Manual de bons usos digitals

Guia de recomanacions i hàbits saludables davant la tecnologia

EDUCAT 1×1

Generalitat de Catalunya
Departament d'Ensenyament

Índex

Ja controles?

Accions d'un bon manteniment de l'ordinador

1.Còpies de seguretat
QUÈ SÓN?

Còpia d'un fitxer o un conjunt de fitxers, generalment actualitzada periòdicament, que permet restaurar les dades originals en cas de pèrdua.

CONSELLS I RECOMANACIONS:

Utilitza un llapis de memòria (o un servei en línia per a còpies de seguretat) per a desar-hi còpies dels teus arxius i de les carpetes més importants. D'aquesta manera, si el teu ordinador pateix alguna incidència, podràs recuperar els teus documents essencials.

2.Robatoris
PER QUÈ?

Els ordinadors portàtils són eines tecnològiques de valor i, per tant, susceptibles de ser robades si no tenim prou cura.

CONSELLS I RECOMANACIONS:

- **No mostris el teu portàtil en espais públics no segurs.**
- **Cal tenir cura i vigilar on deixem el nostre portàtil en tot moment.**
- **Personalitza el teu ordinador amb adhesius o folrant-lo amb cura amb uns plàstics especials.**

3.Usuaris i contrasenyes
QUÈ ÉS?

Usuari: Conjunt de caràcters alfanumèrics que identifica un usuari i que generalment, juntament amb la contrasenya, permet connectar-se a un sistema informàtic o a un servei en línia.

Contrasenya: Codi secret personal emprat per accedir com a usuari a un sistema, xarxa o pàgina web. Aquest usuari representa la nostra persona en l'entorn digital.

CONSELLS I RECOMANACIONS:

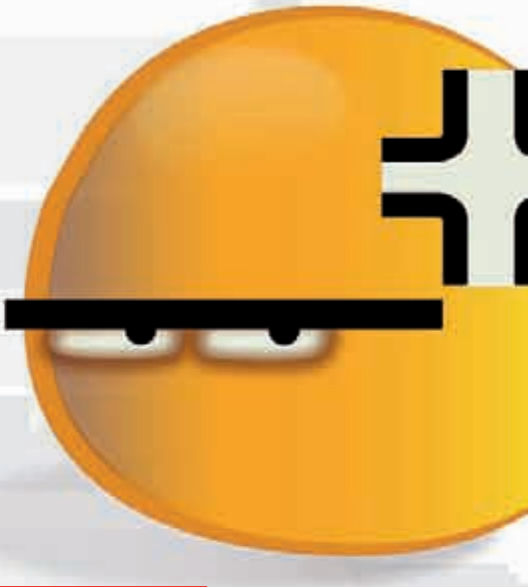
- **Utilitza un àlies (nick) en comptes del teu nom o cognom. No indiquis la teva edat en el nom d'usuari.**
- **Inventa contrasenyes difícils (combinació de nombres i lletres)**
- **És més segur utilitzar contrasenyes diferents per a cada servei. No les comparteixis amb ningú, desa-les en lloc segur i si és possible xifrades. I evita guardar-les en un document anomenat "contrasenyes" o amb qualsevol altre nom que es pugui detectar fàcilment.**
- **No demanis la contrasenya a cap amic, les contrasenyes són personals i secretes.**
- **Quan inicïis la sessió en un ordinador públic, desmarca la casella de "recorda usuari i contrasenya".**
- **Tanca sempre la sessió quan acabis.**
- **Si et vols donar d'alta en algun servei en línia, fes-ho amb els teus pares, tot vigilant quines dades personals dónes.**

4.Virus
QUÈ ÉS?

Programa que s'introdueix en un sistema informàtic, en perjudica el funcionament i pot reproduir-se i transmetre's independentment de la voluntat de l'usuari.

