ÚS SEGUR DE LES TIC

Tema 2

Índex

0. Introducció

L'objectiu d'aquest tema és presentar alguns dels aspectes de major rellevància per a l'ús segur i responsable de les TIC. Els temes tractats, com per exemple els continguts inadequats i alguns dels riscos que aguaiten en Internet i en les xarxes socials, estan en contínua evolució, per la qual cosa es pretén asseure les bases per a reflexionar amb serietat sobre ells.

Cada vegada més prenem consciència de la necessitat de donar a conèixer els perills d'Internet als menors i per a açò nosaltres mateixos com a docents hem d'estar al dia de les últimes tendències. La situació actual no deixa lloc a dubtes: l'edat d'inici en l'ús de la Xarxa és cada vegada menor i la quantitat d'hores de navegació cada vegada major. Per açò, és necessari estar informat i al seu torn formar als joves sobre els problemes de seguretat i els perills que aguaiten en Internet, des de la suplantació de dades a la "sextorsión", passant pel "phishing", el "sexting" o el ciberassetjament (o "cyberbullying").

Vídeo no sigues estrel·la Unicef: https://www.youtube.com/watch?v=KSMJqloIl7w

1. Continguts inadequats

Per contingut inadequat entenem tot material percebut pel menor d'edat que siga nociu per a ell. Són les imatges i estímuls que provoquen un perjudici en el menor, aquests són, aquells perills que circulen per la Xarxa, i les característiques de la informació que contenen. Dins d'aquesta accepció, convé distingir entre **continguts il·lícits**, que són aquells que no estan legalment permesos; i els **continguts nocius**, que sí estan permesos per Llei però es consideren nocius en el desenvolupament personal i social dels menors.

Qualsevol persona amb un mínim de coneixements és capaç de trobar qualsevol tipus d'informació en la Xarxa, i expressar-se lliurement gràcies a l'ampli canal de comunicació que ofereix. Açò ha afavorit la proliferació de tot tipus de webs, amb múltiples i diversos continguts, molts dels quals no són apropiats per als menors. A través d'Internet, la televisió, el cinema, la música o els videojocs, als quals s'accedeix per dispositius com l'ordinador, els smartphones, les tablets, videoconsoles o reproductors d'àudio i vídeo, els menors tenen al seu abast multitud de continguts inadequats.

D'aquesta manera, els continguts inadequats poden provocar greus perjudicis en el desenvolupament de xiquets i adolescents. Fent ús de les TIC (ja siga navegar per Internet, veure la televisió, jugar a la videoconsola etc.) els menors d'edat, poden trobar informació no adequada especialment per a ells. Són imatges, actituds i/o comportaments que manifesten i fomenten valors negatius i moralment reprovables.

Parlem de continguts que, bé poden ser il·legals des del punt de vista jurídic i han escapat al control dels Cossos de Seguretat de l'Estat, o bé poden tractar-se de continguts no recomanables per a les edats primerenques i reservats per a població adulta. Aquests són els exemples més comuns:

- **Continguts pornogràfics.** Tot el conjunt d'obres que contenen imatges sexuals explícites amb la finalitat de provocar l'excitació del receptor. A causa de les seues característiques, aquests materials no són adequats per a menors d'edat per la seua falta de maduresa per a assimilar el que estan veient. A més, els continguts pornogràfics ofereixen una visió distorsionada de les relacions sexuals, categoritzant a homes i dones com a mers objectes de desig. Al seu torn, poden generar il·lusions falses sobre la naturalesa del cos, provocant que el menor s'obsessione amb una aparença física estereotipada o un ideal de bellesa concret com a requisit indispensable per a la satisfacció sexual.
- **Continguts violents.** Els menors d'edat poden accedir, a través de diferents mitjans digitals, a continguts de violència (contra persones, animals o objectes) com són, per exemple, els casos d'imatges i vídeos referents a baralles, pallisses (a una o diverses persones), insults o amenaces a educadors en l'escola, maltracte animal, destrossa de mobiliari urbà etc., **gravats per ells mateixos, o a través d'arxius compartits** i/o difosos en la Xarxa. Igualment, els menors poden accedir, a través dels periòdics i informatius, a continguts violents, per exemple quan tracten notícies sobre guerres; atacs terroristes; maltractament i/o assassinats masclistes; manifestacions i protestes polític-socials que deriven en enfrontaments; accidents de trànsit; baralles en esports col·lectius com a futbol; atacs xenòfobs, homòfobs i discriminatoris, massacres, etc.

En plataformes d'entreteniment, com les videoconsoles o jocs Online, els menors també poden trobar continguts violents: enfrontaments armats, violència sexual explícita, violacions, baralles, col·lisions amb vehicles, batalles bèl·liques, agressivitat verbal, humiliacions, destrucció de béns o objectes, atracaments, coacció a l'autodeterminació d'uns altres, i suïcidis.

- **Continguts falsos o mancats de rigor.** Es refereixen a informacions errònies o visiblement falses que circulen per Internet i arriben fàcilment a un gran nombre de receptors a causa de la naturalesa del contingut i la tendència a propagar-se ràpidament. Aquesta classe d'informació pot ser nociva i inadequada per als menors, ja que podrien ser enganyats en donar com certes imatges i continguts falsos o mancats de rigor, i fomentar en ells actituds i conductes inadequades. Com a exemples destaquem:
  - **Llegendes urbanes**: són històries extravagants però versemblants, que suposadament han ocorregut, donades sempre com a vertaderes. Solen arrelar-se ràpidament en la cultura, com una veritat indiscutible. Per a fer-les versemblants, el narrador les compte com alguna cosa que al seu torn li va explicar i/o va succeir a un amic proper. Es tracta doncs d'històries explicades en cadena, a través de serveis de missatgeria instantània o xarxes socials, amb un contingut extraordinari, morbós, entretingut etc. que les fa atractives per als receptors.
  - **Missatges en cadena**: són tipus de correu brossa la fi de la qual és la propagació i coacció d'alguna manera als receptors perquè els reenvíen a un altre grup de persones. Com a exemples destaquem els missatges del tipus: *"WhatsApp passa a ser de pagament, envia aquest missatge a altres 10 persones perquè el teu compte siga gratuït per sempre"; "Atenció! El teu telèfon Android ha sigut greument infectat per un virus que pot conduir a una fallada total. Prem en OK per a començar el procés de reparació". P*oden donar-se situacions on l'objectiu de l'emissor siga enganyar o crear alarma en el receptor, transmetent informació falsa, i sol·licitant fins i tot dades personals que després utilitza de forma fraudulenta o maliciosa.
  - **Vídeos virals**: és el nou fenomen TIC que causa sensació especialment entre la població més jove. Es tracta d'enregistraments, que bé pertanyen a l'àmbit privat d'una persona, bé pertanyen a un àmbit públic i cèlebre, difoses a una enorme quantitat de persones, i compartides a través d'Internet, missatgeria instantània com Whatsapp, blogs, xarxes socials, correus electrònics i altres llocs web. Es plantegen com a reptes o desafiaments en cadena, i el seu contingut varia enormement, la qual cosa suposa també un risc potencial per a la població menor d'edat. Humor, cinema, televisió, sexe,

violència, o qualsevol contingut que puga vulnerar la dignitat humana, fa dels virals un element a tenir en compte.

- El foment d'hàbits **que danyen la salut física i psicològica**. Durant les últimes dècades, les imatges i missatges en mitjans de comunicació associats a l'aspecte corporal ha augmentat de forma notable. És comú trobar ideals de bellesa en mitjans TIC com la televisió, Internet, cinema, premsa, oci, etc. La mediatització del cos realça els estereotips imperants que són assimilats pels ciutadans. En aquest punt, donem especial rellevància als **Trastorns de la Conducta Alimentària**, caracteritzats per comportaments alterats davant la ingesta alimentària i en el control del pes. Es tracta d'alteracions mentals que comporten problemes físics, psicològics i socials de les persones que ho pateixen i del seu entorn. La informació orientada a la recerca d'ideals de bellesa culturalment establits (incloent mètodes i consells per a perdre pes, productes per a aprimar etc.), que en moltes ocasions no està contrastada ni s'acull als criteris vigents de les Ciències Mèdiques, la qual cosa suposa un risc per a la salut del menor. La cultura del culte al cos, dels cànons de bellesa pre-establits, també envaeix el món TIC, de la qual cosa es xopen forçosament els més joves, condicionant les seues emocions, valors, forma de veure el món que els envolta, creences i comportament. En multitud de pàgines web podem trobar informació de risc, mentre ofereix imatges i pautes que poden causar un dany sever a la pròpia salut. Tal vegada l'exemple més clar són les adreces web, blogs etc. que tracten el tema de l'aspecte físic, i que contenen, entre uns altres, taules d'exercicis físics i dietes per a perdre pes que no s'ajusten als criteris mèdics per a la cura de la salut i el benestar. Una de les conseqüències més destacades de l'accés a aquest tipus de continguts inadequats són les alteracions mentals i emocionals, que comporten greus problemes físics i afecten al funcionament psicològic i social de l'individu i el seu entorn.

- **Els jocs d'atzar**. Cada vegada més presents en les TIC, es basen en la possibilitat de guanyar o perdre diners depenent de la capacitat del jugador així com també de l'atzar. En la seua majoria són jocs d'apostes on la recerca de benefici econòmic porta amb si el risc de ser enganyat, o de perdre quantitats considerables de diners. Aquests models de negoci que han envaït Internet i altres plataformes tecnològiques es basen en un model de "captació", oferint als jugadors atractius premis a canvi de jocs i apostes senzilles, amb el que és fàcil, especialment en els menors d'edat, caure en comportaments addictius.
- L'afició dels menors d'edat als **videojocs i jocs online** pot convertir-se en un risc greu quan passen de l'afició a l'addicció. Els experts assenyalen que el percentatge de joves que empren llargues hores del dia a aquestes activitats es va multiplicant en poc temps.

