# Protecció de menors

## Navegació segura

"[S02] Guies de seguretat TIC."

cesicat

# Presentació

El Centre de Seguretat de la Informació de Catalunya (en endavant, CESICAT) és l'organisme executor del pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009.

La missió del Pla nacional d'impuls de la seguretat TIC a Catalunya és: garantir una Societat de la Informació segura catalana per a tots, operant un Centre de Seguretat de la Informació de Catalunya, com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya.
- Suport a la protecció de les infraestructures crítiques TIC nacionals.
- Promoció d'un teixit empresarial català sòlid en seguretat TIC.
- Increment de la confiança i protecció de la ciutadania catalana en la societat de la informació.

Dintre d'aquests objectius estratègics, es constitueix la Fundació Pública "Centre de Seguretat de la Informació de Catalunya" com a entitat auxiliar i instrumental del govern de la Generalitat de Catalunya i de les entitats que la composen.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix, com a servei preventiu, l'elaboració d'un conjunt de guies de seguretat adreçades a les diferents comunitats.

# Índex temàtic

# Audiència

Aquesta guia està adreçada a totes aquelles persones que són pares, tutors, professors o educadors de menors.

Aquesta guia també està pensada per a aquelles persones que, tot i no tenir menors al seu càrrec, estan interessades en la seguretat a Internet i en conèixer quines precaucions caldria adoptar. S'exposen els fenòmens més freqüents en què un usuari d'Internet es pot veure subjecte a algun frau o risc a la xarxa.

# Abast

L'abast d'aquest document és assolir unes bones pràctiques en seguretat de la informació aplicades a la presència dels menors a Internet. En tot cas, s'ha de prendre com una sèrie de recomanacions flexibles que han de ser adaptades a cada situació particular.



# Aspectes legals i normatius

- Llei Orgànica 10/1995, de 23 de novembre, per la qual s'aprova el Codi Penal
  http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1995-25444
- Llei Orgànica 1/1996, de 15 de gener, de Protecció Jurídica del Menor.
  http://www.boe.es/boe/dias/2000/01/13/pdfs/A01422-01441.pdf
- Llei Orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.
  http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1982-11196
- Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.
  http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

- Llei Orgànica 5/2000, de 12 de gener, reguladora de la Responsabilitat Penal dels Menors.
http://www.boe.es/boe/dias/2000/01/13/pdfs/A01422-01441.pdf
- Reial Decret legislatiu 1/1996, de 12 de abril, pel qual s'aprova el text refós de la Llei de Propietat Intelectual.
http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1996-8930
- Llei 34/2002, de 11 de juliol, de Serveis de la Societat de la Informació i de comerç electrònic.
http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2002-13758
- Llei 22/2010, de 20 de juliol, del Codi de Consum de Catalunya
http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2010-13115
- Reial Decret 899/2009, de 22 de maig, pel qual s'aprova la carta de drets de l'usuari dels serveis de comunicacions electròniques
http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2009-8961

# Descripció general

## Què és i en què consisteix?

Hem vist la transformació d'una societat desconnectada en una altra basada en les noves tecnologies, on la informació viatja ràpidament d'una banda a l'altra del món, i per primera vegada estem davant d'una generació que creix també de la mà d'Internet.

Els menors coneixen els ordinadors i els videojocs des de ben petits i, per a ells, és com un altre llenguatge natural. De fet, a Catalunya, el 93,3% dels nois i noies fa servir Internet fora de l'escola

S'ha produït un error: No s'ha trobat la font de referència
Internet els ofereix tot un món de possibilitats de comunicació, i per això, per la importància que té en el seu entorn social, els pares hem de posar el nostre esforç perquè l'experiència sigui positiva i constructiva.

Segons l'estudi "*Seguretat en l'ús d'Internet dels nois i noies de 8 a 14 anys*" de 2010 (FOBSIC)Seguretat en l'ús d'Internet dels nois i noies de 8 a 14 anys, Fobsic, Març de 2010, el 3,1% dels menors catalans accepta contactar amb desconeguts. Tenint en compte que bona part dels joves es connecten tots els dies a Internet, i si fem cas d'estudis que indiquen que el 22% dels pares no parla amb els seus fills dels riscos presents en aquest entorn i que el 73,3% no controla res o aplica un control baix de la seva navegació, estem davant d'una oportunitat immillorable de donar un gir a aquesta situació per tal de millorar la seguretat de les famílies que desitgen que Internet sigui un element més de la seva vida quotidiana.

Estem habituats a utilitzar expressions de cautela com: "No corris", "Deixa'm que t'ajudi", "No acceptis caramels de desconeguts", "No parlis amb desconeguts", "Mira abans de creuar", "Renta't les mans abans de dinar". A Internet, tot i tractar-se d'un mitjà diferent,

hem d'aplicar els mateixos principis educatius per tal que la seva navegació pugui ser segura i constitueixi una experiència profitosa.

## Finalitat

La finalitat d'aquesta guia consisteix a proporcionar els coneixements i recomanacions necessaris als adults que estan a càrrec de menors amb l'objectiu de protegir-los davant els perills que poden trobar-se a Internet.

# Casos d'estudi

## El meu fill ha accedit a continguts no apropiats per la seva edat

### Descripció

Internet és un reflex del món real, podem trobar-hi coses molt útils, coses meravelloses i coses no tan bones. La gràcia que té és que la informació no és només escrita, també és visual, en forma d'imatges i vídeos, que ajuden a una millor assimilació.

Aprofitant els recursos que ofereix aquest nou entorn, tinc un fill de 13 anys a qui he ajudat a aprendre a utilitzar l'ordinador i fer cerques a Internet per documentar-se per a l'escola. El que no m'esperava pas és que ahir, durant el sopar, em digués que havia trobat una pàgina amb imatges esgarrifoses quan navegava buscant informació per un treball. Com ha pogut passar? Com pot ser tan fàcil que els nois i noies d'aquesta edat trobin informació inapropiada? Hi ha alguna cosa més de què preocupar-se a banda que puguin accedir a aquest tipus d'informació?



## Amenaces

### Exposició a continguts inadequats

El desenvolupament emocional i moral dels menors fa que siguin especialment vulnerables al que puguin trobar, normalment perquè el contingut no està adaptat a la seva edat, o perquè ells no estan preparats per comprendre'l.

Els continguts que poden afectar als nostres fills poden ser, entre altres:

- Contingut sexual explícit.
- Contingut violent, racista o sexista.
- Terrorisme.
- Sectes i missatges religiosos extremistes.
- Exposició a comportaments nocius per a la salut, com per exemple, l'anorèxia o la bulímia.

### Adquisició de material il·legal (per exemple medicaments o productes nocius)

Internet permet realitzar compres sense estar present físicament a la botiga, i tenint en compte que els joves poden disposar d'una targeta de dèbit als 14 anys, aquests podrien arribar a adquirir, via webs de dubtosa reputació, drogues legals i/o il·legals: alcohol, tabac, cocaïna, etc...

Si es produís la compra d'aquests productes, això podria comportar responsabilitats tant als venedors (en cas de ser negocis legítims) així com als menors o als seus representants legals en funció de l'edat dels primers.



# L'ordinador fa coses estranyes (o no)

## Descripció

Des de fa uns dies el nostre ordinador fa coses estranyes: Tot va més lent i quan l'engego triga molt temps a iniciar-se.

La veritat és que no comprenem l'origen d'aquest comportament perquè els meus fills només accedeixen al seu correu electrònic, a les xarxes socials i a Internet per fer treballs de classe.

Crec que tot va començar quan vàrem clicar en un enllaç que ens va arribar per correu electrònic. No sé què vam fer, però ens va aparèixer una finestra d'un antivirus que no sabíem que teníem i que ens avisava que el nostre equip estava infectat amb un virus. Em vaig espantar i vaig seguir les instruccions del programa.