CONSELLS I RECOMANACIONS:

- **No desactivis l'antivirus ni el tallafocs en cap moment. Ho poden aprofitar per infectar el teu ordinador, copiar-te informació o prendre't la teva identitat.**
- **Comprova que l'antivirus i el sistema operatiu estiguin sempre actius i actualitzats.**
- **No obris arxius adjunts de remitents desconeguts.**
- **Tingues present que les descàrregues P2P i de fonts no confiables poden ser una via d'accés de virus, troians, cucs, etc.**



5.Bateria
QUÈ ÉS?

Aparell que acumula càrrega elèctrica i que permet així subministrar electricitat a un aparell sense necessitat que estigui endollat a la xarxa elèctrica.

CONSELLS I RECOMANACIONS:

- **S'aconsella a tots els usuaris que mantinguin els portàtils endollats al corrent el màxim temps possible i en especial durant el funcionament de l'aparell.**
- **Quan recarreguis la bateria, fes-ho fins al 100% de la seva capacitat.**

6.Funda
PER QUÈ?

Cal protegir l'ordinador portàtil amb la seva funda per tal de protegir-lo de possibles cops durant els seus desplaçaments.

CONSELLS I RECOMANACIONS:

- **Desa sempre el teu ordinador portàtil dins de la seva funda quan acabis d'utilitzar-lo i quan t'hagis de desplaçar.**
- **Cal tenir en compte, que tot i portar la funda corresponent, l'ordinador portàtil és vulnerable a cops i caigudes.**

Sigues legal!

Aspectes legals i de protecció de la propietat intel·lectual

7.Actituds i valors del món i la vida digitals
QUÈ ÉS?

Dret d'autor: Drets morals i d'explotació que té l'autor d'una obra literària, artística o científica. En cas que aquesta s'utilitzi, això implicarà un cost o una autorització expressa de l'autor. En el context digital fa referència a música, pel·lícules, imatges i textos publicats a Internet o en un suport digital.

Copyright: El copyright reflecteix la possessió del dret d'explotació i, per tant, només el pot fer constar el titular o cessionari d'aquest dret. Els drets d'explotació formen part dels drets d'autor. Símbol copyright = ©.

CONSELLS I RECOMANACIONS:

- **La majoria de continguts d'Internet (text, imatges, música, vídeos...) tenen drets d'autor. Això implica que cal vigilar què copiem i què baixem d'Internet, si no volem incórrer en un delicte.**
- **Si cerques obres amb llicència Creative Commons podràs baixar i utilitzar materials amb tranquil·litat.**

8.Descàrregues
QUÈ ÉS?

- Descàrrega: Transferència de fitxers des d' un servidor, o a través d'ell, al nostre ordinador.

- P2P o Peer to Peer: xarxa d'ordinadors on els usuaris intercanvien fitxers ubicats en una carpeta concreta. Exemple: Emule, Bittorrent, Napster, etc.

CONSELLS I RECOMANACIONS:

- **Si descarregues o intercanvies fitxers, fes-ho només en aquells llocs que siguin de confiança.**
- **Les xarxes P2P poden ser utilitzades per accedir al nostre ordinador sense saber-ho.**
- **El fet d'intercanviar via P2P o baixar d'algun lloc web música, vídeos i altres fitxers implica una vulneració dels drets d'autor d'aquests continguts.**

Passo de mals rotllos!

Comportaments poc saludables i gens desitjables digitalment

9.Ciberassetjament (Ciberbulling o E-bulling) QUÈ ÉS?

El ciberassetjament és l'ús d'Internet, el telèfon mòbil o els videojocs per humiliar, agredir, maltractar, difamar, insultar, amenaçar o desprestigiar companys o persones conegudes d'una edat semblant.

ON SUCCEEIX?

Podem trobar ciberassetjament en xats, fòrums, SMS, blocs, fotoblocs, jocs en línia, videojocs virtuals, el nostre espai o converses de missatgeria instantània, o fins i tot podem ser-ne víctimes sense adonar-nos-en mentre algú fa servir els seus coneixements informàtics per introduir-se al nostre ordinador i manipular la càmera web, copiar dades i contrasenyes o fotos.

COM EL PUC RECONÈIXER?

