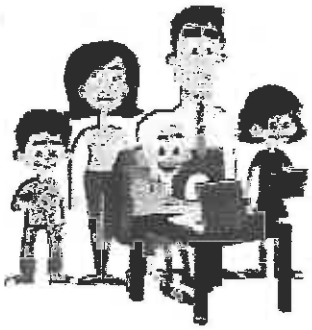


L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS SOBRE INTERNET PER A PARES I MARES

AMICS A LA XARXA

Ajudem els nostres fills/filles a desenvolupar els coneixements i les habilitats socials necessaris per prendre decisions assenyades sobre la gent que coneixen en línia.

1 MASSA BONIC PER SER CERT!

Digueu als vostres fills que cal anar en compte amb les persones que són excessivament amables a les xarxes i que, per exemple, semblen tenir exactament els mateixos gustos que nosaltres per la música, les pel·lícules, els actors, etc. Un assetjador a la xarxa té l'objectiu de guanyar-se la confiança dels nens. Els assetjadors, per tant, seran molt amables amb ells al principi i sovint pretendran ser la seva "ànima bessona".

2 CONTRADICCIÓ EN LES HISTÒRIES

Aconselleu als vostres fills d'estar al cas de les inconsistències o les contradiccions en les històries dels seus amics a la xarxa. Per exemple, s'ha de tenir molt present quan un dels "amics" resulta, de sobte, ser molt més gran del que va dir al principi. Si aquest és el cas, el millor és aturar i tallar en sec tota comunicació.

3 SEGUEIX LA TEVA INTUÏCIÓ

Expliqueu als vostres fills que en cas de tenir la més mínima sospita, no dubtin a comentar-ho amb un adult de confiança.

4 EL DELICAT TEMA DEL SEXE

Les investigacions han demostrat que els adolescents que parlen de sexe amb estranys a la xarxa tenen més probabilitats d'entrar en contacte amb els assetjadors sexuals. Aquests assetjadors intenten que disminueixi la inhibició que el vostre fill pugui tenir per anar introduint gradualment el contingut sexual en les converses. Digueu als vostres fills que si estranys a la xarxa aprofiten qualsevol excusa per parlar de contingut sexual cal avisar un adult de confiança i aturar i tallar la comunicació en sec amb aquestes persones.

5 CONFIA EN EL CONSELL D'UN ADULT

Assegureu-vos que els vostres fills sàpiguen que sempre poden comptar amb un adult de confiança si se senten amenaçats per alguna persona o si se senten incòmodes per alguna cosa que han trobat a la xarxa. **Ajudeu-los a reportar qualsevol preocupació a la policia o al lloc web en qüestió.**

6 TROBADES AMB AMICS FORA DE LA XARXA: MARQUEU NORMES

Si els vostres fills volen conèixer personalment amics de la xarxa, establiu un acord de normes estrictes que cal seguir a la primera trobada. Descarregueu el full de consells "Trobada amb estranys".

MÉS INFORMACIÓ?

OnGuard Online:
www.onguardonline.gov

INHOPE:
www.inhope.org

En trobareu més a la xarxa ***Insafe***
www.saferinternet.org
www.internetsegura.cat

L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

BLOQUEIG

Mentre els vostres fills estan en línia poden trobar-se amb webs inapropiats que mostren elements emergents (*pop-ups*) i anuncis. És important ensenyar els fills com poden eliminar aquests elements emergents. Saber com bloquejar un lloc web pot preservar-los de ser la diana dels emissors de correu brossa (*spammers)* que utilitzen programes publicitaris i *pop-ups* per atacar el vostre ordinador. Intenteu visitar alguns dels seus llocs favorits per esbrinar si comparteixen les dades personals i si hi ha presència d'anuncis inadequats. Hi ha dos camins que poden ajudar a controlar el contingut que els vostres fills veuen en línia.

1 FILTRE I BLOQUEIG

Podeu optar per filtrar i bloquejar qualsevol contingut que considereu inapropiat per als vostres fills. Podeu impedir l'accés a certs llocs web, paraules i imatges per tal d'evitar que els nens es trobin amb contingut inapropiat. Depenent del nivell de seguretat requerit, podeu ajustar el vostre navegador d'Internet o usar programes de filtrat d'Internet.

La configuració del navegador d'Internet és la manera més fàcil de bloquejar certs llocs web. Si feu servir *l'Explorer*, per exemple, aneu a la barra superior d'opcions i seleccioneu el menú 'Eines'. Seleccioneu 'Opcions d'Internet' i busqueu la pestanya 'Privadesa' de la fitxa. Dins la finestra de la privadesa, seleccioneu el botó anomenat 'Llocs' i ja podeu omplir l'adreça del lloc web que es desitja bloquejar. Aquest procés pot ser diferent per a altres navegadors (*Chrome* o *Firefox*), però a la xarxa es pot trobar fàcilment com fer-ho. Tingueu en compte que canviar la configuració del navegador no és sempre 100% efectiu, i és possible que considereu millor comprar un programari addicional de filtrat i bloqueig que ofereixi opcions més àmplies de control parental. Per ajudar-vos a prendre una decisió ben informada sobre quina eina s'ajusta millor a les vostres necessitats, podeu consultar el web SIP Bench II de la Comissió Europea. Hi trobareu els resultats d'un estudi útil sobre eines de control parental.

2 MONITORATGE

És possible que preferiu no limitar l'activitat en línia dels vostres nens, però que decidiu supervisar el que fan a Internet. D'aquesta manera els nens són lliures per descobrir el món en línia pel seu compte, però els podeu supervisar i podeu intervenir quan sigui necessari. Depenent del nivell de monitoratge és possible fer un seguiment i saber la naturalesa dels llocs web visitats, veure els posts escrits a les xarxes socials i als xats, llegir a l'instant converses de missatgeria i fins i tot escanejar els missatges de correu electrònic dels fills.

Mentre que els pares no sempre podeu mantenir una revisió diària de l'activitat en línia dels vostres fills, la majoria de programes de monitoratge ofereixen la possibilitat de rebre una alerta quan es visita un determinat lloc web o es publica un contingut específic. Les eines de monitoratge normalment no es proveeixen amb el navegador, de manera que cal comprar-les.

Independentment de l'opció de programari que trieu per monitorar i/o filtrar, també cal decidir si es fa amb o sense el coneixement del vostre fill. És important sospesar els beneficis i els desavantatges d'un cert nivell de control i tenir en compte la personalitat i l'edat del vostre fill. Els nens petits són els més vulnerables, ja que en general no tenen les habilitats socials per detectar certs perills quan estan en línia i es poden alterar/sorprendre més fàcilment quan es troben amb informació perjudicial. Quan es tracta dels joves, és sensat prendre mesures per bloquejar els continguts no desitjats.

Encara que el control parental podria funcionar bé per als més petits, la situació és diferent per als adolescents. Amb més experiència a la xarxa, poden desactivar més fàcilment els controls instal·lats. D'altra banda, els adolescents estan constantment lluitant per la independència i la llibertat a la recerca del seu camí. El monitoratge secret o el bloqueig d'informació sense el seu consentiment pot acabar tenint l'efecte contrari. Cal ensenyar els adolescents com es pot responsabilitzar 'la personalització de la seva experiència a Internet' mitjançant el bloqueig de llocs web i de continguts no desitjats. Doneu-los les habilitats necessàries per ser bons ciutadans digitals i navegar pels webs de forma segura i de manera còmode.

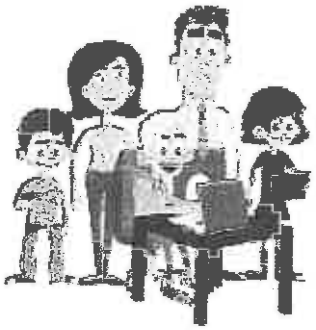
MÉS INFORMACIÓ?

SIP Bench II www.sipbench.eu

En trobareu més a la xarxa Insafe

www.saferinternet.org

www.internetsegura.cat



L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

LA INFORMACIÓ PERSONAL

Qualsevol informació que posem a la xarxa romandrà allà per sempre més a la vista de tot el món: és quasi impossible esborrar-la! La qual cosa vol dir que és important considerar seriosament allò que pares, mares i fills poden o no desvetllar sobre la seva intimitat a Internet. Cal ensenyar els vostres fills quines informacions són i han de ser privades i també ajudar-los a identificar les situacions on poden compartir detalls privats i les situacions on no han d'explicar absolutament res.

1 REVELAR LA IDENTITAT

El nom del vostre fill/a, el número del seu DNI, l'adreça i el seu número de telèfon són informacions molt valuoses per als assetjadors sexuals i els criminals a la xarxa. S'ha de recomanar als fills que només proporcionin aquests tipus de dades als amics en qui confien. Això evitarà, fins a cert punt, que es converteixen en la víctima d'un assetjador sexual a la xarxa i limitarà la possibilitat d'esdevenir víctima de ciberassetjament.

2 REVELAR INFORMACIÓ SOBRE ON ENS TROBEM

Parleu amb els vostres fills, a l'edat i en el moment adequats, del fet d'evitar donar informació sobre la seva localització. Aquesta precaució va molt més enllà de no donar l'adreça, ja que també suposa ocultar detalls com ara a quina escola van i on i quan fan activitats extraescolars. És també important advertir-los de què no han de parlar sobre els seus plans de vacances o viatge, o de quan estaran sols a casa. Aquesta informació és el millor regal per als lladres!

3 SERVEIS BASATS EN LA LOCALITZACIÓ

Un servei basat en la localització utilitza la informació de la posició geogràfica d'un dispositiu mòbil per oferir serveis d'informació i entreteniment relacionats amb la localització de l'usuari. És important comprovar totes les aplicacions actives en el telèfon mòbil del vostre fill/a i decidir si s'han de desactivar o no.

4 INFORMACIÓ FINANCERA

Informeu el vostre fill/a que mai s'ha de mostrar a Internet cap tipus d'informació financera, com per exemple el número d'un compte bancari.

5 CONTRASENYES

Advertiu els vostres fills que al compartir les seves contrasenyes amb altres persones els hi poden donar accés a la seva informació personal. Malgrat que es tracti de bons amics, és millor no fer-ho i estalviar-se problemes en el futur.

6 MISSATGES, FOTOS O VÍDEOS SEXUALMENT EXPLÍCITS

Tots sabem que els fills creixen ràpid, la qual cosa inclou l'exploració de la seva sexualitat, a vegades abans que nosaltres, i com a pares i mares hem d'estar preparats per a això. Recomaneu de forma taxativa als vostres fills que evitin crear i compartir fotografies, vídeos o missatges sexualment explícits d'ells (o d'altres), ja que poden aparèixer fàcilment a Internet i quedar a la vista de tothom. A més de posar en perill la seva reputació i les seves amistats, podrien estar infringint la llei si creen, transmeten o guarden aquest tipus de missatge o imatge.

7 FOTOS O VÍDEOS COMPROMESOS I COMENTARIS FERIDORS O INSULTANTS

Animin els fills perquè s'aturin a pensar abans de publicar res a Internet. El comportament a Internet de les persones, incloent el que publiquen, determinarà la seva reputació en línia. Recordeu, el que ara publiquin en línia roman allà per sempre. Per evitar decepcions en el futur (universitat, formació superior, món laboral, etc.) és millor mantenir una reputació positiva.

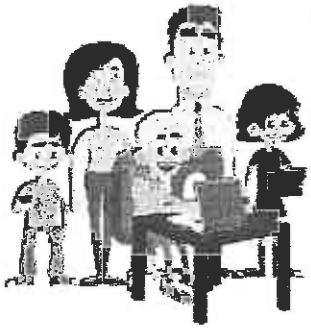
MÉS INFORMACIÓ?

En trobareu més a la xarxa Insafe

www.saferinternet.org

www.internetsegura.cat

ins fe European Schoolnet Centre Internet



L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

JOCS EN XARXA

Els jocs en xarxa poden tenir una influència positiva sobre el desenvolupament dels vostres fills. Tot i això, és essencial aconseguir un equilibri adequat entre el joc i les altres activitats diàries. És també recomanable vigilar el contingut dels jocs que utilitzen i comprovar que són segurs. Per confirmar que els jocs siguin adequats per als vostres fills, per què no els proveu primer abans?

DADES SOBRE EL JOC EN XARXA

1 El 83% dels nens de tot el món juguen en xarxa.

2 Segons un estudi d'EU Kids Online, jugar és la **segona activitat preferida en xarxa.** Sorprenentment, "fer els deures" és la primera!

3 Els jocs requereixen que **els** nens actuïn segons unes regles i unes instruccions, per la qual cosa poden, de fet, **augmentar la seva capacitat per a l'autodisciplina i l'autonomia.**

4 Un de cada quatre menors d'11 a 16 anys afirma que els jocs amb la qualificació **"madur" són els seus preferits.**

5 **No hi ha proves** que demostrin que els videojocs violents produeixin un **augment durador de l'agressivitat o la violència.**

JOCS ADEQUATS PER A CADA EDAT

Fins i tot els jugadors sense experiència poden escollir els jocs adequats gràcies al sistema de qualificació per edats **Pan-European Game Information (PEGI),** que es fa servir actualment en la majoria de països d'Europa. L'etiqueta PEGI apareix a l'anvers i el revers dels jocs per a ordinador en suport físic, proporciona una descripció del contingut i indica un dels nivells d'edat següents: 3, 7, 12, 16 i 18.

Les etiquetes descriptives expliquen perquè un joc ha rebut una qualificació d'edat determinada. Hi ha vuit paraules descriptives: violència, llenguatge inapropiat, por, drogues, sexe, discriminació, apostes i joc amb altres persones. Els nivells d'edat permeten que els pares i les mares sapigueu si el contingut del joc és adequat per als vostres fills, però no tenen en compte el nivell de dificultat del joc ni las habilitats necessàries per jugar-hi.

Amb l'increment del **joc en línia** el PEGI ha creat recentment un logotip en línia, que qualsevol proveïdor de jocs pot mostrar sempre que el lloc web compleixi amb els requisits fixats al **PEGI Online Safety Code (POSC).** Aquests requisits inclouen l'obligació que el lloc web no inclogui continguts il·legals o ofensius, ni enllaços inapropiats creats pels usuaris, i que compti amb mesures que protegeixin els menors mentre juguen.

CONSELLS PER JUGAR EN XARXA

- Limiteu el temps que passen els vostres fills jugant.
- Trobeu un equilibri saludable entre el joc i altres activitats, com quedar amb amics.
- Decidiu si el contingut d'un joc és adequat per al vostre fill/a consultant els símbols PEGI.
- Establiu regles estrictes sobre realitzar compres mentre juguen en xarxa.
- Quan juguen en xarxa a jocs per a molts jugadors, **assegureu-vos** que els vostres fills no comparteixen informació personal.
- Proveu els jocs vosaltres mateixos i si és possible jugueu amb el vostre fill/a. Potser descobriu que us agrada!

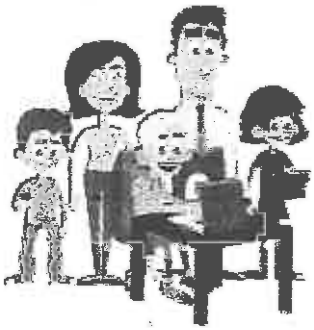
MÉS INFORMACIÓ?

PEGI:
www.pegi.info/es/
www.pegionline.eu/

Good Gaming Guide:
www.pegi.info/en/index /id/media/pdf/241.pdf

Videogamers a Europa 2010: Interactive Software Federation Europe:
www.isfe.eu/sites/isfe.eu/files/video_gamers_in_europe_2010.pdf

En trobareu més a la xarxa Insafe
www.saferinternet.org
www.internetsegura.cat



L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

LA PRIVACITAT A LES XARXES SOCIALS

Les xarxes socials permeten que les persones de tot el món comparteixin informació. Com podem ajudar els nostres fills per tal que estiguin segurs en les relacions socials a Internet? Pot semblar difícil protegir les dades personals a les xarxes socials, però pocs i senzills clics garanteixen l'aplicació d'alguns ajustaments importants de privacitat.

1 PÚBLIC O PRIVAT

Per defecte, a la majoria de les xarxes socials el perfil del vostre fill/a tindrà un nivell mínim de protecció de la privacitat. Hi ha dos ajustaments bàsics:

- Públic: "Tothom pot veure-ho tot" .
- Privat o tancat: "Ningú pot veure res, llevat que desitgem que ho vegi" .

El primer pas per protegir la privacitat dels vostres fills és animar-los a triar un perfil "privat" o "tancat". Fàcil!

2 BLOQUEJAR

En segon lloc, els vostres fills han de decidir a qui permeten veure el seu perfil. Animeu-los a acceptar com a amics només persones que coneixen. Si es troben amb un contacte que no desitgen, sempre poden bloquejar l'accés d'aquesta persona al seu compte.

3 COMPROVAR ELS AJUSTAMENTS

En el món real la quantitat d'informació personal que estem disposats a compartir amb algú depèn de amb qui estiguem parlant. Hauríem d'utilitzar aquesta mateixa política en el perfil del vostre fill/a a les xarxes socials. La majoria de les xarxes socials ofereixen l'oportunitat de decidir quanta informació es desitja compartir en certs grups, cercles o comunitats. Moltes xarxes socials ofereixen l'opció de comprovar els "Ajustaments de seguretat" i permeten als seus usuaris veure el seu propi perfil com si fossin una altra persona. D'aquesta manera poden veure amb claredat si al seu perfil es mostra alguna informació no desitjada.

4 PRENDRE EL CONTROL D'ETIQUETES

Protegir la privacitat no consisteix només en protegir la informació que els vostres fills publiquen a les xarxes socials. Altres persones poden també publicar imatges i vídeos i enllaçar el nom dels vostres fills a aquests continguts sense el seu permís. Això es coneix com a etiquetat o "*tagging*". La majoria de les xarxes socials permeten als seus usuaris desactivar la funció d'etiquetat o tenen l'opció de sol·licitar l'aprovació de l'usuari per a cada contingut que es desitja etiquetar. Animeu els vostres fills perquè configurin aquesta opció per tal de poder mantenir el control sobre la seva reputació a Internet.

5 PROTEGIR LA INFORMACIÓ SENSIBLE

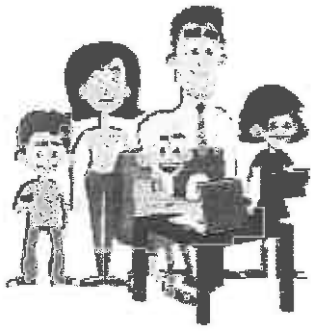
Finalment, però no menys important, si la informació és realment sensible heu de dir als vostres fills que no la publiquin a Internet! **Per a més detalls, descarregueu el full de Consells sobre "Informació personal".**

MÉS INFORMACIÓ?

Política d'ús de dades de *Facebook*:
www.facebook.com/about/privacy/

Servei d'ajuda sobre privacitat de *Facebook*:
www.facebook.com/help/privacy

En trobareu més a la xarxa Insafe
www.saferinternet.org
www.internetsegura.cat



L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

LA REPUTACIÓ A LA XARXA

Vivim en una societat on més del 85% dels encarregats de la contractació de personal afirmen que realitzen cerques a Internet sobre els candidats a un lloc de treball, per la qual cosa és extremadament important que els vostres fills cuidin les vostres reputacions a la xarxa. El que publiquem a Internet crea la nostra imatge pública. Aquí teniu alguns exemples de publicacions en línia que acaben malament.

EXPULSATS PER UN MISSATGE A FACEBOOK

Dos estudiants van ser expulsats temporalment, i un altre definitivament, pels missatges negatius que van publicar a *Facebook* sobre un professor. Els estudiants de la *Chapel Hill Middle School* tenien 12 i 13 anys, segons *My Fox Atlanta*. Els joves van ser acusats de transgredir les normes de funcionament intern de l'escola que suposa una infracció molt greu, la pitjor possible: acusacions "falses, tergiversades, amb omissió d'informació o informació errònia" sobre la conducta inadequada d'un empleat del centre cap a un estudiant.

Alexandra S. va desdir-se i va lamentar haver publicat al seu *Facebook* una frase en la qual acusava el seu professor de pedòfil. Va ser expulsada durant 10 dies. L'Alexandra va declarar: "No tenia la intenció d'arruïnar la seva reputació".

ANIVERSARI FELIÇ

La Thessa, una noia d'Hamburg, Alemanya, va pensar que només havia convidat uns quants amics a la seva festa d'aniversari, però es van presentar unes 1.500 persones, la qual cosa va provocar que aquesta noia de 16 anys fugís de casa. La Thessa no va comprovar els ajustaments de privacitat de la seva invitació d'aniversari, per això tothom amb un compte a *Facebook* hi va tenir accés.

Durant els dies previs a la festa el nombre de confirmacions d'assistència es va disparar a més de 15.000 persones. Això li va donar a la família de la Thessa una idea del que se'ls venia a sobre. Tot i cancel·lar la festa i avisar la policia, res no va aturar els convidats més persistents, ni tan sols un anunci públic: la nit de l'aniversari de la Thessa una gran multitud ho va celebrar sense ella. Durant aquella nit, onze persones van ser detingudes temporalment i un agent de policia va resultar ferit.

EL FENOMEN *INFORMER*

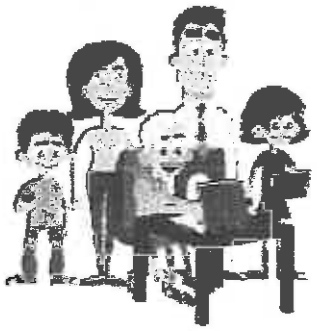
Les pàgines ***Informer*** són administrades des de *Facebook* i tenen com a particularitat que s'utilitzen des de l'anonimat. Segons informacions rebudes dels centres educatius es té constància que, en alguns casos, s'han utilitzat per publicar calúmnies i difamacions d'alumnes o professors. Preocupen especialment les conseqüències patides pels nois, les noies i els professorat, que han rebut amenaces i han sofert vexacions o insults com a conseqüència d'aquest nou fenomen, del qual se n'ha tingut coneixement a partir de gener de 2013.

L'aparició de les pàgines ***Informer*** de Facebook en alguns centres educatius ha fet que el Departament d'Ensenyament intervingui per orientar la comunitat educativa en cas que se'n detecti un mal ús, amb accions preventives, de detecció i valoració (per a famílies o mesures cautelars o de protecció).

MÉS INFORMACIÓ?

Protocol d'actuació per situacions *Informer*
http://www.xtec.cat/web/recursos/tecinformacio/internet_segura/orientacions_informer

En trobareu més a la xarxa Insafe
www.saferinternet.org
www.internetsegura.cat



L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

RISCOS A LA XARXA

Les millors defenses contra els riscos a la xarxa són la franquesa, la conscienciació i l'educació. Parleu-ne amb els vostres fills sobre les seves vides a Internet, compartiu les seves experiències i apreneu d'ells. Ajudeu-los a usar la tecnologia de forma positiva i responsable, i oferiu-los límits, orientació i suport. A continuació es descriuen alguns riscos per parlar-ne amb ells.

1 ROBATORI D'IDENTITAT

El robatori de la identitat és la pèrdua de les dades personals que permeten fer-se passar per una altra persona, generalment per obtenir un benefici econòmic. El problema no és nou, però les seves proporcions ha augmentat gràcies a Internet, que ofereix nous mètodes als criminals per reunir dades personals a una escala més gran. Els criminals utilitzen diversos mètodes per aplegar dades personals, que van des de la recollida de les dades ja publicades a la xarxa (com els perfils en línia i les xarxes socials) a l'ús d'una combinació de les tècniques del correu brossa, el *phishing* i el *pharming*. La millor prevenció contra el robatori de la identitat és, sens dubte, aconsellar el vostre fill/a que no publiqui detalls personals com els números de comptes bancaris, adreces, números de telèfon, detalls del passaport, etc.

2 CORREU BROSSA, *PHISHING* I *PHARMING*

El correu brossa o *spam* consisteix en missatges de correu electrònic no desitjats que habitualment es difonen en grans quantitats. Els missatges de correu brossa poden incloure contingut comercial com ara pornografia, productes farmacèutics, transaccions financeres dubtoses o ofertes "massa bones per ser certes".

Els atacs de *phishing* són aquells en els quals els usuaris rebem missatges de correu electrònic intentant enganyar-nos per tal que "actualitzem" els nostres detalls personals en línia a través d'un lloc web fals (que imita un banc). Aquests llocs web guarden aquesta informació personal i la fan servir amb l'objectiu de realitzar un frau.

Pharming és el procediment de redirigir els usuaris a una còpia fraudulenta d'un lloc web legítim, amb el mateix objectiu de robar dades personals i contrasenyes amb un propòsit delictiu. Parleu amb els vostres fills sobre com identificar els atacs de *phishing* i *pharming*.

3 *GROOMING*

El *grooming* de nens es refereix a totes les activitats que es realitzen expressament per fer-se amic d'un menor i establir amb ell una connexió emocional. L'objectiu d'aquesta "relació especial" és rebaixar les inhibicions del nen com a prèvia per a l'abús o l'explotació sexual. El *grooming* a nens es pot fer servir per atreure menors a activitats il·lícites com la prostitució o la pornografia infantil.

4 CIBERASSETJAMENT

El ciberassetjament és l'ús de la tecnologia per ferir, ofendre, fustigar o avergonyir deliberadament algú. El ciberassetjament es pot produir utilitzant pràcticament qualsevol medi amb connexió a una xarxa, des de missatges desagradables de text i imatge enviats des de telèfons mòbils, a missatges cruels publicats en blogs i xarxes socials, correus electrònics, missatgeria instantània i llocs web malintencionats creats amb l'únic objectiu d'intimidar una persona.

El ciberassetjament pot ser fins i tot més perjudicial que les formes normals d'assetjament divers, doncs existeix:

- La possibilitat d'envair electrònicament la llar i l'espai personal de la víctima.
- Una audiència potencial major.
- Una velocitat més gran a l'hora de distribuir imatges o missatges ofensius.
- Dificultat per controlar el que es publica o es distribueix electrònicament.
- La percepció del ciberassetjament com anònim, degut a la seva naturalesa despersonalitzada, pot fer que els nens s'involucrin en activitats que no somiarien en realitzar en el món real, ja sigui com autor o com a espectador.

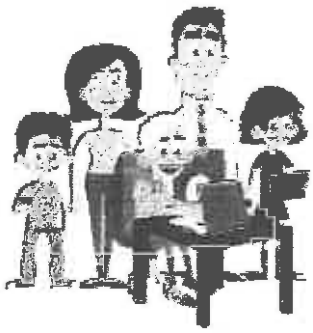
Informeu els vostres fills que és correcte bloquejar "amics" o simplement desconnectar-se d'un lloc web si algú o alguna cosa està fent que se senti incòmode en xarxa. En última instància, ells són qui manen. Si decideixen bloquejar algú o desconnectar-se, és una bona pensada que parlin del que ha passat amb un adult conegut i en qui confien, això pot ajudar-los a reafirmar-se en què han actuat de forma correcta i positiva.

MÉS INFORMACIÓ?

En trobareu més a la xarxa Insafe

www.saferinternet.org

www.internetsegura.cat



L'UNIVERS DIGITAL DELS TEUS FILLS

CONSELLS PER A PARES I MARES

TROBADES AMB ESTRANYS

Actualment per mitjà d'Internet els nens poden comunicar-se amb persones de tot el món. 'Les amistats de la xarxa' de vegades poden evolucionar cap a amistats en la vida real. Això vol dir que els vostres fills poden estar interessats en trobar-se amb un personatge virtual. Depenent de l'edat i la maduresa del nen, així com del context de la trobada, podeu permetre que el vostre fill/a, acompanyat d'un amic en lloc d'un adult de confiança, es trobi amb un desconegut. Pel que fa als joves, de vegades poden ser ingenus i mancats de les habilitats socials per avaluar les intencions de les persones que coneixen a la xarxa, cal marcar-los unes normes clares sobre la trobada amb estranys a la vida real.

PROPOSTA DE NORMES PER ALS VOSTRES FILLS

1 Abans de la trobada amb algú que heu conegut a la xarxa assegureu-vos de tenir tota la informació possible. Pregunteu-li sobre la seva família, les aficions, etc. Si noteu qualsevol inconsistència o contradicció en la seva història, o si sembla massa bo per ser cert, és millor no trobar-s'hi.

2 Expliqueu a un adult de confiança (pare, familiar, tutor,...) que teniu intenció de trobar-vos amb aquesta persona i doneu-li detalls sobre la seva identitat.

3 Expliqueu a un adult de confiança (pare, familiar, tutor,...) on i quan teniu intenció de trobar-vos, i acordeu de manera clara quan serà la tornada.

4 És molt fàcil per a la gent fingir ser una altra persona a la xarxa. Per tant, val la pena fer una verificació d'antecedents mitjançant la cerca a Google o la consulta a amics i familiars.

5 Demaneu que us acompanyi un adult de confiança o un amic a la primera trobada, sempre poden marxar un cop s'ha arribat al lloc i tot sigui correcte. Si el vostre amic a la xarxa es nega a assistir a la reunió si us acompanya un adult o un amic, això pot ser un símptoma de problemes.

6 Quedeu en un lloc públic, no en un lloc privat. Tenir gent al voltant farà la trobada més segura.

7 Comproveu que el vostre telèfon mòbil tingui la bateria carregada i manteniu-lo encès i a sobre en tot moment.

8 Confieu en la vostra intuïció. Si alguna cosa no encaixa, el millor és tallar ràpidament la trobada i posar-vos en contacte amb un adult de confiança.

9 Contacteu amb el vostre nou amic unes quantes vegades fins que estigueu ben segurs que realment és la persona que heu arribat a conèixer a la xarxa.

MÉS INFORMACIÓ?

En trobareu més a la xarxa **Insafe**

www.saferinternet.org
www.internetsegura.cat

Quines normes bàsiques de seguretat han de conèixer els nostres fills?

La majoria dels problemes que pots trobar-te a Internet es produeixen precisament com a conseqüència de no respectar tota una sèrie de normes bàsiques de seguretat. La majoria d'elles són de sentit comú, i totes molt fàcils d'aplicar. Teniu-les presents i repasseu-les sovint. Sempre n'hi ha alguna en la que no ens fixem.

- Correu electrònic
- Sales de xat
- Xarxes socials
- Mòbils, taulèfons i tauletes tàctils
- Jocs en xarxa
- Aplicacions

- Comproveu que l'antivirus i el tallafocs estan sempre actualitzats i operatius. Activeu mesures de control parental per evitar que els vostres fills accedeixin a continguts nocius i/o perillosos.
- Expliqueu-los la importància de les dades personals i quines dades poden facilitar i quines no.
- Acordeu quines pàgines es poden visitar (agregant-les per exemple a la llista de favorits) i reviseu junts l'historial de navegació que queda enregistrat a l'ordinador.
- Estigueu al corrent de les novetats en riscos a Internet. Compartiu-los amb els vostres fills i navegueu per la xarxa amb ells per confirmar que els han entès.
- Estigueu alerta amb les noves amistats que poden fer a les xarxes socials i parleu amb ells si veieu algun 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).

També podeu consultar que és un recull temàtic de situacions que tracten l'ús d'Internet dels vostres fills:

1. Amics a la xarxa (pdf)
2. Bloqueig (pdf)
3. Informació personal (pdf)
4. Jocs en xarxa (pdf)
5. La privacitat a les xarxes socials (pdf)
6. Reputació a la xarxa (pdf)
7. Trobades amb estranys (pdf)
8. Riscos a la xarxa (pdf)

Pel que fa al correu electrònic

- No haurien d'obrir correus electrònics de remitents desconeguts, i menys si es troben en

altres idiomes. Sovint es tracta d'SPAM (correu brossa) i poden contenir arxius o documents adjunts amb virus que perjudiquen el seu dispositiu.

- No haurien d'omplir formularis que els arriben per correu electrònic, en especial aquells que els demanin dades personals. Compte amb els correus de bancs on demanen que confirmin un compte o un pagament bancari. Sempre són falsos.
- En el compte de correu que utilitzen habitualment no incloure el seu nom i cognoms, edat o data de naixement. Haurien d'usar NICKS, noms inventats o neutres. Pep12@... No és una bona idea. És preferible utilitzar altres tipus bonpas@...
- Poden tenir diversos comptes de correu electrònic: un seria amb el seu nom per a qüestions "oficials" i res més, i un altre com el que t'aconsellem per a utilitzar habitualment.
- La contrasenya del seu correu electrònic és molt important. No l'han de compartir amb ningú, i utilitzar combinacions de lletres, números, utilitza alguna majúscula i símbol.
- No haurien d'utilitzar sempre la mateixa contrasenya per a tot.
- No haurien de seguir i reenviar les cadenes que envïis a través del correu electrònic.
- Quan envien un correu a diferents persones alhora, haurien de posar les adreces en "còpia oculta", en l'apartat "CCO".

Pel que fa a les sales de xat

- A Internet la gent no sempre és qui diu ser. És molt fàcil enganyar i mentir i molta gent ho fa. En especial aquelles persones que poden suposar un risc. No s'han de creure tot el que els diuen al xat.
- Aconsellar-los no parlar amb persones que no coneixen a les sales de xat públiques, de la mateixa manera que no es posarien a parlar sobre la seva vida amb un desconegut al carrer que portés una careta.
- No han de facilitar en aquestes sales les seves dades personals que permetin la seva localització o identificació: els seus cognoms, la seva adreça, l'escola o institut on estudien…
- Recordar-los que també han de respectar la privacitat de les persones que coneixen. No facilitar-los tampoc dades dels seus familiars o amics/gues.
- No han d'enviar fotografies seves a través d'aquestes sales. No sabem realment el que poden fer amb les seves imatges i on poden acabar essent distribuïdes.
- Cal bloquejar a aquelles persones que es dirigeixen a ells de forma agressiva o feridora, així com a aquelles que envien missatges obscens. No permetre que ningú els tracti malament. Parlar als demés amb correcció i exigir-los el mateix.
- Si algú l'insulta o amenaça és bo copiar o guardar les converses. Poden ser d'utilitat més endavant i, per suposat, recordar sempre que ens podeu informar: internetsegura[arrova]cesicat.cat

Pel que fa a les xarxes socials

- Recomanem posar en el seu perfil una imatge que no l'identifiqui directament: un avatar o alguna icona que els agradi.

- El seu perfil com a menor d'edat ha de ser sempre privat. És molt important.
- No afegir a persones que no coneguin físicament, i amb les que no mantinguin contacte regular. No serveix de res tenir un perfil privat si després afegeixen a 200, 300 o 400 persones.
- No incloure informació personal rellevant en el seu perfil, que permeti la seva localització o clara identificació. No indicar en quin centre escolar estudia, ni quins dies estàs de vacances fora de casa, ni informació personal sobre la situació de la seva família.
- Recordar-los que també han de cuidar la privacitat dels seus familiars i amics, pel que no han d'incloure informació personal sobre ells sense el seu coneixement i consentiment.
- Compte amb les fotografies que pugen. Tot i que penseu que només les veuen els seus amics, qualsevol d'ells pot fer-ne còpies i penjar-ne alguna en un altre lloc. Si pengen una fotografia han de pensar que pot arribar a veure-la qualsevol persona: pares, professors, companys, etc. i que pot estar circulant sense control durant anys per la xarxa.
- Abans de pujar una fotografia en la que apareguin altres persones al seu costat, haurien de comunicar-ho i obtenir la seva autorització.
- Haurien de ser respectuós/a quan escriuen en el mur dels demés, i haurien d'exigir el mateix. Recordeu-los que les paraules "se les emporta el vent", però el que s'escriu a Internet es queda i és possible identificar a l'autor.
- No haurien de participar en perfils o grups en els que s'insulta, amenaça o falta al respecte a altres persones. Si troben un d'aquests grups haurien de denunciar-ho de forma anònima. Es pot fer a la pròpia xarxa social, s'informa a través de la Línia de Denúncia anònima o directament als Mossos d'Esquadra.

Pel que fa a fer servir el mòbil o tauleta tàctil

- La missatgeria instantània és molt popular en els mòbils: Whatsapp, Telegram, Line, BlackBerry Messenger, Skype, Hangouts, Woowos... Els hem d'explicar que no han de perdre de vista que moltes de les coses que es poden dir amb text poden ser més valorades si es comuniquen cara a cara.
- Perquè no li prenguin el dispositiu han d'evitar exposar-lo davant els amics i protegir-lo amb el desbloqueig amb un patró gràfic, un pin o una contrasenya.
- Han de sospitar de les trucades i SMS de desconeguts i ocults. No haurien de donar dades personals sense estar del tot segur de qui hi ha a l'altre costat de la línia.
- Descarregar només les aplicacions de mòbil que estan a les botigues d'aplicacions oficials (Iphone, Android, Firefox...) per evitar que incloguin virus, siguin fraudulentes o espiïn les seves dades.
- Abans de compartir una notícia o publicar una fotografia o vídeo han de pensar-ho bé. No facilitar o publicar dades, informació, fotografies o vídeos d'altres persones sense que els hagin donat el seu permís.
- Cal vigilar la gran difusió que poden arribar a tenir les imatges amb contingut sexual que poden ser gravades i compartides en grups de missatgeria instantània.
- Si omplen formularis amb les dades personals o fan compres des del mòbil assegurar-se d'usar comunicació segura https i amb el 3G actiu.

- Evitar l'ús de xarxes Wi-Fi obertes de les quals no coneixen el propietari. Algú pot tenir control de les seves sessions a la seva xarxa social o al seu correu electrònic quan l'obren des del mòbil.
- Han de configurar les opcions de l'aparell perquè respecti la seva privacitat. Han de vigilar quan donem permís per connexions de proximitat amb altres dispositius (Bluetooth) i la seva geolocalització (GPS) que demanen diferents serveis (Google Maps, Instamessage, Foursquare, Instagram,...) que pot revelar-se a partir de les imatges que envien.

Pel que fa als jocs en xarxa

- Primer cal assegurar-se si el contingut del joc és adequat per la seva edat. Els nivells de dificultat del joc i les habilitats necessàries per jugar-hi necessiten una edat mínima.
- Quan juguen en línia amb els seus amics, vigila les pàgines on accedeixen i que no donin mai dades personals (nom, adreça, telèfon...) ni dades bancàries.
- Les etiquetes descriptives informen si el joc conté continguts de: violència, llenguatge inapropiat, por, drogues, sexe, discriminació, apostes, joc amb altres persones.
- No haurien de quedar amb persones que coneguin mitjançant la xarxa. I si queden amb algú, que us avisin o vagin amb algun amic i que quedin en un lloc públic. Podeu trobar més informació a: www.pegionline.eu

Si et descarregues aplicacions

- Informa't sobre filtres disponibles d'accés a certs continguts, ja que eviten molts riscos.
- Assegura't que siguin conscients de la importàcia de no revelar cap dada personal (nom, adreça, telèfon...) ni del seu entorn més proper.
- Fomenta l'ús d'apps subjectes a un control i a una regulació que respectin els drets dels menors i tinguin un servei d'atenció al client, informant-te dels continguts de jocs i apps per mòbils o tauletes mitjançant l'etiquetatge PEGI i de les condicions d'ús que l'acompanyen. Actualment disponible a Google Play, Firefox Marketplace, Microsoft's Xbox Live® Store, Nintendo® eShop i the Sony PlayStation® Store.
- Interessa't a què juguen. Conèixer bé al joc a què juguen és la millor manera que tinguin confiança en tu per explicar-te els seus dubtes i les seves preocupacions.
- Cal fomentar actituds de consum responsable amb els serveis i equipaments TIC, com per exemple allargar la vida útil dels equipaments TIC i tenir control dels mitjans de pagament amb els quals els adquirim. Podeu trobar més informació a: International Age Rating Coalition (IARC) www.globalratings.com

Per a qualsevol dubte que tinguis, estem per ajudar-te: internetsegura[arrova]cesicat.cat o al telèfon **116 111 d'Infància Respon** (24 hores al dia, 365 dies de l'any).