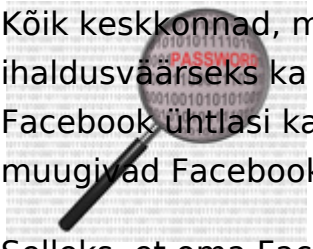
Kuidas kaitsta oma Facebooki kontot?

13 aastat tagasi - 25.03.2013 Autor: 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*).

Facebook is the largest social networking website on the planet and also one of the most targeted websites for cyber criminals. Kaspersky Lab put together a quick tutorial on how to secure your Facebook profile.

HOW TO SECURE YOUR FACEBOOK ACCOUNT

Brought to you by: KASPERSKY lab

THE BIG THREE

1 Set a Strong Password

That means:

- Nothing you can find in a dictionary
- No names
- No birthdates
- No regular keyboard patterns — or the word "PASSWORD"

ACCOUNT SETTINGS > SECURITY > PASSWORD

2 Link to a Mobile Device

Linking your Facebook account to your phone enables multiple security features.

ACCOUNT SETTINGS > MOBILE > ADD A PHONE

3 Enable Secure Browsing

This will encrypt your Facebook browsing and prevent snooping if you're logged in on an unsecure Wi-Fi connection.

ACCOUNT SETTINGS > SECURITY > SECURE BROWSING

LOGIN

Login Notifications

Facebook contacts you when your account is being accessed from a device previously not used.

ACCOUNT SETTINGS > SECURITY > LOGIN APPROVALS

Login Approvals

Select Login Approvals to require a code when you (or somebody else) tries to access your account on a new device.

ACCOUNT SETTINGS > SECURITY > LOGIN APPROVALS

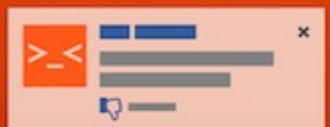
600,000

Logins are compromised per day.

That's over 7 logins a second.

4% of all links shared on Facebook are spam.

1 in 200 users are exposed to phishing, malware, and spam daily.



APP-SPECIFIC PASSWORDS

This feature exists because some Facebook apps can't receive security codes on certain platforms.

So, if you have Login Approvals enabled and you try to Login on your XBOX or other device that can't receive codes, you'll be locked out. To prevent this from occurring, you can designate a specific password for any of the Facebook applications you use.

ACCOUNT SETTINGS > SECURITY > APP PASSWORDS

TRUST

Trusted Devices

This is an extension of Login Approvals. You will be notified if anyone logs in on a device that isn't listed in the trusted devices tab.

ACCOUNT SETTINGS > SECURITY > RECOGNIZED DEVICES

Active Sessions

Check your Active Sessions to see that you aren't logged in anywhere strange.

ACCOUNT SETTINGS > SECURITY > ACTIVE SESSIONS

OUR SOURCES

http://agbeat.com/real-estate-technology-new-media/facebook-touts-their-security-stats-we-do-the-shocking-math/
http://www.scribd.com/doc/70451272/Facebook-Security-Infographic

KASPERSKY lab

SKEEM: KASPERSKY LAB

ILLUSTRATSIOON (ÜLEMINE): Salvatore Vuono / FreeDigitalPhotos.net

- Lahendused
- Turvalisus