



ANNEX 1

1. RISCOS PER ALS INFANTS I ADOLESCENTS EN L'ACCÉS I ÚS D'INTERNET

Les principals funcions d'Internet són les d'informar, entretenir i comunicar. Per això, passem a exposar els riscos per als infants i adolescents tant en l'accés a la informació com en la comunicació.

Pel que fa als continguts que es poden trobar els infants i adolescents tant en la visita de les pàgines web, com en la descàrrega d'arxius, es poden diferenciar entre:

- continguts il·lícits, i
- continguts nocius

1.1. Continguts il·lícits

Es tracta d'aquelles informacions que estan tipificades com a delictes. Sovint ens trobem amb delictes que ja existeixen fora de la xarxa, però que es magnifiquen o resulten de control més difícil via Internet.

Hi ha continguts que afecten directament a la infància i la joventut i d'altres que afecten a la societat en general. Són exemple de continguts il·lícits entre d'altres:

- Pornografia infantil
- Propagació del material que inciten a l'odi, racisme, antisemitisme o altre tipus de discriminació en funció del sexe, religió, origen, orientació sexual.
- Propagació de materials i discursos amb violència extrema o sang desmesurada (gore).
- Incitació al suïcidi.
- Apologia de l'anorèxia i la bulímia.
- Joc en línia il·legal.

1.2. Continguts nocius

És aquella informació perjudicial per la integritat del menor, encara que no es trobi tipificada com a delictes, raó per la qual la seva difusió està permesa.

Els continguts són diversos, com ara pornografia, violència o d'altres.

S'ha de tenir present també, que en la vessant de participació i intercanvi és on es produeixen majors riscos per als infants i adolescents, perquè poden produir-se danys no només emocionals o psicològics sinó també físics. Els riscos van associats a les conductes tant dels infants i adolescents com d'altres persones que es comuniquen amb ells a través del *correu electrònic, les xarxes socials i altres eines (fòrums, xats, jocs en xarxa...)*.

Els més comuns són:

- La difusió de dades d'identitat personal: nom, número de telèfon, adreça, correu electrònic. Molt important de limitar en fer ús de xarxes socials.
- El contacte continuat amb desconeguts, i la posterior invitació a intercanviar-se informació delicada o a trobar-se en algun lloc.
- L'escalada de missatges desagradables amb vexacions, amenaces i injúries.
- L'abús escolar i el ciberbullying.
- El temps incontrolat en l'ús de jocs o dispositius que poden portar a problemàtiques d'addició (gambling -joc amb apostes- o enganxat al mòbil).

2. MECANISMES DE PROTECCIÓ PER A L'ACCÉS I L'ÚS D'INTERNET

Atesa l'existència de continguts inadequats en les pàgines webs així com l'existència d'altres riscos als quals s'exposen els infants i adolescents en l'accés i l'ús de les noves tecnologies,



es fa necessari adoptar mesures de prevenció i de seguretat per tal de garantir un ús profitós d'Internet.

Pel que fa als continguts il·lícits existeixen vies de denúncia tant policial com civils. Aquestes darreres, que les gestionen diverses institucions, sovint a iniciativa privada, possibiliten que els ciutadans denunciïn els continguts il·lícits que circulen per Internet i aquestes línies s'encarreguen de fer arribar la denúncia a l'autoritat competent.

Però a banda de l'activitat legislativa, cal promoure l'experiència positiva en la navegació que ha de reforçar l'ús educatiu, amb usos conduïts i amb temps limitat com alternativa als mals usos i accés il·limitat a continguts nocius per als infants i adolescents .

En aquest sentit, s'adoptaran mesures preventives, de seguretat i control, en concret, es pot recórrer a eines informàtiques: els *filtres de contingut* i les *recomanacions d'ús*.

2.1. Filtres de contingut

Els filtres més habituals són els de contingut, a través dels quals l'usuari o el gestor dels equips informàtics decideix quins són els continguts d'Internet als quals es pot accedir o no en funció de si els considera adients o no.

Permeten determinar quines pàgines web són adequades i quines no a fi de vedar l'accés dels infants i adolescents a determinades pàgines webs.

Existeixen molts filtres de contingut al mercat, tant comercials com gratuïts, com els que ofereixen la major part dels navegadors.

Existeixen també altres tipus de filtratge que permeten reconduir la navegació dels infants i adolescents a Internet. Les utilitats més destacades són les següents:

- Denegar l'accés a alguns dels serveis interactius d'Internet: xat, descàrregues de documents, comerç electrònic.
- Bloquejar informació que s'envia com números de telèfons i dades personals.
- Limitar la durada en temps i les franges horàries de connexió.
- Registre d'intents d'accés a materials inadequats.
- Establir perfils d'usuaris.