L'aïllament en la pròpia habitació del menor (o en la casa d'un amic) durant hores, encadenant partides de diferents parts del món, porta a aquests joves a una desconnexió total de l'entorn (no menjar amb la família, deixar d'interactuar amb pares i/o companys, descurar la higiene personal…). El risc dels jocs online és que posseeixen un potencial addictiu, perquè dóna la possibilitat de jugar a casa, amb un accés senzill. L'anomenat Internet GamingDisorder és un trastorn el tractament del qual s'ha estès en el nostre país i a nivell internacional. Els afectats manifesten problemes associats a aquest ús inadequat com a trastorns de conducta, personalitat o depressió. La baixa autoestima també sembla ser un factor de risc important.

Aquestes situacions d'afició i addicció a jocs d'atzar i/o videojocs online es tradueixen en: alteracions emocionals i conductuals, alteracions familiars, de l'humor, irritabilitat, o ansietat. A més, en molts casos, l'addicció porta associada la pèrdua de contacte social, problemes econòmics derivats de les apostes (jocs d'atzar i pàgines d'apostes esportives), i fracàs acadèmic.

- La **publicitat en línia**, que el seu mitjà de difusió principal és Internet, permet a les companyies donar a conèixer els seus productes i serveis arribant fàcilment a un gran nombre de persones de qualsevol part del món. Aquest tipus de publicitat és presa com a contingut inadequat a causa de l'absència de filtres cap als destinataris, corrent el risc d'incloure temes no recomanats per als menors d'edat. Com a exemple, la publicitat referent a les begudes ensucrades, tan demandades pels joves, ignorant-se (fins i tot per un elevat percentatge de pares i educadors) els perjudicis que poden tenir per a la salut. Les begudes ensucrades són sucre líquid, i contenen una quantitat de dolç major de la qual els professionals de la Salut recomanen que poden consumir xiquets i joves en tot un dia.

- **Continguts fraudulents i virus.** Per a infectar els sistemes i engalipar als internautes els delinqüents es recolzen en tècniques d'enginyeria social, que es refereix a l'ús de la manipulació psicològica sobre les persones per a aconseguir, tenint en compte la tendència general d'aquestes a la confiança, que realitzen determinades accions en el seu profit. Per exemple, obtenir informació que li permeta un accés no autoritzat a un sistema i, per tant, a la informació que residisca en el mateix. A pesar que els objectius generals de l'Enginyeria Social solen implicar activitats i contextos en els quals habitualment es relacionen adults, també és possible trobar situacions en les quals poden veure's implicats els menors: cercar contrasenyes en xarxes socials, correu electrònic i plataformes de jocs en línia.

2. Suplantació d'identitat

A nivell general la suplantació d'identitat consisteix en l'ús d'informació personal per a fer-se passar per una altra persona amb la finalitat d'obtenir un benefici propi. Normalment aquest benefici genera un perjudici a la persona que pateix aquesta suplantació d'identitat.

En el tema que s'aborda, la suplantació d'identitat en Internet en menors, un risc cada vegada més freqüent i que té lloc en edats progressivament més primerenques, es produeix quan una persona malintencionada actua en nom del menor fent-se passar per ell mitjançant la utilització de diverses tècniques –desenvolupades al llarg del present tema.

Per a abordar el terme amb major exactitud s'ha de diferenciar entre dos conceptes, la suplantació d'identitat i la usurpació d'identitat, dos preceptes no tan allunyats quant a significat es refereix, ja que els dos constitueixen una apropiació de drets i facultats que procedeixen de la persona perjudicada sent aquests d'ús exclusiu de la mateixa, com poden ser les seues dades personals: la seua imatge o el seu propi nom i cognoms.

La diferència principal entre tots dos conceptes és l'ús que es faça de l'apropiació d'aquests drets i facultats. La suplantació d'identitat consisteix en l'apropiació d'aqueixos drets i facultats pròpies de la persona suplantada (per exemple, accedir sense consentiment al compte d'una xarxa social), mentre que la usurpació d'identitat consisteix que una vegada suplantada la identitat es comence a interactuar com si realment fóra propietari d'aqueixos drets i facultats (per exemple, realitzar comentaris o pujar fotografies des d'aquest compte).

Per a facilitar la seua comprensió vegem més detalladament alguns exemples de suplantació d'identitat

- Registrar un perfil en una xarxa social amb el nom d'una altra persona sense el seu consentiment i utilitzant dades o imatges de la víctima, seria una suplantació d'identitat i en principi es consideraria delicte.
- Si únicament es registra un perfil fals per mitjà del nomene/àlies i no s'utilitza informació o imatges personals de la persona suplantada, no es consideraria delicte. Per a considerar-se delicte l'apropiació no s'ha de limitar al nom, sinó a totes les característiques o dades que integren la identitat de la persona. En qualsevol cas, encara es tindria la possibilitat de denunciar el perfil en la pròpia xarxa social per a la seua eliminació, la majoria de xarxes socials consideren la suplantació d'identitat un incompliment dels seus termes i polítiques d'ús.

- Accedir sense consentiment a un compte alié per a tenir accés a la informació allí emmagatzemada. Seria una suplantació d'identitat i en principi es consideraria delicte (almenys un delicte de descobriment i revelació de secrets).
- Accedir sense consentiment a un compte alié utilitzant les dades personals i fent-se passar pel suplantat (per exemple, realitzant comentaris o pujant fotografies). Seria una usurpació d'identitat i es consideraria delicte.
- Publicació sense consentiment d'anuncis o comentaris utilitzant el nom d'un tercer o fins i tot utilitzant les seues dades personals per a identificar-se amb terceres persones a través, per exemple, de correu o missatgeria instantània (WhatsApp). Seria una usurpació d'identitat i es consideraria delicte.

Les **dues formes principals** de suplantació d'identitat entre menors tant de primària (6-12 anys) com de secundària (13-17 anys) són:

1. Entrar sense consentiment en el compte d'un altre menor para:

-
-
-
-
-
-
-
-
-
-
-
-
-
-

Accedir a informació sensible com pot ser el cas d'una foto o un video.

- Assetjar o desprestigiar a l'altra persona (casos de ciberbullying), per exemple, publicant comentaris polèmics o denigrantes que seran vists per tercers.

- Guanyar-se l'amistat d'un menor amb la finalitat de cometre un abús sexual (casos de grooming on l'acosador utilitza la usurpació d'identitat per a accedir a comptes que servisquen de “pont” per a facilitar el contacte amb la víctima).

2. Crear un compte per a fer-se passar per una altra persona.

Encara que aquesta forma se sol donar en menors, és un dels casos més freqüentment utilitzats per a suplantar a gent famosa.

En aquest sentit, s'ha de tenir sempre present que exposar informació i dades personals sensibles augmenta de forma considerable els riscos de patir una suplantació o usurpació d'identitat.

Malgrat açò, aquest risc que suposa exposar públicament informació privada o confidencial, és a voltes difícil de comprendre per als adults, risc que es veu incrementat, en el cas dels menors, davant la seua major ingenuïtat i per tant vulnerabilitat en facilitar dades personals, tant seus com de familiars o de companys, la qual cosa obliga a augmentar la precaució.

2.1. L'enginyeria social com a eines per a la suplantació d'identitat.

Un aspecte interessant a destacar en aquest punt és el concepte d'enginyeria social, que es refereix a l'ús que fan els ciberdelinqüents de la manipulació psicològica sobre les persones per a aconseguir les seues finalitats, tenint en compte la tendència general d'aquestes a la confiança. La meta del ciberdelinqüent en aquest cas és manipular a la persona objecte de la suplantació d’identitat, mitjançant diferents tècniques perquè realitze determinades accions en el seu profit. Per exemple, obtenir informació que li permeta un accés no autoritzat a un sistema i, per tant, a la informació que residisca en el mateix. A pesar que els objectius generals de l'Enginyeria Social solen implicar activitats i contextos en els quals habitualment es relacionen adults, també és possible trobar situacions en les quals poden veure's implicats els menors.

Internet s'ha configurat com un dels espais on els enginyers socials actuen majoritàriament per a cercar contrasenyes tant de xarxes socials, on els menors participen habitualment de forma activa, com en altres espais com poden ser el correu electrònic i els entorns de jocs Online. A més, els mètodes bàsics empleats per les persones que utilitzen aquesta tècnica, essencialment marcats per la persuasió, són altament eficaces en el cas dels menors d'edat que, hagut de tant a la seua falta d'experiència i coneixements relacionats amb aquest tema com amb la seua confiança i innocència, són considerats especialment vulnerables.

Així, via Internet o a través de la web s'usa, addicionalment, l'enviament de sol·licituds de renovació de permisos d'accés a pàgines web que sol·liciten respostes i fins i tot les famoses cadenes de missatges, portant així a revelar informació sensible o comprometre la seguretat dels sistemes.

Motivacions per a la realització de suplantació d'identitat.

Com ja hem vist anteriorment, la suplantació d'identitat es pot produir per diversos motius, encara que en el cas dels joves el més comú és fer-ho per mera diversió, per a “burlar-se” d'un company/a o amb motius de venjança, en els adults els motius solen ser més profunds, i sol pretendre's crear un dany en la reputació d'una persona a través de la publicació de fotografies o informació falsa.

Aquests actes poden ocasionar greus problemes a les víctimes relacionats amb la vulneració de la seua intimitat, danys directes a la seua reputació o amb problemes socials motivats per les actuacions realitzades per la persona que usurpa la identitat de la víctima, ja que una vegada que es publica alguna cosa en la xarxa la seua difusió és immediata, fent que es perda el control sobre el contingut i que siga molt complicat solucionar-ho.

A més dels problemes de reputació, existeixen casos en els quals se suplanta la identitat d'un tercer per a cometre algun tipus de delicte sota aqueixa identitat. En aquest cas, la seua solució passa per un procés més llarg. També és molt comú que aquests fets causen perjudicis econòmics a les víctimes, quan se suplanta la seua identitat per a realitzar algun tipus de compra o transacció econòmica.

2.2. Tècniques més utilitzades per a la suplantació d'identitat.

A continuació detallem quins són les tècniques més utilitzades per a la suplantació d'identitat:

- **Phishing**: és un terme informàtic utilitzat per a denominar el frau per suplantació d'identitat, una tècnica d'enginyeria social. El terme "phishing" procedeix de la paraula anglesa "fishing" (pesca) fent al·lusió a “picar l'ham”.

  Donat el cada vegada més creixent nombre de denúncies d'incidents relacionats amb el "phishing" en el context dels menors d'edat, es fa necessària la creació i utilització de mètodes addicionals de protecció dirigits especialment a la presència d'aquest tipus de tècniques en aquells escenaris de major participació infantil i juvenil. S'han creat lleis que castiguen aquest tipus de delictes i campanyes per a prevenir i sensibilitzar als usuaris perquè apliquen aqueixes mesures de seguretat.

  Així, pel què concerneix el context relacionat amb menors, un dels serveis més utilitzats pels ciberdelinqüents per a suplantar la identitat dels mateixos són les xarxes socials. Per a açò solen emprar una sèrie d'excuses per a enganyar a l'usuari tals com enviar un missatge privat en el qual es comunique que s'han detectat connexions estranyes en el compte pel que, per a mantenir la seguretat, es recomana que es canvien les claus.

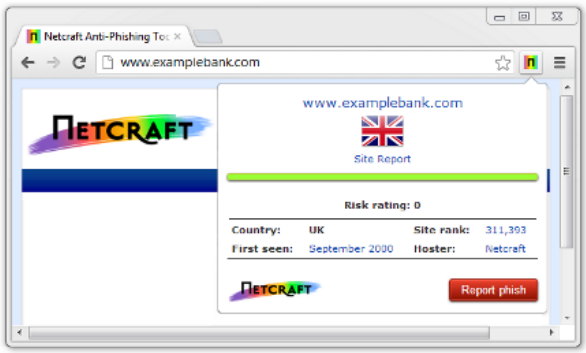
En altres ocasions, com en el cas de la imatge aportada, creen llocs web falsos amb l'aparença de la pàgina d'inici de sessió de Facebook perquè quan s'introduïsca el correu electrònic i la contrasenya es grave i conserve aquesta informació. D'una manera o un altre, l'objectiu en aquest cas és aconseguir l'accés al compte del menor per a obtenir les seues dades privades i suplantar o usurpar la seua identitat.

En el cas que ocupa en aquest monogràfic, el risc es materialitza de la mateixa manera a través de l'ús d'aquest tipus d'aplicacions a través del mòbil, ja que també s'han creat aplicacions que imiten el procediment d'identificació en xarxes socials.

Igualment, es detecten cada vegada més campanyes massives de correus fraudulents que utilitzen com a excusa l'enviament d'un document fals a través de Google Docs. Així, per a enganyar a l'usuari, siga adult o menor, sol·liciten que s'identifique per a poder visualitzar aquesta informació i així obtenir les seues dades d'accés a tots els serveis de Google.

Finalment, es troben casos de "phishing" a menors a través de jocs Online. Igual que en els anteriorment descrits, l'objectiu segueix sent apropiar-se de comptes, dades privades, bancaris i suplantar la identitat dels usuaris. Normalment, l'excusa que solen emprar per a enganyar als menors es troba relacionada amb fallades de seguretat en la plataforma del joc o en el compte dels usuaris.

- **Pharming**: És una modalitat més perillosa de "phishing" per mitjà de la qual el ciberdelinqüent infecta l'ordinador de l'usuari de manera que s'acaba redireccionant el tràfic web d'una pàgina legítima, utilitzada habitualment per l'usuari, cap a una altra pàgina falsa creada pel ciberatacant. La diferència principal amb "phishing" és que en el cas de "pharming" la redirecció a la pàgina falsa és automàtica, sense que siga necessari que l'usuari necessite prémer cap enllaç. Així, els estafadors poden entrar en el nostre equip per a modificar els fitxers a través de virus de manera que, quan s'escriu en el nostre navegador una adreça determinada, s'entra directament en una altra sense saber-ho.



> Suggeriment: instal·la en el teu navegador aquesta extensió de Netcraft per a protegir-te d'atacs de Phishing

Indicis per a pensar que han suplantat la identitat

Els menors han de conèixer l'existència de certs indicis per a detectar la possibilitat que hagen patit suplantació d'identitat. Entre ells podem destacar els següents:

- Accessos o usos anòmals dels comptes. En aquest cas, per exemple, l'indici de suplantació es manifestaria si els contactes del compte reben missatges del compte de l'implicat sense que els haguera enviat. De la mateixa manera ocorreria si li asseguren que estava en “línia” sense que fóra cert.
- Imminent desactivació d'algun servei que es tingués activat sense que s'haja procedit a açò.
- En el cas dels menors, canvis en l'estat dels jocs Online sense que els haja realitzat per si mateix.

2.3. Estratègies. Pautes i recomanacions per a la seua prevenció

Les recomanacions i bones pràctiques que s'han de tenir en compte a l'hora de navegar en Internet permeten augmentar el coneixement d'estratègies sobre seguretat informàtica, per a ser aplicades amb els menors en els entorns escolars o familiars. En el cas de la suplantació d'identitat, l'única forma d'aconseguir que els menors estiguen menys exposats a aquesta situació de risc, és la prevenció i l'ús d'una sèrie d'estratègies que minimitzen les possibilitats de patir-ho. Hem d'ensenyar una sèrie de regles bàsiques sobre seguretat informàtica.

El desconeixement sobre els riscos en seguretat informàtica i sobre els mecanismes de protecció, fan que el menor actue sense precaució en manejar la informació a través dels mitjans tecnològics. A açò se suma el desconeixement que els pares i docents encara presenten en matèria de riscos i seguretat informàtica, l'anomenada “bretxa digital” que els separa d'ells i que afortunadament cada vegada va sent menor.

Per tant, s'ha de tenir molt clar que el problema, com molts altres que es presenten en la nostra societat actual, és d'educació i per açò és fonamental la creació d'alternatives educatives que capaciten al menor per a utilitzar apropiadament els recursos tecnològics i al mateix temps estar completament informats sobre tots els perills i riscos als quals s'exposen en interactuar amb aquestes tecnologies i manejar la seua informació per mitjà d'elles.

2.3.1. Recomanacions per a prevenir la suplantació d'identitat.

Entre les recomanacions que es poden realitzar tant a pares com a menors i educadors per a prevenir el robatori d'identitat es troben les següents:

- Per a aconseguir minimitzar l'exposició de dades sensibles resulta necessari conscienciar als menors sobre la importància de limitar la difusió voluntària de dades personals i privats en xarxes socials, jocs Online, missatgeria instantània, formularis i aplicacions. Per a açò:
    - S'ha d'ajudar a configurar de forma correcta les opcions de privadesa dels diferents llocs web freqüentats pels menors a càrrec seu. Per a obtenir més informació, es pot consultar el monogràfic: Gestió de Privadesa.
    - Des del mateix exemple de l'adult, es trasllada la idea que s'ha de ser discret a l'hora de publicar fotografies en la web i, sobretot, que s'ha de «pensar abans de publicar» de forma impulsiva per a poder valorar les possibles conseqüències del comportament en la xarxa.
- Amb l'objectiu de minimitzar els riscos que puguen afectar els equips i serveis que s'utilitzen no solament s'ha d'educar als menors per a mantenir un **equip segur** a través d'actualitzacions de programari i antivirus sinó que a més es recomana:

- **Comptar amb comptes d'usuari limitats** per a cadascuna de les persones que utilitzen l'equip compartit amb contrasenyes personals per a regular l'accés a aquest. D'aquesta forma, cada usuari podrà tenir el seu propi escriptori -amb aquells arxius i carpetes als quals puga accedir- de manera que tan sols l'usuari administrador, amb permís per a poder administrar els diferents comptes, puga instal·lar aplicacions o modificar aspectes importants de la configuració. Així, es minimitza el risc d'infecció per virus i, per tant, del robatori de contrasenyes dels serveis.
- **Bloquejar les finestres emergents**. A pesar que normalment els navegadors d'Internet tenen activat el bloquejador de finestres emergents per defecte, es poden administrar definint excepcions en particular accedint a les opcions de configuració del navegador.
- **Fer ús dels filtres antispam**. Activats per defecte en la majoria de serveis web, filtren el correu electrònic que consideren brossa a una carpeta on ho emmagatzemen. El correu electrònic és una de les formes de comunicació més utilitzades en l'actualitat i per tant un mitjà molt atractiu per a la propagació de virus, missatges fraudulents, spam, etc.
- **Dur a terme una adequada gestió de contrasenyes**. En aquest sentit s'ha de tenir en compte la importància de no utilitzar una mateixa contrasenya per a diversos serveis, ja que, en aquest cas, serà molt més fàcil accedir a tots ells una vegada que s'haja aconseguit vulnerar la primera. A més d'utilitzar contrasenyes diferents, aquestes han de ser segures, és a dir, han de ser secretes, robustes (de mínim vuit caràcters, que combine majúscules, minúscules, nombres i símbols) i modificades periòdicament.
- Per a poder dur a terme una bona pràctica en l'ús de serveis tals com el correu electrònic, les xarxes socials, la missatgeria instantània o la mateixa navegació no s'ha d'oblidar que **no és recomanable accedir a enllaços que resulten sospitosos**. Igualment s'ha de tenir precaució amb les descàrregues que es realitzen, desconfiar de remitents desconeguts en correus i no obrir fitxers adjunts sospitosos. Així mateix, alguns indicis que s'han de tenir en compte per a sospitar que un correu electrònic té finalitats malicioses són:
  - Enllaços disfressats: en aquest cas, els enllaços en el correu electrònic estaran presentats de manera que semblen autèntics. Malgrat açò, existeixen alguns indicis als quals s'ha d'atendre per a poder discriminar el seu tarannà enganyós: les URL poden ser similars a les autèntiques però s'intercanvien lletres semblants entre si (per exemple, en lloc de www.spotify.com es podria enllaçar a www.spotifi.com), el

text de l'enllaç i hipervincle poden ser diferents o es poden introduir canvis en els acurtadors d'URL de manera que finalment redireccionen a llocs web no seleccionats intencionadament.

- "És urgent que actues": s'ha de ser cautelosos amb els correus que donen sentit d'urgència, amb missatges tals com: "el teu compte està a punt de ser eliminat", "el teu compte ha de ser actualitzat", etc. Es tracta d'un clar exemple de tècnica d'enginyeria social, en constrènyer al lector i dificultar que puga prendre una decisió raonada.
- Compte equivocat: s'ha d'estar segur que els correus arriben al compte adequat i a la qual s'ha facilitat d'entre les vàries que es poden tenir per a açò. En cas contrari es podria sospitar que es tracta d'un frau.

- En el cas de **jocs en línia**, s'ha de parar esment al programari del joc utilitzant el programa oficial del mateix i assegurar-se també que els plugins (programes que s'annexen a uns altres per a augmentar les seues funcionalitats) que es descarreguen siguen realment oficials.
- Es recomana valorar, en funció de la importància del servei i de les situacions de context en les quals s'accedeix al mateix (per exemple, quan s'utilitzen ordinadors públics, compartits o WiFis alienes) l'ús de mesures de seguretat amb segons factors d'autenticació o verificació, ja que les contrasenyes per si soles no són suficientment segures per a protegir la informació i documents que es consideren importants. Per tant, una de les possibilitats que es tenen a l'abast actualment i que ja està implementada en els principals serveis web és la verificació en dos passos o segon factor d'autenticació (Two Factor Authentication 2FA). Aquest mètode comporta l'exigència a Online de la introducció de dues contrasenyes separades abans de ser autoritzat per a iniciar sessió en un compte. La primera contrasenya és la contrasenya del compte principal de l'usuari, que no canvia llevat que l'usuari la canvie voluntàriament. La segona contrasenya s'envia normalment a una ubicació separada (per exemple, al telèfon mòbil) com un token de seguretat únic (un generador de codis) que caduca en un període molt curt de temps (per exemple, 30 minuts). Açò fa que a un atacant que estiga li siga pràcticament impossible detectar el segon factor d'autenticació llevat que tinga físicament el dispositiu al què s'envia el codi.
- Explicar al menor els riscos dels mecanismes de recuperació de contrasenyes tals com la pregunta secreta que demanen en crear el compte. En aquest sentit cal tenir present

que s'han d'establir preguntes secretes que solament siguen conegudes per la mateixa persona com a mesura de seguretat.

- Bloquejar l'ordinador i tancar les sessions en acabar d'usar l'equip com a mesura per a “tancar la porta” a qualsevol persona aliena al mateix.
- És important educar als menors perquè prenguen precaucions en utilitzar ordinadors públics i en connectar-se a xarxes WiFi públiques. Per açò mai s'ha d'utilitzar xarxes WiFi no confiables per a accedir a serveis on s'intercanvie informació sensible o un component important de privadesa. Per a protegir d'aquests riscos en xarxes on els altres usuaris són desconeguts podem aplicar una sèrie de mesures de seguretat tals com:
  - tenir instal·lat i habilitat un tallafocs.
  - personalitzar la configuració de xarxa en el nostre sistema.
- Establir una contrasenya per al bloqueig de la pantalla del telèfon a més dels nombres de seguretat PIN i PUK per a l'accés a la targeta SIM del mateix com a mesura de prevenció davant un possible robatori o pèrdua de dispositius mòbils. Igualment, anotació el nombre identificatiu del telèfon (IMEI) per a utilitzar-ho en cas de pèrdua i siga caut en l'ús del bluetooth. Com ja se sap, són molts les dades de caràcter personal (fotografies, missatges de text, accés a aplicacions de xarxes socials i correu electrònic o agenda de contactes) als quals es poden accedir a través del nostre mòbil.

2.3.2. Recomanacions per a educadors.

En línies generals, destacar que les recomanacions han de partir sempre des del diàleg i la participació, ja que si s'imposen normes com una forma de control i prohibició, probablement resulte més difícil la interiorització d'aquest tipus de pautes per part dels menors. Per contra, es deu enfocar la intervenció com una manera de despertar el sentit crític d'aquests perquè, progressivament, siguen cada vegada més autònoms a l'hora d'instaurar les mesures abordades anteriorment.

S'ha de traslladar al menor la importància de tots els aspectes exposats per a la protecció de la seua pròpia identitat, tenint en compte també l'ús que els adults mateixos fan de les xarxes o de qualsevol altre dispositiu, ja que per als menors som models a seguir. Per tant és recomanable que els menors vegen en les seues figures de referència, predicant amb l'exemple, bons hàbits i pràctiques en l'ús de les tecnologies en el nostre dia a dia.

Així mateix hem de traslladar la importància d'aquests aspectes per a la protecció de la seua identitat en l'activitat docent, incorporant per a açò aquestes pràctiques en la mesura del possible en les polítiques i reglaments TIC del centre.

Per a poder complir amb els objectius proposats, es recomana que s'organitzen de manera periòdica tallers de sensibilització i formació per a menors, pares, mares i comunitat educativa general.

> “ Amb l'objectiu de realitzar una **navegació** per internet el **més segur** possible, et recomanem que visites aquest enllaç i proves alguna de les eines suggerides que t'ajudaran a protegir-te i t'avisaran davant possibles riscos en Internet.

Altres enllaços d'interès:

- Han suplantat la meua identitat en Internet o en xarxes socials què faig?
- “Les nostres dades són la nostra identitat i hem de ser amos d'ella”
- La privadesa no existeix: les dades són el nou petroli
- Coneix a fons què és el phishing

3.Ciberassetjament

https://www.youtube.com/watch?v=D57vDI7w_mA

Un dels perills associat a l'ús de les TIC és el ciberassetjament, el qual es pot definir com "l'acció d'assetjar a una altra persona mitjançant l'ús de mitjans digitals".

El ciberassetjament escolar o ciberbullying és un tipus concret de ciberassetjament aplicat en un context en el qual únicament estan implicats menors. Es pot definir el ciberbullying d'una manera senzilla i concisa com "el dany intencional i repetit infligit per part d'un menor o grup de menors feia un altre menor mitjançant l'ús de mitjans digitals".

Aquesta definició contempla les principals característiques del fenomen:

- **Dany**: la víctima pateix una deterioració de la seua autoestima i dignitat personal danyant el seu estatus social, provocant-li victimització psicològica, estrès emocional i rebuig social.
- **Intencional**: el comportament és deliberat, no accidental. Tanmateix, cal tenir en compte que la intenció de causar dany de manera explícita no sempre està present en els inicis de l'acció agressora.
- **Repetit**: no és un incident aïllat, reflecteix un patró de comportament. Convé destacar que per les característiques pròpies del mitjà en el qual es desenvolupa una única acció per part d'un agressor pot suposar una experiència de victimització perllongada en el temps per a la víctima, per exemple, la publicació d'un vídeo humiliant. Per tant, l'efecte és repetit, però la conducta del que agredeix no té per què ser-ho.
- **Mitjans digitals**: l'assetjament es realitza a través de computadores, telèfons, i altres dispositius digitals, la qual cosa ho diferencia de l'assetjament tradicional.

3.1. Mètodes i mitjans per a cometre ciberbullying

A pesar que els menors fan ciberbullying de molt diverses formes, i aquestes depenen en gran mesura de les noves tendències en l'ús de les tecnologies, els mètodes i mitjans més representatius actualment inclouen:

- **Atacs directes**: insults o amenaces enviades directament a la víctima a través de xarxes socials, missatgeria instantània i correu electrònic. Robatori de contrasenyes per al segrest i tancament de perfils en xarxes socials i altres serveis web, i per al robatori de recursos de jocs en línia. Enviament de virus informàtics per a manipular l'ordinador de la víctima.
- **Publicacions i atacs públics**: rumors, missatges feridors, fotos o vídeos humiliants publicats en xarxes socials, blogs, fòrums, o enviats a través de la missatgeria instantània i del correu electrònic, i exclusió de grups en línia, amb els quals denigrar la persona implicada.
- **Ciberbullying mitjançant tercers**: ús d'altres persones i mecanismes per a exercir el ciberassetjament. Suplantació d'identitat i creació de perfils falsos en xarxes socials i jocs en línia per a enviar missatges amenaçadors o provocatius exposant a la víctima a l'escrutini de tercers. Explotació malintencionada dels mecanismes de seguretat en plataformes de xarxes socials amb el que aconseguir el tancament del seu compte.

3.2. Rols implicats

Els rols principals que participen en aquesta conducta són, en general, els mateixos que en el cas de l'assetjament escolar tradicional o bullying: **l'**assetjador**, la víctima i els espectadors**. El paper dels espectadors és clau en el desenllaç del fenomen, en veure's implicats de forma indirecta poden convertir-se en encoratjadors del fet; en subjectes passius, tractant de no implicar-se en l'acció i, per tant, consentint-la; o en defensors de la víctima que intenten ajudar-lo a eixir de la victimització. Poden existir altres rols secundaris, com els ajudants de l'assetjador que encoratgen la seua conducta estimulant i reforçant l'agressió.

En relació amb els perfils dels alumnes assetjadors no s'ha de pensar que segueixen els patrons preestablits per a l'assetjament tradicional. Les noves tecnologies proporcionen capacitats a menors que mai abans s'hagueren atrevit a coaccionar a ningú si no fora per una major habilitat a l'hora d'utilitzar aquests recursos i les falses aparences d'anonimat en la xarxa. En aquest sentit, pot evidenciar-se certa jerarquia de poder (inclosa una major competència tecnològica o prestigi social de l'assetjador o assetjadors) respecte de la seua víctima, si bé aquesta característica no es dóna en tots els casos.

3.3. Símptomes per a la detecció de ciberbullying

El ciberbullying comporta una sèrie de conseqüències que tenen un impacte en els menors en l'àmbit psicològic, social i educatiu. A continuació es presenten una sèrie de possibles símptomes o manifestacions que poden donar-se en els menors, i que poden ajudar a pares, mares, tutors o educadors a realitzar una detecció o diagnòstic precoç. L'aparició d'algun d'ells podria ser motiu de sospita:

1. **Canvis físics i emocionals:**

- freqüents manifestacions de malalties (per exemple: maldecaps o estómac).
- alteracions de l'estat d'ànim, principalment d'humor.
- moments de tristesa i/o apatia i indiferència.
- símptomes d'ansietat i/o estrès.
- signes inusuals de comportament agressiu.

2. **Canvis de conducta/socials:**

- en les seues activitats d'oci habituals.
- en la seua relació amb els adults, quant a freqüència i dependència d'ells.
- en la quantitat de menjar i maneres de menjar.
- en els hàbits de somni (per exemple malsons).
- d'improvís deixa d'usar l'ordinador i el telèfon.
- variacions sobtades en els grups d'amics, a voltes antagònics.
- autolesions, amenaces o intents de suïcidi.

3. **Canvis en el context acadèmic:**

- es veu involucrat en incidents dins de l'escola.
- es redueix la seua capacitat de concentració i de manteniment de l'atenció.
- alts i baixos en els temps d'estudi i en el rendiment escolar.
- pèrdua d'interès en l'escola.

- pèrdua i/o deterioració de pertinences físiques, lesions físiques freqüents sense explicació raonable.

3.4. Estratègies per a la seua prevenció

La prevenció de situacions relacionades amb el ciberbullying ha de partir des de la mateixa educació als menors en els riscos vinculats amb l'ús de les noves tecnologies. Dialogar i establir una comunicació positiva sobre els riscos associats a aquest fenomen ha de configurar-se com un dels primers passos a realitzar per part dels adults de referència d'aquests. Així, l'alfabetització digital, inclosa la prevenció de riscos de mal ús, ha de començar a abordar-se des dels primers contactes amb les xarxes per part dels menors, ja que és en aquest context on més oportunitats podrem trobar per a inculcar bones pràctiques i estratègies de prevenció i sensibilització.

Al llarg d'aquest apartat es presenten un conjunt d'estratègies, pautes i recomanacions que ajude a prevenir els riscos en matèria de seguretat TIC en general, i del ciberbullying en particular.

El repte al que ens enfrontem no és fàcil i paasa per l'educació, en l'àmbit conductual i en el tecnològic:

- **Nivells adequats de comunicació intrafamiliar**. Els nivells adequats de comunicació no es construeixen quan es necessiten, sinó que han d'estar ja consolidats perquè es poden utilitzar davant l'aparició de la problemàtica.
- **Educació en sensibilitat**. És important fer-los comprendre el dret i el respecte a la víctima i posar-se en el seu lloc per a evitar que s'arribe a situacions no solament de violència, sinó també d'aïllament de determinats menors.
- **Problemes ètics**. És important ensenyar als xiquets dos conceptes. D'una banda, en línia amb la informació que es rep, quina informació és creïble i quin no. I, d'altra banda, **aprendre a analitzar les conseqüències de la informació que es publica**.
- **Model col·laboratiu de resolució de problemes** entre família i escola com a forma d'abordar els problemes de ciberbullying.
- **Educar en competències digitals**. Donar a conèixer els riscos, les eines de protecció i les bones pràctiques d'ús, com per exemple, l'apropiada gestió de les contrasenyes.
- **Establir regles i supervisar d'acord amb un criteri d'edats**. Els alumnes/as es comporten de manera diferent quan senten que algú està parant esment al què estan fent. S'ha d'ajustar el nivell de supervisió a l'edat del menor. Aquests nivells hauran

d'evolucionar cap a la generació d'autonomia, el dret i la salvaguarda de la intimitat i el respecte a la imatge d'un mateix i dels altres.

- **Concepte del delicte**. Sensibilitzar-los sobre les conductes que puguen portar a conseqüències en l'àmbit familiar (càstigs), en l'àmbit escolar (Sancions) o, ja en casos més greus, fins i tot penals (delictes).

3.5. Mecanismes de resposta davant el ciberbullying en centres educatius

Tot centre ha de disposar d'un marc per a l'acció en situacions problemàtiques, i en concret, relacionat amb comportaments inadequats de l'alumnat en matèria d'ús de dispositius digitals. La intervenció ha d'estar taxada, pautada, mesura i adequadament planificada. Sempre de manera que aporte seguretat als processos de detecció, i, sobretot, d'anàlisi i valoració de les situacions, presa de decisions i configuració de processos de sensibilització i presa en consideració a partir dels fets que hagen pogut esdevenir.

A la Comunitat Valenciana disposem d'un protocol d'actuació per a aquests casos dins del pla PREVI les fases del qual són les següents:

1. Detectar i comunicar la situació.

Qualsevol membre de la Comunitat Educativa que tinga coneixement o sospites d'una situació d'assetjament sobre algun alumne o alumna, ho comunicarà a un professor o professora, al tutor o la tutora o a l'equip directiu. En qualsevol cas, el receptor o receptora de la informació sempre informa a l'equip directiu.

2. Primeres actuacions:

- **Equip directiu.** L'equip directiu es posarà en contacte amb el tutor o tutora de l'alumne o alumna afectats i, assessorats pels serveis psicopedagògics escolars, el departament d'orientació, el gabinet municipal autoritzat o el personal que tinga atribuïdes les funcions d'assessorament en el centre, arreplegarà la informació per a analitzar i valorar la intervenció que procedisca.
- **L'equip d'intervenció.** L'equip d'intervenció planificarà de forma ràpida els recursos personals, materials i organitzatius, el moment i el lloc de reunió amb els agressors, la víctima i els espectadors, sempre que siguen alumnes del centre.
- En el **ciberassetjament**, és important tenir informació de la intensitat, difusió i característiques del mitjà o dispositiu utilitzat. Si existeixen proves físiques, aquestes han de conservar-se (impressió pantalla, copia SMS), sense lesionar els drets de tota persona i respectant la confidencialitat de les actuacions.

3**. Mesures d'urgència.**

- Augmentar la supervisió i vigilància del professorat i personal del centre durant els descansos, esbarjos, menjador, banys, vestuaris, entrades i eixides del centre.
- Avisar a les famílies de la víctima, i de l'assetjador o assetjadors.
- Explicar a l'alumne/a assetjat totes i cadascuna de les mesures que es prendran per a donar-li seguretat.
- En cas de ciberassetjament, indicar a l'alumne/a, si és el cas, que ha de canviar contrasenyes i revisar les mesures de privadesa. S'insistirà que no facen desaparèixer les proves físiques que disposen.
- Es demanarà a l'alumne/a assetjat que comunique a un adult qualsevol insult, ofensa, o agressió que reba i se li oferiran els mecanismes i vies perquè ho faça amb la discreció més gran possible.
- Una vegada sentit a l'alumne/a assetjador i analitzada la situació, l'adreça del centre li aplicarà les mesures cautelars que considere necessàries, a través del procediment disciplinari, segons el Decret 39/2008.

4. Comunicació de la incidència.

- L'adreça del centre informarà de la situació i del pla d'intervenció a la Comissió de Convivència.
- L'adreça del centre realitzarà la comunicació al Registre Central i a la Inspecció Educativa.
- Si la situació s'agreuja, o sobrepassa la capacitat d'actuació del centre, s'ha d'informar a la Inspecció perquè, si ho estima oportú, sol·licite l'assessorament i/o intervenció de la Unitat d'Atenció i Intervenció del PREVI de la Direcció territorial corresponent. La Inspecció Educativa decidirà sobre la necessitat i tipus d'intervenció.

5. Comunicació a les famílies i/o representants legals de tots els implicats.

- L'adreça del centre realitzarà les entrevistes necessàries, preferentment de forma individual.
- L'adreça del centre informarà les famílies dels alumnes implicats en el conflicte de les mesures i actuacions de caràcter individual, així com les mesures de caràcter organitzatiu i preventiu proposades per al grup, nivell o centre educatiu.
- Segons la gravetat del cas, l'adreça del centre comunicarà a la família de la víctima la conveniència o no de realitzar denúncia a les Forces de Seguretat de l'Estat.

- Tal com consta en el Decret 39/2008, article 41 en aquells supòsits reincidents i en els casos en què el centre reclame la implicació directa dels pares, mares, tutors o tutores d'alumne o l'alumna i aquests la rebutgen, l'Administració Educativa, si considera que aquesta conducta causa greu dany al procés educatiu del seu fill o filla, ho comunicarà a les institucions públiques competents per motiu de desprotecció, previ informe a la Inspecció Educativa.
- Seguiment del cas per part de les Unitats d'Atenció i Intervenció i de la inspecció del centre. La inspecció i les Unitats d'Atenció i Intervenció de les direccions territorials, col·laboraran amb l'adreça del centre en el seguiment del cas en què hagen intervingut.

6. Definir mesures de tractament individualitzat amb la víctima, l'agressor/a o els agressors/as i de sensibilització amb observadors, les famílies i la resta de l'alumnat.

- Aquestes mesures i actuacions es referiran, tant a les quals siguen aplicable en el centre i en aula, com a les quals siguen aplicable a l'alumnat en conflicte. Hauran de garantir el tractament individualitzat tant de la víctima, de la persona o persones agressores com de l'alumnat espectador, i incloure actuacions específiques de sensibilització per a la resta d'alumnat.

Ciberbullying http://www.ciberbullying.com/

Protocols GVA http://www.ceice.gva.es/web/convivencia-educacion/protocolos

Pàgina web PREVI http://aplicaciones.edu.gva.es/eva/es/previ.htm

4. Grooming

https://www.youtube.com/watch?v=-x1-hdcF2TU

El grooming es pot definir com "el ciberassetjament exercit deliberadament per un adult per a establir una relació i un control emocional sobre un menor amb la finalitat de preparar el terreny per al seu abús sexual".

Suposa el **conjunt de tècniques d'engany i persuasió** que utilitza un adult per a guanyar-se la confiança i disminuir les inhibicions del menor i obtenir d'ell un benefici d'índole sexual, que és la finalitat que persegueix (grooming és una paraula anglesa que significa "engatussament").

Les accions realitzades poden comprendre delictes de corrupció i prostitució infantil, abusos sexuals, o engalipar al menor perquè li facilite material pornogràfic o li mostre imatges pornogràfiques en les quals es represente o aparega dit menor.

Així, el grooming es troba molt relacionat amb els termes pederàstia i pedofilia. Per la seua banda, la pedofilia o paidofilia és la inclinació d'un adult a sentir una atracció sexual primària cap a xiquets o preadolescents mentre que la pederàstia és l'acció que comporta a la pràctica sexual amb un menor que implica un abús per part de l'adult. La pedofilia i la pederàstia són patologies diferents, la diferència està en l'acció; els pedòfils no passen a l'acció i si ho fan els pederastes. És a dir, un pedòfil seria una persona que se sent atret pels xiquets i un pederasta és algú que comet un delicte sexual o un abús amb un xiquet.

D'altra banda, **trobem dues variants** en la manera en què l'assetjador pot realitzar l'assetjament sexual a través d'internet:

- Casos de grooming en els quals **no existeix una fase prèvia de relació i generació de confiança**: En aquest cas l'assetjador aconsegueix el material (fotos i vídeos amb contingut sexual) mitjançant l'obtenció de contrasenyes o hackeig de comptes, o de les fotos que els joves han penjat en determinats llocs d'Internet. Amb aquest material sexual comença el xantatge i l'extorsió, amenaçant de divulgar dita material si la víctima no li facilita més material o accedeix a una trobada.
- Casos en els quals l'assetjador estableix una **fase prèvia on cerca la confiança del menor** perquè li lliure material. En aquest cas, el material és lliurat pel menor i la confiança es torna l'instrument indispensable utilitzat pel groomer.

4.1. Fases del grooming

Es diferencien diversos elements o fases d'assetjament per les quals el groomer aconsegueix fer-se amb la confiança del menor i consumar l'abús. El coneixement d'aquest procés i la seua identificació permetrà la detecció i per tant la protecció dels menors.

El procés de grooming pot mesurar-se en minuts, hores, dies o mesos, mentre l'agressor es guanya la confiança de la víctima. En l'informe final del Child Exploitation and Online Protection britànic sobre l'avaluació de l'amenaça d'explotació sexual a menors es conclou que durant aquest temps d'espera, la dinàmica de l'amenaça ha canviat substancialment en els últims anys, és a dir, que el període de temps entre el contacte inicial amb el menor i l'assetjament és actualment extremadament curt, sent una característica comuna dedicar poc temps a una gran quantitat de potencials víctimes.

Fase d'amistat

Fa referència a la presa de contacte amb el menor d'edat per a conèixer els seus gustos, preferències i crear una relació d'amistat amb l'objecte de guanyar-se la confiança de la possible víctima. Durant aquesta primera fase del grooming, l'adult estudia el comportament del menor en la xarxa a partir de tota la informació que internet li ofereix (gustos, comentaris, webs que freqüenta, etc.). Estudia i avalua al menor, localitza els seus punts febles i tot el que pugues sobre la seua vida personal.

L'assetjador pot utilitzar diferents mètodes per a accedir inicialment a la víctima fins a aconseguir la seua confiança. Els més freqüents es defineixen per les següents actuacions:

- **El premi o pagament**: usant plataformes de contacte o xarxes socials on es troben els adolescents, el grommer contacta i estableix els termes de contraprestació per a adquirir el material amb el qual després acaba assetjant al menor. Poden ser regals o quantitats de diners a canvi de fotos o material sexual explícit.
- **L'engany**: En aquest cas l'assetjador es decanta per crear una falsa identitat amb la finalitat de resultar interessant per al menor i cridar la seua atenció (diu tenir la mateixa edat, atractiu físic, comparteix gustos semblants, etc.). Així, estableix una estratègia prèviament estudiada per a guanyar-se la confiança del menor a poc a poc i per a açò fins i tot podrà manipular o falsificar fotos o vídeos., fingir tenir els mateixos gustos i interessos que els menors o participar en els mateixos llocs web per a crear una falsa sensació d'amistat o familiaritat. Aprofita tota la informació per a accelerar o precipitar la confiança amb els menors.
- **La seducció**: en aquests casos, l'assetjador recorre a elements que atrauen de forma significativa a la víctima, com poden ser les seues característiques personals, aparença, etc.

Una vegada consolidada la relació, la qual cosa al principi eren inofensives converses sobre temes infantils o d'adolescents, aniran derivant cap a l'obtenció de dades personals: nom i cognoms de familiars i amics, adreces, telèfons, adreces, email, lloc de treball, etc.

Fase de relació

En aquesta fase el menor creu tenir **un amic en qui confiar** i amb el qual comparteix gustos i problemàtiques similars. La fase de formació de la relació inclou amb freqüència confessions personals i íntimes entre el menor i l'assetjador. D'aquesta forma es consolida la confiança obtinguda del menor i s'aprofundeix en informació sobre la seua vida, els seus gustos i costums. A vegades, en el transcurs d'aquesta relació s'aconsegueix que el menor accedisca a les seues peticions de naturalesa sexual, com l'enregistrament d'imatges i vídeos a través de la càmera web o enviament de fotografies a través del telèfon.

Una vegada establida l'amistat, l'assetjador proposa al menor seguir comunicant-se fóra dels fòrums per a evitar ser descobert, per a açò li proposarà continuar a través de vies o eines més privades. Una vegada establida la confiança, l'assetjador dirigeix les conservacions a temes amb contingut sexual, envia imatges o contingut pornogràfic.

Fase d'inici de l'abús

Si el menor mostra curiositat pel contingut sexual, el groomer passa a la següent fase. En aquest moment l'assetjador pregunta al menor aspectes relacionats amb la sexualitat (ex. si té borrissol púbic, si s'ha masturbat o si sap com fer-ho), li proposa un intercanvi d'imatges o vídeos, demana al menor imatges amb nus o amb poses provocatives, vídeos o trobades a través de la webcam, etc.

Si el menor facilita aquestes imatges o vídeos, l'assetjador ja té material per al xantatge i li demanarà cada vegada més contingut sexual. Si el menor no accedeix, o no segueix accedint, a les seues pretensions sexuals, el ciberassetjador comença l'extorsió, que sol consistir a amenaçar de difondre el contingut que haja capturat amb major càrrega sexual a través d'Internet (plataformes d'intercanvi de vídeos, xarxes socials, etc.) i/o enviar-la als contactes personals del menor. En aquest moment el menor es converteix en un mer objecte sexual de l'assetjador.

Fase d'abús i agressions sexuals

En ocasions, el control en la fase d'assetjament pot ser tan gran que l'abusador s'atreveix a concertar una cita amb el menor. Davant les amenaces del ciberassetjador, el menor pot accedir als seus capritxos sexuals, arribant fins i tot aquell, a contactar físicament amb el menor i abusar sexualment d'ell.

En el cas que el menor mostre dubtes per a realitzar el que li demana o es negue, l'assetjador utilitzarà frases per a manipular-ho del tipus "tu eres molt intel·ligent. Si t'enganyara t'adonaries...""Mai farem res que tu no vulgues fer.....", "Ho deixem quan tu vulgues" "tu decideixes fins a on podem arribar", etc. En altres casos utilitza arguments per a justificar socialment la

situació com per exemple "Moltes persones de la teua edat ho fan però no ho diuen per por dels seus pares", "En altres cultures les relacions entre menors i adults és alguna cosa normal".

4.2. Manifestacions i símptomes per a la detecció del grooming

El grooming és una nova forma d'abús sexual a menors, i com a tal, els efectes en els menors víctimes i les seues famílies poden ser devastadors. Els efectes del grooming abasten totes les esferes de la vida del menor i la seua família, alterant les seues relacions familiars, desenvolupament escolar així com les relacions amb el grup d'iguals i altres adults.

En un primer moment el menor pot patir problemes psicològics a causa de la manipulació, sent aquests els més preocupants doncs els seus efectes solen ser tan greus com els produïts per l'abús sexual realitzat en persona. En el cas extrem que es materialitze una trobada, les conseqüències inclouen les seqüeles físiques derivades de l'abús sexual (ferides, traumatismes i lesiones conseqüència de la violació o vexació del menor).