Ara, després de veure que l'ordinador no va bé, estem preocupats perquè ens han dit que potser el que nosaltres pensàvem que era un antivirus, possiblement no ho era, sinó que era un virus dels que anomenen troians, que es fa passar per un programari legítim, quan en realitat serveix per aprofitar-se del nostre ordinador i del que nosaltres fem amb ell: accedir al correu electrònic, accedir al banc, etc.

Per acabar-ho d'adobar, ara el meu fill m'ha dit que, de sobte, no pot entrar al seu correu electrònic. Tindran a veure les dues coses? Jo també utilitzo l'ordinador per entrar al banc. Si aquest suposat antivirus és en realitat un troià d'aquests, poden haver-me robat diners del banc?

Tot i que aquest escenari és molt comú, no cal perdre de vista la tendència actual d'evolució del codi maliciós, cada vegada més sofisticat a l'hora de passar totalment desapercebut per a l'usuari. Existeix la possibilitat que el nostre ordinador estigui infectat i ens trobem exposats a les mateixes amenaces sense tenir-ne cap indici.

## Amenaces

### Robatori de credencials d'accés

Molts dels serveis utilitzats a Internet són privats i personals (correu electrònic, xats, xarxes socials, banca online,...) i, per tant, el seu ús implica acreditar-se com a titular del servei mitjançant un identificador

d'usuari i contrasenya. L'existència de codi maliciós en els equips informàtics pot comprometre els sistemes d'identificació de l'usuari, que pot perdre l'accés a aquests serveis a favor d'un tercer (qui ha infectat l'equip), que podrà utilitzar el servei il·legítimament i també impedir que l'usuari titular del servei pugui accedir-hi.

## Frau

En l'utilitzar les credencials sostretes a l'usuari titular del servei, el malfactor s'apodera dels serveis online que s'han vist compromesos, donant-se casos on:

- El malfactor faci xantatge a l'afectat mirant de forçar-lo a algun tipus de compensació per tal que pugui recuperar el control del servei que s'ha vist compromès.
- El malfactor faci un ús indegut dels serveis fent-se passar pel titular del servei.
- El malfactor obtingui beneficis una vegada aconseguit l'accés a serveis de banca online.

## Suplantació d'identitat

Es produeix quan el malfactor es fa passar per l'usuari titular del compte, ja sigui mitjançant l'enviament de correus electrònics a través d'un compte de correu que s'ha vist compromès, un xat, les xarxes socials o en jocs online. Aquest tipus de conducta, en ocasions, està estretament lligada a l'amenaça de frau o amb perjudicis de caràcter econòmic, ja que el malfactor persegueix extorsionar el propi titular a canvi de deixar d'utilitzar el seus serveis i comptes de manera inapropiada o d'enganyar als seus contactes fent-los creure que requereix d'algun tipus de préstec o ajuda econòmica.

## Pèrdua de privacitat

La pèrdua de privacitat es produeix arran de la sostracció de la informació continguda en els serveis online personals, on un tercer té accés a informació particular nostra associada al servei. Per exemple, si un tercer es fes amb el control del nostre compte de correu electrònic, podria llegir tot el nostre històric de correus.

## Infecció de l'equip informàtic

Com a element comú de la major part de les amenaces trobem la infecció de l'equip informàtic, que es pot definir com la presència en aquest equip de programari il·legítim, instal·lat sense coneixement de l'usuari amb la finalitat d'emprar-lo en accions fraudulentes. Un equip infectat, a més a més d'estar subjecte a amenaces ja esmentades, por estar subjecte a d'altres amenaces com la pèrdua de la informació que conté o a ser utilitzat inapropiadament per realitzar accions il·legítimes contra d'altres sistemes.



# El meu fill ha estat enganyat

## Descripció

El meu fill de 15 anys juga a l'equip de bàsquet de l'escola i igual que ell, molts nois del seu equip són fans d'en Pau Gasol.

Quan els seus companys van trobar una web que venia les samarretes oficials d'aquest jugador amb un 35% de descompte no ho van dubtar i varen fer la comanda. Estaven tan contents!

Han passat dos mesos i les samarretes no han arribat. Al meu fill li han carregat al seu compte un import molt superior al preu final de la samarreta i, a més a més, han aparegut posteriorment més càrrecs bancaris, aquests no autoritzats, de companyies que no coneixem de res.

El problema i la desconfiança ve perquè no podem contactar amb l'empresa de les samarretes, ni amb cap de les altres empreses que han fet càrrecs a la targeta. I sembla ser que no som els únics...

## Amenaces

### Frau

No tot és el que sembla ser, i els estafadors han focalitzat moltes energies en aprofitar les característiques d'Internet per adaptar i estendre les seves activitats a un conjunt de víctimes molt més gran. Es possibilita així el frau massiu.

Els menors són crèduls per naturalesa, i en créixer envoltats de tecnologia i Internet, tenen una confiança en la xarxa molt més gran que la dels adults. Són víctimes potencials d'enganys i fraus.

Comprar online en llocs poc fiables suposa acceptar el risc de veure'ns perjudicats per activitats fraudulentes i/o que un tercer es faci amb les nostres dades i les utilitzi amb fins imprevistos que ens repercuteixin directament i negativament.



# Companys de l'escola estan assetjant el meu fill a través d'Internet/ Mòbil

## Descripció

Estem molt preocupats per la situació que vivim a casa des de fa unes setmanes amb el nostre fill.

Al principi no notàvem res estrany, però es veritat que ja no somreia tant com abans i semblava més trist. Ens va costar que parlés amb nosaltres i finalment ens va explicar què li passava: uns companys de classe li envien correus electrònics insultant-lo. No tenint-ne prou amb això, ara han creat un grup al Tuenti per humiliar-lo publicant comentaris desagradables i han penjat un vídeo al Youtube gravat amb el seu mòbil on l'imiten per ridiculitzar-lo. El pitjor és que ho han difós a l'escola i tothom ho ha vist.

Ara, cada matí és l'hem de convèncer perquè vagi a l'escola. Hem de trobar una solució el més aviat possible.

## Amenaces

### Ciber assetjament

El ciber assetjament (cyberbullying) és un nou concepte que expressa l'assetjament mitjançant nous canals de comunicació electrònica. Es tracta d'una situació en la qual generalment l'assetjador i la víctima comparteixen un entorn social pròxim, normalment

companys de l'escola o institut. L'agressor o agressors utilitzen la xarxa i d'altres mitjans tecnològics per disposar de més informació i estendre la humiliació a molta més gent, accentuant el patiment de la víctima. Existeixen dos tipus de ciber assetjament: actiu i passiu. El ciber assetjament passiu es produeix quan el menor és la víctima, i el ciber assetjament actiu, quan el menor és l'agressor. Segons un estudi d'INTECO Guía sobre ciberbullying i grooming, INTECO, Maig de 2009 [PDF] http://www.inteco.es/Seguridad/Observatorio/manuales_es/guiaManual_groming_ciberbullying, a Espanya el 5,9% del menors ha patit ciber assetjament i el 2,9% reconeix haver actuat com a assetjador.

# Algú s'està fent passar pel meu fill a Internet

## Descripció

M'han trucat els pares d'una companya de classe del meu fill per dir-me que estaven molt disgustats per com parlava d'ella a les xarxes socials, que l'estava assetjant i ridiculitzant davant tothom a Internet i que pensaven denunciar-lo per ciber assetjament.

Quan he anat a parlar amb el meu fill d'aquests fets, s'ha mostrat molt sorprès i m'ha dit que ell mai no havia escrit res sobre aquesta noia, i que no es creia el que deien. Hem anat a veure el perfil de la seva companya de classe, i, efectivament, hi havia comentaris ofensius fets per l'avatar del meu fill.

Davant d'aquests fets, hem comprovat quan s'havien enviat aquests comentaris i molts d'ells s'havien produït quan el nostre fill es trobava amb nosaltres. Per tant, ell no els estava enviant!