A continuació et posem alguns exemples concrets de ciberassetjament perquè puguis identificar-lo:

- **Fotos**. Utilitzen les fotos que algunes persones tenen penjades a Internet, ja sigui al seu espai personal o al fotobloc, o fins i tot les que els prenen els troians o virus. Després manipulen i exposen aquestes fotos a Internet per avergonyir i humiliar les seves «víctimes». A vegades les exposen en webs en què es vota la persona més lletja o la més totxa, carregant el seu perfil de punts i fent que aparegui en les primeres posicions d'aquest rànquing. Altres vegades les utilitzen com a arma per xatejar amb la seva víctima i amenaçar-la que ensenyaran la foto en qüestió si no fa el que li diuen.

- **Suplantació de la personalitat.** Amb les dades d'una altra persona editen perfils o pàgines web amb comentaris ficticis sobre les seves experiències sexuals, manies o qualsevol altre comportament per fer-ne burla. Es fan passar per aquesta persona en fòrums i pàgines on escriuen opinions que ofenen altres persones o comentaris violents que provoquen la seva expulsió immediata de la pàgina i que no pugui tornar a accedir-hi.
- **Amenaces.** Se serveixen d'SMS, missatges de correu electrònic o vídeos per amenaçar i insultar la seva víctima.
- **Atac a la intimitat.** S'introdueixen dins del correu electrònic per manipular-lo, llegir els missatges i registrar la persona que n'és propietària en pàgines on pot ser víctima de correus brossa o de virus informàtics.

- **Guarda totes les proves de l'assetjament**, els missatges de text, els correus electrònics, els vídeos o les converses de missatgeria instantània.
- **Demana l'ajuda d'especialistes en informàtica** per identificar el ciberagressor.

VÍDEOS:

"Bloquea el acoso en línea" a http://www.youtube.com/watch?v=ch1SwcAra-E

"Spot Cyberbullyng (dibujos animados)" a http://www.youtube.com/watch?v=9wlkL5-c2SE

SABER ACTUAR:

Si has identificat alguns d'aquests símptomes al teu entorn, et donem uns quants consells perquè sàpigues com has d'actuar i aturar aquest assetjament.

- **Comenta-ho amb els teus pares o professors.** Ells són persones adultes i t'ajudaran a trobar més ràpidament una solució.
- **Sigues sempre molt prudent amb les teves dades personals i les teves fotos,** ja que no saps mai quin ús poden fer-ne. Com menys persones les coneguin, millor!
- **Pots buscar el teu nom i cognoms** o els teus sobrenoms en qualsevol cercador d'Internet per comprovar si algú ha suplantat la teva personalitat o ha utilitzat les teves dades personals per perjudicar-te.

10.Ciberassetjament a menors (Grooming): QUÈ ÉS?

El ciberassetjament a menors a Internet és un terme anglès que s'utilitza per descriure pràctiques en línia de certs adults per guanyar-se la confiança d'un o d'una menor fingint empatia, tendresa, falsa simpatia, etc, amb unes finalitats fraudulentes i sovint il·legals. Aquest fenomen, sovint està relacionat amb l'obtenció d'imatges i vídeos de menors i amb la pornografia .

CONSELLS I RECOMANACIONS:

- **Sigues sempre molt prudent amb les teves fotos i amb els vídeos personals, ja que no saps mai quin ús poden fer-ne.**
- **No acceptis cap tipus de xantatge a la xarxa, i en cas de trobar-te en una situació similar comenta-ho amb els teus pares i tutors.**
- **Desactiva la webcam quan no la facis servir.**
- **Protegeix el teu ordinador de virus i altres programes maliciosos que poden revelar les teves claus als autors de ciberassetjament a menors.**
- **No et deixis enganyar ni seduir per correus que et prometin miracles.**

VÍDEOS:

"Cuidado con la webcam: sus usos positivos y riesgos" a http://www.youtube.com/watch?v=JgzHphn5ldY&feature=fvsr

11.Missatges ham (Trolling) QUÈ ÉS?

El trolling és un terme anglès que defineix el comportament d'aquelles persones que escriuen missatges provocadors a la xarxa (correu electrònic, xats, xarxes socials) de manera intencionada i amb la finalitat de trobar polèmica.