S'adjunta a l'Annex número 1 una relació d'eines de filtratge i control.

2.2. Llistat de recomanacions

Les eines tecnològiques no garantitzen per sí soles una protecció del menor davant els riscos que planteja l'ús d'Internet. Cal a més un acompanyament per part dels seus educadors a fi que aprenguin uns criteris de navegació segura i que els serveixi per enfortir l'autoprotecció.

En aquest sentit són diverses les entitats que proporcionen consells per evitar i/o minimitzar el riscos d'Internet tant per a adults com també per a infants i adolescents .

S'adjunta a l'Annex número 3 i 4 les recomanacions d'ús d'Internet que facilita CESICAT i l'Autoritat Catalana de Protecció de Dades tant pels infants i adolescents com pels educadors.



ANNEX 2

Tal com s'ha posat de manifest a l'informe, els riscos que presenta l'ús d'Internet pels infants i adolescents d'edat ha exigit la creació dels programes de filtratge. Aquest poden ser gratuïts o comercials. Els més comuns són els següents:

- a) Programes gratuïts:
 - Norton Online Family
 - K9 Web Protection
 - Windows Live Family Safety
 - MAC OS X Parental Controls

- b) Programes de pagament:
 - PureSight Owl
 - Net Nanny
 - Kaspersky Pure
 - Trend Micro Online Guardian
 - AVG Family Safety
 - Profil Parental Filter 2
 - Safe Eyes
 - McAfee Family Protection
 - F-Secure IS 2012
 - Cybersieve

Hi ha una pàgina web que s'actualitza trimestralment i compara l'efectivitat i la robustesa d'aquestes eines a diferents edats, dispositius i sistemes operatius: www.sipbench.eu



ANNEX 2. CONSELLS PER A INFANTS I ADOLESCENTS I PER A PARES, MARES I EDUCADORS/ES

CONSELLS PER A INFANTS I ADOLESCENTS

Infants de 8 a 10 anys

Internet és un lloc genial on pots parlar amb els teus amics i amigues, aprendre moltes coses i divertir-te. Segur que t'ho passaràs d'allò més bé si segueixes aquests consells:

1. No envii's fotografies teves ni donis mai el teu nom, la teva adreça o el teu telèfon quan naveguis per Internet. Demana el permís dels pares o els mestres.
2. Guarda en secret la teva contrasenya d'accés al correu i no la donis a ningú (ni tan sols al teu millor amic o amiga). Només els pares la poden saber.
3. Si fas noves coneixences, explica-ho als teus pares i presenta'ls els teus nous amics.
4. Si vols conèixer en persona a algú que hagi conegut per la xarxa, demana permís als pares i que t'acompanyin quan us trobeu.
5. A la xarxa hi ha moltíssimes coses bones, però també n'hi ha algunes de dolentes. Si en una web trobes alguna paraula o foto que et fa sentir malament, surt de la pàgina i no deixis que et molesti. Explica-ho als teus pares o mestres.
6. Fer un xat pot ser súper divertit, però no et quedis en una sala de xats si algú et fa sentir incòmode o et molesta.
7. El correu electrònic és un gran invent. Però per a la teva seguretat, no obris ni llegeixis missatges o fitxers que t'envii alguna persona desconeguda, si no és amb el permís dels teus pares o mestres.

Infants de 11 a 13 anys

Internet és un lloc genial on pots parlar amb gent de tot arreu i fer nous amics i amigues, aprendre coses sobre qualsevol tema que t'agradi i passar-t'ho genial.

Però estiguis on estiguis quan navegues per Internet, hi ha gent de tota mena: algunes amb bones intencions i algunes altres que potser et poden enredar. Per això et donem alguns consells senzills que t'ajudaran a navegar més segur:

1. No donis mai el teu nom, adreça ni telèfon quan naveguis per Internet. Tampoc envii's fotografies teves a desconeguts.
2. Controla la teva llista de contactes de missatgeria instantània i guarda la teva contrasenya en secret i no la donis a ningú (ni tan sols al teu millor amic o amiga). Algú la podria utilitzar i fer-se passar per tu.
3. Si fas noves coneixences, explica-ho als teus pares i presenta'ls els teus nous amics.



