

## KA VERTA ŽINOTI APIE TAPATYBĖS VAGYSTĘ

Tapatybės vagystė (“identity theft”) – gana naujas ir savotiškai “madingu” tapęs reiškinys, iš esmės laikytinas informacinės visuomenės “šalutiniu produktu”. Tačiau technologijų plėtotė prekybos, verslo bei paslaugų srityje tėra tik vienas iš veiksnių, skatinančių tapatybės vagystes, o pavogti kredito kortelių numeriai, atsiskaitant už prekes internetu toli gražu nėra vienintelis tokių vagysčių pavyzdys. Tapatybės vagystės vis dažniau lydi ir tokius, atrodo, įprastus veiksmus, kaip atsiskaitymas čekiu parduotuvėje, dokumentų siuntimas paštu, mobilaus telefono sąskaitos atidarymas ir pan.

Iš esmės, nuo tapatybės vagysčių kasmet nukenčia daugybė žmonių. Vien 2005 metais buvo gauta 255,000 skundų (Federal Trade Commission, 2005), kurie sudarė apie 37% visų vartotojų apgavysčių (“consumer fraud”) skaičiaus. Tapatybės vagystės apima visus atvejus, kuomet be leidimo yra pasisavinami kieno nors asmeniniai duomenys ir panaudojami nusikaltimams ar apgavystėms vykdyti. Asmenys, tapę tokių veiksmų aukomis, praranda begales laiko, o dažnai ir pinigų, besistengdami atitaisyti jiems padarytą žalą. Yra nemažai atvejų, kuomet tapatybės vagysčių aukos, dėl sugadintos kredito istorijos, vėliau turi sunkumų prašant paskolų, nuomojantis būstą, ar įsidarbinant.

Tad kaip gi informacija pasisavinama ir ką daryti, jei tapote panašios vagystės auka?

Pirmiausia, nusikaltėliai dažnai gauna asmeninę informaciją iš institucijų, kurioms Jūs ją patys suteikiate (bankų, kredito kompanijų, ligoninių ir pan.). Ši informacija arba pavagiama, arba kaip nors išviliojama iš tų institucijų darbuotojų. Būtent dėl to jau kuris laikas kalbama apie tai, kiek ir kokios informacijos įvairios institucijos turi teisę reikalauti ir kaip ji privalo būti saugoma. Tarkime, yra įprasta, jog, nuomojantis butą ar atidarant banko sąskaitą yra reikalaujama SSN (Social Security Number), tačiau daugybė verslo bei paslaugų kompanijų neretai reikalauja pateikti SSN vien dėl to, kad galėtų identifikuoti Jus kaip savo klientą. Tokiu atveju, visuomet geriau išsiklausinėti, ar būtina iš tiesų naudoti SSN (gal, pvz., užtektų vairuotojo teisių numerio ar pan.), kaip jis bus panaudojamas, bei, svarbiausia, kaip jis bus saugomas nuo tapatybės vagių. Kompanija, reikalaujanti būtinai naudoti SSN, gali atsisakyti teikti Jums prekes ar paslaugas, jei neleisite jai šio numerio naudoti, tačiau, smulkiau paklausinėję, Jūs bent jau galėsite patys nuspręsti, ar verta rizikuoti, ar ne.

Kitas paplitęs būdas, kurio pagalba pavagiama asmeninė informacija yra pašto vogimas iš asmeninių dėžučių. Tokiu būdu pasisavinamos banko bei kredito kompanijų ataskaitos, banko kortelės bei čekiai, informacija apie mokesčius ir pan.

Trečia – taip, nusikaltėliai nesibodi apieškoti Jūsų išmetamų šiukšlių! Tapatybės vagių rausimuisi po gyventojų bei verslo kompanijų šiukšliadėžes netgi yra sugalvotas specialus terminas – “dumpster diving”. Nusikaltėliai taip pat dažnai apsimeta darbdaviais, butų savininkais, ar kitais asmenimis, turinčiais teisę reikalauti Jūsų duomenų, įskaitant ir SSN. Specialių technologijų pagalba, jie gali surasti ir pasisavinti informaciją, patenkančią į ATM mašinas, parduotuvių ar kredito kompanijų kompiuterines sistemas ir pan. Pagaliau, jie gali tiesiog įsilaužti į Jūsų namus ar pavogti Jūsų piniginę, ieškodami asmeninių duomenų.

Informacijos medžiojimas internete galėtų būti atskira tema. Vis daugiau ir daugiau sukčių siuntinėja laiškus elektroniniu paštu, apsimėsdami banko, kredito kompanijų, interneto parduotuvių atstovais. Kartais jie siūlo abejotinos vertės, tačiau

patrauklias prekes ir paslaugas, - o po to, vos Jums įvedus savo kreditinės kortelės duomenis, pradingsta kaip į vandenį (uždaro savo tinklapį, neatsako nurodytais telefonais ir pan.). Dažniausiai, visgi, nusikaltėliai prašo patikslinti sąskaitos duomenis (adresą, sąskaitos numerį ir pan.), pranešdami, pvz, kad Jūsų sąskaita banke sustabdyta ar kad iškilo kokių nors problemų. Reaguoti prašoma kuo greičiau (kad nespėtų susisiekti su banku ar kredito kompanija), atsiųsti laiškai praktiškai niekuo nesiskiria nuo tikrų e-paštu gaunamų pranešimų, todėl nenuostabu, jog nukentėjusiųjų nuo panašių apgavysčių, vadinamų “online phishing”, daugėja. Panašias strategijas nusikaltėliai kartais naudoja ir atakuodami telefoniniais skambučiais.

Kaip dažniausiai panaudojama pavogta informacija? Priklausomai nuo to, kokie būtent duomenys pavagiami, Jūsų vardu gali būti atidaromos naujos kreditinės kortelės, kurių neapmokėtos sąskaitos vėliau atsiras Jūsų kredito istorijoje, taip pat – mobilaus telefono sąskaitos, automobilio mokėjimo planas, ir pan. Pakeitę mokėjimo adresą (“billing address), vagys gali pasinaudoti ir Jūsų jau esamomis kredito kortelėmis, banko sąskaitomis, atlikdami mokėjimus bei pridarydami skolų, apie kurias Jūs ilgai nieko net nesužinosite. Čekių padirbinėjimas, siekiant ištuštinti aukos sąskaitą, išsiskolinimai už paslaugas, galų gale, bankroto paskelbimas aukos vardu yra įprastos tapatybės vagių piktnaudžiavimo priemonės. Be to, vagys gali pasinaudoti ir pavogtais dokumentais ar jų numeriais (SSN, vairuotojo teisių numeriu) ta, kad padirbti ar gauti sau naujus, tik svetimą numerį turinčius, dokumentus.

Taigi, jei vienokiu ar kitokiu būdu praradote asmens dokumentus, kredito kortelės, ar įtariate bet kokią asmeninės informacijos nutekėjimą, svarbu iškart imtis priemonių užkirsti kelią galimai tapatybės vagystei. Iškart pakeiskite banko sąskaitų bei kredito kortelių numerius ar jas išvis uždarykite ir atidarykite naujas. Paskambinkite į tris nacionalinius kredito biurus ir paprašykite stebėti Jūsų duomenis (naudoti vadinamąjį “initial fraud alert”, kuris reiškia, jog 90 dienų ar ilgiau Jūsų vardu niekas kitas negalės atidaryti jokių naujų sąskaitų. Susisiekite su pavogtus dokumentus išdavusiomis institucijomis ir sužinokite, kaip panaikinti pavogtą dokumentą ir jį pakeisti nauju, bei paprašykite jų taip pat stebėti Jūsų duomenis, kad niekas kitas negalėtų gauti dokumentų Jūsų vardu.

***Organizacijų, kurioms reikėtų pranešti apie įvykusią tapatybės vagystę, duomenys:***

- **Kredito biurai** (paskambinus į vieną jų, kitiems informacija perduodama automatiškai):  
Equifax: 1-800-525-6285  
[www.equifax.com](http://www.equifax.com)  
  
Experian: 1-888-397-3742  
[www.experian.com](http://www.experian.com)  
  
TransUnion: 1-800-680-7289  
[www.transunion.com](http://www.transunion.com)
- **Kompanijos, kur turite sąskaitas**, turėtų būti informuojamos apie apgavystę ne tik telefonu, tačiau taip pat ir raštu. Siųskite pareiškimus

registruotu paštu, kad galėtumėte dokumentuoti savo kreipimąsi, ir pasilikite sau siunčiamų laiškų kopijas.

- **Praneškite policijai.** Jums būtina turėti policijos protokolą dėl įvykusios vagystės, ar bent žinoti surašyto protokolo numerį, nes dauguma kreditorių jo pareikalaus, kai prašysite atlyginti padarytą žalą.
- **Federal Trade Commission (FTC)** renka informaciją apie tapatybės vagystes, siekdama kovoti su nusikaltėliais bei informuoti visuomenę apie atsirandančias vis naujas vagysčių formas. Ši organizacija taip pat gali nukreipti Jūsų skundą į kitas valdžios institucijas ar ištirti institucijų, nesilaikančių FTC nustatytų principų, veiklą. Šiai organizacijai skundą galite pateikti internetu [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) ar paskambinę tel. 1-877-438-4338.

**Pagal Federal Trade Commission medžiagą parengė V. Maleckaitė**