Guia per protegir i utilitzar de forma segura el mòbil

"[S02] Guies de seguretat TIC."

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 adreçada a totes aquelles persones que utilitzen dispositius mòbils, ja siguin terminals bàsics per realitzar únicament trucades de veu i enviar missatges de text, o terminals més avançats com ara PDA o *smartphones*, que poden accedir a un conjunt més extens d'aplicacions i serveis a la xarxa.

Abast de la guia

Aquesta guia vol proporcionar una visió global de la seguretat vinculada a la telefonia mòbil i un conjunt de bones pràctiques que permetin a l'usuari fer-ne un ús correcte. En cap cas s'ha desenvolupat la guia pensant en un tipus de dispositiu, aplicació o servei de telefonia concret.

Aspectes legals i normatius

Pel que fa als aspectes legals, en el desenvolupament de la present guia s'ha tingut en compte la normativa vigent en matèria de comunicacions electròniques i per al tractament de les dades de caràcter personal en la seva prestació.

A efectes merament informatius, els serveis de comunicacions electròniques estan subjectes a la següent normativa:

- Llei 32/2003, de 3 de novembre, General de Telecomunicacions.
- Reial Decret 899/2009, de 22 de maig, pel qual s'aprova la carta de drets dels usuaris dels serveis de comunicacions electròniques.
- Reial Decret 2296/2004, de 10 de desembre, pel qual s'aprova el Reglament de mercats de comunicacions electròniques, accés a les xarxes i numeració.
- Reial Decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris.
- Llei 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Reial Decret 1720/2007 de desenvolupament de la Llei Orgànica de protecció de dades.

És en virtut d'aquesta normativa que la utilització dels serveis de telefonia mòbil i prestacions associades queda clarament regulada i preveu diferents mesures per mitigar possibles prestacions defectuoses. Malgrat això, en matèria de seguretat les mesures preventives seran les que tindran un major impacte per tal d'evitar situacions desagradables. .

Pas a pas

Cinc cèntims d'història i evolució de la telefonia mòbil

Des de la dècada dels 40, la telefonia mòbil no ha parat d'evolucionar. Els seus inicis van ser militars, però, com ha passat amb molts altres invents, de seguida se li van trobar possibilitats i aplicacions per al ciutadà.

L'any 1973, l'enginyer electrònic i inventor Martin Cooper, considerat el pare de la telefonia cel·lular, va introduir el primer radiotelèfon a l'empresa Motorola dels Estats Units. L'any 1979, una empresa japonesa ubicada a la ciutat de Tokyo (NTT, Nippon Telegraph & Telephone Corp.) va presentar el primer sistema comercial de telefonia cel·lular.

La primera generació de telefonia mòbil també data de l'any 1979, amb tecnologia analògica i només amb servei de veu. La introducció de la tecnologia digital va arribar amb la segona generació a principis dels anys 90, moment en què es comença a parlar de GSM (Global System Mobile Communications) i PDC (Personal Digital Communications).

El GPRS es va introduir amb la generació 2.5 amb l'objectiu de millorar la velocitat de la transferència de les dades.

Finalment, parlem de 3G, tercera generació de telefonia mòbil on pren protagonisme l'accés a serveis multimèdia, Internet, veu IP... En aquesta generació, el servei de dades passa a tenir tanta importància com el de veu, i encara més amb l'augment de velocitat de l'anomenada 3.5G (HDSPA, HSUPA, HSPA+...).
Pel que fa a la funcionalitat, en els últims anys s'ha produït una convergència entre els telèfons mòbils tradicionals utilitzats únicament per als serveis de veu i missatgeria curta i els dispositius de mà per a gestió de la informació personal (PDA). Sobretot, l'ús dels anomenats *smartphones* s'ha estès entre els usuaris que volen estar permanentment connectats al correu electrònic, la missatgeria instantània o les xarxes socials, ja sigui per motius de treball o d'oci.

Les relacions humanes al'abast de la mà

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. L'ús de les xarxes socials ha crescut enormement en els últims anys fins a convertir-se en una referència de comunicació social. Entre els serveis d'Internet que més s'utilitzen hi ha el de missatgeria instantània i l'ús de les xarxes socials.

Actualment s'utilitza principalment el telèfon mòbil com a mitjà per comunicar-se de forma intensiva, parlar amb els amics, pujar fotos, comentar el que s'està fent o es farà... Les xarxes socials permeten rebre i enviar un missatge amb un impacte multitudinari en poc temps, i donen així la possibilitat quasi instantània de poder comunicar-se amb persones d'arreu del món.

No hem d'oblidar que un dels punts forts que s'està potenciant a les xarxes socials és la localització. Saber on és la persona amb qui estàs parlant permet poder oferir-li serveis en funció de la seva localització, oferir-li contactes, amics o grups per proximitat i amb les mateixes aficions...

Tecnològicament, els nous models de telèfons mòbils disposen dels requeriments necessaris per poder estar connectats en tot moment a Internet i executar les aplicacions necessàries per interactuar amb qualsevol tipus de xarxa social. A més a més, la majoria de xarxes socials posen a disposició de l'usuari l'aplicació adaptada per al seu mòbil sense cap cost associat, i fins i tot existeixen xarxes socials dissenyades específicament per a mòbils.

L'oficina a la teva butxaca

Les noves generacions de telefonia mòbil, en conjunció amb la contínua evolució tecnològica, han permès que puguem realitzar les nostres tasques laborals des d'un telèfon mòbil, a distància i des de qualsevol lloc on tinguem cobertura del nostre proveïdor de telefonia.

La tercera generació de telefonia mòbil permet estar en tot moment connectat a Internet, i ofereix serveis basats en el tràfic de dades com ara la missatgeria instantània, realitzar trucades per veu IP, integració amb eines de col·laboració, còpia de seguretat remota, comunicacions segures, accés a xarxes virtuals (VPN), videotelefonia, sistemes de localització, possibilitat de configuració d'extensions curtes internes...

