



"Seguretat a la xarxa amb infants"

mossos d'esquadra
■ ■ ■ ■



Ajuntament de
la Seu d'Urgell

Xarxa òmnia
Programa de la Secretaria d'Acció Ciutadana


Pla Educatiu d'Entorn
La Seu d'Urgell



Generalitat de Catalunya
**Departament de Benestar Social
i Família**

PUNT ÒMNIÀ
ACCÉS A LES NOVES TECNOLOGIES

Internet pot ajudar els infants a:

- Trobar recursos educatius, incloses les notícies i l'actualitat informativa, obtenir documents i fotos, i investigar sobre temes molt variats, des de les condicions climàtiques fins a les estadístiques de població.
- Aconseguir ajuda per fer els deures de l'escola, ja sigui mitjançant les enciclopèdies en línia i altres obres de referència, o bé contactant amb els experts.
- Augmentar les habilitats de lectura en accedir a continguts interessants, que poden suggerir la lectura addicional.
- Aprendre a utilitzar millor les noves tecnologies i millorar les habilitats informatives, per saber trobar i usar informació desitjada, resoldre problemes, comunicar-se amb la resta i, en definitiva, adquirir aquelles habilitats que cada vegada són més sol·licitades en el mercat laboral.

El primer que hem de tenir en compte és que **no hi ha cap eina** de control que sigui 100% efectiva i que abans de començar a "posar tanques", **hem familiaritzar-nos amb Internet, navegar amb l'infant i ensenyar-li a fer-ho amb seguretat.**

Podem utilitzar algun tipus de **filtre de continguts**, que deixarà consultar només els webs que es trobin dins d'una *llista segura* i vetarà els webs d'una *llista negra*, o que impedirà l'accés a webs que continguin determinades paraules. **Hi han molts sistemes per filtrar el que veiem a Internet**, però repetim, cap d'ells és totalment fiable.

POSSIBLES EINES

- Google Safesearch
- CANGURO NET
- Windows Live OneCare Protecció Infantil

Web's interessants

<http://internetambseny.cesicat.cat/>
<http://www.livemanual.info/manual-seguretat-infantil-internet/2>
www.elportaldelmenor.es
<http://www.internetsegura2010.es/spot.php>
<http://www.ciberfamilias.com/index.htm>
<http://www.chaval.es/chavales/page?p=index>
<http://deaquinopasas.org>
<http://www.cesicat.cat/ciudadans/>
<http://www.cesicat.cat>

<http://www.laseu.cat/perfils/ciudadans/educacio/>
<http://blog.xarxa-omnia.org/laseu>

CONSELLS per als menors

- *Inventa una contrasenya difícil i no li donis a ningú. No facis anar la teva data de naixement, o el telèfon..... aquests són molt fàcils d'agafar.
- *No tot el que està publicat a la xarxa és cert, documentat sempre abans de donar-ho per bo, pots preguntar als pares o tutors i confrontar informació.
- *Abans de penjar una fotografia o informació personal pensa-t'ho bé.
- *No publiquis mai informació personal o fotografies d'altres persones sense el seu consentiment.
- *No acceptis amistats de desconeguts, tant a la teva xarxa social com al teu xat.
- *Si algú et molesta o t'assetja surt del xat i avisa a un adult
- *No compartir dades com el telèfon, l'adreça de casa.... a Internet tothom és amic, no quedis amb persones que coneixis mitjançant la xarxa.
- *No acceptis cap arxiu de persones que no coneixes perquè poden adjuntar trojans o virus.
- *Obre només els correus de les persones que tu coneixes.
- *Les xarxes NO serveixen per difondre continguts degradants o ofensius cap a d'altres persones, per aquest motiu pots ser denunciat. Has de ser respectuós.
- *Intercanviar música o pel·lícules a través de programes infringeix la llei.
- *No facis res davant de la webcam que no faries davant dels teus amics.

*Recorda que tot el que fas des de la webcam l'altra persona ho pot gravar.

Consells per a pares

- L'ordinador ha de ser un regal familiar, i que qualsevol membre de la família pugui accedir.
- És bo crear usuaris diferents per un mateix aparell i així evitem que puguin esborrar documents, fitxers importants... . Cada usuari ha de tenir una contrasenya diferent per poder accedir al seu espai.
- L'aparell ha d'estar en una habitació compartida. Sinó és el cas pactar el no tancar mai la porta
- Seure i navegar amb el menor
- Pactar normes d'ús de l'aparell
- Pactar un horari
- Expliqueu la importància de les dades personals quines dades poden facilitar i quines no.
- Acordeu quines pàgines poden visitar i quines NO.
- Els menor no podem crear-ne cap correu electrònic sols, ni ser membre de cap xarxa social.
- A totes les xarxes socials podem configurar la privacitat del que pengem, és important saber si tenim el nostre perfil obert.