SABER ACTUAR

Si algú t'envia informació desagradable en un xat, el millor és esborrar aquesta persona de la llista de contactes. Aquesta persona no sabrà qui ho ha fet. Mai no contestis els seus missatges ni les seves trucades

12.Griefing QUÈ ÉS?

El griefing és un terme anglès vinculat als jocs en xarxa, que serveix per definir el comportament d'aquells que perjudiquen de manera intencionada i sistemàtica un jugador en particular.

SABER ACTUAR

Sigues un bon model de joc net tant a la xarxa com a fora.

VÍDEO:

"A Internet posa-hi seny! - Capítol 3 - Jocs en xarxa" a http://www.youtube.com/watch?v=dy3UK8S_FXs

Connecta't, però vigila!

Aprofita la xarxa per informar-te i comunicar-te, però fes-ho amb seny

13.Navegació i correu electrònic
QUÈ ÉS?

- **Navegador:** Programa informàtic que permet moure's pels diversos serveis, recursos o conjunts d'informació d'Internet, per un sistema o per una aplicació.
- **Finestres emergents o Pop ups:** Finestra que apareix automàticament a la pantalla, sobreposada a la finestra activa.
- **Galetes o cookies:** Fitxers amb informació sobre els hàbits, les preferències i les pautes de navegació d'un internauta que visita una pàgina web, que el servidor envia al disc dur de l'ordinador de l'internauta mitjançant el navegador.
- **Tallafoc o firewall:** Aquesta mena de programa és el «porter» del teu ordinador: ningú no hi passarà sense el seu permís. T'avisa de possibles programes que et poden danyar l'ordinador i, a més, et protegeix davant els estafadors que hi vulguin entrar.
- **Correu electrònic o mail:** Aplicació per mitjà de la qual es poden enviar i rebre missatges personalitzats.

CONSELLS I RECOMANACIONS:

Alguna vegada t'has trobat barres d'eines instal·lades en el teu navegador que no saps d'on han sortit? Sovint ens apareixen finestres emergents, quan visitem una pàgina web o instal·lem programes, que en funció de la nostra resposta poden instal·lar continguts no desitjables en el nostre ordinador, com ara virus o troians, o programes o barres d'eines que alenteixen el funcionament del nostre ordinador. Per aquest motiu és molt important llegir atentament les informacions que apareixen en la nostra pantalla.

- **Llegeix** abans de clicar.
- **Esborra les galetes o cookies** emmagatzemades en el teu navegador web.
- **Navega per webs segures.**
- Si trobes continguts que pots considerar desagradables, perillosos o simplement estranys, **no intentis «investigar» pel teu compte** i avisa els teus pares o algun adult abans de continuar.
- Recorda que **no tota la informació que hi ha a Internet és correcta i ben intencionada.**
- **Atenció als missatges de correu electrònic.** Obre només aquells de persones que coneguis i esborra la resta. Els missatges adjunts poden contenir virus.

VÍDEO:

"A Internet posa-hi seny!
Capítol 1 - Navegant per Internet" a
http://www.youtube.com/watch?v=jq3dPGbhRmg

14.Missatgeria instantània i xats

QUÈ ÉS?

- **Xat:** Comunicació escrita que es duu a terme simultàniament i en temps real entre diverses persones per mitjà d'Internet.
- **Missatgeria instantània:** Comunicació escrita en temps real on l'usuari ha d'haver instal·lat prèviament un programa, el missatger, i només es pot comunicar amb la seva llista de contactes.

CONSELLS I RECOMANACIONS:

- Els xats com ara el messenger són una bona manera de comunicar-se amb familiars i amics. De la mateixa manera que en el contacte cara a cara, és important tenir cura de què diem i de com ho diem.
- Sigues crític a l'hora d'agregar un nou contacte al teu messenger. Hi ha persones malintencionades i expertes que utilitzen el messenger i els xats per fer-te algun mal (Grooming) o per prendre't la teva identitat digital (Phising).
- Quan alguna persona et falti al respecte o et posi en una situació desagradable explica-ho de seguida als pares. No deixis que la situació es repeteixi.
- Controla el teu temps. No deixis que els xats o les xarxes socials ocupin tot el teu temps d'oci. Gaudeix d'altres activitats.