Encara que cada cas és únic i per tant les conseqüències del grooming poden variar, en general, en tots els contextos seran considerats símptomes d'alerta les següents manifestacions:

- **Aparició de símptomes psicosomàtics**: En els més xicotets pot aparèixer retraïment i conductes regressives (banyar el llit, xuclar-se el dit) i pors que abans no tenia.
- En totes les edats poden aparèixer **problemes de somni** (por a dormir solament, malsons, etc.), malalties i dolències freqüents, marejos, mal de cap o d'estómac, freqüents diarrees sense que s'acompanye de vòmits o febre, etc. sense que hi haja una explicació física que ho justifique.
- **Canvis en els hàbits d'alimentació** i per tant variacions ràpides de pes.
- **Conductes autodestructives**, automutilacions o lesions físiques freqüents sense explicació raonable: es fa corts, es colpeja, etc.
- Ideació i **conductes suïcides**.
- Crisi d'ansietat, ràbia.
- Fugides o **bloquejos emocionals**.
- Canvis en l'estat d'ànim: **canvis d'humor**, apatia i indiferència, agressivitat, tensió.
- Canvi en **les relacions socials**. En aquest sentit poden donar-se dos extrems que han de cridar l'atenció: Disminució de les relacions socials i aïllament social: el menor no vol eixir

de casa i mostra excessives reserves en la comunicació. O per contra un canvi brusc en el grup d'amics així com les persones i models de referència.

- **S'amaga o oculta quan es comunica per internet o mòbil.**
- **Abandona les activitats d'oci** que abans realitzava, o bé canvia bruscament d'activitats.
- Pot aparèixer una **masturbació precoç** i exacerbada.
- Trastorn de la identitat sexual
- Problemes d'autoestima.
- Pèrdua o deterioració de pertinences físiques

4.3. Estratègies de prevenció.

- **Afavorir una comunicació fluïda**: quan existeixen uns nivells consolidats de comunicació es facilita poder parlar d'internet, de les xarxes socials i dels potencials perills relacionats amb elles, resultant essencial advertir-los sobre les dades que no han de facilitar a través d'internet o xarxes socials.
- Prendre consciència de la importància d'aprendre **el bàsic sobre les noves tecnologies**, conèixer les xarxes socials d'ús més habitual entre els menors, és a dir, assumir i exercir la responsabilitat dels fills en les TIC.
- **Ús del correu electrònic**: els experts recomanen tenir dos comptes de correu: una per a coses importants, com les tasques escolars, compartida amb amics i familiars i una altra amb nick inventat, sense dades personals tals com l'edat per a ús de les xarxes socials, xat, etc.
- **Educar al menor en un ús segur d'Internet, eines, serveis i xarxes socials:** No acceptar a desconeguts en les xarxes socials, jocs Online i serveis de missatgeria. Així, respectant l'evolució cap a actuacions progressivament més autònomes per part d'aquests, l'objectiu comú ha de ser proporcionar-los les eines, coneixements i estratègies necessàries perquè de forma gradual siguen capaces de gestionar per si mateixos aquest tipus de situacions i entorns.

  D'aquesta manera, en el cas de xiquets d'educació primària es recomana realitzar una rigorosa supervisió de l'entorn en la xarxa per a garantir la seua seguretat, alhora que traslladen pautes bàsiques per al seu ús (per exemple, que coneguen a totes les persones

que tenen agregades en les xarxes socials així com que supervisen que aquests no compartisquen informació íntima o privada a través d'Internet).

Proposar una mesura com l'anterior per a menors adolescents seria, a més de complex, en certa manera contraproduent. Per açò, no hem d'oblidar la importància de fomentar el coneixement, el desenvolupament d'habilitats i valors perquè comencen a prendre decisions progressivament més independents, encara que sota el seu seguiment proper sense que aquest siga percebut com a control o prohibició externa. De la mateixa manera, educar sobre els riscos, mecanismes de prevenció i de resposta es configura, al seu torn, com a estratègies clau en el cas de menors adolescents.

- **Comptar amb una adequada seguretat en els equips informàtics**, incloure claus de seguretat o contrasenyes segures que els pares han de conèixer.
- **Utilitzar la publicació de notícies sobre grooming** per a parlar amb els alumnes d'aquest risc i fins i tot preguntar-los directament si en algun moment han sigut assetjats o si coneixen a algú a qui li haja ocorregut.
- **Utilitzar sistemes de control:** la qual cosa inclouria accions tals com limitar els horaris d'ús i accés per edats, establir criteris d'edat per a l'ús d'ordinador, tablet, mòbil, etc. i per a accedir a diferents continguts i serveis. **És recomanable que els menors no accedisquen a les xarxes socials abans dels 14 anys**, i si ho fan que siga sempre sota consentiment i estricte control parental.
- **Vigilar els jocs en xarxa**, les consoles i tots els dispositius que poden tenir accés a Internet.
- **Estar atent a l'ús que altres persones fan de les imatges o informació pròpies:** És recomanable no compartir fotos de menors de 14 anys. ja que les imatges donen molta informació que pot posar en risc al menor i permetre la seua localització.
- **Limitar l'accés a internet en cibercafés i xarxes obertes**. No consultar, ni compartir pàgines personals ni documents privats des de llocs públics o amb wifi obertes.

4.4. Mecanismes de resposta i suport davant un incident

La resposta davant situacions en les quals intervé un adult, com és el cas del grooming, unit a la gravetat d'aquest tipus de conductes i a la seua taxació en el codi penal, requereix configurar un itinerari substancialment diferent del que puguem plantejar amb caràcter general per als casos d'assetjament entre iguals a través de les TIC.

Així, és important denunciar l'assetjament en qualsevol de les seues fases i de la forma més immediata possible, amb la finalitat de protegir al menor d'un dany major. La denúncia hauran de realitzar-la els pares, responsables legals del menor, o si escau el Ministeri Fiscal. Si són persones diferents dels pares els que detecten la situació de grooming, hauran de comunicar-li-ho a aquests, i si escau posar-ho en coneixement de les autoritats.

En els nostres centres seguirem el protocol establit en el pla PREVI vist en el punt 2.5 d'aquest tema.

Com actuar davant un cas de grooming.

Si se sospita o detecta que aquesta situació s'està produint s'ha d'actuar de la següent forma:

- No cedir al xantatge en cap cas, doncs açò facilita més material (noves imatges o vídeos eròtics o pornogràfics) per a augmentar i continuar l'amenaça.
- Avaluar la certesa que l'assetjador té el material que diu tenir i les possibilitats reals que porte a terme les seues amenaces i les conseqüències.
- Evitar que el menor seguisca mantenint qualsevol contacte o relació amb l'assetjador, limitant la capacitat d'acció de l'assetjador: revisar llistes de contactes, canviar claus d'accés, revisió total de l'equip per a evitar malware, canviar el perfil (en xarxes socials, jocs Online multijugador, etc.)
- Bloquejar o eliminar a l'assetjador: eliminar el nom de l'assetjador de les llistes i bloquege el seu nom d'usuari o correu electrònic.
- Demanar que la informació generada vexatòria siga retirada del servidor de continguts d'Internet en la qual es troba, i posteriorment dels índexs dels continguts de cercadors en els quals aparega.
- Denunciar la situació a les Forces i Cossos de Seguretat de l'Estat. És convenient aportar proves gràfiques del material vexatori o calumniós (correus, comentaris en fòrums, fotos, etc.) que l'assetjador haja generat.
- Per a habilitar la via legal analitzar les il·legalitats comeses per l'assetjador i quins poden ser provades: a vegades és molt difícil demostrar que les imatges han sigut aconseguides mitjançant coacció o amenaces, i fins i tot que les haja fet públiques.
- Recopilar proves del delicte: captures de pantalla, converses, missatges, etc. tot allò que puga provar les accions de l'assetjador o donar pistes sobre el seu parador o manera

d'actuar. És especialment important cuidar no vulnerar la llei en l'obtenció d'aquestes proves.

- Formular una denúncia, amb independència que l'assetjament hi haja o no cessat.

5. Sexting

https://www.youtube.com/watch?v=D57vDI7w_mA

El sexting consisteix en la "difusió o publicació d'imatges o vídeos de tipus sexual, produïts pel mateix remitent, principalment a través del telèfon mòbil", o per altres dispositius tecnològics (tablets, portàtils, etc.). El terme sexting és un anglicisme que prové de dos vocables: “sex” (sexe) i “texting” (enviament de missatges de text a través dels telèfons mòbils). Aquesta pràctica es popularitza a partir de 2005 en països com els Estats Units, Canadà, Gran Bretanya i Austràlia, i com altres pràctiques anglosaxones, prompte es va estendre a Llatinoamèrica i a Espanya.

És important destacar que **les imatges o vídeos són realitzats pel mateix remitent de forma voluntària**, o bé són realitzats per una altra persona, però qui les protagonitza presta el seu consentiment per a açò, almenys de manera inicial. És el que es coneix com a "sexting actiu": el protagonista d'aquestes imatges apareix en fotos o vídeos en postures sexys, provocatives o inadequades. Per la seua banda, es coneix com a "sexting passiu" a l'acte de rebre les imatges.

El sexting és una pràctica que els joves realitzen com a regal a les seues parelles, com a element de coqueteig o per a captar l'atenció. **El principal risc que comporta el sexting és que una vegada que el contingut és enviat, el remitent perd el control del** mateix . El receptor de la fotografia o vídeo pot distribuir-la a tercers de forma deliberada (amb l'ànim de presumir o per venjança després de la ruptura amb la parella) o contribuir a la seua difusió involuntàriament (descuit, robatori o pèrdua del terminal). En definitiva, el contingut pot tenir difusió pública -entre el grup d'amics del receptor, en l'entorn escolar, o fins i tot, en pàgines web de caràcter pornogràfic tenint serioses repercussions socials i emocionals en la persona implicada.

De la mateixa manera, el contingut sexual també **pot ser utilitzat com un element per a extorsionar o fer xantatge al protagonista de les imatges**. D'altra banda, l'existència d'aquest tipus de continguts pot cridar l'atenció d'un depredador sexual qui, a més, pot suposar que aqueixa persona és susceptible de realitzar determinades pràctiques de risc i, per tant, ser candidata preferent per a les seues pràctiques d'assetjament. En aquest sentit, s'ha relacionat el sexting en dones adolescents amb un major índex de conductes sexuals de risc.

5.1. Factors influents en el sexting

Per a entendre millor el concepte i abordar-ho amb major exactitud s'han de tenir en compte diversos factors, influents en la seua descripció així com en el dany potencial del protagonista:

- L'origen de la imatge:
    - de producció pròpia (quan el sexting es produeix amb una imatge realitzada pel protagonista de la mateixa).
    - de producció aliena però amb consentiment del protagonista, (quan el sexting es produeix amb una imatge realitzada per una altra persona que no és el/la protagonista però és presa amb el consentiment d'aquest/a).
- El contingut de la imatge: fa referència a la càrrega sexual de les imatges.
- La identificabilitat: al·ludeix a la possibilitat d'identificar o no al protagonista de la imatge.
- L'edat del protagonista de la imatge.

Tots aquests factors afectaran tant al dany potencial que puga patir el protagonista de la imatge que es difon, com en les responsabilitats d'aquelles persones que participen en el procés de difusió.

5.2. Quins són les motivacions per a dur-ho a terme?

En l'adolescència concorren una sèrie de circumstàncies, tals com la revolució hormonal, química i psicològica dels joves, la necessitat d'autoafirmació, de definició sexual i de pertinença a un grup, que els fan més propensos a situacions de sobreexposició en temes sexuals, especialment en l'entorn proper entre iguals, als qui consideren importants per a la seua definició i encaix social. Per aquest motiu, i malgrat els riscos que suposa l'extensió de la pràctica del sexting, se segueix practicant entre els menors d'edat. Les **principals motivacions** per a ells solen ser:

- **La pressió que exerceixen els altres** (parelles, exparelles, xic/a que els agrada…) en demanar-los certes imatges compromeses.
- **Per a impressionar** (en els mateixos casos) o fins i tot autoafirmar-se i reforçar la seua autoestima quan les “respostes” enfront d'aqueixes imatges són encoratjadores i positives. No oblidem que la imatge corporal cobra un paper important en el desenvolupament del concepte que es tu d’un mateix.
- La falta d'experiència dels xics i xiques provoca que **no li donen importància a les conseqüències dels seus actes**, per la qual cosa produir i enviar sexting no és considerat pels mateixos com un perill, sinó com un element més del flirteig, o en determinats casos, com una transgressió sense majors conseqüències.
- Els adolescents prenen a voltes les imatges com un substitut de les relacions sexuals, convertint el sexting com una moneda emocional que necessiten per a mantenir viva una relació sentimental.
- **La pertinença als grups d'amics** també és un element que influeix a l'hora de realitzar sexting. En determinades ocasions, pot ser una pràctica habitual entre ells a pesar que puga no existir intenció de difondre les fotografies o els vídeos. Tanmateix, pot ocórrer que els telèfons mòbils que els contenen siguen robats o extraviats o que es produïsquen situacions sobrevingudes com a ruptures amoroses que provoquen actes venjatius relacionats amb el fenomen que ens ocupa.
- **El context cultural** en el qual viuen xiquets, xiquetes i adolescents, amb un clar i marcat culte al cos i amb la necessitat constant de tenir el millor físic i ser popular entre les seues amistats. De la mateixa manera, contribueix l'adoració que senten per determinades celebritats, per la qual cosa el fet que moltes d'elles produïsquen sexting i després es faça públic (de forma voluntària o no), **influeix perquè aqueixa pràctica es normalitze**.

Exemple d'açò pot ser el cas de l'actriu Scarlett Johansson, qui es va fer unes fotografies nues enfront d'un espill i va guardar en el seu Smartphone. Aquestes imatges van ser divulgades per un hacker (pirata informàtic), i prompte, van ser tretes de context, parodiades i ridiculitzades en les xarxes socials i en els mitjans de comunicació.

A més no hem d'oblidar que un altre important aspecte que incideix en la dimensió psicològica de la problemàtica del sexting és la **sexualización precoç de la infància**, entesa com el fenomen que avança l'adolescència a edats cada vegada més primerenques, la qual cosa ha portat als especialistes en psicologia i psiquiatria infantil a considerar fins i tot que la infància està desapareixent com a tal. A ells contribueixen els anuncis, les pel·lícules, les sèries de TV i els mitjans de comunicació en general, que erotitzen a xiquets i xiquetes, i els porten a intentar imitar comportaments adults, inclosos els sexuals, quan encara no han desenvolupat ni el raciocini necessari, ni la capacitat madurativa per a valorar el bé i el dolent que se'ls proposa. D'aquesta manera, apareix un nou concepte de concepció de la infància i l'adolescència hipersexualitzada i avançada, que “crema” etapes i no permet als xiquets i xiquetes viure cada moment de les seues vides de forma natural. Encara que es produeix d'una forma més manifesta en les xiquetes, ja que els estímuls que reben són més intensos, especialment, de caràcter estètic, també es dóna entre els xiquets, especialment adolescents. Açò els porta a adoptar comportaments i conductes impròpies de la seua edat real i que comporten riscos a molts nivells; entre ells, la producció i emissió de sexting.

5.3. Altres tendències relacionades (#aftersex)

Una altra moda molt estesa actualment, també entre els menors d'edat, i que té relació amb el sexting, és la **realització de fotografies (“selfies” o autoretrats) després de mantenir relacions sexuals**. Aquesta nova tendència, que és etiquetada o “hashtageada” en la xarxa social Twitter com #aftersex (literalment, “després del sexe”), s'ha fet molt popular. Hi ha nombrosos tweets -missatges publicats en Twitter, amb un màxim de 140 caràcters- amb fotografies íntimes, en aparença innocents, ja que no tenen per què ensenyar cossos nus o seminus, però que sí mostren cares de felicitat entre els llençols, donant a entendre el que ha succeït en aqueix mateix lloc minuts abans de les imatges.

El fenomen del #aftersex no deixa de ser una prolongació dels selfies o autofotos, però la seua pràctica té un impacte encara major entre els més joves, així com conseqüències imprevistes i que poden revestir gravetat. Part del desenvolupament emocional i social dels adolescents consisteix a "**experimentar**" **amb la seua imatge personal**, contribuint així a la construcció de la seua identitat i autoestima. Les noves tecnologies els permeten tractar i fins i tot manipular aqueixa imatge, però no sempre tenen domini sobre aquesta, ja que ja no solament comparteixen les

seues selfies en les xarxes socials, sinó que porten la seua privadesa fins al límit; tal vegada no mostrant de forma explícita, però sí insinuant i suggerint. En la seua recerca constant de l'aprovació del grup, **augmenten l'exposició de la seua imatge per a obtenir elogis**, reconeixement i aprovació, ja no solament de si mateixos, sinó de les seues parelles o conquestes sexuals.

En la pràctica del #aftersex es produeix una curiosa combinació: el benestar després d'haver mantingut relacions sexuals (alliberament d'endorfines incloses) i la disponibilitat d'un Smartphone a mà, amb les seues potents càmeres de fotos i connectivitat a Internet, sense pensar a l'excés en les seues conseqüències. Es comparteix llavors un fet íntim que arribarà, no solament als seguidors d'aqueixa persona en Twitter o Instagram, sinó també a molts altres usuaris anònims que, mitjançant l'etiqueta #aftersex, tindran accés a aqueixes imatges, identificant el rostre de qui ho protagonitza i deduint que ha mantingut relacions sexuals. Aqueixes fotografies romandran publicades en Internet durant molt temps, **causant, no sol problemes de reputació i d'identitat digital, sinó uns altres més greus com per exemple la sextorssió**.

Mes informació www.sexting.es i www.sextorsion.es

> Hi ha multitud d'eines que ens poden servir per a protegir als menors en la xarxa, són les denominades de Control Parental, en el CSIRT-CV i en IS4K tens un llistat de les més conegudes.

6. Bibliografia

- Programa de capacitació en matèria de Seguretat TIC per a pares, mares, tutors i educadors de menors d'edat. http://www.red.es/
- Internet Segura For Kids https://www.is4k.es/
- El teu decideixes en Internet www.tudecideseninternet.es
- Portal Pantalles Amigues: www.pantallasamigas.net
- Guias i estudis del CERTSI https://www.certsi.es/guias-y-estudios
- Webgrafía ampliació.

7. Autoria

Elaborat per:

Equip de Coordinació TIC del Servei d'Informàtica per als Centres Educatius

Direcció general de Tecnologies de la Informació i les Comunicacions

Obra publicada amb Llicència Creative Commons Reconeixement Compartir igual 4.0

Activitats

1. **Activitat fòrum.** Cerca almenys **dos articles** que la seua temàtica principal siga la problemàtica associada a la gestió de la seguretat, procurant que aporten visions contraposades o diferents enfocaments del problema. Han de ser articles que donen una informació rellevant, que tinguen enllaços a altres articles i que estiguen correctament redactats. Si algun d'ells és una còpia d'un altre article, procura navegar fins a l'original.

   A continuació **comparteix-los**, afegint un breu comentari a manera de descripció o destacant el més rellevant i també, a partir de les lectures proposades com a material complementari, a més de les aportades pels membres del curs, **realitza una reflexió en el fòrum** sobre l'ús segur de les TIC, la rellevància que en el mapa de les nostres competències digitals ha de tenir la capacitat per a gestionar la seguretat i una anàlisi de les eines que has usat fins al moment per a gestionar la seguretat i l'eficàcia d'aquestes eines, i comenta i enriqueix les aportacions d'altres companys i companyes.

2. Juga al joc de cyberscouts d'is4k, comparteix el resultat en facebook, twitter o qualsevol xarxa social que utilitzes habitualment amb l'hashtag **#cvtic** i envia una captura de pantalla amb el diploma final.