Finalment hem descobert que el nostre fill utilitza la mateixa contrasenya per a tots els serveis online i que aquesta és el nom del nostre gos. Sembla ser que algú que coneix al meu fill ha descobert fàcilment la contrasenya i ho està aprofitant...

## Amenaces

### Robatori de credencials d'accés

Quan les contrasenyes són febles (ja sigui per què són molt curtes o fàcilment endevinables), o les preguntes per recuperar-les són evidents, és relativament fàcil fer-se amb les credencials d'accés d'una persona.

Si a més a més s'utilitza la mateixa contrasenya a tots els entorns online, l'amenaça de suplantació d'identitat s'estén a tots els serveis online utilitzats per l'usuari.

### Suplantació d'identitat

En el context dels menors, el robatori d'identitat és un dels riscos més comuns, tant en xarxes socials com en el servei de correu electrònic, atès que s'utilitza per deixar malament la víctima davant de la resta de companys, per fer accions inapropiades en el seu nom o per apoderar-se d'informació de la víctima i de tercers del seu entorn (inclosos els pares, amics o tutors).

# La meva filla fa nous amics a Internet

## Descripció

La meva filla Montserrat, de 16 anys, és una noia molt responsable i en la qual es pot confiar, i és tan simpàtica que tothom vol ser amic seu. Normalment veu els seus amics a l'institut, i ara, amb les noves tecnologies, també contacta amb ells per correu electrònic, a les xarxes socials i als xats, on el seu pseudònim és Montse_16.



Ahir em va dir que ha conegut gent molt simpàtica al xat, al canal #cinema, on ha contactat amb gent a qui li agrada el cinema tant com a ella.

Tot i això estic prou preocupada. La Montse m'ha explicat que una noia de la seva classe va quedar tota sola amb un amic del xat que no coneixia personalment, i que, quan es van trobar cara a cara, aquell noi era un adult que volia ser amic seu. Ella va tornar a casa ràpidament, però aquest adult la va seguir i temps després encara l'esperava a la porta de l'escola i no deixava de trucar-li per telèfon. Els seus pares van haver d'anar a la policia. Va resultar que aquest home tenia antecedents per pederàstia.

També sabem el cas d'una noia del nostre barri a la qual un "amic d'Internet" li va canviar la clau d'accés del correu electrònic (l'havia pogut endevinar perquè la resposta a la seva pregunta de seguretat era evident!), i li va demanar una foto compromesa per tornar-li l'accés. Com que la noia va accedir-hi, l'atacant va aprofitar per fer-li xantatge i demanar-li fotografies encara més compromeses. No sabem ben bé com va acabar aquesta història, els seus pares no en volen parlar.

## Amenaces

### Exposició a pederastes i pedòfils

A Internet, no tot és el que sembla ser. De la mateixa manera que ens poden enganyar en la vida física, als móns virtuals (xats, jocs online, xarxes socials...) la identitat de la persona que s'amaga darrere d'un pseudònim interessant no està garantida. Aquest és un dels atractius i dels perills dels móns virtuals per als nostres fills.

Els menors poden establir relacions amb desconeguts i, involuntàriament, proporcionar-los informació privada molt útil (horaris, centre d'estudis, edat, adreça, telèfon mòbil...) que, en males mans, poden suposar un gran perill per a la integritat emocional i/o física del menor, com ara segrest i abús sexual per part de pederastes.

### Entabanament (*Grooming*)

El terme *grooming* (entabanament) de menors a Internet s'utilitza per descriure les pràctiques online d'alguns adults per guanyar la confiança d'un o d'una menor, fingint empatia i estima (fins i tot fent-se passar per un altre menor), amb l'objectiu d'aconseguir inicialment imatges amb una certa càrrega sexual.

El pas següent és l'extorsió dels menors. Amb l'amenaça de difondre aquestes imatges als seus contactes/amics/pares, se'ls extorsiona perquè els proporcionin més imatges, o imatges més compromeses (sen-

se roba, realitzant actes de caire sexual...). Aquestes situacions poden fins i tot provocar que els menors accedeixin a quedar físicament amb l'assetjador, amb les conseqüències que això pot comportar.

Aquest comportament està doncs molt relacionat amb la pederàstia i la pornografia infantil. De fet, el *grooming* és moltes vegades el primer pas abans d'un abús sexual.

# La meva filla fa videoconferències

## Descripció

Des que al seu aniversari els seus amics li van regalar una càmera web, la nostra filla utilitza el seu ordinador per fer videoconferències amb amics. Aquesta càmera web és un dispositiu que es connecta a l'ordinador i funciona com una videocàmera que et grava davant del teu ordinador i envia en temps real aquest vídeo cap a les persones que vulguis. D'aquesta manera, dos persones amb una webcam cadascuna, poden veure's a través d'Internet!

M'han explicat que també hi ha webs a Internet que permeten conèixer gent mitjançant la webcam. Tu et connectes, prems un botó de l'aplicació, i apareix a la teva pantalla la imatge d'una persona anònima que no coneixies.

Em sembla un avanç de la tecnologia prou interessant, però em fa por perquè un amic que és policia m'ha explicat que hi ha gent que utilitza les webcams i aquestes pàgines web per videoconferències per fer-se passar per responsables d'una agència de models quan no ho són, i així demanar a noies que es disfressin per fer una prova. És terrible, perquè quan una d'aquestes noies envia les primeres imatges compromeses, el fals "*mànager*" de models s'aprofita per demanar-li més i més fotografies!

Si no en tenia prou de saber això, ara resulta que un amic informàtic m'ha explicat que si no tens cura, les webcam són accessibles per altres des d'Internet, igual com hi ha pares que vigilen l'interior de les seves cases des de la feina amb aquests dispositius. I si algú engega la càmera de la meva filla sense que ella ho sàpiga?

## Amenaces

### Exposició a pederastes i pedòfils

De la mateixa manera que el pseudònim d'una persona pot no tenir res a veure amb la persona que s'amaga darrere d'ell, les imatges que es transmeten a través de la càmera web poden estar dissenyades fraudulentament amb l'objectiu d'aparentar ser una persona més agradable o propera a la víctima de l'engany. La webcam transmet el que un atacant vulgui transmetre i és per això que és una de les eines més emprades pels pederastes.

### Pèrdua de privacitat

La webcam no només permet que els nostres fills vegin d'altres persones, sinó que deixa que la resta de la gent vegi els nostres fills.

A més a més, s'ha detectat en els últims anys que alguns programaris de control de càmeres web per-

meten que tercers puguin accedir i controlar a través d'Internet càmeres que no són de la seva propietat. Tenint en compte que les imatges que transmet la càmera web poden ser enregistrades per la persona que hi ha a l'altre costat (amic o atacant), el robatori d'imatges és un risc associat a la utilització d'aquests perifèrics.

Dins del context anterior, si un atacant pot activar la càmera web lliurement, podrà estudiar els costums dels nostres fills i conèixer aspectes de la vida privada de la família. Aquesta pèrdua de privacitat suposa facilitar informació sensible a possibles delinqüents (lladres, pedòfils,...).

Així mateix, el mal ús que puguin fer el propis menors de la webcam, fent accessibles imatges pròpies compromeses, els pot convertir en víctimes de fenòmens com el sexting, tractat en l'apartat següent.



# Algú ha penjat una foto compromesa de la meva filla a Internet.

## Descripció

L'altre dia navegava per la xarxa social quan vaig veure que uns coneguts de la meva filla havien penjat una foto seva que no em va agradar gens, i que estic segura que la meva filla no voldria veure publicada a Internet.

Quan li vaig preguntar a la meva filla què feia la seva foto a Internet, es va posar molt nerviosa, i finalment em va dir que no sabia com hi havia arribat, que aquesta era una foto privada que li va enviar al seu "ex" feia uns mesos quan encara eren parella.

