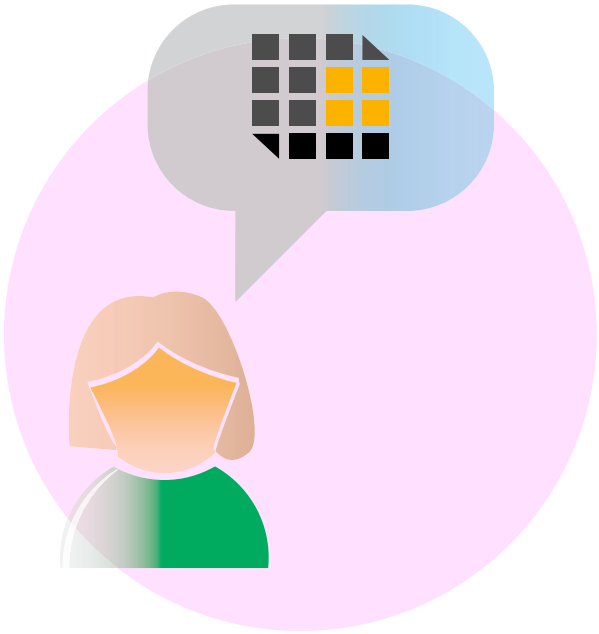
Guia per a l'ús segur de les XARXES SOCIALS

cesicat

Qui fem aquesta guia



El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

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

Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
Donar suport a la protecció de les infraestructures crítiques TIC nacionals
Promocionar un teixit empresarial català sòlid en seguretat TIC
Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

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

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

Índex temàtic

I aquesta guia, per a qui és?

Aquesta guia està dirigida a totes aquelles persones que utilitzen sovint les xarxes socials virtuals o que tenen fills que hi participen. La guia és útil tant per a xarxes amb una finalitat lúdica (Facebook, Tuenti, MySpace, Twitter o Flickr), com per a xarxes socials de perfil professional (LinkedIn o Xing).

Aquesta guia també està pensada per aquelles persones que estan interessades en les xarxes socials, tot i no pertànyer-ne a cap, així com a conèixer quines precaucions caldria adoptar si, finalment, decidissin provar d'utilitzar-ne alguna.

Abast de la guia

Tingueu en compte que aquesta guia no s'ha desenvolupat pensant en cap xarxa social concreta. Per tant, tota conclusió que se'n pugui extreure estarà directament relacionada amb una visió global de la seguretat dels serveis que ofereixen les xarxes socials i no de casuístiques particulars vinculades específicament a alguna d'elles.

Aspectes legals i normatius

Les empreses que ofereixen serveis electrònics de xarxes socials estan subjectes a la Llei Orgànica de Protecció de Dades de Caràcter Personal i a la Llei d'Internet (LSSI), entre d'altres. Tot i això, és important que abans de fer res llegiu amb atenció les condicions concretes que estableix cada prestador de serveis. Sabem que fa mandra haver de llegir una pàgina inacabable de condicions avorrides i que el botó Acceptar ens crida a clicar, però si no fem una ullada a aquestes condicions no sabrem a què ens estem exposant. Així que, mal que us pesi, invertiu uns instants a llegir les condicions de cadascun dels prestadors que vulgueu utilitzar.
A través de les xarxes socials no només podem publicar continguts nostres, sinó que també podem publicar informació d'altres persones del nostre entorn sense que ni elles mateixes ho sàpiguen. Això, no cal dir-ho, planteja molts riscos relacionats amb la privacitat i intimitat dels usuaris. Si esteu interessats a aprofundir en el coneixement dels vostres drets pel que fa al binomi *dades*

personals-xarxes socials, podeu consultar guies com aquestes: Dictamen 5/09 WGP29 (Grup de Treball sobre Protecció de Dades coordinat per la Unió Europea). El document es pot consultar en format pdf aquí:

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdfResol

Resolució Conferencia Autoridades PD 15-17 Octubre 2008.

Pas a pas
Què són les xarxes socials?

Les xarxes socials d'Internet són plataformes virtuals que ofereixen la possibilitat de relacionar-se amb persones de qualsevol lloc del món.

El primer que cal fer per formar part d'una xarxa social a Internet és crear un perfil personal. Es tracta d'una mena de fitxa de presentació on figuren dades personals com el nom, l'edat i el país de residència. En entorns lúdics com Facebook o Tuenti s'acostumen a proporcionar dades de contacte, gustos o aficions i, fins i tot, fotografies personals o filmacions domèstiques. Es tracta de compartir vivències amb els amics ja coneguts a la vida real o de buscar noves amistats.

En xarxes de caràcter professional com LinkedIn o Xing, l'objectiu és diferent: es tracta de donar a conèixer la nostra experiència laboral i els nostres interessos professionals per buscar un nou lloc de treball o, simplement, per contrastar experiències amb altres persones del mateix entorn laboral.

Els graus de separació

Les xarxes socials es van crear com una extensió de la vida material cap al món virtual per aprofitar els avantatges en la comunicació que proporciona Internet. Aquests avantatges resideixen en la possibilitat quasi instantània de poder comunicar-se amb persones d'arreu del món.

Aquestes facilitats possibiliten la multiplicació d'amics o de contactes laborals amb gran rapidesa gràcies als anomenats graus de separació. Al primer grau hi tenim els nostres contactes directes, és a dir, la gent que coneixem fora de la xarxa. En el segon grau trobaríem els contactes dels nostres contactes (els amics dels nostres amics), i així successivament. Mitjançant aquest mètode, la possibilitat de mantenir una àmplia xarxa de contactes és molt ràpida i més efectiva que al món fora de línia. Un nou contacte es pot aconseguir amb tan sols un clic.

Els riscos de les xarxes socials

Les xarxes socials ofereixen serveis útils i pràctics de forma gratuïta. Tot i això, les mateixes propietats d'Internet fan que haguem de parlar de riscos a l'hora d'utilitzar aquestes plataformes. A continuació, us detallem alguns dels perills més habituals que ens podem trobar si som usuaris d'alguna xarxa social.

Algú ha estat utilitzant el meu correu electrònic!

Em dono d'alta

Un bon dia m'assabento que a Internet hi ha un servei anomenat xarxa social. Tothom en parla i, tot i que jo no acabo de veure-li la utilitat, em fa la sensació que la gent s'ho passa bé utilitzant-la i decideixo que ja és hora de posar-me al dia amb les noves formes de comunicació. Busco una de les xarxes socials més utilitzades entre els meus amics i decideixo donar-m'hi d'alta.

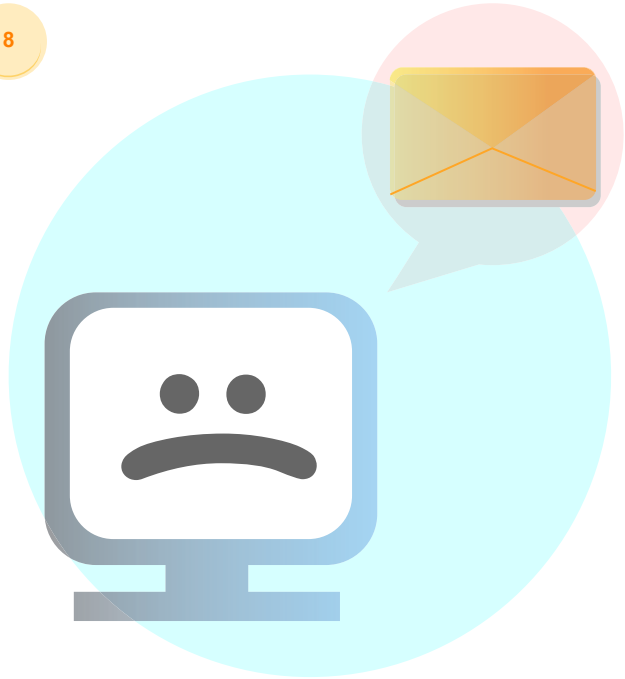
El primer que descobreixo és que, per donar-me d'alta en aquesta xarxa, he d'omplir un formulari amb les meves dades personals. No em sorprèn, perquè no és el primer servei a través de la xarxa que em demana informació personal. Bé hauran de tenir algun tipus de contacte per si mai m'han d'enviar informació... Sense més divagacions, doncs, proporciono el meu nom complet i la meva data de naixement. També he de donar una adreça de correu electrònic que farà les funcions d'identificador d'usuari. És a dir, quan vulgui entrar al meu perfil de la xarxa social, hauré de facilitar aquesta adreça, a més d'una contrasenya. I quina contrasenya puc posar? Mira, com que per entrar al meu perfil he d'escriure l'adreça del meu correu electrònic, per evitar embolics faré servir el mateix *password* que escric per entrar al *mail*. Així segur que no l'oblido!

M'asseguro que la meva informació estarà segura

Ja m'han advertit que quan configuro el meu perfil en qualsevol xarxa social he d'anar amb compte, sobretot, amb dos punts clau:

- Quina informació poso al meu perfil
- A qui li deixo veure aquesta informació

Després d'una estona donant tombs per les opcions que veig a la pantalla, trobo un apartat de configuració que em permet definir quines parts del meu perfil deixo veure i a qui les deixo veure. Ara que m'he assegurat que la meva informació només la podran visualitzar els meus amics directes, ja puc començar a socialitzar-me a través de la xarxa.



Problemes amb el meu correu

Això de les xarxes socials m'ha agradat i al meu perfil hi entro quasi bé cada dia. Intento ser prudent a l'hora de penjar informació i fotografies, perquè cada cop són més les notícies que parlen d'estafes o suplantacions d'identitat a la xarxa. Tot i això, no em preocupo gaire ja que, fins al moment no he notat res estrany amb la meva xarxa social. Ara bé, no puc dir el mateix amb el meu compte de correu electrònic. No sé perquè, però fa dos dies que no em deixa entrar a la safata d'entrada. Què passa?

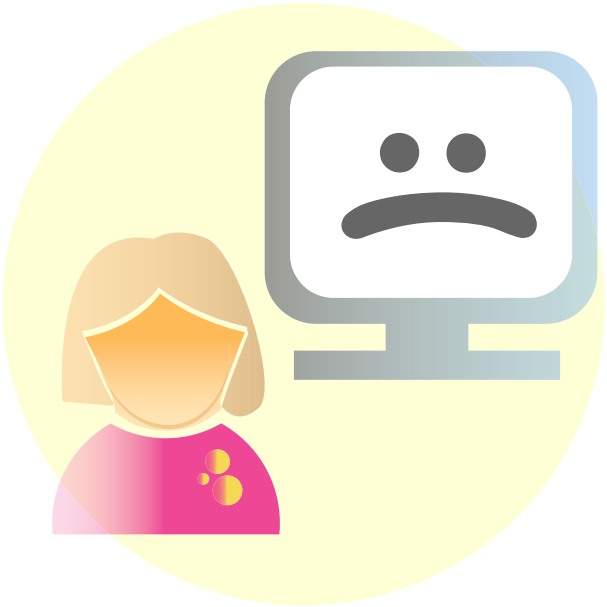
El robatori de credencials d'accés

Cada cop és més habitual el robatori d'identificadors d'usuari i contrasenyes d'usuaris de les més diverses xarxes socials. No hem de viure amb por, però simplement hem de prendre algunes mesures per mitigar, en la mesura del possible, el dany que aquestes fugues d'informació confidencial ens puguin crear.

Cada cop fem servir Internet de forma més intensa: per consultar el correu electrònic, per donar un tomb per la nostra xarxa social preferida, per comprar objectes i serveis o, fins i tot, per fer moviments bancaris de tota mena. Si fem servir la mateixa contrasenya per a tot, només cal que algú descobreixi la nostra contrasenya de la xarxa social per comprometre la resta. Per això és molt important que tinguem una contrasenya diferent per a cada servei que utilitzem a la xarxa.

En el cas de l'exemple que hem proposat, per no haver de pensar en més d'una contrasenya, la persona en qüestió ara no només ha perdut el control d'una, sinó de tres eines que utilitza, com a mínim, un cop al dia.

Penseu, per un segons, quin tipus d'informació teniu emmagatzemada al vostre correu electrònic. El vostre número de DNI? El del compte corrent? El currículum? Aquell mail que vam desar on no deixàvem gaire bé el nostre cap o algun dels nostres amics?
Amb aquesta informació en mans de la persona equivocada poden robar-nos diners, suplantar-nos la identitat o, fins i tot, amenaçar-nos d'escampar dades compromeses sobre la nostra vida privada si no paguem un preu econòmic pel seu silenci.



Al meu ordinador no li ha agradat gaire aquesta aplicació...

Cada dia més amics

Cada dia tinc més amics a la xarxa. Amb això dels graus de separació, cada dia augmenta la meva llista de contactes. Convido els amics dels meus amics a fer-se amics meus i, un cop m'accepten, busco entre les seves llistes i em faig amiga dels amics dels amics dels amics dels meus amics.

La veritat és que no m'hi miro gaire a l'hora d'afegir algú al meu perfil. No diuen que com més serem més riurem? A més, quin mal hi ha en agregar desconeguts? Què em poden fer a través de la xarxa? No perdré l'oportunitat de conèixer algú interessant per temors exagerats.

Aplicant-me en les meravelles de la xarxa social

He descobert que a la meva xarxa social no només puc penjar fotografies i vídeos, sinó que també puc fer servir aplicacions de tot tipus. N'hi ha una que m'agrada molt perquè em dóna la possibilitat de demanar l'opinió sobre llibres que em vull comprar a gent que ja els ha llegit.

Com que aquesta aplicació m'ha semblat del tot útil, n'he buscat més i ara també en tinc una que em serveix per compartir els viatges que he planejat de fer en breu. D'aquí a una setmana marxo a l'estranger i, gràcies a aquesta aplicació, he trobat que un dels meus contactes a la xarxa social viu molt a prop del lloc on m'hostatjaré jo. Hem quedat per veure'ns al bar de la cantonada i així ens coneixem en carn i ossos d'una vegada.

Amb tota aquesta voràgine d'aplicacions, veig que un dels meus contactes m'ha enviat una nova eina: "Descobreix qui entra al teu perfil". Ostres, quina gràcia, amb aquesta aplicació podré espiar els que m'espien!

Males notícies

No sé què he fet, però mentre intentava instal·lar-me l'aplicació que m'havia enviat l'amic de l'amic de l'amic del meu amic, l'ordinador ha començat a fer coses estranyes i ara no sé com aturar la situació.

Virus en forma d'aplicació

Quan instal·lem aplicacions que tenen un origen dubtós o venen amb informació poc fiable, podem estar infectant el nostre ordinador amb codi maliciós sense ni tan sols adonar-nos-en.

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

- Destorbar l'usuari
- Esborrar tota la informació de l'ordinador
- Recopilar informació dels gustos de l'usuari per després bombardejar-lo amb campanyes de publicitat personalitzades
- Obtenir informació de quins serveis utilitza l'usuari per impedir-n'hi l'accés
- Controlar l' ordinador de l'usuari (juntament amb d'altres d'usuaris infectats com ell) per atacar infraestructures de tercers
- Robar les credencials bancàries o d'altres serveis web que l'usuari utilitzi (jocs en línia, xats, correu electrònic...)

Aquests són alguns exemples del que pot fer un virus, però n'hi ha molts més. A causa de la quantitat d'usuaris que fan servir les xarxes socials, aquests entorns s'han convertit en un bon lloc on utilitzar codis d'infecció. Com més víctimes potencials, més possibilitats de triomfar en els seus objectius fraudulents.

He perdut la feina i tot per culpa de la meva xarxa social!

Les fotos de la festa

Fa un temps vaig fer-me membre d'una xarxa social. Era divertit, perquè podia parlar amb els amics, riure una estona amb els seus comentaris i fer una mica el xafarder amb les fotografies que penjaven dels seus caps de setmana.

Entre tanta fotografia, l'altre dia vaig pensar que seria divertit penjar les fotos de la festa que vam celebrar a casa meva dijous al vespre. La que més èxit va tenir va ser la del lavabo. I és que tanta cervesa no és bona. Però tant d'èxit va tenir la foto que fins i tot la va veure el meu cap. I ell també em va fer un cometari, però no a la xarxa, sinó al despatx: acomiadat. L'home considera que una persona que passa el seu temps d'oci així i que, a sobre, ho mostra a tothom, no encaixa amb el perfil adequat que necessita l'empresa.

La meva vida és de tothom

S'ha de tenir molt present que una vegada es penja un contingut a Internet, aquest deixa de ser privat. Qualsevol persona el pot copiar i el pot anar reproduint i modificant a la xarxa tantes vegades com vulgui. Quantes més persones tinguin accés a aquest contingut, més fàcil serà que n'existeixin versions distribuïdes per Internet en general i per dins de la mateixa xarxa social, en particular.

Odio les xarxes socials: la gent se'n riu de mi!

Orelles d'elefant

Fa un temps em vaig donar d'alta en una xarxa social. Al principi m'ho passava bé i vaig aconseguir tenir una llista de contactes força gran en molt poc temps. És cert que la meva llista va créixer de pressa perquè acceptava tothom que em "proposava amistat" encara que no els conegués de res.

Tot es va enrarir el dia que un d'aquests contactes que no tenia controlat va començar a deixar-me missatges grollers al meu mur: que si les meves orelles, que si el meu nas, que si jo en general...

El gall empipador

A part del mal que allò em feia a nivell personal, aquesta persona va aconseguir fer-me quedar malament dins del meu grup de la xarxa social. La situació es va tornar insostenible i vaig decidir donar-me de baixa de la xarxa social. El problema és que, per culpa de la meva poca vista a l'hora de configurar-me el perfil, ara aquesta persona té el meu número de telèfon i em truca constantment des de fa dies. Per si no en tingués prou amb despertar-me a les tres de la matinada amb un número ocult, ara també es dedica a enviar correus als meus amics insultant-los a ells i a mi.

Amistats perilloses

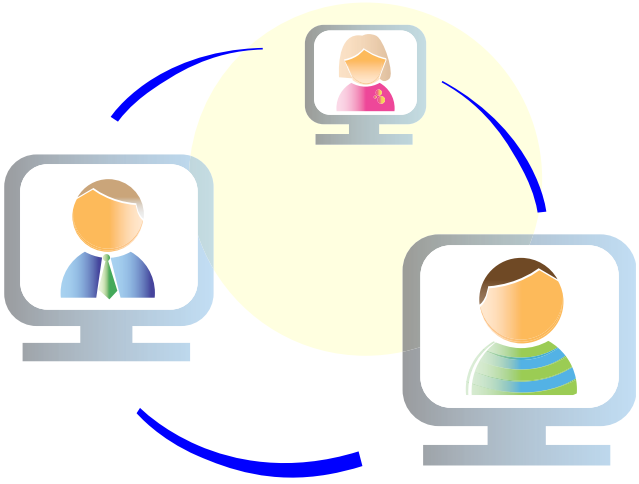
El ciberassetjament existeix. Les xarxes socials ajuden a conèixer gent nova, però mai no hem de perdre de vista que si acceptem "l'amistat" de totes aquelles persones que ens envien una sol·licitud encara que no sapiguem qui són o de qui no tenim dades contrastables (una persona es pot fer passar per un amic nostre sense ser-ho), estem oferint la nostra informació privada a desconeguts amb intencions poc clares.

Proporcionar dades de contacte reals (el telèfon, l'adreça postal o el correu electrònic que fem servir habitualment), pot propiciar que les persones que tenen accés a aquesta informació l'utilitzin d'una manera que no havíem previst, amb la qual cosa afectaran negativament la nostra vida personal i, fins i tot, la dels que ens envolten.

M'he donat de baixa de la xarxa social i encara apareixen dades meves a Internet

Me'n vaig cansar

Era usuari d'una xarxa social, però tanta activitat digital em va atabalar i vaig decidir donar-me'n de baixa. Tot i que ara ja no puc entrar al meu perfil i, en teoria, les meves dades ja no figuren enlloc, he vist a través d'amics que encara hi ha informació meva que continua sent accessible dins la xarxa social. Com pot ser això?



Si ho hagués sabut abans, potser m'ho hauria pensat dues vegades

Quan publicava fotografies al meu perfil no sabia que, si els meus contactes les copiaven o les distribuïen, automàticament jo perdia el control total sobre aquelles còpies. El fet que m'hagi donat de baixa de la xarxa social no canvia res: aquelles fotos seguiran allí fins vés a saber quan. El que tampoc sabia és que passa el mateix amb totes les dades que els meus contactes podien veure. L'embolic és màxim: ja no sé quines dades s'han esborrat i quines quedaran per sempre més a la xarxa i qui hi té accés. Perquè, per embolicar encara més la troca, els que eren els meus amics alhora tenen altres contactes que també podien accedir a la meva informació.

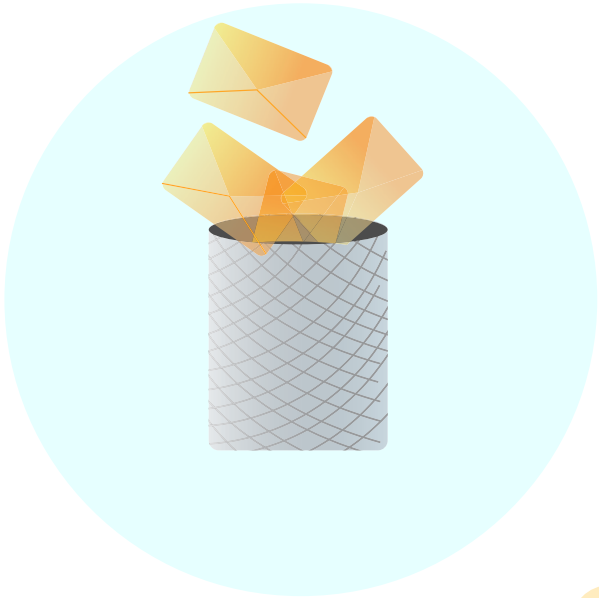
La informació personal, en mans de tots

Publicar informació a Internet és posar-la a disposició dels internautes. Una vegada es té accés a la informació, aquest contingut pot ser copiat, modificat i també redistribuït. Per tant, l'autor d'aquesta informació perd tot control sobre ella.

Utilitzar una xarxa social implica acceptar les condicions de servei de la xarxa social en qüestió. Una vegada l'usuari ha acceptat les condicions del servei, ha atorgat a la xarxa social un conjunt de drets respecte a la informació que hi publiqui. Per exemple, quan diem que acceptem les condicions de servei d'una xarxa social, podem estar concedint el dret a l'empresa en qüestió a

vendre les nostres dades amb finalitats de màrqueting, o cedint els drets d'autor del que anem publicant a la xarxa social per un temps indefinit.

Cada dia rebo més correus brossa a la meva bústia personal



Multiplicació del correu brossa

M'he adonat que, des que sóc usuari d'una xarxa social, rebo més correus del que fins ara era habitual. Al principi era divertit, perquè acostumaven a ser missatges dels meus contactes de la xarxa. Ara, però, també rebo molts correus publicitaris i alguns de contingut dubtós. No ho entenc. Què ha passat aquí? Per què ara, de cop, rebo tants correus brossa?

Publicitat sense demanda

La xarxa social és un entorn on tothom té cabuda. Això vol dir que no només hi ha persones que en fan un ús particular, sinó que també hi ha empreses que busquen informació dels usuaris d'aquestes xarxes. Que per què volen informació? Doncs per crear perfils de consum i així dissenyar campanyes de màrqueting personalitzades, sobretot quan aquests usuaris proporcionen les seves dades de contacte.

Programari maliciós ("malware") al meu ordinador

Més greu que la publicitat encoberta, però, són les accions de collectius criminals que accedeixen a les xarxes socials amb l'objectiu d'obtenir perfils d'usuari. Aquests grups poden esbrinar, entre d'altres coses, el nivell adquisitiu i els coneixements tecnològics dels usuaris de la xarxa tan sols llegint els comentaris que publiquen periòdicament. Un cop amb la informació a les seves mans, els delinqüents poden arribar a infectar els equips dels usuaris amb un codi maliciós que els permeti, per exemple, apoderar-se dels comptes de banca en línia dels amos dels ordinadors.

M'han entrat a robar a casa

Un bon "amic" a la xarxa

Fa poc em van entrar a robar a casa. Poc em podia imaginar jo que la investigació policial determinaria que el lladre era, ni més ni menys, que un amic meu d'una xarxa social. Com fa molta gent, jo acostumava a publicar el meu dia a dia a la xarxa: que si m'agradava molt això, que si m'havia comprat allò...

Entre els meus contactes, he de confessar, hi tenia gent que no coneixia de res però que, com que teníem amics comuns i jo no volia quedar malament, havia acceptat sense gaires reticències. Doncs, vés per on, un d'aquests contactes misteriosos va estar fent la seva llista de reis particular amb tots els objectes que jo comentava que anava comprant.

Al meu perfil hi tenia (ja l'he treta) la meva adreça real, així que al meu amic només li va caler aparcar davant de casa un dia que sabia que treballava fins tard (perquè ho havia publicat a la xarxa social), rebentar la meva porta i robar-me, un a un, tots els objectes de valor que sabia que segur trobaria al pis. Després d'això, com creieu que em sento?

Informació personal de doble tall

Si proporcionem dades reals de la nostra vida en entorns on és difícil controlar qui hi pot accedir i qui no, hem de saber que correm el risc que algú utilitzi aquesta informació per perjudicar-nos d'alguna manera.

Recomanacions

Cadascun dels escenaris plantejats en aquesta guia exposa un seguit d'amenaces que, si es materialitzen al llarg del temps, en major o menor mesura tindran efectes perjudicials per a l'usuari i, fins i tot, podrien repercutir en la seva vida personal i familiar. Per intentar evitar que això succeeixi o, com a mínim, minimitzar-ne l'efecte, a continuació proporcionem un conjunt de recomanacions dirigides als usuaris de les xarxes socials.

Com puc evitar la suplantació d'identitat?

Si voleu disminuir els riscos que un tercer s'apropiï il·legítimament d'un servei telemàtic en què vosaltres us havíeu registrat per fer-ne un ús personal, tingueu en compte els següents consells:

No reutilitzeu una contrasenya d'accés per accedir a entorns independents com podria ser el correu electrònic personal de l'usuari i la xarxa social

En cas que utilitzeu una mateixa contrasenya en diferents entorns, si teniu la mínima sospita que la contrasenya es pot haver vist compromesa, canvieu-la per una de nova en tots aquells serveis telemàtics on l'estàveu utilitzant

Quan feu servir dispositius mòbils, com ara iphones o ipods, que us permetin accedir a la vostra xarxa social, heu de configurar l'aplicació del dispositiu mòbil de tal manera que sol·liciti un usuari i una contrasenya d'accés cada vegada que es vulgui fer servir. Així, si perdeu el dispositiu mòbil, qui el trobi no tindrà accés lliure al vostre perfil privat.

Si heu deixat de tenir accés a un servei telemàtic personal i sospiteu que algú podria estar utilitzant aquest servei en nom seu, heu de posar-vos en contacte amb el proveïdor del servei mitjançant els mecanismes que aquest tingui a l'abast de l'usuari i denunciar el cas. Un cop fet això, si cal, aneu al Cos de Mossos d'Esquadra i realitzeu la denúncia corresponent o envieu-los un correu a mossosdti@gencat.cat, adreça específica per informar-vos sobre delictes en tecnologies de la informació.

Si són menors els que utilitzen la xarxa social, cal ubicar l'ordinador en una zona comuna que faciliti la supervisió dels pares o tutors, promovent també la comunicació entre ambdues parts si el menor té algun tipus de dubte o temor mentre utilitza la xarxa social.

Com puc evitar la infecció del meu ordinador mitjançant correu brossa o pràctiques de "phishing"?

Si voleu disminuir el risc que el vostre equip resulti infectat per codi maliciós, haureu de tenir en compte les següents recomanacions:

- No obriu missatges de correu electrònic, i encara menys fitxers adjunts, si es dóna algun dels supòsits que descrivim a continuació.
- No esteu segurs de saber qui és el remitent del missatge
- Desconeixeu qui és realment el contacte que envia el missatge
- El títol del missatge no indica quin és el motiu del missatge
- El missatge és inesperat o per algun motiu es considera que és estrany, independentment de qui en sigui l'emissor
- Si us trobeu davant d'algun d'aquests casos, esborreu el missatge sense obrir-lo i, després, elimineu-lo de la paperera.
- No respongueu mai a sol·licituds de claus que us arribin mitjançant el correu electrònic. Desconfieu de qualsevol petició de dades personals i mai proporcioneu informació personal o financera en resposta a un correu electrònic. Tampoc utilitzeu enllaços incorporats en aquests correus electrònics o en pàgines web de tercers.

Si hi ha algú que estigui fent un ús abusiu de la xarxa social, notifiqueu-ho a través dels mecanismes que proporcionen les xarxes socials

No instal·leu aplicacions que no provinguin d'una font oficial o d'una font fiable d'Internet

Superviseu el tipus i origen de les aplicacions utilitzades pels menors a les xarxes socials

Com puc limitar la difusió d'informació privada dins la xarxa social?

Si voleu disminuir el risc que la vostra informació privada acabi sent de domini públic, tingueu en compte les següents recomanacions:

Durant el procés d'alta de l'usuari a la xarxa social (es pot consultar amb posterioritat), llegiu amb deteniment la Política de Privacitat i les Condicions del Servei associades a l'ús de la xarxa social per part de l'usuari. Així sabreu de primera mà quins són els vostres drets i quins els de l'empresa que controla la xarxa social.

Abans de començar a utilitzar la xarxa social, aneu a l'apartat de configuració, familiaritzeu-vos amb les opcions que permet i configureu el vostre perfil adequadament. Limiteu:

- qui podrà contactar amb vosaltres
- quines persones tindran accés a la informació que penjareu
- la visibilitat que tindrà el vostre perfil dins i fora de
- la xarxa social (per exemple, mitjançant cerques a través d'un buscador d'Internet)

Eviteu proporcionar dades de contacte reals com ara l'adreça postal i el número de telèfon. D'aquesta manera, reduireu la possibilitat que algú contacti amb vosaltres quan no ho desitgeu.

Creeu una adreça de correu electrònic específica únicament per utilitzar-la dins de l'àmbit de la xarxa social. Així, si us voleu donar de baixa de la xarxa social i no rebre més contactes provinents d'aquesta via, no caldrà que perdeu el vostre correu personal d'ús habitual ni que els missatges provinents de la xarxa social incomodin l'ús habitual que feu del correu personal.

No pengeu cap contingut que no voleu que sigui conegut fora del vostre àmbit més privat. Una vegada penjat al perfil, un contacte que hi tingui accés podrà copiar-lo i reproduir-lo a d'altres llocs de la xarxa social i d'Internet. Si algú ha reproduït contingut del vostre perfil fora d'aquest, encara que us doneu de baixa de la xarxa social, aquest contingut que s'ha reproduït no desapareixerà, i pot aparèixer en altres perfils de la xarxa social, i fins i tot fora dels límits d'aquesta, de manera que acabi estenent-se per tota la Internet.

