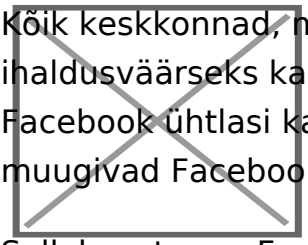
Kuidas kaitsta oma Facebooki kontot?

13 years ago- 25.03.2013 By AM



Kõik keskkonnad, mida hakkavad kasutama piisavalt laiad massid, muutuvad ihaldusväärseks ka küberpättidele. Nii on ka maailma suurim sotsiaalvõrgustik Facebook ühtlasi ka populaarseim küberrünnakute objekt. Statistika järgi muugivad Facebookis kurjategijad iga sekund lahti seitse kasutajakontot.

Selleks, et oma Facebooki lehte mitte kaotada, annab turvatarkvara tootja Kaspersky Lab oma ekspertide abiga mõned nõuanded.

Kaks elementaarset tõhusa kaitse reeglit

Esimene reegel on järgmine: kasutage muukimiskindlat salasõna. Parooliks tavalist sõnastikus leiduvat sõna valides või sünnikuupäeva või „qwerty” laadset lühendit kasutades kaugele ei jõua. Nii lihtsad kombinatsioonid arvatakse ära. Selleks on palju võimsaid vahendeid.

Teine oluline reegel: selleks, et aktiveerida lisakaitsevahendid, tuleb ühendada oma Facebooki konto mobiiltelefoniga. Õngitsemise ohvriks langeb päevas iga kahesajas Facebooki kasutaja, kuid kahtlase sisselogimise korral võib Facebook teavitada sellest konto omanikku kohe SMS-i või e-kirja teel.

Seejuures saab kehtestada igale kasutatavale Facebooki rakendusele eraldi salasõna. Kuid sellel salasõnal ei tohiks olla mitte midagi ühist põhiparooliga.

Isiklike andmete kaitse Facebookis: neli reeglit

Facebooki uue otsingusüsteemi (Graph Search) väljalaskmise järel saab luua erinevaid otsinguid, mis isiklike andmete järgi otsides võivad ohustada turvalisust ja isiklikud andmed võivad olla liiga ligipääsetavad.

Et mitte jagada selleks sobimatut infot kogu maailmaga, tuleks jälgida lihtsaid Kaspersky Labi nelja nõuannet.

1. Kaitske oma avalikult kättesaadavat infot. Muutke seadistusi privaatsemaks (ainult sõpradele, ainult lähedastele sõpradele, ainult

pereliikmetele, ainult iseendale nähtav) selle info puhul, mida ei soovi kõigi Facebooki kasutajatega ja maailmaga jagada.

2. Looge sõprade nimekirjad ja piirake nende ligipääsu Teie isiklikule infole nii, nagu vajalikuks peate. See võimaldab oma kontakte rühmitada ja lubab luua andmetele ligipääsuks igale rühmale oma taseme.

3. Toimetage oma pilte ja postitusi. Kuna sotsiaalvõrgustiku otsimootor kasutab pilte, postitusi ja „Like”-nupule vajutamisi, siis märkige nende väljundite seadistamisel, kes Teie kontaktidest pääseb sellele infole ligi ning kes mitte. Samuti saate määrata, kellega jagate oma tulevasi postitusi.

4. Turvalisuse kontroll. Pidage meeles, et turvaseadeid tuleb regulaarselt uuendada ja kontrollida, läbides aeg-ajalt kõik ülalmainitud sammud.

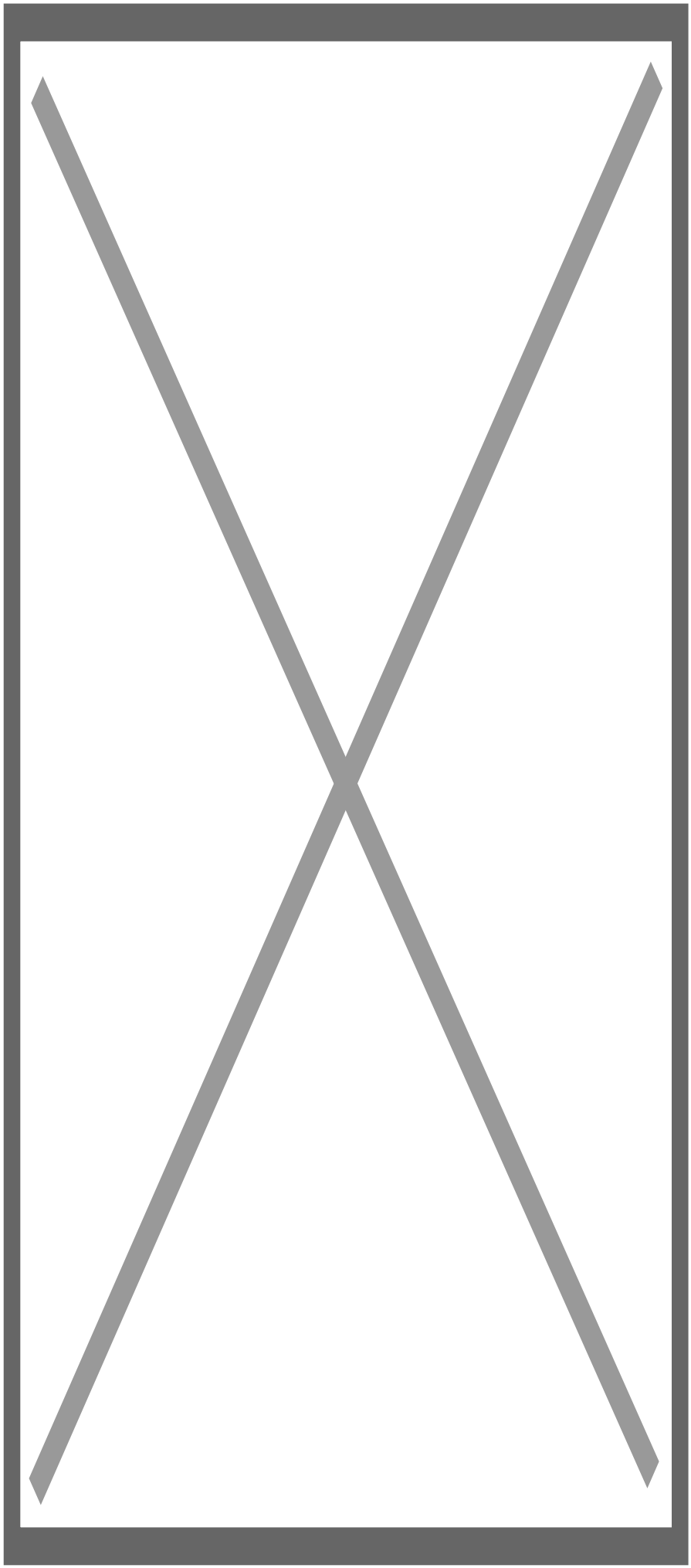
Alati vajalikud Facebooki turvalisuse reeglit

Lisaks ülalolevatele Kaspersky nõuannetele tasub meelde tuletada ka alati olulised Facebooki kasutamise reeglid, mis turvalisust parandavad ja privaatsust hoiavad:

1. Vaadake üle Facebooki vaikimisi seaded. "Privacy" alt saab valida, kuidas teised teiega ühendust saavad ja millist infot näevad.

2. Vaadake, kellele postitada. Iga seinale tehtava postituse all on kohe postitusnupust vasakul valikunupp: sõpradele, lähedastele sõpradele, ainult iseendale või kogu maailmale nähtav. Kui tahate otsimootoreid vältida, ärge valige postitust kogu maailmale (*public*).

3. Vaadake üle oma Facebooki appide õigused. Mõni tüütu rakendus võib teie eest seinale postitada või sõprade seinu risustada (*Post on your behalf*).



SKEEM: KASPERSKY LAB

ILLUSTRATSIOON (ÜLEMINE): Salvatore Vuono / FreeDigitalPhotos.net

- Lahendused
- Turvalisus