## Amenaces

### *Sexting*

Les persones adultes han utilitzat tradicionalment els mitjans de comunicació disponibles per la difusió de continguts eròtics i pornogràfics.

Si pensem en els mitjans de comunicació disponibles avui en dia (vídeos, blocs, webcams, mòbils amb càmera i Internet...), i tenim en compte el comportament dels adolescents i preadolescents, arribem a un escenari on pot ser relativament comú l'intercanvi d'imatges i vídeos privats entre menors.

Aquest és el fenomen anomenat *sexting*, que consisteix en la generació de continguts íntims pels propis menors, mitjançant sons, fotos o vídeos propis, en actituds sexuals o sense roba. Els destinataris són habitualment parelles amoroses o sexuals, i no poques vegades es tracta també d'amics/amigues amb qui es duu a terme aquest intercanvi com si fos un simple joc.

Moltes vegades aquestes imatges surten del context on es varen fer i tornen en forma de greus conseqüències, fins i tot tràgiques.

La imatge o vídeo d'un/a menor que es difon per Internet sense control pot provocar greus danys emocionals i psicològics (ansietat, depressió, pèrdua d'autoestima, trauma, etc...), atès que el/la menor pot veure's humiliat/da públicament.

## Entabanament (*Grooming*)

Un/a menor que és fotografiat/da en actituds sexuals pot suggerir una precocitat sexual a certes persones a les quals els arribi la fotografia o vídeo, i provocar el desig d'una trobada que implicaria un possible abús o corrupció del/la menor o exposar-los a un xantatge de tipus sexual relacionat amb el denominat *grooming*. D'altra banda, la imatge o vídeo també pot ser objectiu de pederastes o pedòfils.

# El meu fill descarrega pel·lícules i programari de les xarxes P2P

## Descripció

El meu fill en sap molt, d'ordinadors. A casa nostra és qui s'encarrega de buscar el programari que necessitem, d'obtenir les pel·lícules que veiem el cap de setmana, o de passar-me best-sellers en PDF per quan estic avorrit amb l'ordinador i no tinc res per llegir.

També utilitza les xarxes P2P per descarregar aquests jocs i continguts audiovisuals que tant li agraden.

## Amenaces

## Infecció de l'equip informàtic

Quan instal·lem aplicacions que tenen un origen dubtós o venen amb informació poc fiable (per exemple, a les xarxes P2P), podem estar infectant el nostre ordinador o d'altres dispositius electrònics (com el mòbil) amb codi maliciós sense ni tan sols adonar-nos-en.

Si descarreguem l'última versió d'un determinat joc o sistema operatiu, no vol dir que aquest fitxer sigui el que diu ser pel nom de l'arxiu. Fins i tot encara que aparentment sigui el que diu ser, els fitxers poden incorporar codi maliciós que s'instal·larà a l'equip de l'usuari sense que aquest en tingui coneixement.

Algunes de les finalitats d'aquest codi maliciós poden ser:

- Destorbar l'usuari.
- Esborrar o apoderar-se de tota la informació de l'ordinador.
- Recopilar informació dels gustos de l'usuari per després bombardejar-lo amb campanyes de publicitat no sol·licitades.
- Obtenir informació de quins serveis utilitza l'usuari per impedir-n'hi l'accés.
- Controlar l'ordinador de l'usuari (juntament amb d'altres d'usuaris infectats com ell) per atacar infraestructures de tercers o enviar correu brossa.
- Robar les credencials bancàries o d'altres serveis web que l'usuari utilitzi (jocs en línia, xats, correu electrònic...).
- Activar perifèrics com la webcam per a la captació d'imatges privades, amb el conseqüent risc de vulneració de la intimitat i l'assetjament a menors.

## Exposició a continguts inadequats

Quan descarreguem pel·lícules o llibres en PDF, ningú ens pot assegurar que el nom del fitxer no l'hagin posat per enganyar-nos i fer que els usuaris el descarreguin.

El nostre fill podria trobar-se d'aquesta manera amb continguts pornogràfics, violents o no adaptats a la seva edat o amb programari maliciós que posés en risc les seves accions i les dels seus familiars a la xarxa.

## Distribució il·legal de material

Quan utilitzem sistemes P2P, al mateix temps compartim les coses que descarreguem, per això és important recordar que, en aquests casos, estarem posant a disposició il·legalment el següent material:

- El programari amb llicència privativa.
- Imatges o vídeos de pornografia infantil descarregats accidentalment.
- Documents privats d'organitzacions o persones físiques.
- Documents relacionats amb apologia del terrorisme.

En alguns casos, posar a disposició de tercers aquests continguts pot suposar la comissió d'un delicte i, per tant, pot tenir importants conseqüències legals tant per als menors com per als propis pares o tutors.

# Recomanacions

A continuació tractarem les recomanacions específiques per a les amenaces més comuns.

## Continguts inadequats

Amb els més joves és molt important acompanyar al menor en la navegació, per orientar-lo als llocs on pot anar i trobar el que busca, per estar al seu costat davant les pàgines que pugui trobar i ajudar-lo a comprendre què està fent i quines repercussions poden tenir determinades conductes a Internet. Estigueu al corrent de les novetats a Internet i compartiu-les amb els vostres fills.

Si el menor ha de navegar tot sol, caldrà tenir en compte algunes recomanacions:

- És fonamental que l'ordinador es trobi en un lloc comú de la casa, per poder supervisar de tant en tant el comportament del menor a Internet.
- Acordeu quines pàgines es poden visitar i reviseu junts l'historial de navegació que queda enregistrat a l'ordinador.
- Estigueu alerta amb les noves amistats que poden fer a les xarxes socials i parleu amb ells si veieu cap comportament estrany.
- Acordeu el temps de connexió i assegureu-vos que no descuiden les activitats escolars i que realitzen altres activitats (esport, quedar amb els amics, etc.).

A més a més, si considerem que algunes de les webs que pot trobar navegant no pot comprendre-les, o no volem que accedeixi a determinats continguts que no estan adaptats a la seva edat, podem comptar amb programari del tipus "Control Parental". Aquests sistemes permeten restringir la navegació a una llista de pàgines o bloquejar continguts que incloguin determinades paraules clau. Per evitar que el menor pugui desactivar-los, porten una configuració protegida per contrasenya.

Aquestes eines poden ajudar-nos en la nostra feina educativa, però mai poden ser un substitutiu complet de la tasca de tutoria dels pares.

En els sistemes P2P, com a adults, haurem de tenir cura amb el contingut compartit perquè poden ser vídeos amb continguts pornogràfics, nocius o la compartició dels quals pugui vulnerar drets de tercers (propietat intel·lectual, intimitat, etc.). Hem d'ensenyar als menors que els noms que tenen els fitxers no sempre són representatius del que contenen.

## Fraus

És habitual que els menors donin més credibilitat a la xarxa de la que donem els adults i, per tant, és més fàcil enganyar-los. És tasca dels pares, educadors i professors fomentar un esperit crític que posi en dubte el que troben a Internet i al món físic, i acostumar-los a comprovar la reputació dels llocs que visiten i de les fonts d'informació. Han de saber que no tot el que es diu o veu a la xarxa és cert.

Per evitar els atacs de pesca de credencials d'accés (*phishing*) és imprescindible no accedir mai a serveis fent click en enllaços que ens arriben en correus o enllaços que trobem a la xarxa. Una de les maneres més segures de procedir és escriure a mà les adreces originals i que coneixem del servei web al qual accedim habitualment,

descartant els missatges de correu electrònic que procedeixin d'emissors dubtosos i/o desconeguts.

Una altra bona pràctica que ens pot ajudar a no caure en aquesta xarxa d'enganys és desconfiar dels serveis quan ens demanen massa informació per a l'acció que volem portar a terme.