VÍDEO:

"A Internet posa-hi seny! - Capítol 2 -
A les xarxes socials" a
http://www.youtube.com/watch?v=9oZ0OdGVtN0

15.Xarxes socials
QUÈ SÓN?

● **Xarxa social:** Conjunt de persones vinculades a un mateix grup d'Internet, que tenen com a element cohesionador el fet de compartir diferents tipologies de continguts, ja siguin personals, audiovisuals, professionals, etc

Les xarxes socials et permeten conèixer gent i tenir amics arreu del món. Pots compartir informació amb tots els teus companys alhora i pots conèixer altres cultures i costums.

VÍDEOS:

"A Internet posa-hi seny!- Capítol 2 - A les xarxes socials" a http://www.youtube.com/watch?v=9oZ0OdGVtN0

"¿Nos conocemos? Protección de menores en redes sociales y chats" a http://www.youtube.com/watch?v=DKmCmYBmKs4&feature=related

CONSELLS I RECOMANACIONS:

● No acceptis "amistats" de desconeguts. A Internet és molt fàcil dir mentides i fer veure que ets una altra persona.

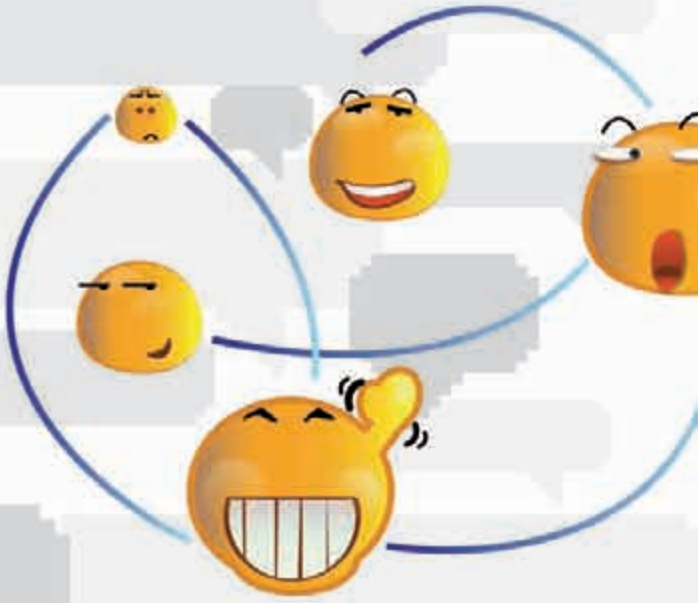
● Publicar informació a les xarxes socials és molt ràpid, però un cop publicada no saps quin ús en poden fer. Abans de penjar una imatge o publicar alguna cosa a la xarxa pensa-t'ho bé. No facilitis o publiquis dades, informació, fotografies o vídeos d'altres persones que no t'hagin donat el seu permís.

● Inventa contrasenyes difícils i fes servir un àlies (nick) que només coneguin els teus amics.

● No comparteixis dades com ara el telèfon, l'adreça o el teu nom o cognoms.

● Si algú et molesta o t'assetja en alguna xarxa social, avisa els teus pares o tutors.

● A Internet, no tothom és amic. No quedis amb les persones que coneguis mitjançant les xarxes socials. I si quedes amb algú, avisa els teus pares o tutors i queda en un lloc públic.



Ei, vols jugar?

Jocs en línia per posar a prova els teus coneixements sobre seguretat digital

Internet amb seny

http://internetambseny.cesicat.cat/

Navega segur!

http://www.domini.cat/santjordi/

Pantalles amigues

http://www.pantallasamigas.net/

Navega segur!

http://www.apdcat.com/ca/contingut.php?cont_id=450&cat_id=0

Vols saber-ne més?

