Els mòbils: canvi d'hàbits i la manca de percepció de risc
Data de publicació: 04/04/2012

Font: www.cesicat.cat

En termes de seguretat de la informació, els dispositius mòbils amb connexió a Internet són tant o més insegurs que els ordinadors. Tanmateix, l'usuari mitjà encara no és massa conscient d'aquesta realitat i encara no té la percepció de risc que els experts han assumit de fa temps

De fet, es tracta d'un fenomen transversal a qualsevol disciplina que afecti les pautes de comportament personals, i en tenim un exemple concret en els darrers anys i pel que fa a la seguretat de la informació: l'ús dels programes antivirus va trigar molt de temps a incorporar-se al dia a dia de l'usuari mitjà, per bé que el risc existia des del principi.

Avui dia, doncs, es pot afirmar que la percepció de perill associada a l'ús dels mòbils de darrera generació és escassa.

En plena penetració d'aquests dispositius al mercat, l'usuari ha canviat en poc temps algunes pautes de comportament i de comunicació que es consideraven tradicionals; el mòbil ha passat a ocupar una part important de la nostra vessant social i fins i tot familiar i més personal: al metro i a l'autobús, una gran majoria de les persones juguen amb una aplicació o envien un WhatsApp, mentre que, al carrer, els vianants caminen distrets i submergits en xats via mòbil. Fins i tot les relacions personals, de parella i familiars, han canviat, amb la incorporació d'un nou membre –el dispositiu mòbil- que sol merèixer una atenció privilegiada, prioritària.

Enfeinat a digerir tots aquests canvis, l'usuari no té temps per pensar en la seguretat de la informació associada al mòbil. I el "reaprofitament" del nom tampoc no hi ha ajudat gaire. El "mòbil" de fa cinc anys només era un telèfon que també permetia enviar missatges SMS, tot plegat amb poc risc. El "mòbil" actual és en realitat un ordinador amb moltes funcionalitats –trucar només n'és una-, connectat permanentment a Internet i, per tant, altament exposat als perills que posen en risc la seguretat de la informació.

Arribats a aquest punt, i havent descrit el paisatge actual, val la pena aportar algunes recomanacions bàsiques perquè l'usuari augmenti el seu nivell de seguretat durant l'ús dels smartphones. Els atacs als mòbils busquen en la majoria de casos el robatori de dades personals per a un ús il·lícit, així que cal ser-ne conscients i prendre algunes mesures al respecte:

Protecció de l'accés al mòbil: a banda del PIN d'arrencada del dispositiu, és imprescindible activar l'opció de bloqueig per tal que ningú no pugui accedir al nostre mòbil si ens l'oblidem a algun lloc o l'hem perdut. Davant de diversos intents fallits d'accés al dispositiu, alguns serveis ofereixen la possibilitat d'esborrar-ne automàticament les dades personals i aquelles que s'han marcat com a sensibles. Les dades també es poden bloquejar i esborrar de

forma remota, en cas que haguem extraviat el mòbil.

Identificador del telèfon: la majoria de dispositius mòbils tenen un número IMEI que identifica de forma única el telèfon. En cas de robatori, qualsevol operador de qualsevol país podrà desactivar el telèfon si els en facilitem l'IMEI. Per saber el número IMEI associat al vostre dispositiu, marqueu *#06#. Posteriorment, copieu-lo en algun lloc segur.

Desactivació de les connexions externes: la xarxa sense fils Wi-Fi, el Bluetooth i els Infrarojos són les vies més freqüents d'accés als mòbils per part dels intrusos. Consegüentment, cal mantenir-los sempre desactivats, excepte quan n'hagueu de fer ús.

Alerta amb els SMS o MMS sospitosos: no seguiu mai les instruccions dels missatges de remitent sospitós, que ocasionalment arriben amb felicitacions per haver guanyat algun premi, per exemple. Convé eliminar-los.

Serveis web amb contrasenya: cal tancar la sessió cada vegada que abandonem un lloc web que requereixi contrasenyes d'accés. Així evitarem que altres persones puguin accedir-hi a través del nostre mòbil.

Aplicacions a les xarxes socials: és important determinar que aquestes aplicacions, que solen ser una porta d'accés a moltes dades personals, ens demanin l'usuari i la contrasenya cada vegada que hi vulguem accedir. Aquesta no és l'opció per defecte que solen oferir aquestes aplicacions, així que caldrà canviar la configuració manualment.

Connexions a altres dispositius: si hem de connectar un mòbil a altres ordinadors o dispositius, de qualsevol tipus, és imprescindible tenir la seguretat que aquests altres dispositius són plenament segurs. Si no és així, el nostre mòbil corre el risc d'infecció.

Actualització del programari i de les aplicacions: és imprescindible descarregar-se les últimes versions del sistema operatiu que controla el mòbil i de les aplicacions que hi tenim, atès que sempre incorporen millores i cobreixen forats en matèria de seguretat.

Alerta amb la instal·lació d'aplicacions: abans de descarregar cap aplicació, cal mirar-ne la procedència i el fabricant per assegurar-nos que és fiable. Sempre que sigui possible, és convenient descarregar-se aplicacions oficials.

Instal·lació d'un antivirus professional per a mòbil: Norton, Kaspersky, Bitdefender i McAfee són algunes de les marques que ja han desenvolupat programari antivirus adreçat a dispositius mòbils de darrera generació, en aquets cas per a Android. Es poden trobar fàcilment a través d'una cerca a la botiga d'aplicacions.

Còpies de seguretat de la informació: és important fer còpies de seguretat, de forma regular, per tal de salvaguardar la informació més rellevant que tenim

emmagatzemada al mòbil. Aquestes còpies es poden guardar a un ordinador o algun altre lloc, sempre que sigui segur. En qualsevol cas, com menys informació sensible guardem al mòbil, millor.

El llistat de recomanacions i mesures descrites no és pas exhaustiu, per bé que es tracta d'una aproximació que permetrà situar el nostre dispositiu mòbil en una zona de risc acceptable. La informació que hi tinguem, per tant, quedarà raonablement protegida, almenys contra un percentatge molt elevat del total d'atacs i amenaces existents. Si voleu informació ampliada sobre aquest tema, podeu consultar la Guia d'utilització segura del mòbil del CESICAT.