En el context de les compres per Internet, és perillós realitzar compres quan la informació no viatja protegida, és a dir, xifrada. Per tant, el primer que hem de comprovar és si l'adreça web on estem accedint comença per *http://* (comunicació no xifrada) o per *https://* (comunicació xifrada), descartant els serveis no xifrats. A més a més, també és important comprovar si el servei té associat un certificat digital, ja que aquest acredita la titularitat del servei. Actualment molts navegadors web mostren a la part superior (a prop d'on es troba l'adreça web) una barra de color verd quan el certificat és correcte i vermella quan el certificat és dubtós. Si fem clic a la icona del cadenat podrem comprovar qui ha generat aquest certificat i qui l'ha signat. Si no es correspon amb el que esperàvem, millor no continuar amb la compra. Així mateix, és convenient que només procedim amb compres per Internet en aquells llocs web que continguin les condicions de compra correctament exposades i ens n'informin detalladament durant el procés.

A més, un cop confiem en el venedor, és recomanable disposar d'una targeta de crèdit només per a compres a Internet, on disposem dels diners que ens costarà la compra o compres que vulguem realitzar. Aquesta acció pot estalviar-nos molts problemes limitant l'impacte d'un frau a la quantia disposada en aquest mitjà de pagament.



## Infecció de l'equip informàtic

Per estar protegits contra els virus i la resta de codi maliciós és important comptar amb mètodes preventius.

En primer lloc hem de tenir el nostre sistema operatiu i els programes que emprem correctament actualitzats. Això vol dir que haurem de configurar els avisos per saber quan hi ha actualitzacions disponibles pel nostre programari.

En segon lloc, haurem de comptar amb un antivirus i un programari antimalware, que hauran de ser actualitzats habitualment i establir anàlisis periòdics. És molt important que aquests programaris siguin descarregats de fonts fiables i instal·lats de forma voluntària i en cap cas després d'haver estat informats mitjançant elements publicitaris pel propi programari d'una suposada infecció massiva (estratègia emprada també per a la instal·lació de programari maliciós).

Una altra eina que ens pot ajudar a prevenir la infecció per codi maliciós és un tallafocs personal que ens permetrà determinar quines aplicacions tenen permís per sortir a Internet i enviar informació. Avui dia és tant important controlar que ningú no entri des de fora, com controlar que ningú no surti sense permís amb les nostres dades, claus, etc.

Les xarxes P2P, xats i xarxes socials són una de les principals fonts de virus a Internet i els creadors de codi maliciós pugen els seus fitxers amb noms molt atractius. Per tant, i aquesta pràctica és recomanable sempre, amb independència de per quin mitjà s'hagi obtingut el fitxer, qualsevol nou arxiu descarregat haurà d'escanejar-se amb l'antivirus actualitzat, prè-

viament a obrir-lo. Existeixen unes bones pràctiques addicionals per prevenir les infeccions, com ara:

- No descarregar fitxers de fonts no fiables.
- No obrir fitxers de fonts desconegudes o sospitoses.

Si hem estat víctimes d'un virus, una vegada desinfectat el sistema i per precaució, haurem de canviar les claus d'accés a tots els serveis online que utilitzem, especialment l'accés al correu electrònic, xarxes socials, jocs en línia, xats i banca electrònica.

## Ciberassetjament

Les recomanacions generals per prevenir el ciber assetjament són majoritàriament comunes amb altres riscos, per aquesta raó és tan important tenir-les present en l'educació del menor:

- Col·locar l'ordinador en un lloc no privat de la casa (per exemple, el menjador) i mai a l'habitació del/a menor.
- S'ha d'educar els menors perquè mai revelin les dades personals ni les claus de serveis online (xat, xarxes socials, correu electrònic, banca electrònica, etc...) a ningú, tampoc a "coneguts" d'Internet.
- Per evitar que un atacant pugui identificar els nostres fills com a víctimes potencials, hem d'ajudar els menors a escollir un pseudònim neutre a la xarxa, que no reveli l'edat ni el sexe, i a fer que comprengui la importància d'aquesta elecció.
- És important conèixer amb qui parlen a Internet i comentar amb ells la seva agenda de contactes, amics de xarxes socials, del xat...
- Establir un horari d'utilització de l'ordinador i Internet.
- Educar en l'ús responsable de la webcam i la difusió d'imatges i comentaris.

Controlar el perfil de la xarxa social i estudiar què diuen a Internet del menor.

Però tant important com això és el fet d'impulsar una comunicació permanent que els ajudi a parlar lliurement de les seves activitats a Internet, i que puguin conèixer-ne els riscos (explicant-los casos reals que podrem trobar a les fonts indicades al final del document) perquè en el cas de ser assetjats, no tinguin por d'acudir als seus pares per buscar ajuda i sàpiguen com actuar.

Els menors han de comportar-se amb tant respecte, responsabilitat i seny a Internet com en general en d'altres entorns. Han de comprendre que tot i que les coses passen a un espai virtual, Internet representa una mitjà on també resulta d'aplicació la normativa vigent i es poden prendre mesures legals i policials cap a qui actuï en contra d'altres o en perjudici de drets de tercers.

En cas de ser víctima de ciber assetjament és molt important:

- Demanar ajuda: pares, professors d'escola/institut, contactar amb els pares de l'agressor.
- Ser respectuós i no respondre a les provocacions.
- Comunicar als assetjadors que no li agrada el que li estiguin fent i intentar evitar-los.
- Notificar explícitament a l'assetjador que s'és menor d'edat.
- Guardar les proves de l'assetjament i de la notificació de la seva condició de menor d'edat.
- Tenir i deixar clar als assetjadors que es poden prendre mesures legals. En cas que l'assetjament

tingui certa intensitat i si els pares o tutors ho consideren procedent s'haurà de posar en coneixement dels organismes competents, com ara Mossos d'Esquadra, i/o prendre les accions legals que correspongui.

## Pèrdua de privacitat i dades personals

Els menors han de valorar què és informació sensible i privada, i conèixer els riscos associats a la seva presència en la xarxa o a la seva divulgació. Explicar casos reals que hagin passat a gent de la seva edat pot ajudar a fer arribar el missatge amb la força necessària.



Les dades privades no són només l'edat, el telèfon o informació d'aquest tipus, si no també fotografies i vídeos, per la qual cosa hem d'explicar la importància de la gestió de la pròpia imatge.

En el context de xarxes socials, per exemple, és molt important valorar adequadament a qui afegim com a amics, atès que a partir d'aquest moment poden accedir al que compartim. Es pot trobar més informació sobre els riscos de les xarxes socials a la nostra guia "*Guia per a l'ús segur de les xarxes socials*" Guia per l'ús segur de les xarxes socials, CESICAT, Febrer de 2010 [PDF] http://www.cesicat.cat/publicacions/Guies%20de%20xarxes%20socials.jsp.

Cal anar amb cura amb la informació que es proporciona als diferents serveis a la xarxa i, per tant, es recomana no omplir formularis que demanin dades de caràcter personal sense l'aprovació d'un adult. Sempre hauran de comptar amb els pares i rebre'n l'autorització si han d'enviar aquesta informació els menors de 14 anys, essent recomanable en la resta de menors.

Algunes bones pràctiques per a l'ús del correu electrònic que també poden ajudar als menors són:

- Disposar de dos comptes de correu, un per als amics i familiars i l'altre per als serveis online que ens demanen registre (xarxes socials, fòrums...)
- No contestar correus de desconeguts.
- Esborrar-los, atès que normalment serà publicitat no desitjada, intents d'engany (phishing) o contindran virus.
- No difondre cadenes de correu, i si es fa, no posar les adreces a la vista de tothom en el PER A o fins i tot en el camp CC.
- Utilitzar el camp BCC/CCO (còpia oculta) quan enviem el missatge a diversos destinataris per no difondre les adreces.
- Conèixer l'existència d'històries inventades que arriben per correu electrònic, i comprovar a Internet si el que ens expliquen ha estat verificat per no difondre mentides.
- No accedir a serveis fent click en els enllaços que ens envien, ja que poden estar manipulats i redirigir-nos cap a webs malicioses per robar les nostres credencials o infectar-nos.
- Posar nosaltres mateixos l'adreça al navegador.