Diccionari

ANTIVIRUS:

Són programes que actuen com a guardaespalles del nostre ordinador. Estan alerta davant de possibles virus que se'ns poden introduir a l'ordinador.

BLOC/FOTOBLOC

Espai virtual personal d'un o diversos autors que és actualitzat periòdicament amb articles, textos (o fotografies en el cas dels fotoblocs), etc, i que s'ordena cronològicament. A través d'aquest espai, els usuaris poden compartir amb altres allò que els passa en la seva vida quotidiana. Les pàgines més comunes són Bloc.cat, Blogger o Wordpress

CIBER-ASSETJAMENT/ CIBERBULLYING

El ciberassetjament o cyberbullyng és una forma d'assetjament a un individu o grup i consisteix en atacs personals difosos mitjançant les tecnologies de la informació i la comunicació (Internet, telèfon mòbil...) . L'assetjament engloba qualsevol tipus de maltractament psicològic des d'amenaques, xantatges, insults, menyspreus,etc.

CONTRASENYA SEGURA

Una contrasenya segura és aquella que altres persones no poden determinar fàcilment endevinant-la o utilitzant programes informàtics. Per a crear una contrasenya segura que puguis recordar fàcilment però que sigui difícil de determinar per terceres persones, intenta una de les tècniques següents: NO utilitzis contrasenyes que siguin paraules (encara que siguin estrangeres) o noms (el de usuari, personatges de ficció, membres de família, mascotes, marques, ciutats, llocs o altres noms relacionats). No usis contrasenyes completament numèriques amb algun significat (telèfon, DNI, data de naixement, PIN...). Tria una contrasenya que barregi caràcters alfabètics i numèrics. Han de ser llargues , de 8 caràcters o més. Estableix contrasenyes diferents per sistemes diferents. És possible usar una contrasenya base i certes variacions lògiques de la mateixa per a diferents llocs. Això permet que, si et roben una contrasenya, no et robin els accessos a tots els llocs quals ingresses.

CONTROL PARENTAL

S'anomena control parental qualsevol eina que permet als pares supervisar i/o limitar l'ús que el menor fa de l'ordinador o d'Internet. Aquests controls ajuden els pares a seleccionar els jocs i els programes, es que els seus fills poden usar, com també llocs web que poden visitar i quan poden fer-ho

GROOMING

El grooming es refereix a l'assetjament de caràcter sexual d'un menor. Les accions dutes a terme tenen l'objectiu d'establir una relació i control emocional sobre un menor o nen per després abusar-ne sexualment. A diferència del ciberassetjament té un objectiu explícitament sexual.

LLEI DE PROTECCIÓ DE DADES

La llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal ens dóna dret a ser informats de la recollida de les nostres dades; a saber la identitat i l'adreça de qui les sol·licita – normalment la persona responsable del tractament de les nostres dades o el seu representant-; a negar-nos a proporcionar-les – si no és que una llei ens hi obligui -; a accedir –hi sempre que es vulgui, rectificar-les o cancel·lar-les; i a oposar-nos al tractament de les nostres dades en determinades circumstàncies.

MISSATGERIA INSTANTÀNEA

En la missatgeria instantània, cada usuari instal·la en el seu ordinador un programa que es denomina missatger, i té una llista de contactes amb els quals es pot comunicar. Els programes més reconeguts per portar a terme aquesta acció són Live Messenger i MSN de Microsoft, Yahoo!Messenger, Gtalk de Google, Skype, etc.

ROBATORI D'IDENTITAT O PHISHING

És una forma d'enganyar els usuaris perquè revelin informació personal o financera mitjançant un missatge de correu electrònic o un lloc web fraudulent. Normalment, una estafa per suplantació d'identitat comença amb un missatge de e-mail que sembla un comunicat oficial d'una font de confiança, com ara un banc, una companyia de targeta de crèdit o un comerciant en línia reconegut. En el missatge de correu electrònic, s'adreça als destinataris a un lloc web fraudulent on se'ls demana que proporcionin les seves dades personals, com ara un número de compte o una contrasenya. Després, aquesta informació s'usa per al robatori d'identitat.

SEXTING

Sexting és l'enviament de contingut sexual (principalment fotografies i/o vídeos), produïts pel propi remitent, a altres persones per mitjà del telèfon mòbil. En aquest cas, s'ha d'anar amb precaució per la gran difusió que arriba a tenir Internet. Un cop a la xarxa, l'usuari perd el control de la difusió de l'arxiu que penja.

TALLAFOCS

Programes que actuen com a porters de l'ordinador. Res no pot entrar sense que li donin permís per fer-ho. Avisen de programes que poden actuar en perjudici del teu ordinador o el fan invisibles davant d'amenaques. En alguns webs trobareu tallafocs que us podeu baixar gratuïtament; és molt recomanable que es n'instal·leu.

TROIANS

Són programes informàtics que semblen ser programari útil però que posen en perill la seguretat de l'ordinador. Habitualment s'utilitzen per espionar e instal·lar -hi programari d'accés remot que permet monitoritzar el que fan l'usuari a l'ordinador.

XARXES P2P

Les xarxes P2P (peer to peer) o d'igual a igual són sistemes d'intercanvi de material. És una forma legal de compartir arxius de forma similar a com es fa en el correu o la missatgeria instantània si bé d'una forma més eficient i generalment , més ràpida.

XARXES SOCIALS

Una xarxa social és una comunitat d'usuaris que es relacionen entre si i on habitualment comparteixen fotografies, vídeos, missatges, etc. Les xarxes més comunes són Facebook, Tuenty, Myspace o Twiter.

XAT

El xat o ciberxerrada és una comunicació escrita a través d'Internet entre dues o més persones, realitzada instantàneament.

VIRUS

Un virus és un codi informàtic que s'adjunta a un programa o un arxiu per a propagar-se d'un equip a un altre. Infecta, amb gran facilitat, a mesura que és transmet. Els virus poden danyar i esborrar el programari (software), perjudicar el maquinari (hardware) i els diferents arxius que conté l'ordinador infectat.

WEBS DE CONFIANÇA

Saber quan confiar en un lloc depèn del coneixement previ que tenim de l'empresa o autor del lloc web, la informació que conté i si el coneixement a través d'alguna persona de confiança.

els blocs i fotoblocs

Què pot passar?

Que s'utilitzin les vostres fotografies per a finalitats no desitjades. Que cometeu una infracció per publicar fotografies d'altres menors sense el consentiment dels seus pares o tutors.

Com prevenir-ho:

- Aviseu els vostres pares o tutors abans de publicar les vostres fotografies.
- Demaneu permís per publicar fotografies dels vostres amics.
- Expresseu-vos educadament.

les descàrregues de música, vídeos....

Què pot passar?

Que us baixeu continguts il·legals ocults.

Com prevenir-ho:

- Utilitzeu la previsualització dels programes que descarregueu i cancel·leu el que sospiteu que és il·legal.
- Activeu mecanismes de control parental.

la càmera web

Què pot passar?

Que us activin la càmera web sense que ho sapigueu.

Com prevenir-ho:

- Desconnecteu o tapeu la càmera web quan no la feu servir.
- Sigueu responsables del què feu davant de la càmera web.

Internet SEGUERA

recordeu

Podeu enviar els vostres dubtes i consultes a l'adreça:

internetsegura@gencat.cat

Podeu contactar amb:

Polícia de la Generalitat-Mossos d'Esquadra

www.gencat.cat/mossos

internetsegura@gencat.cat

ICUA - Agència de Qualitat d'Internet

c/ Entença, 332, 7è 3a

08029 Barcelona

Tel. 93 363 25 65

iqua@iqua.es

ACIM - Associació Catalana per a la Infància Maltractada

c/ Gran de Gràcia, 241, 1r

08012 Barcelona

Tel. 93 511 44 16

www.acim.es



Generalitat
de Catalunya



mossos d'esquadra



Generalitat
de Catalunya



mossos d'esquadra

aspectes a tenir en compte: la contrasenya

Què pot passar?

Si és poc segura poseu en risc l'accés a l'ordinador, al correu electrònic i a tots els vostres arxius i imatges.

Com prevenir-ho:

- Utilitzeu contrasenyes segures. Es considera segura la contrasenya que té més de 8 caràcters i combina lletres i números, majúscules i minúscules.
- Feu servir contrasenyes diferents per a cada servei.
- No doneu les vostres contrasenyes a ningú.
- Guardeu-les en llocs segurs.

els virus: troians i espies

Què pot passar?

Que poden entrar al vostre ordinador sense que ho sapigueu quan obriu un missatge o una imatge. Poden donar accés remot al control de l'ordinador i destruir-vos el contingut del disc dur.

Com prevenir-ho:

- Instal·leu programes antivirus i tingueu-los activats quan navegueu.
- Tingueu cura dels continguts que us descarregueu i no obriu missatges de remittents desconeguts.

el xat i la missatgeria instantània

Què pot passar?

Que us enganyin, usurpin la vostra identitat, o us sostreguin les vostres contrasenyes i entrin al vostre ordinador.

Com prevenir-ho:

- Filtreu els vostres contactes.
- Sigueu responsables amb les vostres dades personals.
- Utilitzeu paraules clau per identificar els vostres contactes i/o amics.

- Guardeu en secret la vostra contrasenya d'accés al correu i no la doneu a ningú.
- Si voleu conèixer en persona a algú que heu conegut per la xarxa, consulteu-ho amb els vostres pares o amb algun adult. Estareu més segurs si quedeu en un lloc públic.
- Si a la web trobeu alguna paraula o foto que us faci sentir malament sortiu de la pàgina i expliqueu-ho a un adult.

- No us cregueu tot el que us diuen al xat.
- No obriu ni llegiu missatges ni fitxers que us envïn persones desconegudes.
- Podeu ensenyar els vostres pares a utilitzar Internet i les pàgines web que visiteu.

Els menors també poden ser responsables de determinades conductes relacionades amb la xarxa.

En aquest sentit, els menors poden ser responsables si:

- Amenacen o assetgen a altres persones.
- Difamen a través de missatges o fotografies.
- Vulneren els drets de propietat intel·lectual quan hi hagi ànim de lucre.

consells per a educadors i pares

La millor manera de prevenir situacions de risc i d'ajudar els menors a navegar amb seguretat per la xarxa és:

- Feu-los conscients de les avantatges i desavantatges que ofereix Internet.
- Eduqueu-los perquè sàpiguen navegar de manera responsable i segura.
- Doneu-los estratègies perquè puguin protegir-se sols de possibles perills de la xarxa.
- Familiaritzeu-vos amb l'ús d'Internet.
- Parleu obertament amb els menors sobre l'ús d'Internet.
- Navegueu per la xarxa amb els vostres fills i/o alumnes.
- Informeu-vos sobre les eines de control.
- Establiu regles bàsiques de seguretat a la llar i al centre educatiu.
- Feu servir llocs web segurs.
- Poseu l'ordinador en espais oberts.

Actualment Internet contribueix a satisfer moltes de les nostres necessitats d'informació, coneixement i comunicació, així també ofereix una sèrie de possibilitats que afavoreixen les relacions personals.

Les característiques actuals d'Internet han generat una especial sensibilització per protegir els menors que són especialment vulnerables respecte d'altres persones que vulguin aprofitar-se'n.

Per aquest motiu, el Departament d'Interior, Relacions Institucionals i Participació ha elaborat un pla per prevenir la ciberdelinqüència en l'àmbit dels adolescents i joves.

En aquest triptic trobareu informació sobre les desavantatges que pot comportar l'ús d'Internet i les mesures que podeu prendre per evitar els possibles perills que ofereix la xarxa.

Internet i els menors

Els menors com a usuaris de la xarxa són especialment vulnerables a determinades activitats delictives relacionades amb el contingut de la informació. En aquest sentit són víctimes si accedeixen a continguts il·legals com:

- Pornografia infantil
- Anorèxia / bulímia
- Jocs en línia

consells per a infants i joves

- No parleu amb desconeguts per la xarxa. Identifiqueu les persones amb les quals us comuniqueu a través del xat.
- Quan navegueu per Internet, no faciliteu mai les vostres dades personals ni fotografies a persones desconegudes.
- Controleu la vostra llista de contactes de missatgeria instantània.

Web's

1. <http://www.gencat.cat/mossos/index.htm>
2. <http://www.cesicat.cat/>
3. <http://internetambseny.cesicat.cat/>
4. <http://www.cesicat.cat/fitxers/publicacions/Guia%20per%20a%20l%20us%20segur%20de%20les%20xarxes%20socials.pdf>
5. www.protegeles.com Associació sense ànim de lucre que sorgeix com associació al 2002. Té una línia de denúncia contra la pornografia infantil que funciona des del 2001.
6. <http://chaval.red.es> (dividida x edats, també per a pares i diferents guies)
7. www.aporelsobresaliente.com – Drets i deures sobre els mòbils.
8. www.ciberfamilias.com – Informació pera pares i educadors sobre la seguretat a la xarxa.
9. www.enlaredprotegete.com – A la xarxa la *Red Protegete*, fomenta la utilització de la xarxa entre els joves d'una manera responsable, ètica i segura.
10. www.portaldelmenor.es
11. www.acosoescolar.info/index.htm
12. www.masqueunaimagen.com – Línia d'ajuda contra la bulímia i l'anorèxia.
13. www.seguridadenlared.org
14. www.micueva.com

Per Jugar

www.super3.cat

www.edu365.cat

www.pequejuegos.com

<http://www.pipoclub.com/>

<http://www.lastresmellizas.com> o www.lestresbessones.cat

<http://www.cesicat.cat/ciudadans/>

ANTIVIRUS

Aquestes dues adreces són espais on podeu descarregar un antivirus gratuït.

<http://free.avg.com/ww-es/inicio>

<http://www.avast.com/es-ww/free-antivirus-download>