Documents i adreces per estar més informat

Espai de l'XTEC sobre Internet segura

http://www.xtec.cat/internet_segura

Espai de l'Edu365.cat sobre Internet segura

http://www.edu365.cat/internetsegura/

Documents CLI-Prometeo sobre Seguretat tecnològica

http://www.asociacioncli.es/sites/default/files/Manual%2015-17%20catalan.pdf

http://www.asociacioncli.es/sites/default/files/Manual%2012-14%20catalan.pdf

http://www.asociacioncli.es/sites/default/files/Manual%209-11%20catalan.pdf

Guia CESICAT per a l'ús segur de les xarxes socials

http://www.cesicat.cat/publicacions/Guies%20de%20xarxes%20socials.jsp?canal=ciutadans

Decàleg

Normes i consells per a utilitzar les tecnologies

1.Seguretat

1.Utilitza un llapis de memòria (o un servei en línia per a còpies de seguretat) per a desar-hi còpies dels teus arxius i de les carpetes més importants.

2.Cal tenir cura i vigilar on deixem el nostre portàtil en tot moment.

3.Comprova que l'antivirus i el sistema operatiu estiguin sempre actius i actualitzats. Protegeix el teu ordinador de virus i altres programes maliciosos que poden revelar les teves claus als autors de ciberassetjament a menors.

4.Quan recarreguis la bateria, fes-ho fins al 100% de la seva capacitat.

5.Desa sempre el teu ordinador portàtil dins de la seva funda quan acabis d'utilitzar-lo i quan t'hagis de desplaçar.

2.Privacitat

1.Utilitza contrasenyes diferents per a cada servei. No les comparteixis amb ningú i desa-les en un lloc segur. Evita desar-les en un document anomenat "contrasenyes" o amb qualsevol altre nom detectable fàcilment.

2.Sigues sempre molt prudent amb les teves dades personals i les teves fotos, ja que no saps mai quin ús poden fer-ne. Quantes menys persones les coneguin, millor!

3.Atenció als missatges de correu electrònic. Obre només aquells de les persones que coneguis i esborra la resta. Els missatges adjunts poden contenir virus.

4.Si trobes continguts que pots considerar desagradables, perillosos o simplement estranys, no intentis «investigar» pel teu compte i avisa els teus pares o algun adult abans de continuar.

5.No acceptis "amistats" de desconeguts. A internet és molt fàcil dir mentides i fer veure que ets una altra persona.

3.Respecte

1.El fet d'intercanviar via P2P o baixar d'algun lloc web música, vídeos i altres fitxers és una vulneració dels drets d'autor d'aquests continguts. La majoria de continguts d'Internet (text, imatges, música, vídeos...) tenen drets d'autor. Això implica que cal vigilar què copiem i què baixem d'Internet, si no volem incórrer en un delicte.

2.Els xats com ara el messenger són una bona manera de comunicar-se amb familiars i amics. De la mateixa manera que en el contacte cara a cara, és important tenir cura de què diem i de com ho diem.

3.Controla el teu temps. No deixis que els xats o les xarxes socials ocupin tot el teu temps d'oci. Gaudeix d'altres activitats.

4.Sigues crític a l'hora d'agregar un nou contacte al teu messenger. Hi ha persones malintencionades i expertes que utilitzen el messenger i els xats per fer-te algun mal (Grooming) o per prendre't la teva identitat digital (Phising).

5.Publicar informació a les xarxes socials és molt ràpid, però un cop publicada no saps quin ús en poden fer. Abans de penjar una imatge o publicar alguna cosa a la xarxa, pensa-t'ho bé. No facilitis o publiquis dades, informació, fotografies o vídeos d'altres persones que no t'hagin donat el seu permís.

Generalitat de Catalunya
Departament d'Ensenyament

Subvenciona:

cesicat
Centre de Seguretat de la Informació de Catalunya

E laboren:

cetei
CENTRE DE TECNOLOGIES ITUARTE
Fundació Joan XXIII

Col·laboren:

apdcat
Agència Catalana de Protecció de Dades

Generalitat de Catalunya
Departament de Benestar Social i Família

Generalitat de Catalunya
Departament d'Interior, Relacions Institucionals i Participació

mossos d'esquadra