Cibercrim, cibercriminals i cibervíctimes

Fernando Miró Llinares

PID_00195939

Universitat Oberta de Catalunya

Índex

Introducció

És innegable que els avenços en la tecnologia també provoquen canvis estructurals en la societat i, per tant, també es reflecteixen en la criminalitat com a fenomen social que és.

Per això és important fer una anàlisi detallada de les diverses formes de la cibercriminalitat i dels actors que hi estan implicats.

Així, aquest mòdul està format per quatre apartats que permeten fer un estudi global de la fenomenologia del cibercrim i la classificació pertinent, a més de conèixer les característiques generals del perfil dels ciberdelinqüents i les cibervíctimes dels diversos tipus de cibercriminalitat.

Objectius

En els materials didàctics d'aquesta assignatura, l'estudiant trobarà les eines bàsiques per a aconseguir els objectius següents:

1. Consolidar els coneixements sobre la fenomenologia dels diversos tipus de cibercrims.

2. Aprendre a classificar els delictes realitzats en el ciberespai.

3. Comprendre els processos de victimització dels cibercrims.

4. Conèixer els diferents perfils dels ciberdelinqüents i les seves característiques.

5. Conèixer els diferents perfils de les cibervíctimes i les seves característiques.

1. Introducció: cap a una classificació criminològica dels delictes en el ciberespai

Per bé que hi ha diverses classificacions sobre la cibercriminalitat, en aquest mòdul proposem una altra classificació atenent els diferents interessos socials amb transcendència jurídica que es poden veure afectats. Es tracta d'una classificació criminològica que ens permet conèixer la fenomenologia dels diversos cibercrims i, al seu torn, analitzar el perfil dels individus que realitzen els delictes i els objectius que persegueixen.

Vegeu també

En aquest mòdul s'ofereix una classificació de *cibercriminalitat* diferent de la que es presenta en el mòdul "Delinqüència associada a l'ús de les TIC", en què es classifica la cibercriminalitat segons la incidència de les TIC en el cibercrim.

En aquest sentit, es poden distingir tres categories de delictes en el ciberespai:

- En primer lloc, distingim els atacs que tenen com a objectiu principal l'obtenció d'un benefici patrimonial.
- En segon lloc, s'agrupen tots els atacs que tenen com a objectiu una persona individual, en qualsevol aspecte del seu desenvolupament personal.
- I en tercer i darrer lloc, una altra categoria que inclou tots els comportaments que tenen un objectiu ideològic o institucional.

La primera categoria s'anomena ***cibercriminalitat econòmica***, atès que el propòsit d'aquest tipus de delicte és l'obtenció d'un benefici econòmic per part dels que realitzen el delicte. La segona categoria, anomenada ***cibercriminalitat social***, té a veure amb les relacions socials entre les persones i és la transposició al ciberespai dels crims tradicionals derivats dels conflictes interpersonals. La tercera categoria inclou tots els delictes ideològics com la difusió per Internet de missatges d'odi racial i el ciberactivisme polític, per la qual cosa s'ha anomenat ***cibercriminalitat política***.

Al seu torn, les tres categories corresponen als tres grans àmbits funcionals de l'ús de les TIC. Indubtablement, el ciberespai s'ha convertit en un espai per a l'intercanvi econòmic transnacional. Al principi, el ciberespai va tenir molta més transcendència per al desenvolupament de relacions econòmiques, per a millorar la comunicació entre les empreses i els clients, fet que comportava l'entrada al ciberespai de béns econòmics (en forma de diners, de dades valuoses, de nous serveis, etc.); a conseqüència d'això, les primeres formes de criminalitat es van centrar a aprofitar aquest nou mitjà per a obtenir beneficis econòmics. Tanmateix, avui dia, Internet també serveix perquè les persones contactin amb altres persones, per a crear xarxes d'amics, per a comunicar-se

i relacionar-se com a éssers socials, la qual cosa fa que les esferes més privades de la personalitat dels que es relacionen socialment en el ciberespai també es puguin veure afectades.

Cal no oblidar també que el ciberespai a més s'ha convertit en un àmbit per al desenvolupament de les relacions institucionals i supranacionals de caràcter no econòmic. Aquí se situa el cibercrim polític, realitzat per subjectes individuals o bé per institucions o grups, fins i tot estats, que utilitzen Internet com a forma de difusió d'un missatge polític determinat o com a forma d'atac a un estat o a unes institucions no governamentals concretes. Al cap i a la fi, el ciberespai és un mitjà magnífic per a difondre idees i missatges, un instrument poderós per a captar persones tenint en compte les seves concepcions polítiques o ideològiques, i un àmbit de risc per a les institucions que poden veure atacats els seus serveis per mitjà d'atacs de denegació de serveis o d'enviaments de *malware* que afectin els seus sistemes i les dades que contenen.

Malgrat que les tres categories comparteixen el mitjà de comissió, són fenòmens diferents, ja que la finalitat amb què actuen els cibercriminals és distinta, els objectius són diversos i, per tant, els perfils dels actors implicats són diferents tal com veurem al llarg d'aquest mòdul.

2. Cibercrims econòmics

Com ja hem comentat, en la categoria dels cibercrims econòmics s'inclouen tots els comportaments criminals que tenen la finalitat d'obtenir un benefici patrimonial, per la qual cosa hi tenen cabuda tots els atacs que afecten el patrimoni de les persones individuals o el sistema econòmic en relació amb les transaccions comercials a Internet, però també els que afecten altres béns jurídics com la intimitat o la seguretat dels sistemes, però que tenen l'objectiu principal d'obtenir un benefici econòmic.

2.1. Caracterització dels ciberdelictes amb mòbil econòmic

En molts casos, per a obtenir el benefici econòmic final cal realitzar una cadena d'atacs, per la qual cosa podem distingir dos tipus de cibercrims econòmics. D'una banda, tenim els medials o instrumentals i, de l'altra, els econòmics en sentit estricte, de manera que els primers són actes preparatoris d'aquests darrers.

N'és un exemple clar l'enviament de *spam*, una forma d'atac a un gran nombre de terminals que en molts casos és el primer pas per a una infecció posterior amb *malware*, amb intenció destructiva d'informació d'usuaris o d'empreses (de vegades amb la finalitat d'extorsió) o amb intenció d'incorporar una *backdoor* que permeti l'accés il·lícit al sistema per a apoderar-se d'informació privada o per a convertir el sistema informàtic en un *bot* que permeti, posteriorment, utilitzar-lo com a *botnet* per a efectuar un atac de denegació de serveis a un altre web o per a enviar quantitats enormes de *spam* amb la conseqüent "tornada a començar" de la cadena d'atac, o també, en la majoria de casos, per a enviar publicitat falsa darrere la qual hi ha un atac de *phishing*, el propòsit del qual pot ser, novament, la infecció amb *malware* per a efectuar el frau, o l'engany directe perquè l'usuari sigui el que envia la informació privada bancària.

També és habitual l'atac en cadena amb altres cibercrims relacionats amb la distribució il·lícita de continguts.

Per exemple, la distribució de material pornogràfic, tant si és de menors com si no, pot significar un primer pas per a un atac de *phishing* o de *pharming* per part del cibercriminal. També amb la descàrrega de material protegit per drets d'autor, que en molts casos pot amagar virus troians o infeccions de *botnet*.

En el cas de la distribució de material pornogràfic "lícit", s'aprofita l'enorme potencial de difusió d'aquest contingut per a atreure els usuaris amb ofertes de gratuïtat. Novament, la cadena comença amb un atac de *spam*, en què el correu electrònic reenvia a una pàgina de *phishing* que conté material pornogràfic i en què quan l'usuari s'enregistra amb la promesa de material pornogràfic gratuït de més impacte (contactes amb altres usuaris, videoxats pornogràfics, etc.) l'usuari descarrega involuntàriament un *malware* amb l'objectiu d'obtenir posteriorment dades privades bancàries. En el cas de la distribució de material pornogràfic il·lícit, usualment de menors, els cibercriminals moltes vegades controlen les mateixes xarxes de difusió d'aquest contingut, i aprofiten la vulnerabilitat de l'individu que tracta de descarregar-lo i el fet que la víctima de l'atac final difícilment denunciarà uns fets que el convertirien a ell mateix en autor d'un delicte, pel fet d'incloure entre els objectes que ha baixat algun tipus de *malware* que permeti posteriorment accedir als comptes corrents de la víctima o per a utilitzar el seu sistema informàtic com a part d'una *botnet* que realitzi atacs posteriors de *spam* o de denegació de serveis.

Pel que fa a la descàrrega d'obres audiovisuals o musicals, les xarxes P2P han esdevingut un àmbit de risc en què els cibercriminals simulen el *malware* com a arxius d'obres protegides amb la infecció consegüent dels sistemes quan l'usuari els descarrega.

La perspectiva criminològica ens permet comprendre, doncs, que fins i tot els atacs que semblen menys lesius com els atacs de *spam* solen formar part d'una cadena d'atac que pot acabar en una defraudació del patrimoni de la víctima o en la utilització del seu sistema per a cometre un altre tipus d'infraccions. Per tant, la prevenció d'aquests comportaments menys lesius és essencial per a evitar la proliferació de ciberatacs econòmics de tota classe i, sense entrar a considerar si mereixen o no una resposta penal, és indubtable que la gravetat d'aquests comportaments no es pot valorar tenint en compte únicament els béns individuals que es veuen afectats sinó que a més, en termes de risc penal, s'han d'interpretar com el que són, autèntics actes preparatoris essencials dels atacs lesius més nocius.

També és una altra modalitat de cibercrim econòmic el *hacking* més directe en què s'accedeix directament a la informació bancària o fins i tot a l'entitat per a realitzar el frau, generalment aprofitant les vulnerabilitats del sistema o les que ha anat creant la mateixa víctima. De vegades, fins i tot, no cal accedir al sistema i es pot recopilar la informació necessària per al frau per mitjà de programes *sniffers*. En altres casos, fins i tot, el procediment pot ser més sofisticat i, per mitjà de la mineria de dades, accedint a dades a partir dels perfils de la víctima a les xarxes socials i d'altres, es pot aconseguir informació sobre una vulnerabilitat o bé configurar un *spam* personalitzat amb més possibilitats d'èxit que el massiu.

La cibercriminalitat econòmica és, per tant, un primer gran àmbit de delinqüència a Internet, que si bé comprèn nombroses tipologies de conducta diferents entre si, totes són part del trencaclosques necessari per a aconseguir el frau econòmic final.

2.2. Els ciberdelinqüents econòmics

Malgrat que la major part de conductes criminals que s'inclouen en aquesta categoria són l'extensió de conductes que ja es realitzen en l'espai físic, els perfils dels que duen a terme cadascun d'aquests delictes es veuen modificats. De fet, no hi ha un perfil únic de ciberdelinqüent, sinó que n'hi ha molts tipus, tal com succeeix en la delinqüència realitzada en l'espai físic com veurem al llarg del mòdul.

La majoria de crims en el ciberespai que s'efectuen amb intenció econòmica estan relacionats amb *hackers* que busquen vulnerabilitats, superen barreres en sistemes o en xarxes per a accedir a un sistema o per a configurar una xarxa telemàtica o de qualsevol altre tipus, interrompen i saturen servidors

i sistemes, o dissenyen eines específiques amb la intenció final d'obtenir de l'activitat que han desenvolupat un benefici econòmic directe o indirecte en cas que siguin *hackers* contractats per grups organitzats.

Tanmateix, no hi ha un sol tipus de *hacker*; de fet, ha anat evolucionant al llarg del temps. Els primers van ser els anomenats *true hackers*, aficionats a la informàtica als anys seixanta, passant pels *hardware hackers* dels anys setanta, que van desenvolupar alguns dels equips i tecnologies més importants, i també pels *game hackers* als anys vuitanta, que van desenvolupar aplicacions de *software* per a jocs; la penúltima meta és constituïda per la dualitat *hacker*/*cracker* dels anys noranta, que inclou els que utilitzen les tecnologies informàtiques per a accedir il·lícitament a sistemes o xarxes i es diferencien segons si la seva manera d'actuar és innòcua o maliciosa, fins a arribar als *hackers* clandestins del Web 2.0 i de l'era de la tipificació delictiva de l'accés informàtic il·lícit, que es poden dedicar tant a la intromissió informàtica com a la realització d'atacs DoS, la creació de pàgines web per al frau, el disseny de virus, la infecció de *bots*, l'enviament de *spam*, i tot això amb finalitat econòmica (generalment) o bé política en el cas dels ciberhacktivistes, i actuant de manera individualitzada o formant part d'un grup, que pot ser una banda organitzada tradicional que ara opera en el ciberespai o una ciberbanda de *hackers* que uneixen esforços per a una finalitat criminal comuna.

Hackers

Cal tenir en compte que el terme *hacker* pot ser emprat des d'una concepció àmplia per a referir-se a qualsevol persona amb coneixements informàtics que realitza alguna activitat il·lícita, o simplement no autoritzada, en el ciberespai. O, des d'una concepció més estricta, per a fer referència a l'expert informàtic que busca superar barreres pel simple fet que hi són, si bé sense entrar en el camp del delicte, en alguns casos fins i tot usant els coneixements propis per a millorar la seguretat de les xarxes i els sistemes.

No s'ha de confondre el terme *hacker* amb el de *cracker*, que va ser creat pels primers per a referir-se als que per mitjà de l'accés informàtic roben informació rellevant o causen algun altre tipus de dany, i diferenciar-los així dels que superaven les barreres d'accés pel simple fet de fer-ho. Per bé que la frontera entre *hackers* i *crackers* és tan estreta que alguns la salten una vegada i una altra, i passen d'activitats lícites a il·lícites mitjançant l'ús de *nicks* diferents.

La major part de *hackers-crackers* ja no són experts informàtics sinó usuaris, generalment joves, que comencen a realitzar aquestes activitats gràcies als coneixements bàsics d'informàtica que tenen i aprofiten programes i aplicacions senzilles per dur a terme les incursions. Es tracta dels anomenats *scriptkiddies*, que, tot i que no són *hackers* experts capaços d'accedir a sistemes mitjançant programacions pròpies, realitzen els atacs informàtics, generalment després de triar les víctimes a l'atzar, aprofitant programes i *scripts* bàsics i causant danys en molts casos fruit més de la seva imperícia o de la danyositat del *malware* utilitzat que de les seves habilitats.

Els *hackers* no són els únics que cometen cibercrims econòmics. Un altre cibercriminal clàssic és l'*insider*, que aprofita la posició que té dins de la institució o empresa per realitzar l'atac. Els *insiders* són els protagonistes principals dels *data breaches*, qualsevol forma de destrucció, modificació o accés a dades d'empreses o de particulars. Generalment tenen èxit perquè és més possible que passin desapercebuts a banda que representen un risc més gran que els atacs externs, ja que tenen més accés a la informació.

No obstant això, els últims estudis apunten al fet que els grups organitzats estan creixent de manera qualitativa i quantitativa. Cada vegada destaca més la interrelació entre cibercriminalitat i delinqüència organitzada. Hi ha moltes proves que mostren que les bandes organitzades s'han aprofitat de les TIC per a facilitar o millorar la comissió de delictes com el tràfic de secrets empresarials obtinguts per Internet, l'extorsió i els ciberfraus, el blanqueig de diners per mitjà de sistemes de pagament *online*, la distribució il·legal de materials per mitjà d'Internet i l'ús d'Internet com un mercat de venda il·legal de productes falsificats i de les drogues farmacèutiques.

Dins la cibercriminalitat organitzada, cal diferenciar dos tipus de grups: d'una banda, les organitzacions tradicionals (la màfia siciliana, les màfies russes, les tríades xineses o els *yakuza*, etc.) que sumen a les seves múltiples activitats la realització de delictes per mitjà d'Internet; i d'altra banda, les ciberbandes organitzades o conjunt de *crackers* que s'organitzen com a grup criminal i l'únic àmbit d'actuació del qual és el ciberespai.

Finalment, dins dels perfils dels cibercriminals econòmics cal destacar la figura de les **cibermules**, que, des d'una perspectiva criminològica, no són cibercriminals, ja que no són autors del delicte en el ciberespai, sinó col·laboradors o recol·lectors dels beneficis a Internet que després envien per mitjans segurs de transmissió dels diners als autors del delicte (les ciberbandes) o als responsables dels grups organitzats tradicionals que operen a Internet.

Cibermulers

Els cibermulers són reclutats per Internet amb la promesa de rebre quantitats importants de diners que han de transmetre i quedar-se'n un tant per cent com a guany. Generalment, aquests cibermulers són els únics detinguts en aquests delictes i poden ser-ne fets responsables com a cooperadors necessaris o còmplices.

2.3. Les víctimes dels ciberdelinqüents econòmics

Tal com succeeix amb els perfils dels ciberdelinqüents econòmics, hi ha un gran nombre de perfils de víctimes. De fet, qualsevol usuari pot ser víctima de cibercrims de tipus molt divers, segons la classe d'activitat que realitzi l'usuari.

La majoria de conductes que pateixen els usuaris d'Internet són cibercrims econòmics i de manera concreta la infecció de virus, el *hacking* i la utilització de *spyware*. Aquestes formes d'atac tenen com a finalitat obtenir un benefici econòmic i solen ser adoptades per a realitzar el frau posteriorment, una vegada es disposa de la informació necessària.

La realització d'aquest tipus de criminalitat depèn del fet que s'hagin incorporat o no sistemes d'autoprotecció i de les accions que dugui a terme l'usuari dins del ciberespai, com ara entrar en un tipus de pàgina determinat o descarregar arxius sense conèixer-ne amb seguretat el contingut.

Internet, amb les facilitats que presenta, ha esdevingut un àmbit de comerç. Amb l'augment de l'ús d'Internet per a comprar o realitzar moviments bancaris els darrers anys s'ha convertit en un àmbit de victimització.

El primer factor que sembla que està directament relacionat amb la victimització per ciberfrau és la realització de **compres a Internet**, ja que augmenta la possibilitat de ser objectiu d'un ciberfrau en un 377%. Si es té en compte que el nombre d'usuaris d'Internet que realitzen transaccions econòmiques continua creixent, podem entendre la importància d'aquest factor i la necessitat d'incrementar la protecció per als compradors en el ciberespai.

Els compradors per Internet solen ser persones de **nivell cultural mitjà o alt** que, a més, tenen un nivell d'ingressos més aviat alt. De fet, sembla que hi ha una relació entre tenir uns ingressos elevats i un nivell formatiu més alt amb el fet de comprar més per mitjans *online*. I encara sembla més clara la relació entre el gènere i l'activitat de compra *online*. Segons tots els estudis, els **homes** solen fer més compres *online* que les dones, encara que passin el mateix temps connectats. L'explicació és que, de la mateixa manera que els homes compren més *online*, segurament, i independentment que passin el mateix temps que les dones en el ciberespai, també duran a terme altres conductes no segures, com la descàrrega d'arxius, que explicarà que tinguin un índex de victimització més elevat que les dones.

Relacionar la compra *online* amb la victimització per ciberfrau té sentit si tenim en compte que molts ciberfraus dels que hi ha tenen a veure amb aquesta activitat, però també, si pensem que quan es paga en *online* generalment es "teclegen" les dades bancàries personals de manera que s'inclouen en el sistema com a objecte potencial d'atac. Òbviament, no és l'activitat de compra en si mateixa sinó el que hi va associat el que incrementa el risc de ser víctima del delicte.

3. Els cibercrims socials

Aquesta segona categoria comprèn tots els comportaments criminals realitzats en el ciberespai relacionats amb la comunicació interpersonal i que en realitat són crims tradicionals que ara es duen a terme en el ciberespai i que per les característiques que tenen semblen delictes nous.

3.1. Caracterització dels ciberdelictes socials

Tot i que al principi Internet es va concebre com un àmbit dedicat als terrenys econòmic i empresarial, és innegable que en els darrers anys ha revolucionat la comunicació interpersonal i s'ha convertit en una eina fonamental per a establir relacions socials.

En aquest sentit s'han creat molts sistemes, des de les pàgines web fins al correu electrònic passant per la creació d'altres sistemes de comunicació com les sales de xat, els programes de missatgeria instantània com el Messenger o la creació de xarxes socials com Facebook, MySpace, Twitter, etc. En definitiva, s'ofereixen noves formes de comunicació social.

Precisasment les xarxes socials han fet un gir important a la comunicació per les implicacions que porten associades. Encara que ja hi havia mecanismes que permetien establir perfils d'amics i altres funcionalitats de les xarxes socials, no és **fins a la meitat de la dècada passada**, amb la popularització de MySpace, primer, i de Facebook i altres xarxes més localitzades geogràficament, després, que les **pàgines web que faciliten i fomenten les relacions entre persones sense els límits especials i temporals tradicionals** esdevenen un element essencial de la vida social per a moltes persones i molt especialment per al sector dels joves. Una de les raons, encara que no única, de l'èxit de les xarxes socials prové del fet que han aconseguit la convergència de molts serveis que ja oferien les TIC que fins al moment estaven separats, com el correu electrònic, la missatgeria directa, els xats, la creació de webs, els diaris electrònics, els àlbums de fotos, la selecció de música o els vídeos. Això permet als usuaris controlar el grau de comunicació amb les persones i converteix les xarxes socials, d'una banda, en esferes de desenvolupament del lleure i de les relacions socials en què el grau d'intimitat plasmat en la web pot ser molt alt, però de l'altra, també en un mitjà integral de gestió de la pròpia identitat, de la personalitat i de les relacions socials.

Xarxes socials i joventut

El paper que tenen i poden exercir aquestes xarxes socials en el desenvolupament de les relacions socials és encara molt més significatiu en els joves. En l'etapa adolescent i preadulta, en què la construcció de la identitat pròpia té una dimensió molt significativa, un instrument per a la comunicació i el contacte social com les xarxes socials pot exercir una funció cabdal en la vida dels joves. Segons les investigacions que s'han fet fins ara, els adolescents utilitzen Internet per a comunicar-se amb els amics, per a buscar-ne de nous, per a buscar parella, per a compartir informació personal, etc.

Certament, les xarxes socials en concret i Internet en general avui dia constitueixen un nou àmbit de desenvolupament personal, un nou espai vital en què cada individu s'hi està unes quantes hores al dia, es comunica amb els altres, crea relacions, etc. Ho fa des de casa o des de la feina, pel que fa a l'espai físic, però aquest espai ja no té cap importància quan el subjecte és a Facebook

comentant una opinió política, a Tuenti parlant d'un company o en el seu blog personal pujant un vídeo concret. Als efectes que ens interessen, per tant, podem dir que totes les esferes personals que, de relació amb els altres, es poden posar en perill, també ho estan en el ciberespai; i que totes les conductes criminals d'atac a les persones que no requereixin immediatesa física també es duran a terme per mitjà d'Internet.

Com qualsevol altre mitjà de difusió de continguts, des de fa temps Internet serveix per a cometre calúmnies, injúries i amenaces executades per mitjà de correus electrònics o mitjançant la publicació en pàgines web. També, la **violació de la intimitat personal**, i no solament com a part del cibercrim econòmic com a mitjà per a cometre el frau posterior, sinó amb la simple finalitat d'esbrinar secrets personals i danyar la intimitat de la víctima, es va començar a mostrar com una conducta delictiva en el ciberespai a causa de l'enorme quantitat d'informació personal que els usuaris particulars col·loquen en els sistemes informàtics i comparteixen en els correus electrònics i que es posen en risc pel fet que aquests sistemes estan connectats a la Xarxa. Fins i tot es podia atacar la lliure formació de la sexualitat dels menors, no solament per mitjà de la pornografia infantil, que en general només utilitza el ciberespai per a transmetre els continguts enregistrats prèviament en l'espai físic, sinó també per part d'abusadors sexuals que fan servir les sales de xat o sistemes de comunicació com el Messenger per a realitzar proposicions sexuals a menors que després tracten de fer realitat mitjançant un contacte amb les víctimes.

Amb l'augment de la popularitat de les xarxes socials i l'ús d'aquestes per mitjà també dels sistemes de telefonia mòbil, el catàleg de comportaments criminals que poden afectar les esferes més personals de l'individu augmenta de manera quantitativa, però també qualitativa, pel que fa a la danyositat significativament superior.

Totes les formes d'assetjament d'una persona o grup de persones a una altra s'estan començant a produir també en el ciberespai, amb el simple ús del correu electrònic o d'altres formes de comunicació que serveixin per a enviar missatges ofensius contra la víctima o d'una manera una mica més elaborada per mitjà de les xarxes socials que permeten tant l'exclusió d'una persona per part d'un grup com la creació de perfils falsos i la difusió d'imatges, vídeos i textos relatius a la víctima amb l'ànim d'ofendre-la i danyar la seva imatge o la seva dignitat.

Ciberassetjament entre adolescents

Si bé això ja es comença a produir en l'àmbit laboral com a part de les dinàmiques de *mobbing*, encara és més habitual trobar casos d'assetjament entre adolescents, especialment en l'àmbit escolar, en què no solament s'utilitza el ciberespai com una manera de reforçar l'assetjament d'un grup de menors contra un altre que ja s'esdevé en l'àmbit escolar, amb la publicació d'imatges difamatòries, de missatges o d'altres aspectes, sinó que fins i tot pot ser la principal o única forma d'assetjament tot i que amb una potencialitat lesiva semblant a la que s'exerceix en l'àmbit "real".

La Xarxa també és un àmbit favorable per a l'***stalking*** o assetjament continuat a una persona amb sol·licituds constants de contacte que la víctima rebutja de manera contínua.

L'autor del *cyberstalking* aprofita les facilitats que ofereix Internet per a comunicar-se i sumar, al típic assetjament telefònic, l'enviament massiu de correus electrònics, la sol·licitud de ser agregat a les xarxes socials en què hi ha la víctima, directament per part d'aquesta o bé per part dels amics de la víctima, la creació de blogs i webs en què es narra la relació amb la persona assetjada, entre altres possibles conductes.

També s'inclouen dins d'aquesta categoria les conductes d'**assetjament sexual** especialment a menors i que, si bé es pot dur a terme per mitjà de missatges de correu electrònic o en xarxes socials, és més habitual que es produeixin en sales de xat en què la comunicació entre l'agressor i la víctima és més directa. Segons els estudis realitzats fins ara, un de cada set joves de tretze a disset anys ha rebut una proposició sexual en el ciberespai.

La dinàmica del ***child grooming*** es divideix en quatre fases:

1) En la primera fase es produeix el primer contacte del ciberagressor amb un menor per mitjà d'Internet, generalment utilitzant el Messenger, el xat o les xarxes socials freqüentades per menors. Fingeix que és algú atractiu per al menor (un altre menor de si fa no fa la mateixa edat, un bon aspecte físic, gustos semblants, etc.) per tal de guanyar-se la seva confiança.

2) En la segona fase, l'assetjador aconsegueix que el menor li enviï alguna fotografia compromesa, que engegui la *webcam*, posi mig nu, etc.

3) Una vegada aconseguit això, en la tercera fase, quan el menor no accedeix a les pretensions de l'assetjador, aquest l'amenaça amb difondre la imatge que li hagi enviat amb més càrrega sexual per Internet o enviar-les als contactes personals del menor.

4) I, finalment, es produeixen l'abús i les agressions sexuals, quan el menor per por de represàlies accedeix als capricis de l'agressor de manera que fins i tot es pot esdevenir el contacte físic.

Una altra conducta realitzada per menors i que cal destacar és el ***sexting***, que com s'ha dit consisteix a enviar a un altre menor per missatgeria telefònica (encara que també per mitjà de correus electrònics o sistemes de missatgeria en xarxes socials) fotografies de nus, postures eròtiques o parts del cos amb la intenció de formar part d'algun missatge de tipus sexual, realitzades generalment per un menor.

Aquesta conducta d'entre les que qualifiquem de *cibercriminalitat* duta a terme per menors no és l'única en què s'utilitza el telèfon mòbil, ja que aquest també es fa servir per a enviar missatges dins de les dinàmiques del *cyberbullying*, per exemple. La singularitat d'aquest cas, però, es troba en la dificultat de considerar-lo il·lícit, ja que el mateix menor és el que realitza la fotografia de si mateix i en molts casos l'envia amb consentiment a un altre menor.

El telèfon mòbil com a instrument d'enregistrament o realització de fotografies i Internet en general i les xarxes socials en concret com a vehicle per a difondre el que s'ha enregistrat convergeixen i generen un altre tipus de conductes violentes en què, si bé l'acte criminal principal es realitza en l'espai físic i no és pròpiament un cibercrim, sí que han de ser esmentades, atès que la utilització d'aquestes imatges en el ciberespai pot tenir una entitat lesiva singular i pròpia.

En aquest cas parlem de ***happy slaming***, conductes realitzades per grups de menors o adults joves que consisteixen a enregistrar comportaments violents o vexatoris contra altres persones, generalment menors coneguts víctimes de *bullying*, però també persones grans o qualsevol altre individu que pugui ser objecte de violència i burla.

Finalment, el *cyberbullying* és la modalitat *online* de l'assetjament escolar, definit per Smith i altres com:

> "Comportamiento agresivo e intencional repetido a través de medios electrónicos realizado por un grupo o individuo contra el que la víctima no puede defenderse por sí misma".
>
> (Smith i altres, 2008, pàg. 376)

Hi ha diverses classificacions dels tipus d'assetjament depenent de l'àmbit a què faci referència. Segons el canal, l'assetjament es pot produir pels mitjans següents:

- Missatges de text que es reben en el telèfon mòbil.

- Fotografies o vídeos realitzats amb les càmeres dels mòbils i que després s'envien o s'utilitzen per a amenaçar la víctima dient-li que es faran públics.

- Trucades assetjadores al telèfon mòbil.

- Correus electrònics insultants o amenaçadors.

- Sales de xat en què s'agredeix un dels participants o s'exclou socialment.

- Programes de missatgeria instantània i pàgines web on es difama la víctima, es penja informació personal o es fan concursos en què es ridiculitza els altres.

També es pot classificar a partir de la classe d'acció que es realitza:

- Provocació incendiària
- Fustigació
- Denigració
- Suplantació de la personalitat
- Violació de la intimitat
- Exclusió
- Amenaces o infondre por

Finalment, podem distingir dos tipus de *cyberbullying*: el reforçador del *bullying* ja emprès i l'assetjament entre iguals per mitjà de les TIC sense antecedents. En el primer tipus, l'agressor és fàcil d'identificar i els efectes de les víctimes són sumatius als que patia, però també els amplifica i incrementa. En el segon tipus, es tracta d'una forma d'assetjament indirecte altament premeditat i intencionat, en què l'assetjador és desconegut, cosa que magnifica el sentiment d'impotència per part de la víctima. Es caracteritza pels aspectes següents: exigeix el domini i ús de les TIC, comprèn moltes formes o tipus d'assetjament, provoca el sentiment de desemparament legal ja que quan tanquen un web en pot obrir un altre, envaeix àmbits de privacitat i seguretat aparent com és la llar, i l'assetjament es fa públic.

3.2. Els ciberdelinqüents socials

Tal com succeeix amb els ciberdelinqüents econòmics, és molt difícil establir característiques generals dels delinqüents que realitzen ciberdelictes socials, de manera que aquesta categoria inclou delictes amb motivacions molt diferents.

Davant la incapacitat de poder analitzar cadascun dels perfils dels autors de tots els cibercrims socials, ens centrarem en els que tenen més incidència en l'àmbit de la comunicació social, com ara el *cyberstalking*, el *cybergrooming* i el *cyberbullying*.

Pel que fa al *cyberstalker*, els pocs estudis que hi ha apunten al fet que el perfil varia de l'*stalker offline*. Solen ser homes solters amb feina, que tenen coneixements mitjans o alts d'informàtica, d'una edat mitjana de quaranta anys tot i que l'interval d'edat pot variar de divuit a seixanta-set anys.

Hi ha quatre tipus de *cyberstalker* seguint la classificació proposada per Bocij i McFarlane:

- El venjatiu (*vindicative*)
- L'integrat (*composed*)
- L'íntim (*intimate*)
- El col·lectiu (*collective*)

D'acord amb aquesta classificació, el *cyberstalker* de tipus venjatiu es correspon amb el tipus més violent, que generalment té antecedents delictius. A més a més, sol tenir un nivell alt de maneig de les tecnologies i utilitza una àmplia varietat de mètodes per a assetjar les víctimes com l'enviament de correus massius, l'enviament de troians o el robatori d'identitat. El tipus integrat té com a objectiu molestar i irritar les víctimes sense la intenció de mantenir-hi cap tipus de relació sentimental. Té un nivell alt de maneig d'Internet i, a diferència del *cyberstalker* de tipus venjatiu, no sol tenir antecedents delictius ni cap historial psiquiàtric previ. La tercera categoria proposada, els *cyberstalkers* íntims, tenen com a objectiu establir una relació íntima amb les víctimes i per a contactar-hi solen emprar el correu electrònic i els webs de cites. El nivell de maneig d'Internet d'aquest tipus de *cyberstalkers* varia des del que amb prou feines en té coneixements fins al que en té un coneixement elevat. I finalment, parlem de *cyberstalkers* col·lectius en els casos en què dues persones o més s'uneixen per assetjar una mateixa víctima utilitzant mitjans tecnològics. Aquest tipus d'agressor es caracteritza pel fet de tenir coneixements amplis d'informàtica i emprar tècniques molt diverses per a assetjar les víctimes.

Quant al perfil del *cybergroomer*, a diferència del que succeeix amb el *cyberstalking*, sí que pateix modificacions pel que fa a l'agressor a l'espai físic. Des d'una perspectiva criminològica, el *cybergroomer* és menys perillós que l'agressor tradicional. Mentre que l'agressor tradicional sol dur a terme els atacs contra infants com una forma d'autogratificació a causa d'una necessitat d'exercir domini, poder o control sense ser conscient del dany que provoca, el ciberagressor realitza l'atac com a resposta a fantasies sexuals provocades per desordres psicològics, la necessitat d'escapar de la solitud, la dificultat en les seves relacions personals i la baixa autoestima, i és conscient de la seva conducta i del dany que pot fer. No té la intenció real de dur a terme les seves fantasies i en la major part dels casos es tracta d'individus que molesten els menors a Internet i que no sempre entrarien en la categoria de pedòfils i agressors violents o sàdics.

En definitiva, els ciberagressors tenen més empatia amb les víctimes, més autocontrol, menys impulsivitat i un índex de desviació sexual inferior que els agressors tradicionals.

Un dels factors presents en els ciberagressors és la relació entre l'aïllament social i l'existència d'una sexualitat compulsiva. Internet facilita el fet de vèncer la barrera de l'aïllament i comunicar-se amb altres factors que, sumat a d'altres com poder investigar prèviament el perfil de les possibles víctimes i triar la més vulnerable, augmenta la possibilitat que els abusadors sexuals potencials ho arribin a ser. Un altre punt que cal tenir en compte és que el ciberespai afavoreix l'anonimat i augmenta la sensació de seguretat de l'agressor, en el sentit que disminueix la percepció del risc de ser descobert.

Finalment, una de les formes de cibercriminalitat que més repercussió té actualment en els mitjans és el *cyberbullying*. Respecte al perfil d'agressors, se'n poden diferenciar de dos tipus: d'una banda, els proactius, que cometen atacs per aconseguir un fi; i de l'altra, els reactius, que agredeixen com a resposta a una provocació, agressió o amenaça. La majoria dels estudis situen la prevalença dels agressors entre un 4% i un 18%.

Pel que fa a les característiques dels *ciberbullies*, es troben sobretot en els cursos de segon i tercer de secundària, com succeeix en el *bullying* tradicional. Quant al sexe dels agressors, la majoria dels estudis indiquen que solen ser nois, no obstant aquest resultat, no es replica en tots els estudis, i en alguns d'aquests trobem que les noies igualen els nois en agressions i fins i tot els superen. Tenint en compte que les característiques que presenten els tipus de conductes de *cyberbullying* són de tipus psicològic i emocional, com ara insultar, estendre rumors falsos o parlar malament, no és estrany que les noies siguin les que les duen a terme, ja que en el *bullying* tradicional aquestes conductes són les que més executen les noies, mentre que les relacionades amb la força física i les amenaces les duen a terme els nois.

Finalment, s'han trobat factors que potencien el fet que un alumne es converteixi en agressor. Entre aquests factors destaquen els següents: tenir una percepció favorable sobre les conductes d'assetjament escolar, tenir coneixements específics d'Internet i utilitzar-lo sovint, tenir accés a un ordinador privat i ferne ús en estances poc vigilades.

3.3. Les víctimes dels ciberdelinqüents socials

En els darrers temps, el ciberespai s'ha convertit en un àmbit de comunicació social en què, especialment en les xarxes socials, els usuaris poden crear un perfil i traslladar al món virtual elements de representació de la seva realitat física.

Davant el gran nombre de tipus de victimització social que hi ha, esdevé molt difícil extreure elements comuns que ens permetin establir un perfil únic de cibervíctima social; tanmateix, certament alguns estudis apunten al fet que en la majoria de casos les víctimes són joves, cosa no gens estranya ja que, com mostren els estudis, la victimització social està relacionada amb la quantitat i el tipus d'ús que es fa d'Internet. Avui dia es tenen a l'abast un gran nombre d'eines com la missatgeria instantània i les xarxes socials que permeten realitzar activitats de risc, i especialment tenint en compte la facilitat d'accés des dels *smartphones*, com penjar fotos personals perquè les vegin els amics, fer comentaris sobre l'estat d'ànim o sobre notícies i temes d'actualitat, posar informació personal sobre el lloc de naixement o l'estat civil a la web personal, agregar persones al cercle de contactes individual, comentar les fotografies dels altres, tenir converses verticals en pàgines pròpies o alienes, mantenir converses privades en xats de les xarxes. Totes aquestes formes de comunicació estan més generalitzades entre la població juvenil i per tant no és estrany que els joves siguin els que més pateixen aquest tipus de victimització. Així i tot, els joves no són les úniques víctimes d'aquest tipus d'atac; els adults també poden ser víctimes de ciberassetjament a la Xarxa.

Els adults, concretament, són els que pateixen més les conductes de *cyberstalking*. El primer problema a què s'enfronten els investigadors a l'hora d'estudiar la victimització per aquest tipus delictiu és que **inclou moltes conductes com ara assetjament**, contacte repetit no volgut, robament d'identitat, rebre insinuacions sexuals, amenaces, etc. i que **dificulten el fet d'establir característiques generals dels victimitzats**.

> Un exemple clar d'aquesta dificultat són les dades de prevalença del fenomen tan diverses. Així, el percentatge de víctimes que ofereixen els estudis varia entre el 4% i el 41% depenent generalment de la manera com s'avalua. Entre les conductes que més es pateixen trobem les de rebre el contacte repetit no volgut de persones a les quals prèviament se'ls ha demanat que parin, publicar informació sense autorització i suplantar la identitat, i en menor grau trobem les conductes d'amenaces i assetjament sexual.

Malgrat els escassos estudis que hi ha sobre els perfils de les **víctimes de *cyberstalking***, sembla que hi ha concordança en les característiques de la modalitat *offline*, en què en la major part dels casos les víctimes són **dones de menys de trenta anys no casades o divorciades**. Efectivament, tots els estudis indiquen que tenen més risc de patir aquest tipus de cibervictimització les dones, fins a dues vegades més que els homes, encara que aquests també són víctimes d'aquest tipus de delinqüència. A diferència de l'*stalking*, és molt més probable que la víctima no conegui l'agressor.

També s'ha comprovat que **la víctima més probable és l'agressor**, si més no així es constata en l'estudi en què van determinar que el que realitza més comportaments desviats a Internet com contactar amb algú unes quantes vegades quan li han demanat que pari, assetjar o molestar algú per Internet, sol·licitar sexe a algú que no ho vol, amenaçar per Internet, baixar música o pel·lícules pirata i enviar o rebre imatges de contingut sexual, incrementa la probabilitat de patir actes de *cyberstalking* o, potser amb més precisió, de *cyberharrassment*.

En concret, multiplica per sis la probabilitat que algú contacti unes quantes vegades amb algú quan prèviament se li ha demanat que no ho faci, per deu la probabilitat de patir assetjament *online*, per quinze les sol·licituds de sexe no desitjat i el *cyberstalking* en general augmenta catorze vegades.

Altres factors de risc associats són l'ús constant de les xarxes socials i, d'una manera específica, el major nombre de fotos pujades a les xarxes socials, el nombre d'actualitzacions d'estat i el nombre de comptes de xarxes socials. També, la missatgeria instantània i el contacte amb estranys. Això indica que el **comportament de la víctima a Internet és un predictor significatiu de la victimització**.

Vegeu també

Com veurem en el mòdul "La prevenció del ciberdelicte", cal tenir en compte aquests elements amb vista a la prevenció del delicte i, sobretot, si pensem en les greus conseqüències que pot tenir per a les víctimes.

Certament, les conseqüències poden variar molt depenent dels diversos factors que hi intervenen; tanmateix, s'ha trobat que entre les conseqüències més habituals hi ha els canvis bruscos d'humor i son, tenir malsons, trastorns d'alimentació, ansietat, angoixa, impotència i por per la seguretat.

Per acabar el perfil de les víctimes de *cyberstalking*, convé destacar que si bé no existeixen estudis que permetin establir la xifra negra sí que n'hi ha que parlen de les **raons per les quals les víctimes prefereixen no denunciar la situació d'assetjament a la Xarxa**, i són principalment tres:

- En primer lloc, hi ha tipus de conductes que la víctima no pot denunciar com a assetjament perquè no estan recollides com a tals.

- En segon lloc, hi ha casos en què la víctima considera que els actes no constitueixen delicte o no són prou greus perquè la policia els tingui en compte.

- I en tercer lloc, la persona assetjada considera que denunciar no servirà per res. En alguns casos es menysprea aquest tipus de delinqüència i se'n minimitza la gravetat pel fet de no haver-hi contacte físic entre l'assetjador cibernètic i la víctima; no obstant això, pot ser tan amenaçador i aterridor com els casos d'assetjament tradicional.

Dins d'aquest apartat, ara parlarem d'un sector que també és víctima de cibercrims socials i que requereix més protecció per part de tots els sectors de la societat atesa l'especial vulnerabilitat, els **menors**.

Si casa i l'escola, la protecció familiar i institucional, semblaven barreres complexes de superar, ho són una mica menys des del moment en què s'ha obert als menors, i també als agressors potencials d'aquests, una finestra tan gran per a la intercomunicació social com és el ciberespai.

Citació

"Internet ha posat fi a l'era de la casa com a refugi, igual que l'artilleria va posar fi a la del castell com a fortalesa."

K. Pease (2001, pàg. 24)

Entre els usuaris privats que són víctimes potencials de la cibercriminalitat, actualment, per la importància social que tenen i pel creixement exponencial de la seva incorporació al ciberespai, destaquen els menors d'edat, nascuts ja

en l'era d'Internet, acostumats totalment a l'ús de les TIC i tendents a passar molt més temps en el ciberespai que qualsevol altre usuari, que també veurem posteriorment i en farem una anàlisi més detallada.

Els menors poden veure atacat el seu **patrimoni**, quan s'intenta utilitzar la seva ingenuïtat per a fer-los estafes tradicionals realitzades per mitjans informàtics o bé danyar les dades informàtiques que tinguin mitjançant els atacs de *malware*; tanmateix, aquest no és el bé jurídic que està més en risc en el seu cas. Més aviat es poden veure afectats per la cibercriminalitat béns jurídics personalíssims com la intimitat, la llibertat sexual o la lliure formació de la sexualitat pels que estiguin en període de formació en aquest àmbit.

Pel que fa a la **intimitat**, avui la Xarxa és la forma d'interrelació social més poderosa que existeix, i en una època en què la cerca de la identitat porta a multiplicar la comunicació social amb l'adolescència, instruments com el correu electrònic o les xarxes socials poden ser tant un magnífic instrument per a conèixer altres joves, com una perillosa manera de difondre informació privada que pot ser utilitzada amb finalitats dolentes.

Succeeix una cosa semblant amb la **llibertat sexual** i la **lliure formació de la sexualitat** en el cas dels menors de tretze anys. Per a aquests, Internet no solament és un mitjà d'informació que pot ser perillós sense cap tipus de control educatiu, sinó que especialment és un mitjà de proliferació de la difusió de pornografia infantil que reverteix en la multiplicació d'aquest fenomen i en la consegüent explotació de milers de menors arreu del món per al lucre d'organitzacions criminals poderoses. En el cas dels adolescents, la Xarxa també pot convertir-los en objectiu d'assetjadors sexuals que aprofitin l'anonimat del ciberespai per fer-se passar per "iguals" i establir un primer contacte per tractar d'aconseguir posteriorment el contacte sexual.

L'ús d'Internet per part dels menors està augmentant d'una manera exponencial i ho continuarà fent els propers anys. Els últims estudis apunten que el primer mòbil s'adquireix cap als deu anys i el primer *smartphone*, entre els dotze i els catorze anys. Però el més significatiu és que aquest ús massiu d'Internet per part dels joves es realitza sense pràcticament cap control dels pares.

Hi ha molts estudiants que utilitzen els seus ordinadors personals, *smartphones* i altres serveis mòbils i els dels amics sense cap supervisió dels pares, i sense cap orientació prèvia, ni de la família, ni de les institucions escolars o d'altres de públiques sobre l'ús segur d'Internet. I això es correspon amb la constatació que la major part dels pares, professors i adults en posicions de responsabilitat en relació amb els nens estan desinformats sobre els riscos del ciberespai i no són capaços d'educar per a prevenir els menors dels atacs en el ciberespai. La qüestió és important, ja que, segons estudis recents, el monitoratge per part dels pares del comportament dels menors a Internet redueix significativament el risc d'estar exposat a materials o a conductes perillosos.

En el mateix estudi, però, es constata que l'eficàcia del monitoratge disminueix a mesura que augmenta l'edat dels menors. A això, cal sumar-hi la conclusió d'altres estudis relatius a l'efecte de les mesures de protecció parental per a evitar la victimització *online* dels menors. La instal·lació de filtres i altres formes de programari per al control parental no té efectes significatius en l'exposició dels menors a continguts nocius o en la victimització per cibercrims.

L'anàlisi de les conductes que realitzen els menors a Internet és necessària per a conèixer el procés de victimització. Respecte a les xarxes socials, el 55% les usa com una forma de comunicació social per a les relacions d'amistat, amoroses i familiars, però també per a contactar amb desconeguts o amb coneguts com companys de l'escola. I l'ús no és del tot ocasional: el 23% dels joves visita el seu perfil unes quantes vegades al dia, el 34% almenys una vegada al dia, i el 17% com a mínim una vegada a la setmana; i de tot això en la major part dels casos els pares no en tenen coneixement segons els mateixos menors: el 42% dels enquestats que accedien a les xarxes socials afirmaven que els pares coneixien l'existència del seu perfil, però només el 26% confirmaven que la família l'havia visitat.

L'accés i la utilització de xarxes socials comporta, d'alguna manera, la realització d'activitats que poden incidir en una victimització potencial:

- El 49% penja informació personal relativa a l'escola on estudien,
- el 29%, el nom complet,
- i el 29%, l'adreça de correu electrònic,
- però també és alarmant comprovar que el 59% intercanvia imatges amb contingut sexual, entre les quals destaquen les fotografies amb nus parcials d'homes (el 28%) i de dones (el 17%).

Juntament amb les xarxes socials, també és habitual l'ús dels canals de xat per part dels menors i, com veurem més endavant, aquest àmbit de comunicació comporta un risc més gran de victimització que altres vies com les xarxes socials a causa del tipus de contacte virtual immediat que el caracteritza. El percentatge de menors que fa ús d'aquest tipus d'eina és d'un 18%, però pel que sembla s'està deixant d'utilitzar i se substitueix per altres formes d'interrelació personal en les xarxes socials.

Passa una cosa semblant amb l'ús de l'*e-mail* per part dels menors d'edat; malgrat que és una eina potent per a la comunicació entre les persones, el seu ús està essencialment associat a la comunicació professional i, per tant, a l'entorn laboral, i l'ús que en fan els menors d'edat és escàs (el 14%) segons els estudis que hi ha actualment.

Per contra, els blogs són eines de comunicació que han començat a ser molt populars entre els adolescents. El percentatge d'adolescents que han creat un blog o diari personal en el ciberespai va passar d'un 19% el 2004 a un 28% el 2006. Hi ha diferències significatives d'ús segons el sexe: les adolescents creen blogs en un percentatge molt més alt (35%) del que ho fan els adolescents (20%), i aquesta diferència de percentatge augmenta amb l'edat (les adolescents de quinze a disset anys els creen en un 38% respecte del 18% dels adolescents de la mateixa edat).

Si analitzem de manera concreta els perfils dels menors que són víctimes, aquests perfils dependran del tipus de comportament delictiu a què fem referència. Així i tot, en general la investigació demostra que la majoria dels menors són victimitzats per persones properes al seu entorn.

En el cas concret del *cyberbullying*, el percentatge de menors que diuen que han patit algun tipus de conducta varia entre el 20% i el 50%, percentatge que es redueix a un interval del 2% al 7% quan la violència patida és greu. I aquesta variació de dades es deu a les diferències metodològiques en els estudis, cosa que impedeix fer una generalització sobre la prevalença i la incidència del fenomen.

Tampoc no hi ha coincidència en els percentatges relatius al gènere. Alguns estudis informen sobre la tendència dels nois a ser agressors i de les noies a ser víctimes, mentre que altres estudis no hi troben cap diferència. Aquestes dades, malgrat la necessitat de més investigació, sembla que contradiuen les xifres del *bullying* tradicional, en què tant els agressors com les víctimes són majoritàriament nois, excepte en determinades conductes com "parlar malament", que les fan i les reben més les noies.

Quant a l'edat, passa una cosa semblat. Alguns estudis assenyalen que com més edat més probabilitat de risc hi ha, mentre que d'altres situen la franja de més risc entre els dotze i els quinze anys, i fins i tot hi ha altres estudis en què el factor important no és l'edat sinó les accions que duu a terme l'estudiant com veurem tot seguit.

Un dels elements predictors més importants, que augmenta la probabilitat de ser víctima en un 70%, és ser agressor. Això enllaça amb altres estudis, com el de Patchin i Hinduja, que mostra com a element configurador significatiu del ciberagressor el fet d'haver estat prèviament víctima. Per contra, els estudiants que havien estat víctimes tenien un índex de risc lleugerament inferior de ser ciberassetjador que els estudiants que no ho havien estat.

Lectura recomanada

S. Hinduja; J. Patchin (2008). "Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace". *JA* (vol. 31, núm. 1).

Un altre factor associat a la victimització és la freqüència d'accés a Internet tant per als nois com per a les noies. Respecte a l'ús concret, els joves que han participat en més activitats en línia són més propensos a experimentar l'assetjament en línia. En concret, l'ús de la missatgeria instantània i les *webcams* augmenten la probabilitat de ser assetjats de manera repetida.

També s'ha demostrat que els infants que tenen pares menys acostumats a la pràctica d'Internet tenen més probabilitats de convertir-se en víctimes. En relació amb els adults, cal destacar que més de la meitat de les cibervíctimes no els informen dels incidents i només el 35% dels alumnes que són testimonis d'aquest tipus d'accions ho fan, la qual cosa pot indicar que, de la mateixa manera que succeeix amb el *bullying* tradicional, impera la llei del silenci.

D'altra banda, i en relació directa amb les característiques especials del nou àmbit d'oportunitat criminal que és el ciberespai, sembla que hi ha una relació entre l'anonimat que pot oferir Internet i la victimització per ciberassetjament en l'àmbit escolar. Aquesta conclusió es pot derivar de la dada que gairebé la meitat de les víctimes cibernètiques no coneixen els assetjadors. Davant la necessitat d'un contacte personal i directe que comporta el *bullying*, amb els riscos conseqüents que això comporta per a l'agressor, a més de la percepció pròpia del dany que s'està fent, el ciberassetjament permet ocultar la identitat de l'agressor i, d'aquesta manera, evitar les conseqüències o si més no l'efecte d'aquestes en la motivació de l'agressor.

Riscos per a l'agressor

Especialment el risc de ser identificat, però també de rebre represàlies o de percebre un retret social.

Finalment, la investigació ha demostrat que el *cyberbullying* té conseqüències psicològiques per a les víctimes, entre les quals destaquen que el 42,5% se senten frustrades, el 40% enfadades i el 27% tristes. Altres estudis parlen de l'ansietat i la depressió com a factors de risc per a patir victimització; no obstant això, cal tenir precaució amb aquestes conclusions ja que aquests factors poden ser tant la causa com la conseqüència del fenomen.

Juntament amb el *cyberbullying*, el comportament criminal en què es pot produir una victimització significativa dels joves és l'*online grooming* o ciberassetjament sexual a Internet. El *grooming*, terme que els analistes dels depredadors

sexuals utilitzen per a referir-se a les conductes d'acostament dels pederastes a les víctimes prèvies al mateix contacte o atac sexual, ha passat dels parcs a la Xarxa, on per motius obvis són molts més els menors, especialment les noies, que poden ser objecte d'un atac d'aquest tipus.

En la qüestió del perfil de les víctimes potencials del *grooming*, i deixant de banda l'estudi dels trets de la personalitat que incideixen en el risc de patir un atac d'aquest tipus, és especialment interessant a l'efecte de valorar posteriorment el model penal d'intervenció la qüestió de l'edat de la víctima. El Codi penal ha situat el sostre legal en tretze anys, respecte del que establia primerament l'esmena que va presentar la necessitat de tipificar el precepte que es remetia com a límit a la "minoria d'edat". En el *grooming* tradicional, el dut a terme pel pedòfil, hem vist que l'objectiu de l'agressor és el menor de dotze anys; tanmateix, els estudis que s'han fet fins avui assenyalen que en el *grooming* en què s'utilitzen les TIC l'edat de la víctima augmenta. El 99% de les víctimes d'intents d'atacs sexuals per mitjà d'Internet tenien edats compreses entre els tretze i els disset anys, l'1% eren víctimes de dotze anys, i no hi havia atacs a menors d'aquesta edat. És significatiu, a més, que el 48% dels atacs de *grooming* es duien a terme a menors de tretze i catorze anys. Això concorda amb la manera de comportar-se dels joves a Internet i amb l'evolució de la "innocència" en els menors: fins als catorze anys els menors tendeixen a retreure's i a vigilar a l'hora de tractar aquestes temàtiques i de contactar amb estranys a Internet. Això canvia a partir dels quinze anys, quan els menors comencen a prendre riscos, a contactar amb persones desconegudes i a renunciar a part de la seva privacitat.

Ara, per contra, ens interessa analitzar la victimització i, especialment, els aspectes de la pròpia conducta de la víctima en relació amb el risc de ser víctima d'un ciberatac de *grooming*.

Doncs bé, l'anàlisi de la conducta de ciberassetjament sexual a menors constata que pràcticament totes les modalitats d'atac es configuren entorn d'una dinàmica semblant en què el pas inicial sol ser l'enviament previ, per part de la víctima, d'informació personal a persones desconegudes.

Efectivament, els estudis victimològics que s'han fet fins avui sembla que demostren que, si bé el simple fet de penjar informació personal en pàgines web o en xarxes socials no és un factor que incideix en l'augment de risc de rebre un atac de *grooming*, sí que ho és enviar directament informació personal a desconeguts. La dada és important si tenim en compte que el 55% dels usuaris joves de dotze a disset anys fan pública part de la seva informació en webs o en xarxes socials, i també és lògic si tenim en compte que l'individu que realitza

grooming duu a terme un acostament personal que tindrà més possibilitats de ser reeixit si la mateixa víctima ja s'ha prestat a enviar informació privada a l'agressor.

Novament, les activitats quotidianes de la víctima, en aquest cas una d'estretament relacionada amb la seva privacitat, constitueix un element decisiu en la selecció de l'agressor de la víctima del ciberatac.

4. Els cibercrims polítics

El ciberespai també s'ha convertit en un mitjà de comunicació poderós que serveix als estats i les institucions per a aplicar polítiques. Internet es pot convertir, per tant, en un instrument per a la lluita política o ideològica de moltes maneres diverses: pot ser un mitjà de transmissió de la informació que al seu torn pot ser una forma de captació ideològica molt poderosa, pot ser un mitjà per a l'atac a serveis estatals o institucionals de tot tipus en un moment en què tots els estats depenen d'alguna manera i en moltes de les funcions que duen a terme del funcionament d'Internet, i pot ser un mitjà senzill de comunicació entre individus o grups separats geogràficament però units per una mateixa finalitat política o ideològica.

4.1. Caracterització dels ciberdelictes polítics

Entre les diverses formes de cibercriminalitat política destaca especialment el **ciberterrorisme**, que es refereix a la utilització d'Internet per a dur a terme atacs terroristes que atemptin contra la vida o la salut de milers de persones arreu del món.

El terme *ciberterrorisme* es va utilitzar al principi o bé per a referir-se als atacs a sistemes informàtics amb efectes tan greus que generaven un temor comparable al que produeix el terrorisme tradicional o bé per a englobar els atacs a sistemes informàtics motivats políticament i realitzats per a intimidar o coaccionar els estats a canvi de determinades prestacions; avui, aquesta paraula s'utilitza, en sentit ampli, per a referir-se a l'efecte de risc social que comporta la unió entre el terrorisme global i les noves tecnologies de la informació i la comunicació, és a dir, per a englobar tot un grup de comportaments diferents duts a terme per organitzacions terroristes però caracteritzats tots ells per la utilització de la Xarxa per a la difusió i la comunicació de continguts relacionats amb l'activitat de la banda armada o per a la realització d'atacs informàtics directes, tal com ja han demostrat alguns estudis criminològics.

Al seu torn, els delictes de ciberterrorisme es poden dividir en les tres categories següents:

1) Incitació i propaganda terrorista

2) Activitats de suport informacional

3) Ciberatacs directes

1) Dins del primer grup, **incitació i propaganda terrorista**, s'inclouen les accions relacionades amb l'ús de les TIC per a dur a terme amenaces contra persones en concret, estats, organismes o formes d'organització social i cultural, com ara fòrums de propaganda de terrorisme islamista, en què s'enalteixin i es justifiquin les seves activitats, etc.

2) En el segon grup, **activitats de suport informacional**, s'inclouen les accions en què s'utilitzen les TIC per a difondre missatges interns o ordres explícites o fins i tot per a recaptar fons per mitjà de pàgines web de suposades associacions benèfiques o d'ONG; com a forma de reclutament de futurs terroristes mitjançant fòrums, xats i canals IRC, visitats per individus receptius a aquesta ideologia extremista; com a "camp d'entrenament virtual" per als terroristes, amb la transmissió dels coneixements necessaris per a realitzar els atemptats o per a dotar-se dels instruments necessaris per a fer-ho.

3) En tercer lloc, els **ciberatacs directes**, entre els quals destaquen principalment la denegació de serveis contra objectius sensibles de l'estat que s'ataca, en què aquest és l'objectiu directe, o bé com una manera d'impedir l'exercici dels serveis d'intel·ligència o qualsevol altre servei necessari per a la defensa de l'estat de què es tracti. També entrarien dins d'aquesta modalitat l'enviament de *malware* o el mateix accés informàtic il·lícit sempre que l'objectiu sigui danyar una estructura de defensa de l'"enemic".

Una altra forma destacada de cibercriminalitat política és la **ciberguerra** o guerra cibernètica, que consisteix en la utilització d'Internet per part de governs de tot el món per a realitzar atacs contra altres estats o institucions.

Exemples de ciberguerra

Un clar exemple de ciberguerra va ser l'atac de denegació de serveis de Rússia a Geòrgia durant la guerra d'Ossètia i la infecció del virus *Stuxnet* als sistemes informàtics del programa nuclear iranià dut a terme per Israel.

Finalment, dins la cibercriminalitat política podem incloure els atacs de **ciberhacktivisme**, que cada vegada adquireixen més rellevància. Comprèn tot un conjunt d'atacs duts a terme per *hackers* informàtics, però no amb una finalitat maliciosa de defraudar les víctimes, de robar-los informació per a traficar-hi o de causar danys per a perjudicar-los econòmicament, ni tan sols amb la simple voluntat de superar barreres que semblava que distingia els *hackers* i els *crackers*, sinó amb la intenció de llançar un missatge ideològic, de lluita política i defensa d'idees generalment relacionades amb la llibertat a Internet, si bé hi tenen cabuda altres conviccions ideològiques.

El hacktivisme o ciberactivisme polític es pot manifestar en atacs de diversos tipus, des d'atacs de denegació de serveis contra pàgines web, fins a l'entrada il·lícita en webs aliens per a canviar-ne el contingut públic i adequar-lo als seus missatges, passant per la difusió lliure de programari que permeti la realització d'aquests atacs per altres usuaris, la creació de blogs i web o de grups en les xarxes socials més importants en què s'informa dels objectius politicoideològics del hacktivisme, s'organitzen protestes i accions i es defineixen els objectius que s'han de combatre.

4.2. Els ciberdelinqüents polítics

Així doncs, no hi ha un perfil únic de ciberdelinqüent polític. Com hem vist en el subapartat anterior, la cibercriminalitat política comprèn delictes diversos i, si bé hi ha un objectiu polític o ideològic, presenta perfils molt diferents. No és el mateix el *cyberhate* que la ciberguerra duta a terme pels serveis d'intel·ligència dels estats o el ciberterrorisme comès per grups organitzats.

La primera tipologia que destaquem és la dels grups més o menys organitzats que realitzen tant el ciberhacktivisme com el ciberterrorisme. Aquests grups solen ser agrupacions en forma de cèl·lules horitzontals unides en l'eix vertical únicament per un missatge o idea comuna que es transmet a totes i que cadascuna executa a la seva manera. Aquesta estructuració, pròpia del terrorisme d'Al-Qaeda, pot ser present d'una manera més tènue en els grups terroristes més tradicionals que operen en el ciberespai i que segueixen sota l'estricte ordre jeràrquic, però sobretot és present en el terrorisme jihadista que utilitza el ciberespai com a forma de transmissió global de missatges d'odi i d'incitació a la violència. Aquest mateix tipus de funcionament organitzatiu en què l'únic ordre jeràrquic és ideològic o "de missatge" i en què a partir d'aquí hi ha unes relacions horitzontals i no verticals entre tots els membres del grup, sembla que domina també en el hacktivisme, tal com mostra, segons les dades que hi ha fins avui, el desenvolupament del grup Anonymous.

Anonymous

Anonymous és un grup de hacktivistes obert i indefinit, format per *hackers* entre els quals hi ha experts i també iniciats, que estan units per conviccions ideològiques antisistema, en general, i en concret contràries a les restriccions legals a Internet, que realitzaven activitats *hacker* en general i atacs DDoS en particular a estats i organitzacions empresarials.

Els ciberactivistes solen ser grups oberts i indefinits de persones que tenen coneixements informàtics entre les quals hi pot haver tant *hackers* com iniciats, generalment joves, units per conviccions ideològiques antisistema, en general, i en concret contràries a la restricció d'Internet. El poder d'aquest tipus de grups rau, d'una banda, en la fàcil substituïbilitat dels membres que en formen part unida a la immutabilitat de la idea o missatge; de l'altra, en l'atractiu que té per a un sector de la població com el juvenil que pràcticament ha entrat en l'etapa adulta alhora que ha explotat el ciberespai com a lloc d'interconnexió mundial, les idees consistents a fomentar que Internet es mantingui lliure d'intromissions i censures.

A més dels grups organitzats, els cibercrims polítics també poden ser perpretats per un individu sense cap relació organitzativa amb altres subjectes. Això sol succeir amb el *cyberhate*, en què una persona crea una pàgina web en què difon missatges d'odi sense dependre de cap estructura organitzativa, i amb el hacktivisme, en què una persona ataca altres webs o institucions per conviccions polítiques.

Jester

Jester és un *hacker* que els anys 2009 i 2010 va realitzar atacs contra el que ell havia definit com a "webs jihadistes" utilitzant el programa que va anomenar *Xerxes* i va afectar més de vint-i-nou pàgines web.

4.3. Les víctimes dels ciberdelinqüents polítics

Les **víctimes dels ciberatacs polítics** tampoc no responen a un perfil concret; de fet, n'hi ha tants com tipus de cibercrims existeixen. No obstant això, a diferència de les víctimes que ja hem estudiat en aquest mòdul, presenten la particularitat que en general **s'adrecen a un col·lectiu o un estat**.

Dos exemples: denegació de serveis a Geòrgia i infecció del virus *Stuxnet*

En són dos exemples clars l'atac de denegació de serveis de Rússia a Geòrgia durant la guerra d'Ossètia i la infecció del virus *Stuxnet* als sistemes informàtics del programa nuclear iranià dut a terme per Israel.

El primer es va produir l'agost del 2008, quan tropes militars russes van respondre al que van considerar una provocació de Geòrgia pel fet d'haver entrat al territori semiautònom d'Ossètia. No solament van atacar amb bombes i bales, sinó també amb un atac de DDoS, que va afectar moltes pàgines web del Govern de Geòrgia; van deixar sense ús diversos serveis d'Internet i van obstruir i dificultar la comunicació d'unes quantes oficines amb les seves tropes i ciutadans. Juntament amb els atacs de denegació de serveis es van produir atacs de *hackers* en què es modificaven els webs oficials del Govern de Geòrgia amb missatges de propaganda nacionalista russa. Malgrat que Geòrgia va acusar el Govern rus de perpetrar un ciberatac contra ells, Rússia va negar el patrocini o el suport d'aquestes conductes al·legant que probablement provenien de persones que tenien un sentiment nacionalista excessiu i com a resposta a l'agressió de Geòrgia.

Precisament en relació amb Rússia té a veure també l'atac perpetrat contra Estònia la primavera de l'any anterior, el 2007, quan es va decidir retirar una estàtua de bronze al "soldat soviètic" d'un parc del port marítim de Tallinn. Les autoritats del país esperaven protestes irades dels russos o dels habitants del seu país d'origen rus, però no tot el conjunt de ciberatacs, generalment de denegació de serveis, que va tenir pràcticament paralitzat durant unes quantes setmanes el ciberespai d'aquest país i que va durar gairebé un mes fins que el Govern va poder estabilitzar la situació.

Un altre atac, potser el més cridaner, és el del virus cuc *Stuxnet*, presumptivament creat pel Govern d'Israel, i destinat a infectar els sistemes informàtics utilitzats en el programa nuclear iranià. Per bé que els ciberatacs entre Israel i els països àrabs o els *hackers* islamistes radicals (molt particularment un grup de *hackers* marroquins però també d'altres països) existeixen des del 1999, quan va començar una guerra d'atacs cibernètics que no ha parat, el capítol de *Stuxnet* és diferent, ja que representa un boicot informàtic de primer ordre que parla per si mateix del poder del ciberespai. A més a més, sembla que *Stuxnet* realment ha tingut èxit, si més no segons les notícies arribades a Occident: aquest virus ha aconseguit, aprofitant una vulnerabilitat del sistema desconegut, prendre el control d'una part del sistema operatiu que havia de ser d'ús exclusiu dels iranians per a controlar el seu programa nuclear, i l'està retardant de manera molt significativa.

Enllaç recomanat

Podeu llegir l'article del virus Stuxnet a: http://www.europapress.es/internacional/noticia-israel-iran-israel-probo-gusano-informatico-sabotear-instalaciones-nucleares-iranies-20110116062133.html

Finalment, cal destacar que l'anàlisi d'aquest tipus de victimització és realment complicada, sobretot tenint en compte que les víctimes es poden sentir temptades de no divulgar els atacs ja que si ho fan poden evidenciar la vulnerabilitat dels seus propis sistemes.

Resum

Des d'una perspectiva criminològica podem distingir tres tipus de delictes que responen als individus que realitzen el delicte i els seus objectius, de manera que es poden diferenciar els delictes que tenen com a objectiu l'obtenció d'un benefici patrimonial, els que tenen com a objectiu l'atac a una persona individual i els que tenen un objectiu ideològic o institucional.

Aquestes tres categories responen al seu torn als tres grans àmbits funcionals de l'ús de les TIC, que ha passat de ser un àmbit dedicat al terreny econòmic a convertir-se en un mitjà de comunicació interpersonal i també en un mitjà poderós que serveix als estats i les institucions en l'aplicació de polítiques.

Aquesta evolució de les TIC comporta l'aparició de moltes formes de criminalitat de manera que, si els objectius que persegueixen els cibercriminals són diferents, també aquests responen a perfils diversos com hem vist. Fins i tot hem pogut comprovar que l'evolució de les TIC també ha repercutit en els cibercriminals i ha canviat les característiques específiques del seu perfil.

Per tant, cal fer un estudi detallat de cadascun dels ciberdelictes i de les característiques dels actors implicats i dur a terme avaluacions periòdiques que permetin obtenir la informació necessària per a elaborar mesures destinades a prevenir la ciberdelinqüència.

Exercicis d'autoavaluació

1. El terme *ciberterrorisme* en sentit ampli es refereix...

a) als atacs a sistemes informàtics amb efectes tan greus que generen un temor comparable al que produeix el terrorisme tradicional.
b) als atacs realitzats per coaccionar un estat.
c) als efectes de risc social que comporta la unió del terrorisme global i les TIC.
d) Cap de les respostes anteriors no és correcta.

2. L'assetjador que s'adreça a les seves víctimes d'una manera calmada i tranquil·la amb la finalitat de causar malestar a les víctimes per mitjà d'una varietat de comportaments amenaçadors és un ciberagressor...

a) venjatiu.
b) col·lectiu.
c) integrat.
d) íntim.

3. El *cyberbullying* és un cibercrim de tipus...

a) social.
b) econòmic.
c) polític.
d) pur.

4. El comportament que duu a terme un adult per mitjà d'Internet per guanyar-se la confiança de menors amb la finalitat de concretar trobades i obtenir concessions de caràcter sexual s'anomena...

a) *cyberstalking*.
b) *cybergrooming*.
c) *cyberbullying*.
d) *stalking*.

5. El *cyberhate* és...

a) l'assetjament a menors aprofitant les possibilitats de les càmeres web.
b) la realització de fotografies de nus totals o parcials per a penjar-les a les xarxes socials.
c) la inflicció de dany d'una manera voluntària o repetida per mitjà de text electrònic.
d) la incitació a l'odi racial en el ciberespai.

6. Un conjunt d'atacs duts a terme per *hackers* informàtics amb la intenció de llançar un missatge ideològic, de lluita política i defensa d'idees generalment relacionades amb la llibertat a Internet s'anomena...

a) *cybergrooming*.
b) atac DoS.
c) *spam*.
d) hacktivisme.

7. Entre els aspectes que diferencien el *childgrooming* en el món virtual i en el món físic trobem que...

a) el perfil de l'agressor és el mateix en les dues modalitats.
b) l'agressor en el món virtual és menys perillós que en el món físic.
c) el perfil de la víctima coincideix en les dues modalitats.
d) Totes les opcions són correctes.

8. Quina de les característiques següents no és típica de les víctimes de *cyberstalking*?

a) Tenir parella.
b) Ser jove.
c) Ser dona.
d) Ser home.

9. Quan parlem de l'individu que accedeix a un sistema informàtic per robar informació o causar algun altre tipus de dany, ens referim al ciberdelinqüent anomenat...

a) *hacker.*
b) *cracker.*
c) *insider.*
d) *scriptkiddy.*

10. Respecte a les víctimes dels cibercrims econòmics...

a) els homes són els que pateixen més aquest tipus de delinqüència.
b) solen tenir un nivell formatiu baix.
c) solen tenir un nivell econòmic mitjà baix.
d) les dones són les que pateixen més aquest tipus de delinqüència.

Solucionari

Exercicis d'autoavaluació

1. c

2. c

3. a

4. b

5. d

6. d

7. b

8. a

9. b

10. a

Glossari

backdoor *f* Programa que s'introdueix en l'ordinador i estableix una porta posterior per mitjà de la qual és possible controlar el sistema afectat, sense coneixement per part de l'usuari.

blog *m* Abreviatura de *weblog*. Terme encunyat per Jorn Barger el 1997 que actualment es confon amb l'ús dels web, tot i que pretén ser una publicació d'un diari *online*, en què els textos apareixen del més recent al més antic.

bot *m* Tipus de virus que permet l'accés remot del sistema informàtic per mitjà de la Xarxa.

botnet *f* Conjunt de xarxes d'ordinadors compromesos i controlats pel missatger.

bullying *m* En català, *assetjament escolar*. Comportament nociu, intencional i repetit per part d'una o més persones, adreçat contra qui té dificultat per a defensar-se.

ciberagressor -a *m i f* Persona que utilitza les tecnologies de la informació i la comunicació per a realitzar un crim, generalment mitjançant l'atac a una altra o unes altres.

cibermula *m i f* Col·laborador o recol·lector dels beneficis a Internet que després envia els diners, per mitjans segurs de transmissió, als autors del delicte.

cibervíctima *f* Persona que pateix els efectes d'un ciberdelicte.

cuc *m* Programa que realitza còpies de si mateix, i les allotja en diferents ubicacions de l'ordinador amb la finalitat de col·lapsar els ordinadors i les xarxes informàtiques, de manera que impedeix el treball als usuaris.

data breach *f* Qualsevol forma de destrucció, modificació o accés a dades d'empreses o de particulars.

hacking *m* Conducta per la qual un subjecte accedeix a un sistema o equip informàtic sense autorització del titular d'aquest, de manera que té capacitat potencial d'utilitzar-lo o d'accedir a qualsevol tipus d'informació que es trobi en el sistema.

hacktivisme *m* Difusió de missatges de protesta a Internet generalment adreçats contra organismes o estats en relació amb la voluntat de mantenir el ciberespai lliure de normes.

moobing *m* Assetjament laboral.

nick *m* Abreviatura de *nickname*. Sobrenom que utilitza un usuari per a identificar-se i comunicar-se a la Xarxa.

pharming *m* Tàctica fraudulenta que consisteix a canviar els continguts del DNI per mitjà de la configuració del protocol TCP/IP o de l'arxiu lmhost perquè l'usuari, quan tecleja l'adreça web de la seva entitat bancària al navegador, entri, en realitat, a un web fals molt semblant o igual que l'original, en què esbrina les seves dades bancàries.

phishing *m* Mecanisme criminal que empra tant enginyeria social com subterfugis tècnics per a robar les dades d'identitat personals dels consumidors i les dades de les targetes de crèdit o dels comptes bancaris corresponents.

protocol P2P (*peer-to-peer*) *m* Protocol que permet l'intercanvi directe d'informació, d'igual a igual.

scriptkiddy *m i f* Persona jove que no és cap *hacker* expert, però que és capaç d'accedir a sistemes mitjançant programacions pròpies, i que efectua atacs informàtics generalment després de triar les víctimes a l'atzar, aprofitant programes i *scripts* bàsics i causant dany en molts casos fruit més de la seva imperícia o de la danyositat del *malware* utilitzat que de les habilitats pròpies.

sexting *m* Enviament a un altre menor per missatgeria telefònica (encara que també per mitjà de correus electrònics o sistemes de missatgeria en xarxes socials) de fotografies de nus, postures eròtiques o parts del cos amb la intenció de formar part d'algun missatge de tipus sexual realitzades generalment per un menor.

smartphone *m* Telèfon mòbil dissenyat perquè l'usuari pugui instal·lar-hi aplicacions.

sniffer *m* Programa de captura de trames d'informació que no hi estan destinades.

stalking *m* Assetjament continuat a una persona amb sol·licituds permanents de contacte que la víctima rebutja de manera continuada.

troià *m* Programa maliciós que mitjançant finestres emergents recull claus; i en general qualsevol altra tècnica que, utilitzant programari permet perfeccionar l'engany fent creure a la víctima que està fora de perill.

Bibliografia

Alleyne, B. (2010). "Sociology of Hackers Revisited". *TSR* (vol. 58).

Boyd, D. M.; Ellison, N. B. (2007). "Social network sites: Definition, history, and scholarship". *JCMC* (vol. 13, núm. 1).

Brown, I.; Korff, D. (2009). "Terrorism and the Proportionality of Internet Surveillance". *EJC* (vol. 6, núm. 2).

Calmaestra Villén, J. (2011). *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto*. Tesi doctoral. Còrdova: Servicio de Publicaciones de la Universidad de Córdoba.

Cano Paños, M. A. (2008, desembre). "Internet y terrorismo islamista: aspectos criminológicos y legales". *Eguzkilore* (núm. 22). Sant Sebastià.

Corte Ibáñez, L. de la; Giménez-Salinas Framis, A. (2010). *Crimen.org. Evolución y claves de la delincuencia organizada*. Barcelona: Ariel.

Curran, K.; Concannon, K.; Mckeever, S. (2008). "Cyber terrorism attacks". A: L. J. Janczewski; A. M. Colarik (eds.). *Cyber Warfare and Cyber Terrorism*. Hershey/Londres: IGI Global.

Green, J. (2002, novembre). "The myth of cyberterrorism". *WM*.

Henson, B. (2010). "Cyberstalking". A: B. S. Fisher; S. P. Lab (eds.). *Encyclopedia of victimology and crimeprevention*. Thousand Oaks, CA: Sage.

Hinduja, S.; Patchin J. (2008). "Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace". *JA* (vol. 31, núm. 1).

Jagatic, T.; Johnson, N.; Jakobsson, M.; Menczer, F. (2005, desembre). "Social Phishing". *Communications of the ACM*. Bloomington.

Janczewski, L. J.; Colarik, A. M. (eds.). (2008). *Cyber Warfare and Cyber Terrorism*. Hershey/Londres: IGI Global.

Kohlmann, E. F. (2008, juliol). "«Homegrown» Terrorists: Theory and Cases in the War on Terror's Newest Front". *Annals* (núm. 618).

Lenhart, A. (2009). "Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging" [en línia]. *Pialp*. Washington, DC. <http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx>

Li, Q. (2007). "Bullying in the new playground: Research into cyberbullying and cyber victimization". *Australasian Journal of Educational Technology*.

Livingstone, S. (2008). "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression". *NMS* (vol. 10, núm. 3).

Mason, K. L. (2008). "Cyberbullying: A Preliminary Assessment for School Personnel". *Psychologyin the Schools* (vol. 45, núm. 4).

McFarlane, L.; Bocij, P. (2003). An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers (vol. 8, núm. 9).

Mitchell, K. J.; Finkelhor, D.; Wolak, J. (2007). "Youth Internet users at risk for the most serious online sexual solicitations". *AJPM* (vol. 32, núm. 6).

Ortega, R.; Calmaestra, J.; Mora-Merchan, J. (2008). "Cyberbullying" [en línia]. *International Journal of Psychology and Psychological Therapy* (vol. 8, núm. 2). <http://redalyc.uaemex.mx/redalyc/pdf/560/56080204.pdf>

Pease, K. (2001). "Crime futures and foresight: Challenging criminal behaviour in the information age". A: D. Wall (ed.). *Crime and the Internet*. Londres: Routledge.

Pittaro, M. L. (2007). "Cyber stalking: An Analysis of Online Harassment and Intimidation". *IJCC* (vol. 1, núm. 2).

Pittaro, M. (2011). "CyberStalking: Typology, Etiology, and Victims". A: K. Jaishankar (ed.). *CyberCriminology. Exploring Internet crimes and criminal behavior*. Boca Raton: CRC Press.

Pratt, T. C.; Holtfreter, K.; Reisig, M. D. (2010). "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory". *Journal of Research in Crime and Delinquency*.

Raymond, E. S. (2001). *How To Become A Hacker* [en línia]. <http://www.catb.org/~esr/faqs/hacker-howto.html>

Reyns, R. W.; Henson, B.; Fisher, B. S. (2011). "Being Pursued Online: Applying Cyber-lifestyle-Routine Activities Theory to Cyberstalking Victimization". *CJB*.

Rollins, J.; Wilson, C. (2007, gener). "Terrorist Capabilities for Cyberattack: Overview and Policy Issues". *CRS Report for Congress*.

Smith, P. K.; Mahdavi, J.; Carvalho, M.; Fisher, S.; Russell, S.; Tippett, N. (2008). "Cyberbullying: Its nature and impact in secondary school pupils". *Journal of Child Psychology and Psychiatry* (vol. 49, núm. 4, pàg. 376-385).

Spitzner, L. (2000). "Know Your Enemy: The Tools and Methodologies of the Script Kiddie" [en línia]. *Honeynet Project*. <http://project.honeynet.org/papers/enemy>

Subrahmanyam, K.; Reich, S. M.; Waechter, N.; Espinoza, G. (2008). "Online and offline social networks: Use of social networking sites by emerging adults". *JADP* (núm. 29).

Taylor, P. A. (2005). "From hackers to hacktivists: speed bumps on the global superhighway?". *NMS* (vol. 7, núm. 5).

Vandebosch, H.; Cleemput, K. van (2009). "Cyberbullying among youngsters: profiles of bullies and victims". *New Media and Society*.

Yar, M. (2006). *Cybercrime and society*. Londres: Sage.