En el cas de les càmeres web, hi ha una sèrie de recomanacions per prevenir els riscos que es deriven de la seva utilització:

- Col·locar l'ordinador en un lloc no privat de la casa i mai a l'habitació del/a menor.

- Instal·lar i mantenir actualitzat permanentment un bon antivirus i un bon tallafocs, per evitar el malware que pugui activar la càmera des de fora. No permetre mai l'ús d'una webcam en un equip on no estiguin instal·lats aquest tipus de programes.
- Considerar la possibilitat d'instal·lar un programa de control parental que incorpori control de la càmera web i de l'accés a webs que transmetin el que captura la webcam.
- Utilitzar càmeres amb llum pilot incorporada que ens indiqui si està gravant o no.
- Desconnectar la webcam (desendollant el cable de connexió amb l'ordinador) quan no s'utilitza.
- Si el menor té problemes psicològics o de conducta (depressió, risc d'autolesió, etc.) cal reconsiderar la conveniència d'aquest dispositiu tenint en compte pot ser especialment vulnerable o procliu a determinats usos.
- Si el teu fill o filla comencen a experimentar amb la sexualitat, poden veure's temptats a utilitzar la webcam amb finalitats sexuals: sexting, exhibicionisme, pornografia... Tingueu-ho en compte per establir les mesures de seguretat i de control parental.

Quan parlem amb els nostres fills, haurem d'educar-los en l'ús d'aquest dispositiu i que segueixin les següents recomanacions com a usuaris:

- Mai xatejar amb webcam amb persones que no coneguem fora d'Internet, ni usar serveis de videoxat aleatori.
- No transmetre imatges que, ara o en el futur, puguin ser utilitzades per fer-nos xantatge o fer-nos mal de qualsevol altra forma, per exemple xantatge de tipus sexual (veure grooming). Recordem que la tecnologia actual permet fer innumerables còpies iguals d'un mateix contingut.
- Quan no s'està utilitzant la webcam, considerar la possibilitat de desconnectar-la de l'ordinador. Si està incorporada al maquinari i no es pot desconnectar físicament, es pot tapar amb alguna cosa (un paper, una cinta adhesiva, un tros de tela...).
- No gravar sense permís el que altres persones emetin amb les seves webcams, i menys encara difondre-ho, ja que vulneraríem el dret a la seva intimitat i la seva imatge. No obstant això, si s'és víctima o testimoni d'algun delicte (assetjament, grooming, amenaces, etc.), es permet realitzar gravacions limitades a una finalitat exclusivament probatòria i per posar-les a disposició de les autoritats.
- No és recomanable que els menors d'edat realitzin emissions de càmera web a Internet, i en qualsevol cas mai sense coneixement dels seus pares.

La millor manera d'arribar als adolescents és amb el diàleg, amb exemples reals, explicant les notícies sobre el tema concret que ens preocupa, preguntant-los el seu parer, escoltant les seves històries i les seves inquietuds.

És crític que comptin amb els seus pares, i que si alguna cosa va malament, o alguna persona lliura informació sensible seva a d'altres persones, puguin tenir la confiança d'explicar-los el que ha passat.

## Robatori de credencials i suplantació d'identitat

Si voleu disminuir aquests riscos, és important assegurar-vos que els menors coneixen i segueixen una sèrie de bones pràctiques:

- No reutilitzeu una contrasenya d'accés per accedir a entorns independents com podria ser el correu electrònic personal de l'usuari i la xarxa social.
- En cas que utilitzeu una mateixa contrasenya en diferents entorns, si teniu la mínima sospita que la contrasenya es pot haver vist compromesa, canvieu-la per una de nova en tots aquells serveis telemàtics on l'estàveu utilitzant. Fins i tot encara que no tinguem sospites, és convenient canviar-la periòdicament.
- Quan feu servir dispositius mòbils, de tipus smartphone, que us permetin accedir a la vostra xarxa social, heu de configurar l'aplicació del dispositiu mòbil de tal manera que sol·liciti un usuari i una contrasenya d'accés cada vegada que es vulgui fer servir. Així, si perdeu el dispositiu mòbil, qui el trobi no tindrà accés lliure al vostre perfil privat.
- Molts proveïdors de serveis de correu electrònic i xarxes socials tenen la funcionalitat de registrar els accessos que es realitzen al nostre compte. És recomanable revisar aquests accessos de tant en tant per vigilar que no hi hagi connexions alienes al menor, des de llocs sospitosos o fora dels horaris acordats o habituals.
- Si sospiteu que algú podria estar utilitzant aquest servei sense el seu consentiment i suplantant la seva identitat, heu de posar-vos en contacte amb el proveïdor del servei mitjançant els mecanismes que aquest tingui a l'abast de l'usuari i denunciar el cas. Un cop fet això, si cal, aneu al Cos de Mossos d'Esquadra i realitzeu la denúncia corresponent o envieu-los un correu a *mossosdti@gencat.cat*, adreça específica per informar sobre delictes en tecnologies de la informació. En cas que es vulgui emprendre mesures legals, és molt important conservar la major quantitat d'evidències possibles relatives a la suplantació.

## Exposició a pederastes i pedòfils

Tant a la missatgeria instantània com a les xarxes socials i als fòrums és molt important transmetre als menors que cal, per precaució:

- Escollir un pseudònim neutre a la xarxa, que no reveli l'edat ni el sexe, i comprendre la importància d'aquesta elecció.
- En xats i missatgeria instantània, no contactar amb persones que no coneguin directament a la vida física i, per descomptat, no compartir cap contingut amb ells, especialment informació personal, imatges o vídeos.
- No han de quedar amb gent que hagin conegut primer per Internet i si ho fan, ha de ser sempre en un lloc públic i en presència d'un adult preferiblement i si no, acompanyats de diversos amics.
- Han de tractar amb respecte les altres persones, com els agradaria que els tractessin.

En qualsevol cas, la comunicació és molt important i els menors han de poder comptar amb els pares si alguna cosa els molesta.

D'altra banda, és important tenir en compte les accions que realitzen els pederastes i pedófils per obtenir els continguts, i moltes d'elles passen per fer xantatge o enganyar els menors (veure *grooming* o *sexting*) per obtenir cada vegada continguts amb una càrrega sexual superior. És important que els menors siguin conscients dels usos i difusió que poden tenir imatges o vídeos en què ells puguin aparèixer en determinades actituds o situacions, encara que en el nostre context semblin continguts innocents o inofensius

## *Sexting*

Davant el *sexting*, és molt important reconèixer el problema i que també pot afectar els nostres fills. De la mateixa manera que sabem que quan tenen una parella el sexe és una possibilitat, sabem que la combinació d'adolescència i les noves tecnologies pot comportar altres riscos. És important conèixer què els pot passar, però també què poden arribar a fer ells a d'altres persones.

La comunicació és d'una gran importància, i si és veritat que necessitem parlar amb ells sobre la seva sexualitat i les seves relacions, hem de transmetre'ls que les imatges i vídeos que s'envien a través d'Internet o dels mòbils no són anònims ni privats, i que més endavant altres persones que siguin importants en la seva vida podrien trobar-les amb conseqüències negatives (nova parella, companys de treball, pedòfils...).

A més a més, existeixen portals web dedicats a recopilar i difondre aquestes imatges de caire sexual, obtenint ingressos per publicitat de la gent que els visita. D'altra banda, han de saber que la difusió o possessió d'imatges sense roba d'un/a menor d'edat pot implicar un delicte de pornografia infantil. Si reben alguna d'aquestes imatges, han d'avisar a un adult per posar-ho en coneixement dels Mossos d'Esquadra.