No incorporeu contactes indiscriminadament. Heu de ser selectius i tenir present que dins les xarxes socials també es menteix i, per tant, una persona pot no ser qui diu ser. Un contacte no és un amic. Un amic és una persona que es coneix i en qui es pot confiar, i per aconseguir això, cal una mica més que un sol clic.

Conclusions

Les xarxes socials no suposen un risc en si mateixes. Són aquells que les utilitzen els que les poden convertir en una eina perillosa d'utilitzar.
Tot i que el seu ús s'ha estès de manera espectacular a tot el món, mai no hem d'oblidar que sempre n'hem de fer un ús responsable.

A les xarxes socials només hi tenim contactes. Els amics es fan a la vida real.

A les xarxes socials no hi hauríem de dir o posar el que no voldríem que a la vida real conegués molta gent. Un cop es penja un document a Internet, esborrar-lo del tot es converteix en una tasca pràcticament impossible.

Cal prestar especial atenció als menors que utilitzen les xarxes socials. Els pares o tutors haurien de supervisar les activitats que realitzen en aquests entorns per poder protegir-los de xarxes criminals. Si voleu saber més sobre com aconsellar una navegació segura per a nens i nenes, visiteu el web www.cesicat.cat/internetambseny

En definitiva, a les xarxes socials hauríem d'actuar amb la mateixa prudència amb què actuem en el nostre dia a dia.

Si teniu alguna consulta relacionada amb la seguretat a les xarxes socials, podeu enviar-nos un correu electrònic a info@cesicat.cat.

Glossari

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

Control d'accés: mecanisme per controlar l'accés a serveis d'Internet i aplicacions. El mecanisme més utilitzat acostuma a ser la combinació d'un identificador d'usuari i contrasenya, conegut únicament per l'interessat que s'ha subscrit o ha contractat el servei privat.

Identificador d'usuari: és un component dels mecanismes de control d'accés que permet identificar quin és l'usuari que intenta accedir a la seva àrea privada.

Contrasenya: paraula de pas personal i intransferible utilitzada per accedir a l'àrea privada de l'usuari.

Phishing: pràctica delictiva que consisteix a suplantar una empresa de confiança a la xarxa. L'objectiu dels criminals és el d'apropiar-se dels identificadors d'usuari i de les contrasenyes associades als seus clients en línia. Si aconsegueixen la informació, poden entrar als seus comptes i obtenir informació confidencial o bé, treure'n un benefici econòmic directe. Les pràctiques més habituals utilitzen webs de bancs, caixes d'estalvis o asseguradores.

Correu brossa: pràctica d'enviar missatges de correu electrònic no sol·licitats. Generalment es tracta de publicitat de productes, serveis o pàgines web, però també podrien incorporar codi maliciós o enllaços web per perpetrar atacs de phishing. Les adreces de correu electrònic acostumen a ser robades, comprades, recol·lectades pel web o preses de correus en cadena. La pràctica del correu brossa constitueix un problema que afecta de forma negativa tots els usuaris de la xarxa. La legislació vigent prohibeix de forma expressa la seva emissió.

Web 2.0: aquest terme fa referència a l'evolució de la tecnologia web cap a entorns basats en comunitats d'usuaris (com ara les xarxes socials o els blocs) que promouen la col·laboració i un intercanvi àgil d'informació entre els usuaris que formen part de la comunitat.

Referències i enllaços web

A continuació es detallen les referències i enllaços web emprats en l'elaboració d'aquesta guia.

Security Issues and Recommendations for Online Social Networks, ENISA, Octubre de 2007
[PDF] http://www.enisa.europa.eu/act/it/oar/social-networks/security-issues-and-recommendations-for-online-social-networks/?searchterm=security issues and recommendations

Dictamen 5/2009 sobre las redes sociales en línea, Agencia Española de Protección de Datos, 12 de Juny de 2009
[PDF] http://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2009/index-ides-idphp.php

Protégete en las redes sociales, OSI – Oficina de Seguridad del Internauta
http://www.osi.es/econf/Protegete/Redes_Sociales/

Consells de seguretat de MySpace

http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safetytips

Recomanacions de seguretat de Facebook

http://www.facebook.com/help/?safety

Condicions d'ús de Facebook

http://www.facebook.com/terms.php?ref=pf

Wikipèdia

http://es.wikipedia.org/wiki/Wikipedia:Portada

cesicat

Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat