Älypuhelin on tietoturvan painajainen

Älypuhelimet ja tablet-koneet ovat tietoturvan kannalta hankalin mahdollinen ympäristö. Ne on helppo hukata ja varastaa, laitteet eivät tahdo kestää arjen kolhuja ja niiden tietoturvaominaisuudet jättävät toivomisen varaa. Pienissä laitteissa ei ole näppäimistöä, joten kunnon salasanan sijaan käytetään helposti arvattavaa pin-koodia.

Mobiililaitteissa on ollut luvattoman paljon teknisiä turva-aukkoja, osa niistä aivan alkeellisia:

- iPad 2 -koneissa suojakoodin (passcode) pystyi ohittamaan laitteen omalla magneettisella kannella
- iPhone ei tarkistanut varmenneketjua loppuun asti, jolloin hyökkääjän oli mahdollista päästä vakoilemaan muutoin salattua tietoliikennettä
- iPhone-puhelimissa pystyi katsomaan valokuvia tietämättä lukitun puhelimen suojakoodia
- mikä tahansa iOS-sovellus pystyi lataamaan puhelimen osoitekirjan sisällön itselleen lupaa kysymättä
- iPhone-laitteissa sovellukset pystyivät lataamaan kaikki puhelimessa olevat valokuvat omaan palveluunsa, mikäli puhelimessa oli sallittu paikkatietojen käyttö
- Android-puhelimissa sovellukset pystyivät lataamaan lupaa kysymättä valokuvat itselleen, koska kuvat tallennetaan aina samannimiseen kansioon johon sovelluksilla on oikeudet
- Nokian E75-puhelimesta löytyi bugi, joka mahdollisti suojakoodin ohittamisen puhelinta käynnistettäessä (CERT-FI-haavoittuvuustiedote 043/2011).

Nämä kaikki virheet on sittemmin tavalla tai toisella korjattu, mutta montako uutta ongelmaa on vielä löytymättä?

Mobiililaitteissa on useita osapuolia: laitevalmistaja, käyttöjärjestelmä, sovellus, pilvipalvelu, operaattori ja niin edelleen. Käyttäjällä ei ole mitään keinoa varmistua kaikkien osien turvallisuudesta ja lainmukaisesta toiminnasta.

Vaikka tekniikka toimisi, asetelma on mahdoton myös tietosuojan kannalta. Puhelimissa säilytetään ihmisten kaikkein henkilökohtaisimpia tietoja, joita käytetään ulkomailla sijaitsevilla ilmaispalveluilla. Kukaan ei voi lopulta tietää, millä keinoilla ne hankkivat rahoituksensa ja miten ne hyödyntävät saamiaan tietoja.

Älypuhelin ei ole itsenäinen laite vaan ekosysteemi, joka imaisee käyttäjän väkisin sisäänsä. Puhelimet, alustat ja palvelut on sidottu niin tiukasti yhteen, ettet voi välttyä niiden käytöltä. Ainoa, mitä voit tehdä, on valita leirisi: Apple, Google tai Microsoft. Sen jälkeen tietosi ja koko elämäsi päätyy jollekin näistä yhtiöistä.

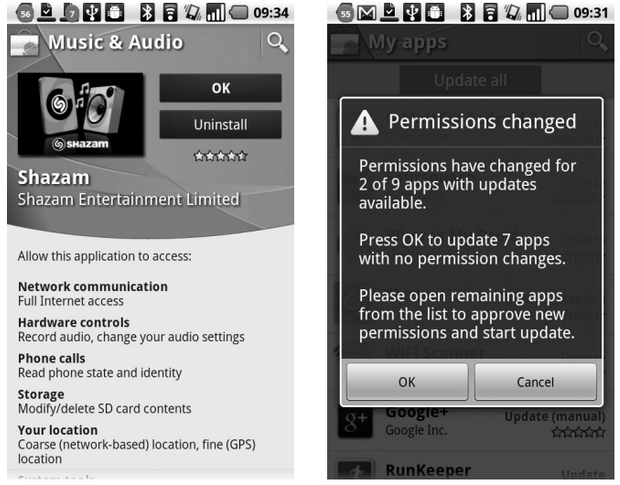
Kyse ei ole pelkästä tietosuojasta, vaan tilanne on painajainen myös yrityksille. Mobiilialustojen kautta niiden sisäinen viestintä, yrityssalaisuudet ja taloudelliset tiedot valuvat väistämättä amerikkalaisten omistamaan pilveen. Se avaa pelottavia mahdollisuuksia niin teollisuusvakoilulle kuin valtioiden tiedustelutoiminnallekin.

Haittaohjelmat

Puhelimeen päässyt haittaohjelma voi tehdä paljon suuremman vahingon kuin mikä tietokoneessa olisi mahdollista. Windowsin ohjelmaympäristö on hajanainen, eivätkä vieraat sovellukset pysty kovinkaan helposti lukemaan toistensa tietoja. Tietokoneissa ei liioin ole tapaa, jolla käyttäjää voisi rahastaa – ainoa keino on huijata uhri itse syöttämään luottokorttinsa numero tai menemään verkkopankkiin.

Älypuhelin on paljon vaarallisempi ympäristö, sillä puhelinalusta tarjoaa valmiit palvelut henkilökohtaisten tietojen lukemiseen ja muuttamiseen. Lisäksi raha liikkuu puheluita soittamalla.

Pahimmassa tapauksessa puhelimeen päässyt haittaohjelma voisi ensin tuottaa käyttäjälle suuren puhelinlaskun soittamalla maksulliseen palvelunumeroon ja lopuksi nolata hänet levittämällä sähköpostit, tekstiviestit, valokuvat ja osoitekirjan nettiin kaikkien nähtäville. Siinä sivussa haittaohjelma voisi myös varastaa puhelimeen tallennetut työdokumentit ja myydä ne kilpailevalle yritykselle.



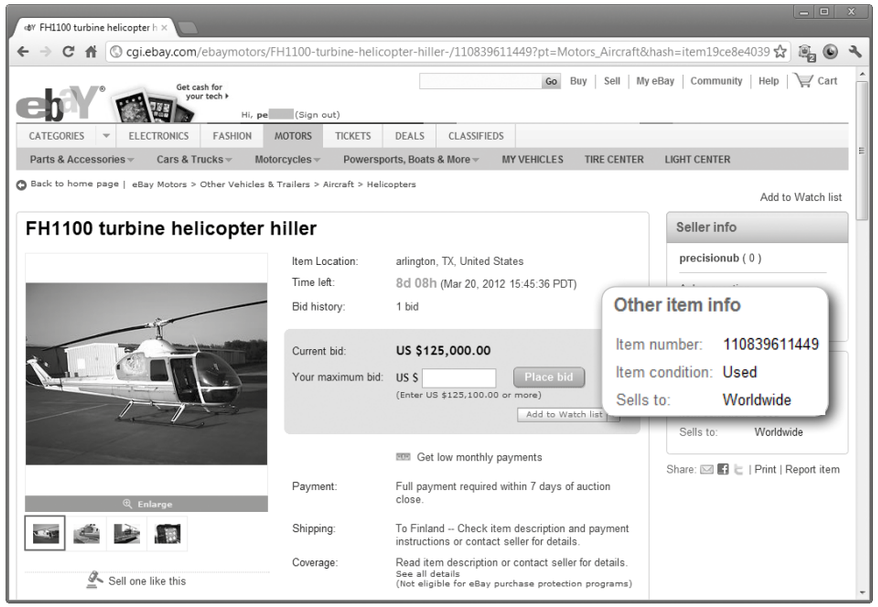
Android-sovellukset kertovat havainnollisesti, mitä oikeuksia ne tarvitsevat puhelimeen. Päivitysten myötä oikeudet saattavat laajentua.

Onneksi älypuhelinten suunnittelijat ovat oppineet avoimen pc-maailman virheistä. Puhelinalustat ovat suojattuja ja mikä tärkeintä, ohjelmat pyritään jakamaan sovelluskaupan kautta. Keskitetty jakelu helpottaa haitallisten ohjelmien havaitsemista ja niiden poistamista jakelusta. Jokaisella alustalla on oma kauppapaikkansa:

Nettihuutokaupat

Nettihuutokaupat poikkeavat monin tavoin tavallisesta verkkokaupasta, jossa myyjänä on yritys. Kuluttajien (samoin kuin yritysten) keskenään käymää kauppaa säätelevät eri lait, joissa ostajan turva on huomattavasti heikompi.

Alan tunnetuin toimija on amerikkalainen eBay (*www.ebay.com*), jossa miljoonat esineet keräilykorteista lentotukialuksiin vaihtavat omistajaa päivittäin. Suomessa tunnetuin kauppapaikka on Huuto.net (*www.huuto.net*).



Ostaisinko vaikka käytetyn helikopterin? eBaystä löytyy. Toimitus järjestyy vaikka Suomeen.

Nettihuutokauppojen lisäksi kuluttajat käyvät keskenään kauppaa muillakin foorumeilla. Esimerkiksi monilla harrastesivuilla on yhtenä keskustelualueen osiona jäsenten väliset osto- ja myynti-ilmoitukset.

Myyjien ja ostajien arviointi

Nettihuutokaupassa ostetaan ja myydään tavaroita tuntemattomilta ihmisiltä. Turvallisuuden parantamiseksi ostajat ja myyjät antavat toisilleen palautetta. Mitä paremmat arvostelut, sitä turvallisempaa asiointi on.

Näin ainakin periaatteessa. Käytännössä kannattaa tarkistaa, kuinka moneen arvioon lukema perustuu. Yksi tai kaksi tyytyväistä asiakasta ei vielä takaa mitään.

Lisäksi lukuja saatetaan vedättää ylöspäin tekemällä lumekauppoja kavereiden tai valehenkilöiden kesken.

Älä luota ruutukuviin äläkä ilmoituksiin

Ostaja saattaa ilmoittaa, että on juuri maksanut pyydetyn summan verkkopankissa, vaikka se näkyykin myyjän tilillä vasta seuraavana päivänä. Ostaja vetoaa kiireeseensä ja pyytää toimittamaan tavaran välittömästi. Todisteeksi maksusta ostaja lähettää sähköpostilla ruutukuvan, josta näkyy verkkopankissa tehty tilisiirto.

Kyse on huijauksesta. Ruutukuva on tietenkin väärennetty kuvankäsittelyohjelmalla. Helppo homma.

Älä toimi liian aikaisin

Jos olet myyjä, älä toimita tavaraa ennen kuin raha näkyy omalla tililläsi. Jos olet ostaja, älä maksa ennen kuin olet saanut tavaran haltuusi.

Myyjä saattaa ilmoittaa jättäneensä paketin juuri postiin tai matkahuoltoon. Todisteena hän lähettää sähköpostilla skannaamansa kuitin paketista ja pyytää ostajalta pikaista maksua. Kuitti on aito, mutta kertoo vain paketin painon – ei mitään sen sisällöstä. Eräässä tapauksessa suomalainen ostaja löysi paketista kitaran sijaan painoa vastaavan määrän jauhopusseja. Siinä vaiheessa yli tuhannen euron kauppasumma oli jo siirretty myyjän tilille.

Erilaisten maksuvälittäjien, kuten PayPalin tai Western Unionin nimissä lähetetyt ilmoitukset muka saapuneista suorituksista on niin ikään helppo väärentää. Peli on selvä vasta, kun raha näkyy omalla tilillä.

Huutokauppahuijaukset

Nettihuutokauppojen on helpompi valvoa myynti-ilmoituksia kuin niihin tulleita vastauksia, jotka menevät suoraan myyjälle. Siksi myyjän riski tulla huijatuksi on lähtökohtaisesti suurempi kuin ostajan.

Yleensä huijauksen tekijä on parikymppinen mies, joka on huomannut, miten helppoa olemattomien tavaroiden myynti on. Vaikka kotimaiset tekijät jäävät ennen pitkää kiinni ja saavat petoksesta lyhyitä vankeustuomioita, heistä moni jatkaa toimintaa heti vapauduttuaan.

Ulkomaiset huijarit eivät jää kiinni. Tämän kirjan valmistuessa poliisilla ei ollut tiedossa yhtään tapausta, jossa ulkomaiselle huijarille maksettuja rahoja olisi onnistuttu saamaan takaisin.

Huijarien tuotevalikoima on rajaton. Tietokoneet ja pelikonsolit ovat erityisen suosittuja, mutta listalta löytyy niin lastenvaunuja, konserttilippuja, matkapuhelimia kuin lautatavaraakin. Huijari pystyy myymään mitä tahansa, koska ei aiokaan toimittaa sitä.

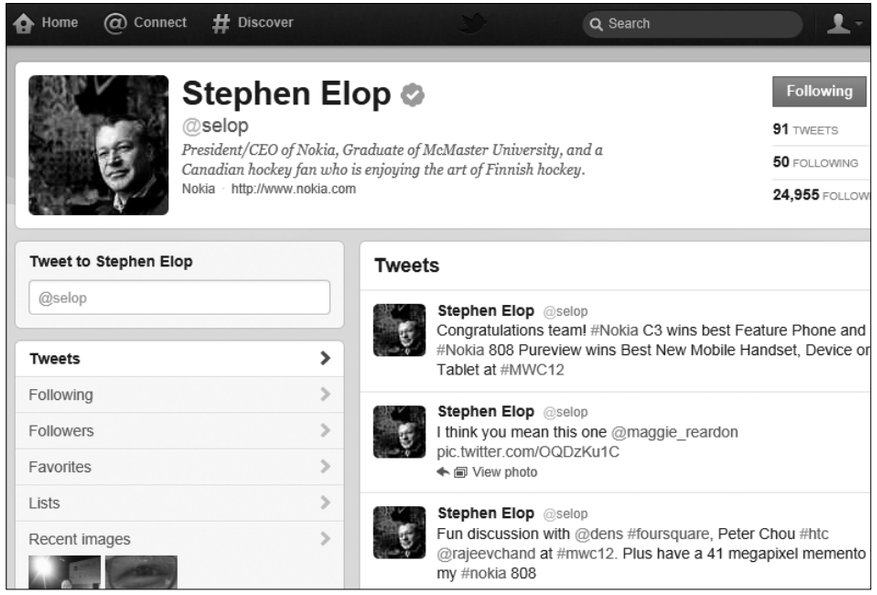
Identiteettivarkaudet

Identiteettivarkaus-termiä käytetään kahdessa eri merkityksessä. Molemmat ovat kiusallisia, mutta vain toinen on kriminalisoitu.

Toisen nimellä netissä

Nettipalvelut eivät yleensä pysty tarkistamaan käyttäjän henkilöllisyyttä, joten toisen nimellä esiintyminen on helppoa. Keskustelufoorumeilla käytetään yleisesti nimimerkkejä tai vääriä nimiä. Netistä voisi päätellä, että Suomessa on lukuisia Aku Ankkoja ja Matti Meikäläisiä.

Mikään laki ei kiellä väärän nimen käyttöä netissä. Myös osoitteen, puhelinnumeron ja muut tiedot saa valehdella (paitsi viranomaisille). Ratkaisevaa on se, mitä keksityillä henkilötiedoilla tehdään.



Nokian toimitusjohtajan aito Twitter-tili.

Vale-Elopin tunnistaa kuvaustekstistä, jossa mainitaan sivun olevan parodiaa. Vale-Elop on aktiivisempi tviittaaja – ja hänellä on hauskemmat jutut.

Laki ei tunne identiteettivarkautta, joten blogin, Facebook-profiilin tai Twitter-tilin perustaminen jonkun tunnetun henkilön nimellä ei itsessään ole laitonta. Ei edes silloin, kun sivuilla käytetään kohteen oikeita henkilötietoja valokuvan kanssa. Ellei palvelun ylläpito pyydettäessä poista valesivuja, poliisilla ei ole juurikaan keinoja sivujen sulkemiseen. Usein sivut ovat ulkomailla palveluissa, joihin Suomen viranomaisilla ei ole edes toimivaltaa.

Vaikka tekijän tarkoitus olisi vain pilailla, valesivuista voi aiheutua suurta mielipahaa uhrille. Lisäksi ne johtavat harhaan muita nettikäyttäjiä.

Laittomaksi toiminta muuttuu, mikäli sivuilla loukataan toisen kunniaa, levitetään yksityisyydensuojan piiriin kuuluvia tietoja, kiihotetaan kansanryhmää vastaan tai syyllistytään johonkin muuhun laissa kiellettyyn tekoon.

Identiteettivarkautta on ehdotettu kriminalisoitavaksi niin, että selvä itsemääräämisoikeuden loukkaus tehtäisiin rangaistavaksi silloinkin, kun siitä ei koidu uhrille todistettavaa vahinkoa. Kriminalisointi tuottaisi omat ongelmansa, sillä palvelujen tarjoajilla ei ole mahdollisuuksia tarkistaa jokaisen käyttäjän oikeaa henkilöllisyyttä ja varsinkin nettikeskusteluissa kyse voi olla puhtaasta nimikaimasta.