Els menors han de comprendre que la imatge d'una persona no pot ser utilitzada sense el seu permís, i es considera una dada de caràcter personal protegida per la Llei. Rebre o fer-li una foto a una persona no ens dóna dret a difondre-la. Són coses diferents: tot i tenint permís per fer-la, no implica poder passar-la a tercers sense que això pugui vulnerar els drets d'aquella persona.

També és important que els nostres fills comprenguin que no han de participar activament, ni riure davant d'aquestes situacions, ni quedar-se parats davant aquests fenòmens.



La millor manera d'arribar als adolescents és amb el diàleg, amb exemples reals, explicant notícies sobre el tema que ens preocupa, preguntant-los els seu parer, escoltant les seves històries i les seves inquietuds. És crític que comptin amb els seus pares o tutors, i que si alguna cosa va malament, o alguna persona lliura informació sensible seva a d'altres persones, puguin tenir la confiança per explicar què ha passat.

Pactar uns límits davant l'ús d'Internet, i que l'ordinador, les càmeres web i els mòbils s'hagin d'utilitzar en un horari determinat i en un lloc no privat de la casa, són recomanacions que poden ajudar a prevenir aquest comportament.

D'altra banda, conèixer amb qui parlen, qui són els seus amics a la xarxa, amb qui s'envien fotografies, pot ajudar a valorar la situació i protegir els menors davant situacions d'abús.

## Entabanament (*Grooming*)

Amb l'objectiu de prevenir els casos d'entabanament de menors o grooming haurem d'educar els nostres fills perquè respectin unes normes bàsiques de privacitat a Internet. Els pares o educadors haurem de posar en pràctica també aquestes recomanacions:

- Col·locar l'ordinador en un lloc no privat de la casa (per exemple, el menjador) i mai a l'habitació del/a menor.
- Instal·lar i mantenir actualitzat permanentment un antivirus i un tallafocs per evitar la infecció de l'equip i una posterior pèrdua de claus d'accés a serveis online (xat, xarxes socials, correu electrònic, banca electrònica, etc...) en favor de delinqüents de grooming.
- Evitar la instal·lació d'una webcam a l'ordinador i, en cas de fer-ho, restringir la seva utilització mitjançant programes de control parental, claus d'accés o d'altres mitjans físics si es considera adient. També són interessants els consells d'un apartat anterior (6.5 Pèrdua de privacitat i dades personals).
- No hauran de revelar les dades personals ni les claus d'accés als serveis online (xat, xarxes socials, correu electrònic, banca electrònica, etc...) a ningú, tampoc a "coneguts" d'Internet, per què poden servir per iniciar el xantatge.
- Ajudar-los a escollir un pseudònim neutre a la xarxa, que no reveli la seva edat ni sexe, i a fer que comprenguin la importància d'aquesta elecció.
- És important conèixer amb qui parlen a Internet, i comentar amb ells la seva agenda de contactes, amics de xarxes socials, del xat...
- No omplir formularis que demanin dades de caràcter personal sense l'aprovació d'un adult. Sempre hauran de comptar amb els pares i rebre'n l'autorització si s'ha d'enviar aquesta informació.
- No veure's amb ningú que hagin conegut a Internet sense coneixement del pares, i en qualsevol cas, sempre en públic i amb altres persones.
- No establir relacions a Internet amb ningú que no coneguin en el medi físic.

Com hem comentat abans, la millor manera d'arribar als adolescents és amb el diàleg, explicant exemples reals, i parlant de notícies relacionades amb el tema que ens preocupa, preguntant-los els seu parer, escoltant les seves històries i les seves inquietuds.

És crític que comptin amb els seus pares, i que si són víctimes d'un xantatge d'aquest tipus, puguin tenir la confiança per explicar-los què ha passat o està passant.

## Distribució il·legal de material

Es recomana utilitzar programari que s'hagi comprat legítimament o programari lliure i gratuït: es poden trobar moltes alternatives al programari propietari. Cal tenir en compte que descarregar i difondre programari protegit sense els drets i les autoritzacions pertinents pot ser constitutiu d'una infracció penal.

Pel que fa a altres continguts que puguin revestir el caràcter d'il·legals (imatges compromeses de tercers, continguts nocius) caldrà que analitzem el seu origen per determinar-ne la seva licitud i, en cas de dubte, informar-nos en fonts fiables o comunicar-ho a organismes competents en la matèria que ens puguin orientar.

En cas d'haver descarregat per error qualsevol tipus de material il·legal (programari, pornografia infantil...),

és recomanable comunicar als fòrums que aquells arxius no eren el que deien ser i realitzar una còpia dels fitxers en un dispositiu extraïble, per posar-ho en coneixement de la Unitat Central de Delictes Informàtics dels Mossos d'Esquadra o del CESICAT en cas de ser programari maliciós. En aquest cas, convé aportar el material tal com va ser descarregat, així com tota la informació sobre la font que els va conduir fins a l'enllaç i el programa que van utilitzar.

# Conclusions

Internet ofereix un univers de possibilitats, tant als adults com als menors, si bé és cert que de la mateixa manera que eduquem els nens i adolescents perquè siguin responsables a la vida real, hem de realitzar el mateix esforç per què puguin experimentar la xarxa amb seguretat.

Internet disposa d'infinitat de continguts, serveis, informació, etc. i deixar que els menors naveguin sols a Internet pot resultar tan perillós com deixar-los sols al mig del carrer.



Hem vist els principals riscos als quals estan exposats els menors a Internet i com amb la nostra ajuda podem minimitzar la seva exposició a aquests riscos. Concloem aquesta guia amb una sèrie de recomanacions bàsiques de seguretat a Internet que haurem de tenir sempre presents:

- Parlar amb els vostres fills sobre Internet i les seves experiències en aquest entorn. Establir una relació de confiança que afavoreixi que el menor acudeixi als pares davant un problema a Internet. Comentar la importància de la seguretat a la xarxa i ensenyar-los els conceptes bàsics.
- Establir normes clares per la utilització d'Internet i els telèfons mòbils, i unes conseqüències clares i proporcionals en cas d'incompliment.
- Llegir sobre els últims perills que es trobaran els menors a la xarxa i, en la mesura del possible, familiaritzar-se amb les eines i serveis que els menors empren (xarxes socials, serveis de blogging, fòrums, etc.).
- Conèixer com gasten el temps a la xarxa.
- Ubicar l'ordinador i qualsevol altre dispositiu amb accés a Internet en un lloc comú, com per exemple al saló o menjador.
- Mantenir el sistema operatiu actualitzat. Instal·lar i mantenir actualitzats antivirus, antimalware i tallafocs.
- Establir mesures de control parental en funció de l'edat (Control Parental, consentiment parental, comprovació d'edat i bloqueig de continguts).
- Conèixer els sistemes proporcionats per l'operador d'Internet i pel proveïdor del sistema operatiu que ens donen servei.
- Comprovar habitualment la pàgina web o el perfil del menor.
- Conscienciar el menor sobre bones pràctiques a l'hora de fer servir contrasenyes: no s'han de difondre, s'han de guardar a llocs segurs, no s'han de reutilitzar.
- Ensenyar al menor què és la privacitat. No ha d'utilitzar el seu nom complet, ni donar informació personal (telèfon, escola,...) ni compartir contrasenyes. Cal ensenyar-los a crear contrasenyes segures per tal de garantir, al màxim possible, la integritat i seguretat dels serveis que utilitzem.
- Ensenyar els perills que implica pujar fotografies o altres tipus de continguts a la web.
- Explicar que no han de quedar amb gent que hagin conegut primer per Internet, i evitar els desconeguts a la xarxa.
- Ensenyar que han de respectar els altres usuaris de la xarxa.