4. Si vols conèixer en persona a algú que hagi conegut per la xarxa, demana permís als pares i que t'acompanyin quan us trobeu.
5. A la xarxa hi ha moltíssimes coses bones, però també n'hi ha alguna de dolenta. Si en una web trobes alguna paraula o foto que et fa sentir malament, surt de la pàgina i no deixis que et molesti. Explica-ho a als teus pares o mestres.
6. Fer un xat pot ser súper divertit, però no et quedis en una sala de xats si algú et fa sentir incòmode o et molesta.
7. El correu electrònic i la missatgeria instantània són uns grans invents. Però per a la teva seguretat, no obris ni llegeixis missatges o fitxers que t'envii alguna persona desconeguda.
8. Si vols comprar o fer alguna cosa per Internet que pugui costar-li diners a la teva família, fes-ho sempre amb el permís i l'ajuda dels pares.
9. Els teus pares i tu sou un equip. Els pots ensenyar a utilitzar Internet i mostrar-los les pàgines web que visites i què fas quan navegues. Ells i els teus mestres, et poden ajudar a seguir unes pautes perquè t'ho passis bé i estiguis segur mentre navegues.
10. Quan naveguis per Internet i algun amic o amiga et proposi fer alguna cosa, no ho facis si creus que als teus pares no els agradaria. Ets una persona forta i responsable, i de vegades cal que li diguis a algú "no" perquè puguis fer allò que està bé.
11. L'accés autoritzat a la majoria de xarxes socials és als 14 anys. És important no avançar-se ja que et pots trobar amb problemes pel sol fet de no controlar prou bé qui pot veure la informació que hi publiquis. Deixa't assessorar per un adult en la configuració de la privadesa quan accedeixis per primera vegada.

Infants de 14 a 15 anys

Internet és genial: et permet parlar amb gent de tot arreu, fer nous amics i amigues, aprendre coses sobre qualsevol tema que t'agradi, divertir-te... De vegades però podem trobar-nos en situacions desagradables que pots evitar seguint uns senzills consells:

1. Quan naveguis o et comuniquis a través d'Internet, no enviiis fotografies teves ni donis mai les teves dades personals (nom, adreça, telèfon) a ningú, encara que sembli ser amic teu. Tampoc publiquis res en el teu bloc que et pugui identificar a tu o als teus amics.
2. Controla la teva llista de contactes de missatgeria instantània i guarda la teva contrasenya en secret i no la donis a ningú (ni tan sols al teu millor amic o amiga). Algú la podria utilitzar i fer-se passar per tu.
3. Potser facis noves coneixences. Recorda que la gent no sempre és tan legal en la realitat com ho demostra per la xarxa. Explica a algú de confiança a qui has conegut i presenta'ls els teus nous amics. I si vols quedar amb algú que has conegut, parla'n amb algun amic o amiga o



amb els teus pares i demana-li que t'acompanyi a la primera cita. Estaràs més segur si quedes en un lloc públic.

4. A la xarxa hi ha quantitat de coses bones i certes, però també n'hi ha de dolentes i falses. No et creguis tot el que trobis a Internet i, si en una web trobes alguna cosa que et fa sentir incòmode, parla'n amb algun amic o amiga, amb els teus pares o amb el mestre.

5. Fer un xat pot ser súper divertit, però no et creguis tot el que la gent et diu. Si algú et molesta o et fa sentir incòmode o preocupat, surt de seguida i digues-ho a algú de confiança. Recorda que en un xat la teva seguretat depèn bàsicament de tu.

6. El correu electrònic i la missatgeria instantània són uns grans invents. Però per a la teva seguretat, no obris ni llegeixis missatges o fitxers que t'envii alguna persona desconeguda. I si reps algun missatge desagradable o insinuant, per evitar-te problemes millor que no contestis, perquè només aconseguiries animar a la persona que l'ha escrit.

7. Si vols comprar o fer alguna cosa per Internet que pugui costar-li diners a la teva família, parla'n abans amb els teus pares. No donis a ningú el número de la teva targeta de crèdit o dades bancàries, perquè algú ho podria fer servir per robar-te.

8. Ves en compte amb els programes que et descarregues de la xarxa, doncs podries descarregar-te algun virus o programes espies. Tampoc has de descarregar música o pel·lícules d'Internet per fer-ne còpies. La majoria estan protegides per les lleis de propietat intel·lectual i t'exposes a ser demandat.

9. A la xarxa hi ha molta informació fiable, però també n'hi ha de dubtosa. Abans d'empassar-te alguna mentida, consulta la font d'informació i confirma-ho amb algun adult de confiança. Si has d'utilitzar algun text, imatge o dibuix d'Internet no oblidis citar l'autor o la font de les quals els has obtingut.

10. Si vols estalviar-te possibles problemes i ser un bon ciutadà en línia, actua correctament i evita fer res que pugui perjudicar altra gent perquè pots estar cometent algun delictes com per exemple amenaçar, difamar, atacar el dret a la intimitat enviant fotografies de companys...

CONSELLS PER A PARES, MARES I EDUCADORS/ES

La millor manera de prevenir situacions de risc i ajudar els nostres infants i alumnat a navegar amb seguretat és:

Fer-los conscients dels beneficis i riscos d'Internet.

- Educar-los perquè sàpiguin navegar de manera responsable.
- Donar-los estratègies perquè puguin protegir-se ells mateixos i elles mateixes mentre naveguen.



Per això a continuació us oferim alguns consells pràctics molt senzills que us hi poden ajudar. Si ho creieu convenient, podeu adaptar-los al vostre cas i afegir-ne algun més.

Familiaritzar-se amb internet

Per poder ajudar els nostres infants i alumnat a navegar per Internet de manera segura, millor si el coneixem una mica. No cal entendre'l ni que en siguem experts, n'hi ha prou amb provar de navegar-hi una mica. Fins i tot, si en saben més que nosaltres podem demanar-los que ens n'ensenyin.

Per aprendre a utilitzar Internet hi ha ajuntaments, biblioteques públiques, centres cívics i associacions que ofereixen cursos gratuïts o a preus molt econòmics. També podem posar-nos en contacte amb l'associació de mares i pares d'alumnes de l'escola dels nostres infants i organitzar cursos per a adults.

A més de conèixer una mica Internet, per ajudar els i adolescents a navegar de manera gratificant val la pena que siguem conscients dels **beneficis** i els **riscos** d'Internet.

Parlar obertament amb els infants i adolescents sobre l'ús d'internet

Interessar-nos per allò que els nostres infants i adolescents fan amb l'ordinador, tant a casa com a l'escola, a la biblioteca pública, a casa dels amics... ens ajudarà a estar a l'aguait de possibles riscos i a construir una atmosfera de confiança.

És convenient mantenir una bona comunicació amb els nostres alumnes o fills i intentar que ens informin sempre que vegin alguna cosa que no els agrada o que els fa sentir incòmodes. També és important que s'acostumin a presentar-nos les amistats que mantenen per la xarxa.

Si els nostres infants o alumnes ens expliquen que s'ha trobat amb algun estrany o alguna cosa que l'ha molestat, o s'ha saltat les regles, millor no culpar-lo, sinó ajudar-lo a evitar problemes en el futur. Cal recordar que segons la manera com reaccionem, l'infant ens tindrà o no prou confiança per recórrer a nosaltres la propera vegada que es trobi amb algun problema. La nostra millor estratègia és treballar amb ells de manera que puguin aprendre del que ha passat, adquirir uns hàbits de seguretat, i saber com protegir-se per si mateixos. Establir una atmosfera de confiança pel que fa a l'ús de la xarxa ens ajudarà a prevenir situacions de risc.

Navegar junts

Un altre bon mètode de prevenció contra els possibles riscos d'Internet, especialment amb els més petits, pot ser acostumar-nos a navegar junts amb els nostres infants i fer d'Internet una activitat lúdica i familiar. Els ordinadors poden oferir uns dels millors i més divertits viatges que els grans i petits puguem compartir.

Mentre ens connectem junts, no cal amoïnar-nos si veiem que els nostres infants tenen més facilitat d'utilitzar l'ordinador que nosaltres. Podem deixar-los que dirigeixin les sessions, demanar-los que ens n'ensenyin, fer totes les preguntes necessàries; això pot ser una bona ajuda per a la seva autoestima.

A la vegada, nosaltres podem ensenyar-los a navegar de manera segura i donar-los recursos perquè sàpiguen utilitzar Internet responsablement. Per exemple, podem comentar amb ells la



diferència entre publicitat i contingut educatiu o d'entreteniment i mostrar-los exemples de cada cosa.

Informar-se sobre les eines de control

Existeixen diversos programes informàtics que permeten els adults controlar l'ús que els infants i adolescents fan d'Internet. Les eines més habituals són els filtres, que limiten l'accés a continguts nocius. És important que famílies i educadors coneguem l'existència d'aquestes **eines de control** per tal que puguem considerar lliurement la possibilitat d'instal·lar-ne algun a l'ordinador de casa o de l'escola. Per això, és recomanable informar-nos-en i estudiar quin producte s'adiu més als nostres valors.

També es recomana parlar amb el proveïdor de serveis d'Internet que hem contractat i preguntar-li si ofereix algun servei especial d'accés per a infants i adolescents.

En cas que decidim utilitzar algun tipus de control, hem de ser conscients que **no són efectius al 100%** i que, per tant, hauríem de continuar supervisant la navegació dels nostres infants i adolescents. És important fer-ne seguiment i resoldre les peticions que es puguin formular.

Preguntar en el Centre escolar quina política de seguretat segueixen

Seria interessant informar-nos sobre quines mesures de prevenció d'accessos a continguts nocius d'Internet estan prenent els centres escolars i les biblioteques on van els nostres infants. Podem parlar del tema amb altres pares i mares que coneguem i contribuir, tant com puguem, a sensibilitzar les persones implicades sobre la utilització segura d'Internet. Entre tots podem decidir la millor manera de protegir els nostres infants.

Establir regles bàsiques de seguretat a la llar

Cal decidir amb els infants i adolescents unes regles de seguretat per a l'ús d'Internet. Aquestes normes serveixen senzillament perquè els més joves s'ho puguin passar bé i estar segurs mentre naveguen.

Podem acordar amb els infants i adolescents els llocs web per a visitar, l'horari de connexió més apropiat, etc. Per tal que les regles siguin més efectives, haurien de ser fruit de la comunicació amb ells, d'un acord. Podem penjar-les amb rètols informatius en un lloc visible i respectar-les tots per igual.

Col·locar l'ordinador a la vista de tothom

Per a estar a prop dels nostres infants mentre naveguen, millor si col·loquem l'ordinador de casa en una sala comuna, a la vista de tothom, en lloc de l'habitació dels infants (com a mínim mentre no són adolescents). Això ens ajudarà a supervisar-ne la navegació i poder donar un cop d'ull més sovint al que fan a Internet.

Ensenyar els infants i adolescents a navegar amb seguretat

Per als infants i adolescents Internet és un lloc genial on es pot parlar amb gent d'arreu i fer nous amics i amigues, aprendre coses sobre qualsevol tema, i passar-s'ho d'allò més bé. Però valdria la pena que per a la seva seguretat arribessin a:

- Ser conscients que l'ordinador és una eina educativa que serveix per a comunicar-se de manera positiva.
- Saber distingir entre els continguts d'Internet que són recomanables i els que no ho són.



- Ser conscients que a Internet hi ha gent de tota mena, com a qualsevol altre lloc.
- Saber reaccionar de manera responsable i saber resoldre per si mateixos possibles situacions de risc.
- Per això és convenient que ensenyem els nostres infants i alumnat a seguir aquests consells pràctics:
 - No facilitar mai les dades personals (el nom complet, l'adreça, el telèfon) ni la seva contrasenya a ningú per Internet.
 - Presentar-nos els seus "ciberamics", de la mateixa manera que ens presenten els altres amics. I si volen quedar amb algú que hagin conegut a través d'Internet, suggerir-los que els acompanyi una persona adulta i es trobin en un lloc públic.
 - Si hi ha alguna cosa que els resulta desagradable, que ho diguin a algun amic o adult i no deixin que els perjudiqui.
 - Si volen comprar o fer alguna cosa per Internet que pugui costar diners a la seva família, millor que ho facin sempre amb el permís i l'ajuda dels pares.

Cercar llocs web segurs

Específicament per als més petits, caldria cercar llocs web segurs, adreçats a ells, de la mateixa manera que busquem llibres, programes de TV o pel·lícules que els són apropiats. Les Biblioteques (com les de les xarxes de les Diputacions) fan reculls que podeu trobar actualitzats en les seves pàgines web amb recomanacions educatives i lúdiques adreçades als nens i nenes, en les quals navegar segurs i gaudir dels beneficis de la xarxa.

Sobre els primers passos en l'ús del mòbil

El telèfon mòbil, present ben d'hora a la butxaca de molts joves, s'ha convertit en el mitjà en què la comunicació és de forma instantània amb persones d'arreu del món. Les xarxes socials permeten parlar amb els amics, enviar-se fotos o vídeos, intercanviar missatges de text curts... A més la tecnologia permet fer ús de la geolocalització i l'ús d'aplicacions que l'usen per interactuar amb les qüestions de proximitat relacionades amb objectes o altres usuaris.

Els mòbils com altres dispositius tenen els riscos associats al malware que poden provocar la fuga d'informació (virus espies de contactes, agenda i fotografies) però també els riscos associats a la connexió de dades que usem (molt sovint xarxes públiques wi-fi insegures) permetent la interceptació de les comunicacions o la suplantació en l'ús de determinats serveis a la xarxa si no prenem precaucions.

Davant un possible problema, reaccionar a temps

Si en alguna ocasió tenim indicis que els nostres infants o alumnat està en risc, podem parlar-ne amb ells i notificar-ho a internetsegura@gencat.cat o trucar a la policia al 112.

En cas de trobar pornografia infantil, material presumptament il·legal o qualsevol altre que considereu que pot ferir la sensibilitat dels infants o adolescents, podem posar-nos en contacte amb la policia. També podeu denunciar-ho a CESICAT a través de info@cesicat.cat o del telèfon 977 010 893.



ANNEX 3. PÀGINA WEB PER AL NAVEGACIÓ SEGURA PER LA XARXA DEL CENTRE DE SEGURETAT DE LA INFORMACIÓ DE CATALUNYA: CENTRE INTERNET MÉS SEGURA (<http://www.internetsegura.cat/>)

CONSELLS GENERALS DE SEGURETAT

Quan naveguem per Internet, parlem amb els amics a través del xat, descarreguem arxius o utilitzem les xarxes socials, hem de fer-ho amb seguretat per evitar problemes.

Cal estar alerta quan naveguem per la xarxa, perquè Internet és un mitjà que també utilitzen els delinqüents per cometre frauds, robar dades, assetjar, etc...

A continuació et donem una sèrie de consells generals per a tenir una bona experiència a Internet.

NAVEGANT PER INTERNET... AMB SEGURETAT

Internet és un lloc ple d'oportunitats on pots aprendre, comunicar-te amb amics arreu del món, jugar... i divertir-te d'allò més. Però també hi ha alguns riscos i consells de seguretat que has de conèixer per evitar problemes.

El Centre de Seguretat de la Informació de Catalunya (CESICAT) vol ajudar-te a utilitzar bé Internet i totes les seves aplicacions.

Aquesta és una guia de recomanacions perquè gaudeixis amb seguretat de la xarxa.

Navegant per internet

- Quan naveguis per Internet intenta sempre fer-ho per pàgines segures i de confiança. No tothom té bones intencions a la xarxa, per això has d'anar amb compte.
- No desactives l'antivirus ni el tallafocs en cap moment. Ho poden aprofitar per infectar el teu ordinador, copiar la teva identitat o informació i fins i tot es poden fer passar per tu o pots perdre tota la informació que tens guardada.
- Crea contrasenyes que barregin lletres, majúscules i minúscules, números i símbols especials.
- No facilitis les teves dades personals ni les d'altres persones quan visitis webs de poca confiança. Quan deixis les teves dades, assegura't per a què les volen.
- No te'n refiïs de tot allò que trobis o llegeixis a Internet. Intenta verificar-ho, i si tens algun dubte demana ajuda als pares o tutors.

Descarregant arxius / xarxes P2P / Jocs online

- Obre només els correus electrònics de les persones que coneguis. Esborra els missatges sospitosos i no et descarreguis els arxius que sovint s'hi adjunten perquè poden contenir virus.
- Si descarregues o intercanvies arxius, fes-ho només en llocs segurs i de confiança. No t'inscrivis en pàgines insegures.
- Si et registres en un lloc web, utilitza contrasenyes difícils. Mai facis servir el teu nom, la teva data de naixement o el teu DNI com a contrasenya. Són molt fàcils de descobrir.
- No realitzis mai cap compra a través de la xarxa sense estar acompanyat dels teus pares o tutors.
- Les xarxes P2P no són sempre segures. Podem exposar el nostre equip a intrusos si no sabem configurar adequadament les opcions de seguretat i privacitat.
- Has de saber que intercanviar música, vídeos i pel·lícules a través de programes P2P infringeix els drets de propietat intel·lectual si el seu autor no ho autoritza expressament.
- No utilitzis les xarxes P2P per difondre continguts ofensius, degradants o humiliants per a altres persones. Pots arribar a ser denunciat per això.



- Quan juguis en línia amb els teus amics, vigila les pàgines on accedeixes i no donis mai dades personals (nom, adreça, telèfon...) ni dades bancàries.

A les xarxes socials

Les xarxes socials et permeten conèixer gent i tenir amics arreu del món. Pots compartir informació alhora amb tots els teus companys i pots conèixer altres cultures i costums. L'ús de les xarxes socials s'ha estès de forma molt ràpida, però també és un mitjà que utilitzen els delinqüents (sobretot assetjadors sexuals) per captar les seves víctimes. Per això cal estar alerta:

- No acceptis "amistats" de desconeguts. A Internet és molt fàcil dir mentides i fer veure que ets una altra persona.
- Publicar informació a les xarxes socials és molt fàcil i ràpid, però un cop publicada no saps quin ús en poden fer. Abans de penjar una notícia o publicar una fotografia pensa-t'ho bé. No facilitis o publiquis dades, informació, fotografies o vídeos d'altres persones sense que t'hagin donat el seu permís.
- Inventa contrasenyes llargues i complexes. Fes servir un àlies (nick) que només coneguin els teus amics.
- Si algú et molesta o t'assetja en algun xat o grup, surt del grup i avisa als teus pares o tutors. Sigues respectuós tu també amb totes les persones del grup.
- No comparteixis dades com el telèfon, l'adreça o el teu nom i cognoms. No enviïs mai les teves fotos ni donis les teves dades personals a cap desconegut.
- A Internet no tothom és amic. No quedis amb les persones que coneguis mitjançant la xarxa. I si quedes amb algú, avisa els teus pares o algun amic que t'acompanyin i queda en un lloc públic.
- No acceptis arxius de persones que coneguis al xat, perquè podrien incloure algun virus. Fins i tot les cançons o les fotos que t'envien poden ser perilloses.

Si fas servir mòbil

- Perquè no te'l prenguin evita d'exposar-lo davant els amics i protegeix el desbloqueig usant un patró gràfic, pin o contrasenya.
- Sospita de trucades i sms de desconeguts i ocults. No donis dades personals sense estar del tot segur de qui hi ha a l'altre costat de la línia.
- No instal·lis aplicacions al mòbil que no estiguin a les llistes oficials ja que poden contenir virus o prendre't dades de contactes.
- Evita usar xarxes wi-fi obertes en què no coneixem el propietari. Podem perdre control de les sessions de xarxes socials o correu electrònic que obrim des del mòbil.

Recomanacions per a tutors/es i educadors/es

- Comproveu que l'antivirus i el tallafocs estan sempre actualitzats i operatius. Activeu mesures de control parental per evitar que el menor accedeixi 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 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.)

GLOSSARI

1. ANTIVIRUS Són programes que actuen com guardaespalles del nostre ordinador. Estan alerta davant de possibles virus que se'ns poden introduir a l'ordinador (vegeu Virus).

2. CIBERASSETJAMENT (cyberbullying)

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

3.CONTRASENYA SEGURA

És aquella que altres persones no poden determinar fàcilment endevinant-la o utilitzant programes informàtics. Per crear una contrasenya segura que puguis recordar fàcilment però que sigui difícil de determinar per terceres persones, intenta una de les tècniques següents:

- No utilitzis contrasenyes que siguin paraules (encara que siguin estrangeres) o noms (el de l'usuari, personatges de ficció, membres de la família, mascotes, marques, ciutats, llocs, o altre relacionat).
- No usis contrasenyes completament numèriques amb algun significat (telèfon, D.N.I., data de naixement, PIN, etc.).
- Tria una contrasenya que barregi caràcters alfabètics (majúscules i minúscules) i numèrics. Han de ser llargues, de 8 caràcters o més.
- Estableix contrasenyes diferents per a sistemes diferents. És possible usar una contrasenya base i certes variacions lògiques d'aquesta per a diferents llocs. Això permet que si et roben una contrasenya no et robin els accessos a tots els llocs als quals ingresses.

4. CONTROL PARENTAL

És qualsevol eina que permet als pares supervisar i/o limitar l'ús que el menor fa de l'ordinador o d'Internet.

Aquests controls ajuden als pares a seleccionar els jocs i els programes que poden usar els seus fills, així com els llocs web que poden visitar i quan poden fer-ho.

5. CORREU BROSSA O SPAM

Els missatges no sol·licitats, habitualment de tipus publicitari, enviats de forma massiva. La via més utilitzada és el correu electrònic però pot presentar-se per programes de missatgeria instantània o per telèfon mòbil.

6. GROOMING

Es refereix a l'assetjament de caràcter sexual d'un menor. Les accions dutes a terme tenen l'objectiu d'establir una relació i control emocional sobre un nen/a per a després abusar-ne sexualment. A diferència del ciberassetjament, aquest tipus d'assetjament té un objectiu explícitament sexual. (Vegeu ciberassetjament)



7. DADES PERSONALS

Són les informacions escrites, gràfiques o imatges relacionades amb una persona i que serveix per identificar-la, contactar-la i/o localitzar-la. Es consideren dades personals, doncs, el nom, l'edat, l'adreça, el número de telèfon, el número del carnet d'identitat, les contrasenyes i el números de comptes bancaris, entre d'altres. Internet ha fet que sigui més fàcil recopilar aquest tipus d'informació i

fer-ne un mal ús.