Tecnològicament, els terminals avançats, com ara *smartphones* o PDA, permeten l'execució de tot tipus d'aplicacions ofimàtiques, comunicació, compres, finances, multimèdia, banca... A més a més, el mercat proporciona la informació i les eines necessàries per poder desenvolupar aplicacions internes per a l'empresa, intentant així donar cobertura a qualsevol necessitat que no pugui cobrir el mateix mercat.

En resum, podem disposar de terminals mòbils connectats a Internet i a la xarxa corporativa amb les mateixes funcionalitats que un portàtil o ordinador de sobretaula.

Riscos de la telefonia mòbil

M' he quedat sense mòbil. Pèrdua o robatori

Les exigències del mercat i l'oferta de nous serveis de la tecnologia mòbil fan que cada vegada hi hagi més quota d'utilització de telèfons intel·ligents o avançats, que tenen un alt cost i una mida cada cop més reduïda. Això, juntament amb l'existència d'una demanda al mercat submergit de productes robats, fa que existeixi un alt risc de robatori de telèfons mòbils.

Hem de ser conscients de l'impacte que pot tenir per a la nostra vida quotidiana la pèrdua o robatori del nostre mòbil. No només pel possible ús fraudulent dels serveis que tinguem contractats, sinó per la pèrdua o ús il·legítim de les nostres dades, agenda de contactes personals, missatges de text enviats o rebuts, galeria de fotos, documentació que tinguem emmagatzemada, credencials d'accés a serveis a la xarxa com ara bancs, pàgines d'empresa, correu...

És, per tant, molt important tenir present quines dades són les que tenim emmagatzemades en el nostre mòbil, quines aplicacions poden deixar registrades credencials d'accés, i saber a priori què significaria la seva pèrdua o que algú fes un ús il·legítim de la nostra informació. De la mateixa manera, cal conèixer quines són les accions que s'han de realitzar en cas de robatori o pèrdua del mòbil, i tenir registrades de forma segura les dades que ens podrien demanar per solucionar el problema.

No paren de trucar-me per demanar les meves dades personals

A qui no li han trucat des d'un telèfon que no pot identificar o del qual no en coneix el número? La persona que truca s'identifica com a treballadora de l'operadora de telefonia mòbil o d'una empresa que ens presenta una oferta interessant.

La finalitat de la trucada sempre és la mateixa: ens acaben demanant dades internes de consum, d'acreditació o personals. En casos molt concrets, ens poden arribar a demanar introduir dades via teclat per donar la falsa aparença de privacitat, o executar accions al nostre mòbil que desconeixem i no podem controlar.

L'obtenció d'aquestes dades podria permetre la contractació o modificació de serveis al nostre nom, o fer-se servir per atacs més elaborats que acabarien repercutint en una despesa no controlada, o en altres perjudicis tècnics i legals.

Per tant, hem de conèixer els procediment que la nostra operadora de telefonia mòbil té per contactar amb nosaltres. Hi ha establerts uns procediments per realitzar una validació segura: el número des d'on se'ns truca ha de ser conegut, i en cap cas hem de proporcionar cap tipus de dades si no estem realment segurs de qui hi ha altre costat de la línea.

Missatge amb remitent sospitós

Enviar i rebre un missatge de text o multimèdia és una de les accions que realitzem amb més freqüència des del mòbil. La simplicitat d'aquesta acció ens proporciona una falsa confiança, fet que pot ser aprofitat per intentar infectar el nostre mòbil o forçar-ne un comportament anòmal.

Els últims modes d'infecció s'aprofiten de la possibilitat de suplantar el remitent, de manera que la persona que sembla ser qui envia el missatge en realitat no ho és, i a més no podem verificar realment qui ha enviat el missatge.

Una gran part de l'esforç de l'atacant a l'hora d'intentar que acceptem el missatge es basa en guanyar-se la nostra confiança. Per això, els seus missatges acostumen a contenir ofertes de feina, remitent d'operadora de telefonia amb notificació d'anomalia al servei, premis d'un concurs fictici, necessitat d'aplicar una actualització o configurar d'una forma determinada el teu mòbil, notificacions d'actualització d'aplicacions...

Les noves funcionalitats tecnològiques que inclouen els mòbils més avançats han obert noves vies d'atac que abans semblaven impossibles i que són similars a les que pot tenir un ordinador de sobretaula. És important que, a més de protegir de forma adequada el nostre telèfon, utilitzem el sentit comú i siguem conscients de què pot implicar obrir o realitzar les accions indicades en un missatge que ens sembla sospitós. Un missatge SMS o MMS presenta les mateixes opcions d'infecció que un correu electrònic, per la qual cosa hem d'aplicar les mateixes precaucions.

Aquesta aplicació fa coses rares

En aquests últims anys, els mòbils avançats han evolucionat i introduït noves característiques en la part de funcionalitats, com ara la possibilitat de poder desenvolupar programari fet a mida.

Les principals plataformes de telefonia mòbil tenen disponible per a l'usuari l'entorn de desenvolupament de programari per als seus mòbils (SDK), Blackberry, iPhone, Android, Symbian... El mercat d'aplicacions, que semblava tancat, ara pot oferir tot tipus d'aplicacions que no han de ser forçosament les oficials del proveïdor per cobrir qualsevol necessitat del consumidor.

Som conscients de tot el que fa l'aplicació que volem instal·lar? Actualment, els proveïdors d'aplicacions apliquen mesures més agressives per detectar possible codi maliciós o comportaments anòmals. És important conèixer o tenir referències sòlides de l'aplicació que volem instal·lar, utilitzar sempre que sigui possible les aplicacions proporcionades pel proveïdor oficial i, finalment, instal·lar software original.

També hem de tenir present que en casos molt concrets, en cas d'incidència o mal funcionament del nostre mòbil, hi ha la possibilitat que la nostra operadora o fabricant no es faci càrrec de la reparació o substitució del terminal si no tot el software instal·lat és original.

El primer codi maliciós per telefonia mòbil data del 14 de Juny del 2004, i des d'aleshores el creixement de noves variants de virus ha estat exponencial. Les noves prestacions que proporcionen els dispositius avançats produeixen una convergència del codi mali-

ciós per als ordinadors comuns i els telèfons avançats de tipus *smartphone*. El que fins ara era una quantitat testimonial d'espècimens, la majoria proves de concepte, s'ha convertit en una de les principals amenaces presents i futures per a la indústria de la seguretat.

Recordem que el nostre mòbil de tipus *smartphone* pot tenir prestacions similars a les que podria tenir un ordinador de sobretaula, i que en conseqüència pot estar exposat als mateixos riscos d'infecció, o fins i tot majors, perquè les característiques de seguretat no estan tan desenvolupades i provades com a les plataformes d'escriptori.

En l'àmbit de la telefonia mòbil hi ha riscos addicionals per les característiques específiques dels dispositius mòbils:

- Existeix la possibilitat de generar un cost directe per a l'usuari, utilitzant la xarxa de telefonia per fer trucades a números o subscripció a serveis de tarifació addicional que reporten un benefici directe al criminal. A aquest tipus d'aplicacions se les anomena *DIALWARE*.
- En alguns sistemes de control d'accés (per exemple, per a banca en línia) els dispositius mòbils s'utilitzen com a mecanisme addicional per verificar la identitat de l'usuari, habitualment mitjançant missatges SMS que generen codis de confirmació. Alguns dels virus més recents i sofisticats són capaços d'interceptar aquests missatges i utilitzar-los per suplantar a l'usuari (l'anomenat Man-in-the-mobile[1,2]).

He perdut totes les dades!

Quin ús estic fent del meu mòbil? Quins serveis de la xarxa estic utilitzant? Quina informació es guarda al meu mòbil? Puc perdre l'agenda, fotografies, missatges de text? Són preguntes que ens hauríem de fer, així com valorar quin impacte tindria la pèrdua de la informació emmagatzemada al nostre mòbil.

El mòbil és un tipus de dispositiu que normalment duem sempre a sobre, cosa que facilita que l'utilitzem com a agenda o calendari, per prendre notes, llegir documentació, registrar contactes... i fer ús d'altres aplicacions que poden gestionar informació més confidencial i en la majoria de casos crítica.

És important, per tant, identificar de quines dades és necessari realitzar una còpia de seguretat i amb quina regularitat.

Aquestes fotos eren privades!

Sabem què és la fuita d'informació o sostracció de dades ? La fuita d'informació es produeix quan es filtra informació de forma involuntària. Un dels casos més típics són fotos o altra informació penjada en xarxes socials i a la qual tenen accés usuaris desconeguts, o als quals no els permetríem accés en una situació similar no vinculada a la xarxa. També hi ha filtracions de dades menys òbvies, com ara informació sobre la nostra localització, ja sigui en els nostres missatges d'estat en xarxes socials o en les metadades de les fotografies preses amb el mòbil.

1 http://www.cesicat.cat/noticies/2010-10-13_Nota_premsa_MitMo_CESICAT.jsp?canal=home
2 http://www.youtube.com/watch?v=RHUs8TNumsA

Hi ha aplicacions o xarxes socials com Foursquare i Google Latitude que tenen com a funcionalitat principal difondre on som. És recomanable controlar el grau d'accessibilitat d'aquesta informació, ja que pot arribar a terceres persones que preferiríem que no hi tinguessin accés. Volem que qualsevol pugui saber quan no som a casa?

Un altre cas molt comú de fuita d'informació es produeix quan ens desfem dels terminals mòbils sense eliminar la informació privada que, conscient o inconscientment, ha estat emmagatzemada.

En el cas del robatori de dades, una persona malintencionada obté informació privada mitjançant tècniques d'intrusió o un robatori físic del propi dispositiu, per posteriorment penjar-la a llocs públics. És important, doncs, conèixer els nostres drets i quines accions podem dur a terme per evitar tant com sigui possible la difusió i persistència a la xarxa de la informació robada.

Xarxes sense fils

Atesa la naturalesa mòbil dels dispositius a què es refereix aquesta guia, ja siguin *smartphones* o *tablets*, la capacitat de connectar-se a la xarxa utilitzant xarxes sense fils (3G o Wifi) és una de les seves característiques bàsiques.

Des del punt de vista de la seguretat, les xarxes sense fils tenen un desavantatge clar respecte de les cablejades: qualsevol atacant amb l'equip i els coneixements adequats pot capturar la informació que viatja per l'aire en forma d'ones electromagnètiques. És per això que les tecnologies i protocols utilitzats han d'implementar mecanismes de confidencialitat, integritat i autenticitat en la base al seu disseny.

La característica de connexió permanent a la xarxa, juntament amb la típica itinerància dels dispositius mòbils, fa que s'estableixin habitualment connexions amb xarxes WiFi desconegudes o controlades per tercers, de les quals en desconeixem el propietari i no sabem si algú més pot estar-hi connectat i escoltant. Això augmenta el risc que la informació que es transmet arribi a tercers que no són el destinatari legítim de la comunicació.

Una altra amenaça existent és la suplantació de xarxes Wifi conegudes i legítimes a casa o a l'oficina, i sobretot en punts d'accés públics com aeroports, biblioteques, cibercafès... En aquest cas, l'atacant controla el trànsit que circula pel seu punt d'accés a la xarxa, i l'usuari té una falsa percepció d'us de xarxa legítima.