# Glossari de termes

**Antimalware:** Programari especialitzat en identificar i eliminar codi maliciós.

**Ciberbullying:** Consisteix en l'ús de mitjans de comunicació com ara correu electrònic, xarxes socials, blogs, missatgeria instantània, missatges de text, telèfons mòbils, entre d'altres, per assetjar un individu o grup, mitjançant atacs personals o atacs que atemptin contra la seva imatge i reputació.
Es tracta d'una situació en la qual generalment l'assetjador i la víctima comparteixen un entorn social pròxim, normalment companys de l'escola o institut. L'agressor o agressors utilitzen la xarxa i els mitjans tecnològics per disposar de més contingut i estendre la humiliació a molta més gent.

**Grooming:** S'utilitza per descriure les pràctiques online d'alguns adults per guanyar la confiança d'un o una menor, fingint empatia i estima (fins i tot fent-se passar per un altre menor), amb l'objectiu d'aconseguir inicialment imatges amb una certa càrrega sexual amb les quals iniciar un xantatge de tipus sexual.

**Malware o codi maliciós:** Es considera qualsevol codi informàtic destinat a realizar accions fraudulentes. Es considera codi maliciós els virus i cucs informàtics, els troians (que permeten fer-se amb el control d'una màquina), etc.

**Phishing:** També conegut com "pesca electrònica", consisteix a suplantar una persona o empresa de confiança o enganyar respecte de la identitat pròpia (els mitjans més utilitzats són el correu electrònic o trucades de telèfon) per tal d'apropiar-se dels identificadors d'usuari i de les contrasenyes associades a serveis en línia o altres informacions sensibles per guanyar accés a un sistema. Si aconsegueixen la informació, poden entrar a comptes bancaris, correu electrònic, obtenir informació confidencial o bé, treure'n un benefici econòmic directe. Les pràctiques més habituals utilitzen webs de bancs, caixes d'estalvis, institucions públiques confiables (Hisenda, Guardia Civil, etc.) o proveïdors de serveis a Internet (correu electrònic, serveis de pagament…).

**Sexting:** Generació de continguts íntims per part dels propis menors, mitjançant sons, fotos o vídeos propis, en actituds sexuals o sense roba. Els destinataris són habitualment parelles amoroses o sexuals, i no poques vegades es tracta també d'amics/amigues amb qui duen a terme aquest intercanvi com si fos un simple joc.

# Referències i enllaços web

S'ha utilitzat com a referència en l'elaboració de l'actual guia:

- **[1] Menores en la red ¿Un juego de niños?, Panda Security, Desembre de 2008 [PDF]**

http://www.pandasecurity.com/NR/rdonlyres/4AB3AA58-DA59-494D-B0ED-B218D-7CA4DB1/0/Guiamenoresenred.pdf

- **[2] Segundo estudio sobre el nivel de seguridad de menores en la Red, Panda Security, Juny de 2010 [PDF]**

http://prensa.pandasecurity.com/wp-content/uploads/2010/06/Estudio-de-Menores-en-la-Red-Nacional2010.pdf

- **[3] Guía sobre ciberbullying i grooming, INTECO, Maig de 2009 [PDF]**

http://www.inteco.es/Seguridad/Observatorio/manuales_es/guiaManual_groming_ciberbullying

- **[4] Guia per l'ús segur de les xarxes socials, CESICAT, Febrer de 2010 [PDF]**

http://www.cesicat.cat/publicacions/Guies%20de%20xarxes%20socials.jsp

- **[5] Guia de menores en internet para padres y madres, INTECO, Desembre de 2008 [PDF]**

http://cert.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiapadresymadres.pdf

- A la web es pot trobar informació rellevant relacionada amb la matèria desenvolupada en aquesta guia:

**Internet amb seny (CESICAT)**

http://internetambseny.cesicat.cat/

**Menores en Oficina de Seguridad del Internauta (INTECO)**

http://menores.osi.es/

- **On Guard Online (Govern d'Estats Units d'Amèrica)**

http://www.onguardonline.gov/topics/net-cetera.aspx

- **Protégeles.**

http://www.protegeles.com/

- **Pantallas Amigas.**

http://www.pantallasamigas.net

http://www.internet-grooming.net

http://www.sexting.es

http://www.ciberbullying.net

http://www.privacidad-online.net/

http://www.e-legales.net/

http://www.cuidadoconlawebcam.com

- **Proteja a su familia (Microsoft)**

http://www.microsoft.com/spain/protect/family/default.mspx

- **Los riesgos del flirteo 2.0, El Pais, Febrer de 2010.**

http://www.elpais.com/articulo/sociedad/riesgos/flirteo/elpepusoc/20100222elpepisoc_7/Tes

- **¿Búscas una suite de seguridad (HIPS, Firewall, etc) para tu Windows?**

http://www.securitybydefault.com/2010/05/buscas-una-suite-de-seguridad-hips.html

## Eines

### Control Parental

- **WINDOWS PARENTAL CONTROLS: Control parental al sistema operatiu de Microsoft.**

http://www.microsoft.com/spain/protect/products/family/onecarefamilysafety.mspx

- **APPLE PARENTAL CONTROLS: Control parental al sistema operatiu de Apple**.

https://www.apple.com/findouthow/mac/#parentalcontrols

- **CYBER PATROL: Programari complet de control parental.**

http://www.cyberpatrol.com/

- **PARENTAL CONTROL BAR – Control parental integrat en el navegador.**

http://www.parentalcontrolbar.org/

- **FAMILY SHIELD: Servei DNS específic per la família que permet configurar el filtrat web i ens protegeix de webs malicioses. Només s'han de canviar els servidors DNS a la configuració d'Internet. Servei gratuït ofert per OpenDNS.**

http://www.opendns.com/familyshield

## Antivirus

- **AVAST: Antivirus Gratuït.**

http://www.avast.com

- **AVG: Antivirus Gratuït.**

http://free.avg.com

- **NOD32**

http://www.eset.es/productos/eset-nod32-antivirus

- **MCAFEE**

http://www.mcafee.com/ES/

- **MICROSOFT SECURITY ESSENTIALS: Antivirus gratuït.**

http://www.microsoft.com/es-es/security_essentials/default.aspx

- **PANDA**

http://www.pandasecurity.com/spain/

- **SYMANTEC**

http://es.norton.com/antivirus/

- **TREND MICRO**

http://es.trendmicro.com

## Antimalware

- **MALWAREBYTES ANTIMALWARE**

http://www.malwarebytes.org/

- **LAVASOFT AD-AWARE**

http://www.lavasoft.com/

- **SPYBOT**

http://www.safer-networking.org/es/home/index.html

## Tallafocs

- **MICROSOFT WINDOWS FIREWALL: Tallafocs integrat als sistemes operatius de Microsoft.**

**COMODO FIREWALL: Tallafocs gratuït.**

http://personalfirewall.comodo.com/

- **ONLINE ARMOR: Tallafocs gratuït.**

http://www.online-armor.com/

- **CHECKPOINT ZONEALARM FIREWALL**

http://www.zonealarm.com/security/es/home.htm?lid=es

## Recursos de suport on-line

### Antivirus online

- **PANDA – Servei antivirus online de PANDA Software.**

http://www.pandasecurity.com/spain/homeusers/solutions/activescan/

## Anàlisi d'arxius i webs malicioses

- **VIRUSTOTAL – Servei d'antivirus online que treballa amb 43 antivirus diferents per l'anàlisi d'arxius sospitosos o URLs.**

**Ofert per HISPASEC.**

http://www.virustotal.com

- **THREATEXPERT – Servei gratuït d'anàlisi de malware.**

http://www.threatexpert.com/

- **ANUBIS – Servei gratuït d'anàlisi de malware ofert per ISECLAB.**

http://anubis.iseclab.org/

- **WEPAWET – Servei d'anàlisi de malware basat en web ofert per ISECLAB.**

http://wepawet.iseclab.org/

## Llibreta de contactes en cas d'incident

- **Mossos d'Esquadra**

E-mail: mossosdti@gencat.cat

Telèfon:: 012

http://www.gencat.cat/mossos

- **CESICAT**

E-mail: cert@cesicat.cat

Telèfon: 902112444

http://www.cesicat.cat

cesicat

Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat