Gizarte-sareetan ere badira erasoak eta iruzurrak

Zibergaizkileak ere erakarri ditu gizarte-sareen arrakastak, eta oinarrizko neurri batzuk hartzea komeni zaie erabiltzaileei

Esku-luzeak jenderik gehien biltzen den tokietan ibiltzen dira, zer harrapatuko. Berdin gertatzen da Interneten ere. Gizarte-sareen arrakastak era guztietako zibergaizkileak eta mafia antolatuak jarri ditu erne. Erabiltzaileei iruzur egitea da horien helburua; gezurrezko mezuak edo inkestak bidaltzen dizkiete, edo gezurrezko dohaintzak egiteko aukera ematen diete, eta horrela eskuratu nahi izaten dituzte erabiltzailearen datu pertsonalak, nortasun digitalak eta, batik bat, dirua. Hori ikusita, zerbitzu horien segurtasuna areagotzeko eskariak ere ugaritu dira.

Facebook da gizarte-sarerik hedatuena gaur egun, eta eskakizun asko jasotzen ari da segurtasuna dela eta; ondorioz, Segurtasun Zentro berria jarri du abian ***(http://es-es.facebook.com/help/?safety=general)***, eta material asko eta asko eskaintzen dio erabiltzaileari, gurasoek, hezitzaileek, nerabeek eta segurtasun indarrek jakin dezaten nola jokatu.

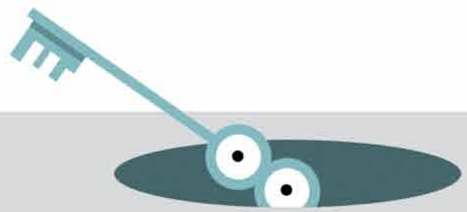
Kasu eman 'hodeiari'! . Erabiltzaileak bere ordenagailuan gorde dezake informazioa, baina, zenbait zerbitzuri esker, aukera du web-ean gordetzeko, ordenagailuan egin beharrean (*hodeian* gordetzen dela esaten da). Horren adibide dira, besteak beste, posta elektronikoko kontuak (Yahoo!, Gmail, Hotmail), argazki-albumak (Flickr eta Picasa, bereziki) eta bideo-zerbitzuak, Youtube eta Vímeo-ren gisakoak. Besterik pentsa baliteke ere, zerbitzu horietan guztietan ere gertatzen dira erasoak. Ordenagailuak duen eremu babestutik ateratzen bagara, eta zerbitzu horiek segurtasun egokia eduki ezean, eraso egin eta datuak lapurtzeko edo galtzeko arriskua izaten da.

Zerbitzurik garrantzitsuenak seguruak dira, norbere ordenagailua baino gehiago, baina hain ezagunak ez diren beste batzuei erasotzea errazagoa gerta liteke, kodeetan eta segurtasun mailan ahulagoak direlako. Komeni da jakitea kontuko zer informazio egiten den publiko, zer aukera dauden pribatutasuna konfiguratzeko eta zenbateko segurtasuna eskaintzen duten plataformek. Datu horiek ikusteko moduan egon behar dute, eta zerbitzua erabiltzen duten guztien eskura.

Idazmahaiko aplikazioetatik egiten dituzten erasoak. Gizarte-sareetara sartzeko, Interneteko nabigatzailea erabili ohi dugu; nabigatzaile horiek idazmahaiko aplikazioak dira, eta segurtasun hutsuneren bat edukiz gero, ordenagailua ***kutsatu*** egiten da. Bide hori erabili zuten, adibidez, hainbat txinatar disidenteren posta-kontuetara sartzeko, eta berdin Google-k Txinan daukan ordezkaritzaren barne-informazioa lortzeko ere. Beste arriskuetako bat *troiar* izenarekin ezagutzen diren programek eragin dute 2009. urtean; kontuetako pasahitzak lapurtzen dituzte edo sare lokaletan barrena eta kanpoko biltegiratze-tresnen bidez zabaltzen dira. Iruzur modu horietan, gai jakin bati lotutako mezuak erabiltzen dituzte mozorro gisa (Eguberrietako zorion agur bat bidaltzen dute, artxibo kaltegarri bat erantsita duela), edo gaurkotasuna duten albisteak (Michael Jackson-en heriotzari buruzko argazkiak udan, edo Berlusconik jasan zuen erasoaren inguruko bideoa); jendea erakarriko duten amuez baliatzen dira, beraz, ahalik eta ordenagailu gehien kutsatzeko.

Hirugarren baten orritik ere bai. Badira erabiltzaileen profila eskuratzeko beste iruzur-bide batzuk ere. Hirugarren baten web-orriak edo aplikazioak erabiltzen ditugu zenbaitetan datuak sinkronizatzeko, eta hortik etor liteke kaltea, edo, bestela, gizarte-sare baten APIa erabiltzen dugunean (zerbitzu baten kode zati bat da, aske edo libre uzten dena, erabiltzaileek beste zerbitzu osagarri batzuk sor ditzaten horietatik abiatuta). Facebook eta Twitter gizarte-sareetan, adibidez, plataforma horietatik kanpoko orrietan ematen ahal zaio onespena erabiltzaileen kontuari, izenik eta pasahitzik sartu gabe, eta horrek badu bere arriskua, jakina. Ahal dela, beraz, ez da komeni erabiltzea kanpoko guneen pasahitzak eskatzen dituzten orriak eta zerbitzuak. Ohikoena izaten da mezu ez-eskatuak bidaltzea erabiltzailearekin harremanetan dauden gainerako kideei, nahiz eta horrela ere gerta daitekeen erabiltzaileak nortasun digitala galtzea eta baimenik ez duen norbait sartzea haren datu pertsonaletara

Nortasuna faltsutu. Twitter-en gertatu izan da zenbait gaizkile edo *cracker*-ek erabiltzaile baten kontua bereganatu eta mezu faltsuak bidaltzea, iraingarriak ere bai tartean, eta kontu-jabea ezer egin ezinik geratzea, harik eta zerbitzuak berak esku hartu zuen arte. Zenbait gizarte-sarek, bestalde (tartean, Facecook-ek), aukera ematen dute plataforman bertan aplikazioak sortu eta trukatzeko. Izan daitezke sareko jolas xumeak, profilei buruzko bozketa eta inkestak… Zenbaitetan, aplikazio horien bidez, kode kaltegarria duten programa exekutagarriak zabaldu izan dituzte. Hau da, aplikazioak ekintza jakin bat egiten duen bitartean, erabiltzailearen ezkutuan, beste ekintza bat egiten ari da (adibidez, kanpoko zerbitzari batera datu pertsonalak bidaltzen). Gizarte-sareak kudeatzen dituzten enpresek kontuan hartzen dituzte segurtasun arazo horiek, eta saiatzen dira sistemak hobetzen.



ZENBAIT AHOLKU, gizarte-sareetan arazoak saihesteko

- **Erabilera-baldintzak eta pribatutasun-klausulak irakurri behar dira beti.**
- **Segurtasun-zehaztapenak eta datuak zifratzeko protokoloak non dauden bilatu. Bistan ez badaude, hobe da ez fidatzea zerbitzu horrekin.**
- **Mundu guztiaren bistan geratuko den informazioa ongi neurtu: ez ibili nabarmenkerian eta ez trukatu datuak eta solaskideak ezezagunekin.**
- **Solaskide berriak tentuz hautatu: pertsonaren bat ez badugu inondik ezagutzen edo haren berri ez badigu hurbilekoren batek eman, ez da komeni solaskideen artean hautatzea.**
- **Eskaintza ekonomikoak edo sexu-eskaintzak egiten badizkigute, berehala moztu komunikazioa. Horren atzean iruzurren bat egongo da, ziur.**
- **Aski konfiantza ematen ez duten mezuak ez dira ireki behar: gizarte-sareetako enpresek bidaltzen dituzte mezuak, solaskideak onartzeko, aplikazio berriak erabiltzeko edo informazioa emateko, baina sekula ez dute eskatzen datu pertsonalak posta elektronikoz haiei bidaltzeko.**
- **Daturen bat aldatu nahi izanez gero, sekula ez da egin behar zerbitzuak eskaintzen duen posta elektronikoa erabiliz; bilatzailera joan, zerbitzuaren hasierako orria bilatu, eta handixe egin. Gaizkileek mezuetan eskaintzen dituzten helbideak haien estalgarri izaten dira.**
- **Ez da komeni beste zerbitzu batzuetatik egiaztatzea pasahitza: hau da, ez da sartu behar Twitter-en edo Facebook-en, Gmail-eko edo Yahoo! Mail-eko pasahitzetatik.**
- **Erabiltzaile-izen bat eta pasahitz bat baino gehiago erabili. Ez da erosoa izaten pasahitz guztiak gogoan hartzea, edo orri batean biltzea, baina beti bera erabiltzen badugu, erraza-goa izango zaie gure zerbitzu guztietara sartzea.**