Aquest risc existeix també a les xarxes de telefonia GSM/3G en forma d'atacs de suplantació de punts de connexió a la xarxa mòbil (estacions base). Investigadors del món de la seguretat han demostrat que aquest tipus d'atacs es pot dur a terme utilitzant equips a l'abast de tothom, encara que els requisits de coneixements i la inversió econòmica necessària poden ser majors que per a la intercepció de les comunicacions a xarxes WiFi.

Recomanacions

Com protegir l'accés físic

La primera mesura de protecció òbvia és tenir el dispositiu en tot moment controlat, com qualsevol altre objecte de valor. No obstant això, podem (i hauríem de) contemplar la possibilitat d'una pèrdua, robatori o ús no autoritzat i establir alguns mecanismes de protecció bàsics:

- Protegir el desbloqueig del terminal, demanant la introducció d'un PIN, contrasenya o patró gràfic perquè l'usuari pugui interactuar amb el terminal quan aquest es trobi bloquejat.
- Activar el bloqueig automàtic del dispositiu després d'un cert temps d'inactivitat. Hem de ser conscients que hi ha aplicacions que per les seves característiques deshabiliten temporalment aquesta funció, com poden ser jocs o reproductors multimèdia. En aquest cas, el bloqueig ha de ser manual quan el deixem d'utilitzar.
- Mantenir sempre actiu el bloqueig de la targeta SIM d'accés a la xarxa mòbil, de manera que s'hagi d'introduir el PIN cada vegada que s'encén el telèfon.
- Instal·lar una aplicació de rastreig al mòbil, que es pugui activar remotament i de forma segura en cas que perdem o ens prenguin el dispositiu. Aquestes eines utilitzen diversos mecanismes per ajudar-nos a localitzar el dispositiu:
  - Emetre determinats sons per ajudar-nos a localitzar-lo si és a prop.
  - Enviar-nos les coordenades GPS o la localització aproximada de la connexió que utilitzem en aquest moment.
  - Fer fotografies o gravar sons i enviar-nos-les
  - Enviar una alerta en cas que es canviï la SIM, i enviar-nos el número de mòbil de la nova targeta.

Algunes d'aquestes mesures poden semblar incòmodes, però cal tenir en compte que sempre s'ha de buscar un compromís entre el nivell de seguretat desitjat o necessari i la usabilitat del dispositiu. En el cas de contrasenyes i patrons, la complexitat és directament proporcional a la seguretat. És preferible tenir una contrasenya o patró (relativament) simple, a desactivar aquesta funció totalment, encara que s'ha d'evitar errors habituals[3].

Altres mesures senzilles i amb un menor impacte que podem tenir en compte són:

- No donar a conèixer a tothom el tipus de mòbil que tenim, sobretot si es tracta d'un terminal de gamma alta. Per això és recomanable utilitzar el mode vibrador en l'avís de trucada (sempre que el terminal disposi d'aquesta opció), i ser discrets quan efectuem o contestem una trucada.
- En els automòbils no és recomanable deixar el mòbil al seient de l'acompanyant o a les safates, ni deixar el terminal a la vista quan no hi som.
- En cas de canvi del terminal, comunicar a la nostra Operadora el codi IMEI del nou terminal, perquè l'associï al nostre número de telèfon.

Com protegir les meves dades

La quantitat d'informació que acabem emmagatzemant en els nostres *smartphones* és sorprenentment alta: des de fotos fins a contrasenyes d'accés al banc, missatges SMS, correu electrònic, documents de treball... fins i tot la llista de la compra.

És segura la transmissió de les teves contrasenyes a les pàgines webs que visites o en els serveis que utilitzes? El teu navegador mòbil guarda les contrasenyes per accedir-hi? Saps si el teu telèfon emmagatzema el registre dels llocs pels quals passes? On i com es guarda el registre de les teves converses de missatgeria?

Els principals riscos associats a l'ús que li donem als nostres dispositius mòbils estan relacionats amb la filtració o robatori de dades, o a la pèrdua irrecuperable d'aquestes dades per una fallada en el terminal o un esborrat accidental.

El primer pas per protegir-los és ser conscients d'on estan emmagatzemades les dades, amb quines restriccions d'accés i nivell de protecció, i com es transmeten a través de la xarxa. En el cas de la informació personal a la qual permetem que altres accedeixin, hem d'intentar controlar qui la té i per a què pot utilitzar-la, així com conèixer els nostres drets d'accés, modificació, cancel·lació i com podem exercir-los.

Filtració de dades

Per protegir-nos contra la filtració de dades, podem aplicar les mateixes recomanacions de privacitat en l'ús d'Internet i xarxes socials que es donen per a ordinadors de sobretaula. A més, convé tenir en compte alguns consells específics per a dispositius mòbils:

- Conèixer les opcions relatives a la privacitat del nostre dispositiu i configurar segons les nostres preferències. Les més rellevants són:
  - Serveis de localització del mòbil mitjançant xarxes mòbils i GPS. Molts dispositius guarden un registre dels llocs per on passem, i aquesta opció en la majoria de casos es pot desactivar.

3 http://www.gizmodo.es/2011/06/14/los-10-pin-mas-habituales-en-iphone-veredicto-reconoce-lo-el-tuyo-es-uno-de-ellos.html

- Accés dels llocs web que visitem a les nostres dades de localització. Busca l'opció perquè es demani permís explícitament en la configuració del navegador.
- Geoetiquetatge automàtic de les fotos fetes amb la càmera del mòbil. És millor tenir-lo desactivat per defecte si no volem que aquesta informació sigui coneguda, i activar-lo només quan realment sigui necessari.
- Geolocalització automàtica de les nostres publicacions en xarxes socials com Facebook i Twitter, que poden permetre a qualsevol que les llegeixi saber on som en el moment de la seva publicació.

- Llegir els permisos que demanen les aplicacions que instal·lem, així com les condicions de servei, per evitar que puguin accedir a informació i utilitzar-la de manera que no sigui la desitjada.

Robatori d'informació

Per protegir-nos contra el robatori d'informació, la nostra principal arma és el sentit comú, que ens permetrà detectar possibles intents d'obtenir informació sensible directament de nosaltres (enginyeria social), per exemple, mitjançant trucades que intenten suplantar la companyia telefònica o el nostre banc.

Des del punt de vista tecnològic, és convenient conèixer les funcionalitats que utilitza el nostre telèfon per mantenir la confidencialitat, principalment el xifrat d'informació, tant la que es transmet a través de la xarxa com la que s'emmagatzema en el terminal.

Per a la **connexió segura amb serveis a la xarxa**, els navegadors mòbils utilitzen els mateixos mecanismes de protecció que els de sobretaula, però de vegades les limitacions pròpies del dispositiu (mida de pantalla), o el seu disseny, poden ajudar a un possible atacant. Per això, quan ens connectem a llocs sensibles com ara bancs en línia, hem d'assegurar que la connexió és segura (xifrada amb SSL) i procurar realitzar l'accés des de xarxes fiables. Sempre cal estar molt atents als errors en els certificats, que poden indicar que algú està intentant interceptar les nostres dades.

En el cas que algú aconsegueixi **accés físic al nostre dispositiu** hi ha formes d'accedir a les dades emmagatzemades sense necessitat de conèixer el codi de desbloqueig del dispositiu. L'exemple més senzill és treure els mòduls de memòria i accedir-hi amb un lector extern. L'única forma de protegir les nostres dades és utilitzar mecanismes de xifrat.

Alguns dispositius suporten el xifrat nativament. Comprova si en el teu es pot activar. En cas que no sigui així, és probable que hi hagi aplicacions de tercers (comercials o lliures) per xifrar el contingut de les nostres targetes o fins i tot el dispositiu complet, incloent l'emmagatzematge intern per als casos en què es manegi informació altament confidencial.

Finalment, si volem protegir les **comunicacions de veu** que tinguin un caràcter més crític enfront de possibles escoltes, hi ha aplicacions específiques per realitzar aquest tipus de xifrat utilitzant protocols de veu sobre xarxes de dades. Per poder utilitzar-les és imprescindible que les dues parts coneguin aquestes aplicacions i n'hagin acordat prèviament el seu ús.

Pèrdua d'informació

Per protegir-nos davant la **pèrdua d'informació**, l'única mesura possible és fer còpies de seguretat periòdiques i relativament freqüents, i emmagatzemar-les en un lloc segur.

La majoria de fabricants ofereixen programes per sincronitzar el nostre telèfon amb un ordinador, amb la funcionalitat de realitzar còpies de seguretat dels nostres contactes, missatges, etc. El principal inconvenient és que els formats solen ser incompatibles entre les diferents marques, i és convenient utilitzar formats estàndard per assegurar-nos que podrem importar aquesta informació en un dispositiu diferent.

Per sort, cada vegada més fabricants i aplicacions inclouen també la possibilitat de sincronitzar alguns tipus d'informació amb servidors "en el núvol" (en línia), com els contactes, el correu electrònic o la música que tinguem emmagatzemada. És recomanable conèixer i utilitzar aquesta capacitat si el nostre dispositiu la té, però avaluant sempre que aquests serveis compleixin amb les mesures de seguretat necessàries.

Una situació que mereix una atenció especial és quan ens desfem del mòbil, el venem o el cedim a algun amic o familiar. En aquest cas, és recomanable realitzar un esborrat complet de la informació que conté mitjançant la funcionalitat de "restauració a la configuració de fàbrica", i sense oblidar eliminar les dades de les targetes de memòria que puguin estar incloses en el dispositiu.

Com protegir-me dels virus

Gràcies a l'arquitectura lògica de les generacions més recents de les diferents plataformes d'*smartphones*, les accions que poden executar les **aplicacions de tercers** són controlades mitjançant una sèrie de permisos. Com a conseqüència, actualment la majoria dels virus utilitzen sobretot mecanismes d'"enginyeria social" per aconseguir que siguem nosaltres mateixos els que els instal·lem en els nostres dispositius. Com ja s'ha esmentat anteriorment, davant aquest tipus d'atacs el més útil és utilitzar el nostre sentit comú i estar atents al que acceptem en interactuar amb les aplicacions.

Una mesura de protecció bàsica és limitar les aplicacions que instal·len a aquelles distribuïdes mitjançant els proveïdors d'aplicacions oficials de cada plataforma. Les més populars són:

- Android: Android Market.
- Apple iOS (iPhone): App Store de Apple
- BlackBerry: BlackBerry App World
- Symbian (Nokia): OVI Store
- Windows Phone: Windows Phone Marketplace

No obstant això, no seria la primera vegada que s'introdueixen aplicacions malicioses a les botigues o repositoris d'aplicacions oficials, així que és convenient mantenir els sentits alerta i comprovar la reputació i els comentaris sobre les aplicacions, així com els permisos que demanen en instal · lar-les.

Les aplicacions distribuïdes per canals no oficials no

passen cap tipus de validació i el risc que siguin malicioses és major. Per això cal posar especial atenció si les volem instal · lar, tot comprovant que el seu origen sigui d'una font fiable i que no demanen permisos que no tinguin res veu veure amb la finalitat declarada.

Si ets dels que vols esprémer totalment l'aparell mitjançant un **desbloqueig total del sistema** (*root, jailbreak*), has de tenir una cura addicional. No cal confondre aquest tipus de modificacions amb el desbloqueig de l'operadora mòbil, que la nostra operadora està obligada a realitzar si així ho demanem i que no ha de suposar cap risc.

L'avantatge del desbloqueig és alhora la seva major debilitat, ja que permet que l'usuari executi aplicacions de tercers (no oficials) amb capacitat de fer qualsevol cosa al dispositiu i evitar les mesures de seguretat que el fabricant hagi implementat en el sistema.

A més, en alguns casos el desbloqueig habilita mecanismes addicionals de connexió des de l'exterior cap al nostre dispositiu (per exemple, el servei de gestió remota SSH), configurats amb la mateixa contrasenya per a tots els dispositius. És com posar una porta a casa que s'obre amb la mateixa clau que totes les dels veïns, i que, a més, qualsevol pot aconseguir. Els cucs per mòbil més cèlebres fins ara utilitzen aquesta debilitat per propagar-se[4], i la solució en aquests casos és aplicar una contrasenya robusta i que només nosaltres coneguem.

Instal lar un **sistema operatiu modificat** (ROM personalitzada) descarregat d'Internet pot ser també molt perillós. A més de la pèrdua de garantia, podem assumir el risc de confiar totalment el control del que fa el nostre dispositiu a l'usuari o entitat que ha creat aquesta ROM. És possible que els desavantatges siguin majors que les millores que puguem aconseguir.

Amb l'augment de la complexitat i la difusió dels *smartphones*, és cada vegada més comú que apareguin **fallades de seguretat que faciliten la propagació de virus**. Per això, és convenient mantenir actualitzat en la mesura del possible tant el sistema base com les aplicacions, inclosos els plugins del navegador com ara el Flash si el nostre dispositiu ho suporta. Per això, recomanem activar les notificacions automàtiques de l'aparició de noves versions per aplicar-les sempre que sigui possible.

En alguns casos els fabricants o les operadores deixen d'actualitzar els dispositius que són relativament antics, encara que continuïn sent molt populars entre els usuaris. En aquest cas, les ROM personalitzades poden permetre executar una versió posterior del sistema (amb els errors solucionats) en dispositius antics, encara que amb els riscos associats comentats anteriorment.

Una altra de les vies de propagació de *malware* a dispositius mòbils és la **connexió bluetooth**. Encara que va ser la primera històricament, ha caigut bastant en desús, però és important que configureu adequadament aquesta la funcionalitat. Cal, doncs:

- Desactivar el bluetooth sempre que es faci servir per connectar-nos a un kit de mans lliures o enviar dades a altres dispositius.

4 http://www.hispasec.com/unaaldia/4033

- Desactivar la visibilitat de manera que el nostre telèfon no aparegui quan algú faci una cerca. En la majoria de terminals podem activar la visibilitat de forma temporal quan ho necessitem, ja que no és una cosa extremadament habitual.
- Protegir l'associació mitjançant un PIN, i si és possible que no sigui el típic 0000 o 1234.
- Configurar un nom de dispositiu que no reveli massa informació (model de mòbil, nom propi).

Finalment, les solucions de seguretat per a mòbils inclouen una protecció equivalent als antivirus tradicionals dels ordinadors de sobretaula basada en l'anàlisi de signatures i comportaments que pot ser molt eficaç. Però, tal com ja ha passat en aquesta plataforma, han sorgit una sèrie de falsos antivirus que, després d'enganyar l'usuari perquè els instal·li (mitjançant una falsa alerta d'infecció o publicitat falsa), s'utilitzen per robar dades o realitzar fraus. Cal validar que la font de l'aplicació és de confiança.

Què fer en cas de pèrdua

Per molta cura que tinguem, és difícil mantenir localitzat en tot moment el nostre telèfon. Gairebé tots hem tingut algun episodi de pànic en adonar-nos que hem perdut el nostre estimat *smartphone*. Amb una mica de sort i una trucada des d'un altre telèfon podem trobar-lo, però en cas que no sigui així, cal tenir clar quins són els passos a seguir.

- Demanar a l'operadora el bloqueig de totes les trucades de sortida des de la nostra línia, per evitar trobar-nos amb trucades fraudulentes a la nostra factura.
- Si tenim instal·lada una aplicació de rastreig, la podem activar des d'un altre dispositiu, normalment accedint amb les nostres credencials al lloc web de gestió de l'eina.
- Si la plataforma ho suporta i ho hem configurat així, o bé hem instal·lat alguna aplicació per a això, podem bloquejar el telèfon de forma remota perquè no es pugui utilitzar.
- Si no hem aconseguit localitzar-lo, hi ha la possibilitat de realitzar un esborrat remot de dades per evitar que qui tingui el mòbil en el seu poder pugui accedir a informació confidencial.
- Demanar a la nostra operadora el bloqueig del terminal mitjançant el número IMEI. D'aquesta manera ens assegurem que el nostre telèfon no podrà utilitzar-se a la xarxa mòbil de cap operador, ja que hi ha una llista negra centralitzada de terminals robats.
- Si estem segurs que és un robatori, és recomanable denunciar-ho a la policia.

Malgrat totes les mesures anteriors, és convenient canviar les contrasenyes que poden estar emmagatzemades al dispositiu. A més, cada vegada més serveis de correu electrònic i missatgeria permeten visualitzar i tancar remotament les sessions obertes.

Per dur a terme les accions esmentades anteriorment, cal que abans haguem guardat en lloc segur (però accessible i que recordem immediatament) alguna informació sobre el dispositiu i la targeta SIM:

- El número IMEI del telèfon
- El PIN i el PUK de la nostra targeta SIM
- El número de bloqueig del telèfon, opció que porten alguns terminals i que permet bloquejar l'ús del terminal per a una sola targeta SIM.

Com connectar-me a una xarxa sense fils de forma segura

A l'hora d'utilitzar xarxes WiFi per connectar-nos a Internet, convé seguir una sèrie de consells perquè l'ús sigui el més segur possible:

No activar l'opció de "desar connexió" o "connexió automàtica" a xarxes no segures o desconegudes.

A l'hora de connectar-nos a xarxes conegudes, no fiar-nos només del nom de la connexió (SSID), i comprovar que el tipus de seguretat és el mateix que el de la xarxa coneguda.

Sospitar si el nostre telèfon ens demana que tornem a introduir la contrasenya d'una xarxa que ja teníem guardada com la de la nostra casa o l'oficina.

Informar dels possibles avisos que ens dóna el nostre terminal si es realitza una connexió sense xifrar

- En el navegador web
- En realitzar trucades GSM

Per últim, utilitzar les xarxes desconegudes només quan sigui realment necessari i deixar les activitats d'ús més sensibles preferentment en xarxes conegudes o d'interacció directa amb la xarxa de telefonia mòbil 3G. És preferible utilitzar xarxes 3G o superiors, ja que a més de l'autentificació del client també es realitza autenticació de l'operador (autenticació mútua), a diferència de les xarxes 2G (GPRS).

Per moltes mesures que prenguem, les connexions sense fils sempre s'han de considerar poc segures, ja que no podem saber qui hi té accés i pot estar capturant-ne el trànsit. Per això és important assegurar-nos que les aplicacions i els llocs web als quals ens connectem utilitzen xifrat per transmetre les dades, especialment les contrasenyes. De vegades, el xifrat s'inclou com una opció, tot i que encara en moltes aplicacions ve desactivada per defecte.

Bones pràctiques en telefonia mòbil

En aquest apartat s'inclouen alguns consells que no encaixen directament en algun dels casos anteriors o que n'afecten a més d'un, i que poden contribuir a fer més segur l'ús del nostre mòbil:

Coneix les possibilitats de configuració del teu dispositiu i desactiva aquelles funcions que no són necessàries.

Procura no revelar dades personals en informació accessible a qualsevol com el nom del nostre dispositiu Bluetooth. Pot ser que algú utilitzi aquestes dades per dur a terme un atac més elaborat.

Canvia les contrasenyes per defecte en les aplicacions que les incloguin (per exemple en cas de root, jailbreak o instal·lar una ROM modificada).

Si has vist moltes pel·lícules, sabràs que no has de triar com PIN la teva data de naixement, i tampoc el nom de la teva mascota o d'una persona propera com a contrasenya. Fes que siguin aleatòries, almenys aparentment, encara que tinguis alguna forma indirecta de recordar-les que només tu coneixes.

- Intenta no introduir números PIN i contrasenyes a la vista de tothom.
- Compte amb les pantalles tàctils i les marques de dits: poden facilitar la tasca a algú que intenti endevinar el nostre PIN o patró gràfic de desbloqueig.
- Tanca sessió explícitament en llocs web sensibles després d'una sessió de navegació, per exemple després d'accedir al banc en línia.
- Revisa el detall de trucades que et facilita la teva operadora a la factura per detectar possibles trucades fraudulentes procedents d'una targeta SIM clonada. També et pot venir bé per evitar costosos errors en la facturació.
- Sospita de les trucades des de números desconeguts i ocults, i no donis dades personals fins a tenir la certesa que és un tràmit legítim.
- Fes servir els serveis de restricció de trucades de la teva operadora i, si no has de viatjar a l'estranger, desactiva l'ús de xarxes d'altres operadors (Roaming). En cas que el perdis o te'l robin, aquesta mesura pot reduir el dany produït.

Desconfia dels SMS/MMS

No instal·lis aplicacions que no siguin de confiança.

No accedeixis a llocs que no siguin de confiança.

Intenta mantenir el terminal controlat en tot moment.

Conclusions

L'augment de la popularitat i de les capacitats dels dispositius mòbils fa que, cada vegada, aquests tinguin més importància en el nostre dia a dia. La quantitat i el nivell de confidencialitat necessari de la informació que emmagatzemen s'equipara cada vegada més als d'un ordinador personal. Per tant, i encara que no hi estiguem tan acostumats, hem d'aplicar els mateixos principis de seguretat per als nostres dispositius i establir les mesures necessàries per protegir-los.

Davant aquest repte, és important estar informat dels diferents riscos que s'han plantejat en aquesta guia, així com dels diferents mecanismes i hàbits recomanables per prevenir incidents i mitigar-ne l'impacte.

La seguretat física passa a ser un factor determinant en aquests sistemes, ja que a causa de la seva natural mobilitat no estan en un entorn protegit per panys o cadenats. Nosaltres mateixos esdevenim guardians de la seguretat física de dispositius que moltes vegades són d'una importància crucial per a la nostra vida personal o professional.

Tots hauríem de fer una reflexió sobre l'ús que li donem al mòbil i sobre què passaria si el perdéssim o un tercer hi tingués accés. Aquesta reflexió ens ajudarà a tenir clar el procediment a seguir en cas que això passi i, probablement, contribuirà a convèncernos de la necessitat de realitzar còpies de seguretat regulars de la nostra informació. Potser decidim sacrificar una mica la nostra comoditat d'ús a canvi d'una major seguretat.

Per sort, cada dia els diferents models i plataformes van evolucionant i van incorporant mecanismes de seguretat que existeixen des de fa temps per als ordinadors de sobretaula. També les funcionalitats específiques d'aquest tipus d'aparells es poden apro-

fitar per desenvolupar mecanismes de seguretat poc habituals fins ara (GPS, càmera per rastreig), o bé per facilitar l'ús de les que coneixem des de fa temps (càmera, pantalla tàctil per autenticació) .

Per tant, és important conèixer les capacitats dels nostres dispositius, perquè poden ajudar-nos a protegir-los i a protegir la nostra informació. No obstant això, la naturalesa extensible de les plataformes més populars fa que també sigui important controlar les aplicacions que hi executem. L'homogeneïtzació de plataformes i la popularització del desenvolupament de programari per a mòbils comporta el problema de la difusió de malware que afecta als ordinadors personals des de fa anys.

Alhora, aquesta mateixa extensibilitat fa que sorgeixin aplicacions amb la finalitat de completar les possibles mancances de les plataformes quant a protecció, i les solucions integrals de seguretat per al mòbil s'han convertit en un mercat més per a les empreses tradicionals de seguretat, i per a d'altres que ho estan aprofitant per entrar amb força. És recomanable avaluar els riscos, establir el nivell de seguretat desitjat i estudiar si necessitem un d'aquests productes per complementar les capacitats de seguretat al nostre terminal mòbil.

Glossari

SIM

De les seves sigles en anglès (Subscriber Identity Module), mòdul d'identitat de subscriptor. És una targeta intel·ligent desmuntable utilitzada en dispositius de telefonia mòbil per identificar de forma segura la línia davant la xarxa.

PIN

De les seves sigles en anglès (Personal Identification Number), número d'identificació personal. És un tipus de contrasenya requerida per accedir a algun dispositiu o sistema, que normalment consisteix en un nombre de 4 dígits. En telefonia mòbil s'acostuma a utilitzar per restringir l'accés a les funcionalitats de la SIM.

PUK

De les seves sigles en anglès (Personal Unlocking Key), clau de desbloqueig. És el codi necessari per desbloquejar una targeta SIM quan ha estat bloquejada per la introducció d'un pin incorrecte almenys 3 vegades. Normalment és un nombre de 8 dígits que es lliura a l'usuari juntament amb el PIN però a diferència d'aquest, no pot modificar-se.

PDA

De les seves sigles en anglès (Personal Digital Assistant), Assistent Digital Personal o agenda digital. Van néixer com a dispositius relativament senzills amb capacitat de gestió de calendari, contactes, notes, documents i altra informació personal, encara que van evolucionar cap a petits ordinadors de butxaca amb pantalla tàctil i la capacitat d'executar tot tipus d'aplicacions.

Smartphone

En anglès, telèfon intel·ligent. Es denominen així els dispositius que combinen les característiques de telèfon mòbil i assistent personal digital (Personal Digital Assistant o PDA).

SMS

De les seves sigles en anglès (Simple Messaging Service), servei de missatges curts (normalment fins a 160 caràcters) dissenyat per a les xarxes de telefonia mòbil GSM, i que actualment es pot utilitzar en tot tipus de xarxes de telefonia, incloses les fixes.

MMS

De les seves sigles en anglès (Multimedia Messaging System), servei de missatgeria multimèdia que estén la capacitat de la missatgeria SMS incloent la possibilitat d'enviar arxius multimèdia (so, vídeo, fotos o altres continguts).

IMEI

De les seves sigles en anglès (International Mobile Equipment Identity), Identitat Internacional d'Equip Mòbil. És un nombre que identifica unívocament i a nivell mundial un terminal de telefonia mòbil. Normalment es pot veure a la caixa del mòbil o fent * # 06 # al telèfon.

Malware

De la conjunció de les paraules angleses malicious i software, és un codi o programari que efectua accions de forma oculta, sense permís i sense coneixement de l'usuari, amb algun objectiu que s'aparta de la seva finalitat declarada (robatori de dades, frau, control remot de sistemes i moltes altres coses).

Spyware

De la conjunció de les paraules angleses spy i software, és un codi o programa espia que recull informació sobre l'activitat de l'usuari, sense que aquest en tingui coneixement. Les dades es recopilen i distribueixen normalment a empreses i organitzacions interessades amb finalitats de seguiment o publicitàries.

SDK

De les sigles en anglès (Software Development Kit), és un conjunt d'eines i interfícies de programació que permeten el desenvolupament d'aplicacions en una plataforma determinada.

Bluetooth

Tecnologia de connectivitat sense fils d'àrea personal (limitada a uns pocs metres) utilitzada amb diverses finalitats, com ara la connexió de dispositius mòbils entre si, amb ordinadors de sobretaula i amb diversos perifèrics com auriculars i kits de mans lliures.

DLP

De les seves sigles en anglès (Data Leakage Prevention) sistemes de seguretat de prevenció de fuites d'informació per a punts finals que pretén evitar que es filtrin dades confidencials o sensibles de manera involuntària cap a fora de l'organització.

Referències i enllaços web

Riesgos, oportunidades y recomendaciones sobre seguridad de la información en teléfonos inteligentes. ENISA (European Network and Information Security Agency). Desembre 2010
http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users

Online As Soon As It happens. ENISA (European Network and Information Security Agency). Febrero 2010
http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens/at_download/fullReport

A Window Into Mobile Device Security. Examining the security approaches employed in Apple's iOS and Google's Android. Symantec. Juny 2011
http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. Michael Becher , Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf. IEEE Symposium on Security and Privacy, Oakland, Maig 2011.
http://emma.rub.de/research/publications/mobile-security-catching-up/

***Malware* en *Smartphones*. Informe del CNCCS (Consejo Nacional Consultivo de Cyber-Seguridad). Febrer 2011**
http://www.s21sec.com/descargas/Malware_Smartphones_CNCCS%20.pdf

Guidelines on Cell Phone and PDA Security. Octubre 2008
http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

CESICAT: Guia per gestionar les contrasenyes. Febrer 2010
http://www.cesicat.cat/publicacions/Guia%20per%20gestionar%20les%20contrasenyes.jsp?canal=home

cesicat

Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat