Internet se sve više uvlači u naše živote i služimo se njime na poslu, ali i za **bankarsko plaćanje** , kao i **virt ualno druženje** . Ako spadate među onih 10% koji su proživjeli muke **ukradenog identiteta** preko interneta, onda je se za vas ovaj članak pojavio prekasno. Nerijetko je za pristup pojedinim stranicama ili obavljanje izvjesnih transakcija potrebno dati ime i prezime, mail adresu, ponekad i lozinku.

Vrste krađe identiteta

- kloniranje identiteta
- krađa financijskog identiteta
- krađa internetskog identiteta

Kloniranje identiteta provodi se kopiranje osobnih isprava obično otuđenih (osobne iskaznice, vozačke dozvole, putovnice, najčešće s izmjenjenom fotografijom).

Krađa financijskog ideniteta je preuzimanje informacija iz baze podataka banaka, e-trgovina, obračunskih ustanova i drugih koje pohranjuju takve informacije. Kad je to u pitanju, treba nadzirati svoje bankovne izvode i izvode kreditnih kartica ne bi li uočili čudne transakcije i paziti s kim ćemo poslovati. Danas sve rjeđi način krađe finacijskog identiteta je krađa kreditne kartice ili čekova. U tim slučajevima bitno je ne zapisivati PIN-ove kartice na njima, ili u mobitelima, te imati uza sebe telefonski broj banke za prijavu krađe.

Phishing napadi su najštetniji napadi prevaranata. Mnogi počinju porukom e-pošte vaše banke. U njima obično piše da postoji problem s vašim bankovnim računom koji treba riješiti, te vas zamole poslati podatke (korisničko ime, broj računa i lozinku) kako bi riješili problem s našim računom.

Krađa identiteta putem interneta često se dešava putem društvenog inženjeringa koji se odvija u socijalnim on-line mrežama (MySpace, Facebook, Bebo i dr.) gdje je običaj objavljivati svoje osobne podatke poput adrese, datuma i godine rođenja i drugih koje su internetskim lopovima izuzetno korisni. Iako je većina web stranica legalna i moralna, postoje one koje su u "sivoj zoni" (npr. XXX-stranice za odrasle). Perfidniji način krađe je putem crva, virusa i sl. (Trojan horses, hacking).

Osobito lukav način je ponuda zaposlenja, često u inozemstvu, pri čemu je potrebno poslati curriculum vitae s imenom i prezimenom, adresom, brojem telefona i bankovnog računa.

Spoofing znači kreiranje lažne ili krivotvorene verzije nečega, poput Web lokacije ili adrese e-pošte. Korisnik se prijavljuje sa svojim korisničkim imenom i lozinkom koje tako dolaze u ruke kriminalaca, a oni ih zlorabe za pristup stvarnoj Web lokaciji.

Metode zaštite

Prilikom kupovine kompjutera ili zakupna interneta, raspitajte se kod tehničke službe o mogućnosti ugradnje provjerenih anti-virus softwera kako bi bez bojazni "surfali" netom.

Navodimo savjete za redovito održavanje softwera kompjutera:

- Instalirajte kvalitetan i provjeren anti-virus i anti-spam software!
- Instalirajte firewall za zaštitu vaših informacija!
- Redovito obnavljajte "update" svoje anti-virus, firewall i operativne sisteme!
- Provjerite izvor i sadržaj prije preuzimanja "download"!
- Budite oprezni s pop-up-ovima!
- Čuvajte se nepoznatih adresa dokumenata!
- Nemojte objavljivati svoje podatke na web stranicama!

- Redovito restartajte kompjuter!
- Isključite kompjuter kad ga ne koristite!
- U slučaju sumnje, savjetujte se sa stručnjakom!
- Osobne podatke spremite na CD i koristite u slučaju potrebe!

Ne budite naivni prilikom davanja svojim osobnih podataka i provjerite tko je vlasnik web stranice odn. domene. Za kraj, nije neophodno prekinuti sve virtualne kontakte niti izbjegavati on-line kupovine iz udobnosti naslonjača, samo biti na oprezu pri korištenju interneta.

Identity Theft Resource Center