectar de forma automàtica pels sistemes anti-spam i normalment no arriben al destinatari.
  - Algú utilitza la bústia de correu d'una altra persona sense el seu consentiment per enviar correu brossa. Per fer-ho, o bé ha robat les seves credencials o bé ha instal·lat algun programari maliciós en el seu ordinador. **Són els més perillosos** perquè acostumen a saltar les barreres de detecció automàtica. Cal sospitar del contingut.
- No es pot considerar correu brossa el correu publicitari que rebem si hem cedit voluntàriament les nostres dades a una empresa o entitat. En aquests casos la llei obliga a facilitar la baixa d'aquests enviaments i normalment el mateix correu porta un accés per fer-ho.
- Davant del més mínim dubte, **no accedeixis a cap enllaç**, **no descarreguis cap fitxer adjunt** i **no contestis el correu**.

Phishing

- El ***phishing*** o **suplantació d'identitat** és una estafa que consisteix a suplantar la identitat d'una persona, empresa o institució de confiança per aconseguir **dades personals** com ara dades bancàries, adreça o les **credencials d'usuari** o per **transmetre algun tipus de programari maliciós**.
- **La propagació del *phishing*** normalment es realitza a través del **correu electrònic**, tot i que també es pot propagar per altres canals com les **xarxes socials (facebook, twitter, whatsapp,...)** o el **SMS**.
- Funciona de la següent manera: rebem un correu electrònic, SMS o missatge de xarxes socials amb aparença real i un enllaç a una web externa falsa controlada pels ciberdelinqüents. La web falsa suplanta la web o servei original esperant que "piquem" i **introduïm les nostres dades**, passant d'aquesta manera a ser "pescats". També poden enllaçar directament a la descàrrega d'un programari maliciós.
- Amb les dades obtingudes, els **ciberdelinqüents** poden suplantar la nostra identitat, realitzar estafes econòmiques directament o vendre aquestes dades a tercers.
- El *phishing* pot ser indiscriminat o dirigit.
  - **El *phishing* indiscriminat fa servir l'*spam*** per arribar al màxim possible de víctimes. Suplanten a bancs o serveis de missatgeria coneguts i el que busquen és obtenir dades o infectar al màxim nombre d'usuaris. La seva força és el volum.

- **El *phishing* dirigit o *spear phishing* està orientat a una organització o persona concreta**. Els atacants utilitzen uns correus molt més preparats per generar confiança al destinatari. Les webs falses o el programari maliciós que distribueixen també estan personalitzats per generar confiança. La seva força està en la dificultat per identificar-ho.

Detectem i combatem el *phishing*

- Els missatges relacionats amb el *phishing* fan servir el que s'anomena l'**enginyeria social**, és a dir, **fent servir la persuasió i l'engany busquen guanyar la nostra confiança**.
- Fan servir excuses com **canvis urgents** en les condicions de serveis, premis, promocions o multes per forçar-nos a prendre **una decisió ràpidament**.
- Si el *phishing* és indiscriminat acostumen a ser generats de manera automàtica i sovint contenen **errors gramaticals, errors ortogràfics o paraules traduïdes en altres idiomes** que ens han de fer sospitar.
- Com més valor tingui el recurs al qual suposadament enllaça el *phishing*, més cura cal tenir. Compte sobretot amb els correus de bancs on demanen canvis de contrasenyes, confirmar un compte o confirmar un pagament bancari, **sempre són falsos**.
- Rebutja de forma sistemàtica qualsevol correu electrònic o comunicat per al que sigui necessari facilitar **dades confidencials**. Contrasta la informació per altres vies.

Correu brossa i phishing a la Diputació de Barcelona

- Gràcies a les eines d'anàlisi, **més d'un 90% del correu que arriba als correus @diba.cat és identificat com a brossa i ja no es lliura a les bústies**. Però resulta impossible aturar-ho tot.
- A la Diputació de Barcelona **també patim atacs dirigits de *phishing*** per robar les nostres credencials d'usuari i accedir als nostres recursos.
- Recorda que des de la **Direcció de Serveis de Tecnologies i Sistemes Corporatius** (DSTSC) no t'enviarem en cap cas un missatge per demanar les teves credencials.
- Quan a la DSTSC sóm conscients que algun missatge perillós ha estat distribuït a les bústies, es prenen mesures concretes per evitar els efectes.
- Davant de qualsevol sospita d'un missatge recorda que pots enviar el correu a l'adreça correusospitos@diba.cat on es revisarà el contingut i es prendran les mesures tècniques adients per evitar la propagació. Aturar el phishing és cosa de tots (servei 24 hores).

Programari maliciós (*malware*)

- El **programari maliciós o *malware*** (de l'anglès, *malicious software)* és el programari que realitza funcions no desitjades o perjudicials en un sistema sense consentiment de l'usuari.
- L'objectiu del programari maliciós és: **robar informació** dels usuaris, inserir eines de **gestió remota** per controlar els ordinadors o **xifrar la informació** que contenen els dispositius.
- Des del punt de vista tècnic hi ha molts tipus de programari maliciós depenent de com es distribueix, de com actua o de quina finalitat té: **virus, cucs, troians, programari espia**...

Punts d'entrada típics del *malware*

- ***C*orreu electrònic**: És una manera molt directa i ràpida d'arribar a una persona i fer que **obri un fitxer** o **accedeixi a una web**. Aquestes accions poden provocar que el programari maliciós es traspassi a l'equip utilitzat. El correu pot ser correu brossa i utilitzar tècniques d'engany (*phishing*) o provenir d'un destinatari infectat sense saber-ho.
- **Navegació web**: Els cibercriminals **infecten servidors web lícits** que no estan protegits per afegir el codi maliciós a les pàgines que publiquen. Si es navega per aquesta web i l'equip no està protegit, n'hi ha prou amb la navegació per a què el programari maliciós es traspassi al nostre equip.
- **Aplicacions descarregades d'internet**: Els cibercriminals ofereixen **aplicacions falses,** per a ordinador o per a mòbils, que infectaran els dispositius de les persones que les descarreguin. Generalment l'engany és oferir de forma gratuïta programari de pagament o aplicacions amb funcionalitats molt atractives.
- **Dispositius d'emmagatzematge extern (memòries USB, discs durs, targetes de memòria, espais al núvol personal, ...)**. L'execució, la descàrrega o la simple connexió a espais externs d'emmagatzematge pot suposar l'entrada de programari maliciós a l'equip, per tant no es recomana el seu ús.

Segrest d'informació *(ransomware)*

- Aquest tipus de programari maliciós **xifra el màxim d'informació possible** de l'equip utilitzat i dels que hi estiguin connectats, abans que la víctima en sigui conscient. Una vegada realitzada l'encriptació de les dades, es mostra una **nota de rescat** (*ransom*, en anglès) exigint pagament econòmic per recuperar la informació.
- Si l'usuari no disposa de còpies de seguretat perdrà totes les dades encriptades. Cal dirigir-se a les autoritats.
- Malgrat els esforços dels governs per perseguir-lo, actualment és un dels programaris maliciosos més difosos a internet.
- La seva entrada acostuma a ser a partir d'un correu enganyós (*phishing*) amb un enllaç a una web externa o directament amb un fitxer adjunt.

Com combatem el programari maliciós?

- La **Direcció de Serveis de Tecnologies i Sistemes Corporatius** (DSTSC) disposa de totes les mesures adients per reduir l'entrada i propagació de programari maliciós, però

tancar algunes vies d'entrada està únicament a les mans de les accions que pugui fer una persona amb el seu equip.

- El teu equip de Diputació ja utilitza un programari antivirus oficial i manté actualitzat tot el programari de l'equip. Fes el mateix amb el teu equip personal.
- No obris enllaços o fitxers adjunts de missatges de correu de persones desconegudes o que semblin sospitoses (publicitat desconeguda, notícies urgents, escrit en diversos idiomes, amb faltes d'ortografia,...)
- No descarreguis fitxers o aplicacions sospitoses. Elimina complements sospitosos del navegador.
- Sigues molt prudent amb l'ús de dispositius d'emmagatzematge extern. Assegura't que provenen d'algú que també utilitza mesures de protecció.
- Per últim, davant de la més mínima sospita, truca al **telèfon d'atenció a l'usuari (22007).**

Dispositius mòbils

- Els nostres dispositius mòbils (*smartphones*, *tablets* o portàtils) emmagatzemen molta informació personal privada i són la porta d'accés a molts serveis personals i, per tant, cal cuidar-los i protegir-los.
- Cal protegir amb més cura l'accés als dispositius mòbils perquè estan molt exposats a pèrdues o robatoris.
- Cal vigilar l'accés als dispositius mitjançant un *pin*, una contrasenya, un patró de desbloqueig o amb l'ús de dades biomètriques. Cal establir algun d'aquests mecanismes de desbloqueig del dispositiu mòbil superat un temps d'inactivitat.
- Procura no emmagatzemar informació sensible en el dispositiu mòbil. Si ho fas, xifra la informació.
- Realitza còpia de seguretat de tota aquella informació allotjada en el teu dispositiu i mantén actualitzat tant el sistema operatiu com les aplicacions instal·lades.
- No consultis informació sensible ni utilitzis les teves credencials en xarxes wifi que no et generin prou confiança.
- Existeix programari maliciós específic pels dispositius mòbils. L'ús que es fa d'aquests dispositius facilita la propagació i la infecció.

Aplicacions (apps)

- Les aplicacions o apps mòbils que instal·lem als nostres dispositius aporten funcionalitats per facilitar gestions o activitats, ja siguin de caire personal o professional.
- Aquestes aplicacions són una porta d'entrada per al programari maliciós.
- Els cibercriminals ofereixen **aplicacions falses** que infectaran els dispositius de les persones que les descarreguin. Generalment l'engany és oferir de forma gratuïta programari de pagament o aplicacions amb funcionalitats molt atractives.
    - Vigila amb les aplicacions de moda que surten abans de la data anunciada pel desenvolupador.
    - Compte amb les versions gratuïtes d'aplicacions de pagament.
    - Desconfia de les ofertes massa bones.
- La prevenció és clau, sigues molt prudent al descarregar aplicacions per als teu dispositiu mòbil:
    - Cal optar sempre per la descàrrega a les **botigues d'aplicacions oficials**.
    - Si dubtes, comprova la seva popularitat pel número d'instal·lacions, qualificacions o comentaris de la resta d'usuaris.
    - Cal revisar i estar atents a quins **permisos i drets sol·licita una aplicació**. Si ens demana permisos que no semblen necessaris per a la seva funció, no s'hauria d'instal·lar.

Dispositius mòbils a la Diputació de Barcelona

- No modifiquis la configuració dels dispositius corporatius ni hi instal·lis aplicacions no autoritzades. Respecta les indicacions del "Manual d'ús dels sistemes d'informació i comunicació DIBA"
- L'ús de la connexió de dades en itinerància (sortides a l'estranger) està limitat a la Diputació per raons de racionalització de la despesa.

- La la **Direcció de Serveis de Tecnologies i Sistemes Corporatius** (DSTSC) és troba en procés de desplegament d'una eina de gestió de la seguretat en els dispositius mòbils i en mobilitat coneguda com MDM.
- Si detectes qualsevol activitat sospitosa o un funcionament anormal del teu equip, notifica-ho a l'equip d'atenció a l'usuari, al telèfon 22007 o al correu sgot.22007@diba.cat.

Xarxes socials

- Les xarxes socials formen part del nostre dia a dia, ens permeten comunicar-nos amb altres persones i compartir informació. La gran quantitat de dades i usuaris que s'hi mouen ens obliga a anar molt amb compte per fer-les servir de forma segura.
- Cal tenir **cura amb la informació que es publica**. Sovint es comparteix informació personal (fotografies, opinions o gustos) de la qual, una vegada publicada i encara que l'esborrem, en perdrem el control. Per tant, pensa-ho bé abans de publicar res.

Informació que cal evitar publicar:

  - Lloc i data de naixement
  - On vius
  - Dades bancàries
  - Número de mòbil
  - Plans per a les vacances

- Cal ser **respectuosos** amb els comentaris que es fan i **no publicar missatges ofensius**.
- No facilitis o publiquis dades, informació, fotografies o vídeos **d'altres persones sense que t'hagin donat el seu consentiment**.
- Configura correctament les opcions de **privacitat del teu perfil** i dona només accés a les persones que tu vulguis, d'aquesta manera reduiràs el risc de que la teva informació sigui accessible a gent malintencionada.
- **Desconfia de les sol·licituds d'amistat o contactes de persones que no coneixes.** Si les acceptes pots estar donant accés a la teva informació i a la dels teus contactes.
- **Jocs en línia com la Balena blava** (joc que incita a realitzar una sèrie de tasques i que es relaciona amb el suïcidi d'adolescents a diferents països del món) **s'aprofiten de les xarxes socials i de l'accés a la informació dels contactes per fer xantatge** quan es vol abandonar el joc.
- Tal com succeeix amb els ordinadors i els dispositius mòbils, existeixen aplicacions malicioses (*malware*) dins de les xarxes socials. Cal revisar i estar atent a quins **permisos i drets sol·licita una aplicació**.
- **Desconfia dels enllaços**, perquè les xarxes socials s'han convertit en un mitjà molt important per a la distribució de **virus o d'estafes**.
- **Vigila la teva identitat digital**. Amb tanta informació publicada, els cibercriminals poden intentar robar la teva identitat (s'apropien de les teves credencials d'accés i es fan passar per tu publicant informació o enviant missatges) o suplantar-la (creen un perfil nou amb les teves dades).
- **El robatori de dades, la suplantació d'identitat i l'assetjament són els delictes més freqüents a les xarxes socials**. Si sospites que estàs patint un d'aquests delictes, **cal denunciar-ho a la mateixa xarxa social i als cossos de seguretat**.

Sextorsió o xantatge amb gravacions sexuals

- La **sextorsió** és una de les extorsions que ha crescut més darrerament a internet. Aprofita imatges o vídeos de caire sexual, **obtingudes amb consentiment o robades**, per demanar diners a canvi si no es vol que les imatges es reenviïn als contactes o es publiquin a les xarxes socials. Si l'assetjament el fa un adult a un menor és ***grooming***.
- En molts casos l'estafa comença amb una **sol·licitud d'amistat a les xarxes socials** de persones atractives que després busquen mantenir converses privades a través de xats

i finalment, un cop guanyada la confiança, intercanviar imatges de caire sexual (***sexting***).

- **Darrere d'aquests perfils falsos s'oculten màfies criminals** que poden estar operant des de servidors ubicats a qualsevol lloc del món.

Missatgeria instantània

- Aquestes aplicacions permeten l'enviament instantani de missatges de text o multimèdia a un o més usuaris. Amb l'arribada dels mòbils **el seu ús s'ha estès i popularitzat** i tothom les utilitza a diari: *Whatsapp, Telegram, LINE, Hangouts, Google Allo, Skype, Messenger (Facebook), SnapChat,...* La seva immediatesa i l'alt volum d'usuaris i missatges les converteix en un espai ideal per a enganys.
- **És habitual que aquest tipus d'aplicacions no demanin credencials d'accés quan les fem servir**. Cal tenir validació d'accés al dispositiu mòbil per evitar que algú pugui consultar els nostres missatges i sobretot fer-ne en nom nostre.
- Esborra regularment **l'històric de converses** per evitar el seu accés en cas de pèrdua.
- Existeix programari maliciós especialitzat en missatgeria instantània. Cal anar amb compte amb els enllaços externs o fitxers adjunts. Desconfia dels arxius multimèdia.
- **No facis difusió dels números de telèfon dels teus contactes sense consentiment previ**. Quan es creen els grups de difusió, depenent de l'aplicació, publiquem tots els números de telèfon dels participants.
- **Sospita de missatges de desconeguts o ocults**. El millor és no respondre fins poder verificar la identitat. Mai donis dades personals sense estar segurs de la identitat de la persona que ho rebrà.
- Cal ser especialment curós en el reenviament dels missatges, **podríem estar cometent delicte per fer difusió de contingut il·legal**. Si reps contingut d'aquest tipus, notifica als cossos de seguretat i esborra'l, fer-ne difusió és delicte!
- **Actualitza sempre les aplicacions a la última versió**, a banda de noves funcionalitats, aquestes actualitzacions corregeixen els forats de seguretat.

Notícies falses i enganys (*hoax*)

- Les aplicacions de missatgeria instantània moltes vegades es fan servir **per transmetre i fer difusió de notícies falses o enganys**, també conegut com a *hoax.*
- **L'objectiu d'aquests missatges és molt divers: crear alarma social**, desprestigiar alguna marca o persona, donar consells enganyosos, actuar sobre l'opinió pública, transmetre codi maliciós,...
- No et creguis tots els missatges que reps encara que vinguin d'un conegut. **Contrasta la informació per altres vies**.
- Aquests tipus de missatges solen demanar que els facis arribar a més persones. Trenca la cadena, no formis part d'aquesta difusió. No reenvïis aquest tipus de missatge als teus contactes.

Missatgeria instantània a la Diputació de Barcelona

- L'ús de la missatgeria instantània ha d'estar directament relacionat amb el desenvolupament de les tasques pròpies del lloc de treball. Respecta les indicacions del "Manual d'ús dels sistemes d'informació i comunicació DIBA".
- Sigues molt curós amb l'ús que fas de la missatgeria instantània, ja que no es pot controlar per on viatja o en quins servidors s'emmagatzema la informació. Si l'aplicació ho permet, fes servir xats encriptats d'extrem a extrem.
- La **Direcció de Serveis de Tecnologies i Sistemes Corporatius** (DSTSC) actualment recomana el correu electrònic corporatiu per l'enviament de dades corporatives i que aquestes preferentment han de ser adjuntades xifrades.

Recordeu que en missatgeria instantània la creació de grups de treball puntuals també està subjecte a l'obtenció fefaent del consentiment dels participants per part de l'administrador del grup.

Navegació segura

Navegar per internet forma part del nostre dia a dia. Ho fem des de diferents dispositius en diversos moments del dia. Ho fem com a lleure, per cercar informació o per treballar.
Quan es fa una transacció econòmica o s'introdueixen credencials per accedir a un espai amb dades personals és un dels moments on cal tenir més cura. Et proposem que prenguis algunes precaucions.

Com podem saber si un web és segur?

El sistema més utilitzat pels ciberdelinqüents és fer servir **noms de webs** molt semblants als originals on anem redirigits des d'algun correu maliciós o per error a l'escriure el nom. Aquests webs falsos pretenen obtenir les nostres dades personals o **distribuir programari maliciós**.

- Si la URL del web comença per **HTTPS://** indica que les dades viatgen xifrades i no resulta fàcil interceptar-les i obtenir-les. Els webs bancaris, de serveis de compres o de pagaments han de començar sempre per HTTPS://, mai per HTTP://
- Si apareix un cadenat al costat de la URL indica que el web fa servir certificat que garanteix la seva identitat. Podem clicar sobre el cadenat per obtenir la informació del certificat web, verificant d'aquesta manera que és autèntic i que el web és legítim, és a dir, és qui diu ser. Aquests certificats els emeten les Autoritats de Certificació que funcionen com a intermediaris i ens verifiquen la autenticitat del certificat.
- Els navegadors afegeixen **colors a la barra** per indicar si s'ha pogut verificar el certificat, en color verd si ha pogut i en color vermell si no ha pogut. Pot succeir que el certificat utilitzat sigui perfectament vàlid i segur però surti de color vermell perquè no el reconeix per defecte. En aquest cas el navegador ens demanarà si volem o no confiar i caldrà verificar la autenticitat del certificat.

Altres recomanacions

- Evita fer servir l'opció de recordar contrasenyes al navegador i esborra i configura per tal de no guardar dades com l'historial de navegació o les dades introduïdes als camps dels formularis.
- Tanca les sessions correctament en comptes de tancar directament la finestra.
- En ordinadors públics fes servir l'opció de **navegació privada (incògnit)** que incorporen tots els navegadors.
- Cal mantenir els navegadors actualitzats i ser conscients de quins complements, extensions o *plugins* tenim instal·lats.

Galetes (*cookies*)

- Les galetes (*cookies* en anglès) són petits magatzems de dades que els webs creen i gestionen en l'ordinador on es navega.
- Si el web únicament utilitza galetes per facilitar-nos la navegació no ens demanarà cap autorització.
- Alguns webs utilitzen les galetes per emmagatzemar dades sobre els nostres gustos, preferències o forma de navegar que després s'utilitzaran per oferir-nos publicitat dirigida o personalitzar navegacions. Si la informació de la galeta va a parar a un altre proveïdor (**galetes de tercers**) el web sol·licita el nostre consentiment.
- Resulta molt complicat evitar l'ús de galetes de tercers perquè si no responem i continuem navegant ho interpreten com un consentiment. A través de les

configuracions de privadesa dels nostres navegadors podem activar el bloqueig de les galetes de tercers.

Certificats digitals a la Diputació de Barcelona

- Els webs de la diputació de Barcelona fan servir certificats emesos per les entitats CatCert (Consordi AOC) i geo Trust.
- L'entitat CatCert no està incorporada per defecte en els navegadors més utilitzats del mercat. Els ordinadors corporatius porten el certificat CatCert instal·lat per defecte.
- Si accedeixes a una web de la Diputació de Barcelona des d'un dispositiu personal sense el certificat CatCert, el navegador pot posar la URL de color vermell. Si vols instal·lar el certificat de l'entitat pots fer-ho seguint les instruccions del seu web: https://www.aoc.cat

El lloc de treball

Les mesures de ciberseguretat han de començar abans d'utilitzar l'ordinador o el mòbil. No només perquè algunes actuacions en el nostre lloc de treball poden obrir les portes a tota la nostra informació digital sinó també perquè cal tenir la mateixa cura en la seguretat dels documents i dades que encara mantenim en paper.

Cal seguir els següents consells en nostre lloc de treball:

- Eviteu les còpies impreses, però si us calen recordeu:
  - Quan imprimeixis un document cal mantenir el seu nivell de seguretat. Si en format digital no era públic tampoc ho pot ser en format paper.
  - Imprimir documents amb dades personals afectades per la LOPD (Llei de protecció de dades) pot constituir un delicte.
  - Revisa quins papers queden accessibles a la taula quan deixis el lloc de treball encara que sigui temporalment.
  - Cal destruir de forma segura els documents no públics.

- Ordinador personal, telèfon intel·ligent o tauletes
  - Cal bloquejar l'accés als dispositius si els deixem fora de la vista i apagar-los si no els hem d'utilitzar durant un temps.
  - No donis les teves credencials a ningú per cap mitjà ni amb cap pretext.
  - No mantinguis cap còpia escrita de les teves credencials.
- Dispositius portàtils d'emmagatzematge
  - No connectis un dispositiu sense la certesa de saber a qui pertany.
  - Si hi mantens dades, guarda'ls en llocs segurs.
- Telèfon
  - Cal verificar la identitat del teu interlocutor si en la conversa surten dades personals o informacions privades.
  - No donis les teves credencials per telèfon.

Aquestes pautes valen tant per llocs de treball corporatius o en mobilitat.

Estacions de treball a la Diputació de Barcelona

- Utilitza les unitats de xarxa per compartir i emmagatzemar informació i evita suports locals o portàtils.
- Respecta les indicacions del Manual d'ús dels sistemes d'informació i comunicació DiBA
- Si detectes qualsevol activitat sospitosa o un funcionament anòmal del teu equip, notifica-ho a l'equip d'atenció a l'usuari, al telèfon 22007 o a la bústia electrònica sgot.22007@diba.cat

Estacions de treball en remot a la Diputació de Barcelona

El personal de la Diputació de Barcelona autoritzat a prestar serveis en modalitat en remot haurà de seguir les normes de ciberseguretat que es descriuen en aquest document, i seguir els requeriments tècnics i les condicions d'utilització dels mitjans tecnològics.

- En alguns casos la Direcció de Serveis de Tecnologies i Sistemes Corporatius proveeix d'equipament informàtic amb el programari informàtic homologat carregat i configurat de forma adient. Aquell personal que disposi d'equipament corporatiu, en farà ús de forma preferent d'aquests equips informàtics sense dur a terme canvis substancials en la configuració dels mateixos.

- En cas que s'utilitzin mitjans propis, es podrà requerir modificar la seva configuració per garantir la ciberseguretat del dispositiu. Caldrà sempre :
    - El mitjà emprat haurà de tenir instal·lat i permanentment actualitzat un programari d'antivirus i un sistema operatiu degudament actualitzat
    - S'haurà de configurar l'accés al mitjà amb un mecanisme d'autenticació robust basat en un identificador i contrasenya forta.
    - Actualment el servei wifi corporatiu empra un segon factor d'autenticació però si l'usuari no disposa d'una connexió corporativa a l'abast, podrà fer ús d'una xarxa wifi de confiança, amb protocol wpa2 o superior i que requereixi de contrasenya forta per a connectar-se.

Els serveis tecnològics a disposició del personal seran accessibles des de navegador web o en el seu defecte seran proveïts a través d'una connexió VPN per oferir confidencialitat sobre les dades, conservant les evidències digitals necessàries pel compliment legal.

- No es recomana l´ús de dispositius locals d'emmagatzematge. Per assegurar la disponibilitat de les dades que es treballin des d'aquestes estacions de treball, caldrà fer ús dels espais i eines corporatives per a les funcions d'emmagatzematge de documents. La Direcció de Serveis de Tecnologies i Sistemes Corporatius disposa de procediments de còpia de seguretat i mecanismes anti-malware per mitigar els efectes que es poguessin produir a nivell de disponibilitat i d'integritat de la Informació.
- No es permès deixar informació corporativa en espais al núvol personals.
- Cal tenir cura de no deixar còpies de la informació que amb la que es treballa en l'estació de treball en remot.