8. MISSATGERIA INSTANTÀNIA

És un sistema que permet intercanviar missatges entre dues o més persones en temps real per Internet. Els programes usats permeten guardar una llista de contactes o grups i si es troben disponibles es pot xatejar i intercanviar imatges, música o vídeo. Els populars Windows Live Messenger, Google Talk, Facebook Messenger o Skype han evolucionat cap als Whatsapp o BlackBerry Messenger als *smartphones*.

9. PROGRAMARI MALICIÓS O MALWARE

És un programari que té com a objectiu infiltrar-se en el sistema i danyar l'ordinador sense el consentiment de l'usuari. (Vegeu virus i troians).

10. ROBATORI D'IDENTITAT O PHISHING

És una forma d'enganyar als usuaris perquè revelin informació personal o financera mitjançant un missatge de correu electrònic o lloc web fraudulent.

Normalment, una estafa per suplantació d'identitat comença amb un missatge de correu electrònic que sembla un comunicat oficial d'una font de confiança, com un banc, una companyia de targeta de crèdit o un comerciant en línia reconegut. En el missatge de correu electrònic, s'adreça als destinataris a un lloc web fraudulent, on se'ls demana que proporcionin les seves dades personals, com un número de compte o una contrasenya. Després, aquesta informació s'usa per suplantar la identitat.

11. SEXTING

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

12. TALLAFOCS

Programes que actuen com a porters de l'ordinador: res pot entrar-hi si ells no donen permís per fer-ho. T'avisen de programes que poden actuar en perjudici del teu ordinador i et fan invisible davant de les possibles amenaces. En alguns webs trobaràs tallafocs que et pots baixar gratuïtament; és molt recomanable que te n'instal·lis un. (Vegeu programari maliciós).

13. TROIANS

Són programes informàtics que aparenten ser programari útil però que posen en perill la seguretat de l'ordinador. Habitualment s'utilitzen per espiar en instal·lar-hi programari d'accés remot que permet monitorar el que fa l'usuari a l'ordinador.

14. XARXES P2P

Són sistemes d'intercanvi d'arxius. És una forma legal de compartir arxius de forma similar a com es fa en el correu o en missatgers instantanis, si bé d'una forma més eficient i, generalment, més ràpida.



15. XARXES SOCIALS

Conjunt de persones vinculades a un mateix grup d'Internet, que tenen com element de cohesió el fet de compartir diferents tipologies

de continguts: textos, fotografies, vídeos, música, enllaços... Les més usades són Facebook, Twitter, Google+ o Tuenti però n'hi ha més: habo, hi5, Instagram, Tumblr, Pinterest, Taringa...

16. VIRUS

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

17. VIDEOCONFERÈNCIA

A partir de portàtils amb webcam o un smartphone combinem l'àudio, vídeo i xarxes de comunicació perquè individualment o en grup es trobin cara a cara en temps real per interaccionar. Actualment Skype o algunes aplicacions per mòbil ho permeten de forma fàcil.

18. WEBS DE CONFIANÇA

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



ANNEX 4. ALGUNS ENLLAÇOS PER SABER-NE MÉS

Institucions

<http://www.saferinternet.org/spain>

<https://www.cesicat.cat/ca/section/publicacions/manuals-i-guides>

- [www.cesicat.cat/media/files/80911267-Guia-completa-proteccio-de-infants-adolescents .pdf](http://www.cesicat.cat/media/files/80911267-Guia-completa-proteccio-de-infants-adolescents.pdf)
- www.cesicat.cat/media/files/80911723-Guia-completa-seguretat-mobils.pdf
- www.cesicat.cat/media/files/Guia%20per%20a%20l%20us%20segur%20de%20les%20xarxes%20socials.pdf

<http://www.protegeles.es/>

http://www.xtec.cat/web/recursos/tecinformacio/internet_segura/

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

http://www.apd.cat/ca/contingut.php?cont_id=567&cat_id=692

Guia de infants i adolescents a Internet per navegar per la xarxa sense problemes

<http://www.apd.cat/ca/media/2411.pdf>

Protegir la teva privacitat i controlar les teves dades <http://www.apd.cat/media/2646.pdf>

Proveïdors ISP

<http://www.google.cat/goodtoknow/>

<http://www.facebook.com/safety/>

<http://support.google.com/youtube/bin/answer.py?hl=ca&answer=157105>

<http://support.google.com/youtube/bin/answer.py?hl=ca&answer=126289>

Recursos per a joves

<http://www.internetsegura.cat/>

<http://www.super3.cat/supercrac/>

<http://internetambseny.cesicat.cat/>

Dossier 'Seguretat a la xarxa' al www.jove.cat

<http://www.super3.cat/infok/9888/Dia-dInternet-mes-segura/>

<http://www.youtube.com/Internetposahiseny>