Internetiniai vagišiai darosi vis sumanesni: kaip apsaugoti savo turtą ir atpažinti pavojų?

*Informacija žiniasklaidai, 2020.09.30*

**Pavogta tapatybė, nuo sąskaitos nuskaičiuoti pinigai ar išviliotos viso gyvenimo santaupos, visa tai – internetinių sukčių darbas. Nors dar visai neseniai jie apgaudavo tik mažiausiai technologijas išmanančius, šiandien sukčiai darosi kaip niekad apsukrūs ir pinigus sugeba išvilioti net ir iš tų, kurie niekada nebūtų to tikėjęsi. Kaip apsisaugoti nuo tokių vagysčių ir ar iš tikrųjų, jums nežinant, sukčiai gali pasiimti jūsų vardu kreditą?**

Skaitmeninių finansinių paslaugų įmonės „Credit24“ klientų patirties valdymo vadovė Donata Stoškuvienė teigia, jog internetinėje erdvėje pasiimti paskolą kito vardu – ganėtinai sudėtinga.

„Vyrauja kalbos ir visi esame skaitę istorijų, kaip žmonės iš skolų išieškojimo įmonių staiga sužino apie jų vardu paimtus kreditus ir milžiniškas skolas, į kurias yra įklimpę. Tačiau šiais laikais – tai praktiškai neįmanoma. Ypač internetinėje erdvėje yra labai daug saugiklių, kurie užtikrina, jog niekas be jūsų žinios negalėtų pasiimti kredito jūsų vardu“.

Visgi, D. Stoškuvienė teigia, jog paskolos ėmimo procesas gali būti pradėtas ir jums apie tai nežinant. Tad norint apsaugoti savo pinigus, būtina žinoti, iš kokių ženklų galite spręsti, jog į jus kėsinasi internetiniai sukčiai.

**Internetinė tapatybės vagystė – kas tai?**

Tapatybė fizinėje erdvėje yra visiškai kitokia nei internetinėje erdvėje. Fizinėje erdvėje mes savo tapatybę patvirtiname asmens dokumentu: pasu ar ID kortele, kurią turi kiekvienas pilietis. O štai elektroninėje erdvėje mūsų tapatybę dažniausiai patvirtina vardas ir mūsų susikurtas ar mums duotas slaptažodis.

Tapatybės vagystė dažiausiai susijusi su suklastotais ar apgaulės būdu išviliotais asmens duomenimis. Dažniausiai tai įvyksta siekiant pasinaudoti apgauto žmogaus pinigais, o kartais net jo vardu pasiimti paskolą.

**Dažniausiai pasitaikantys elektroniniai vagystės būdai:**

1. Prisistatymas pareigūnais, siekiant įsilaužti į banko sąskaitą,
2. Duomenų vagystė,
3. Nepageidaujami laiškai.

**Įsilaužimas į banko sąskaitą**

Dažnai įsilaužimas į kito žmogaus asmeninus duomenis prasideda telefoniniu skambučiu aukai. Paprastai žmogui paskambina neva iš valstybinės įstaigos: „Sodros“, VMI ar net policijos. Maloniai prisistatęs sukčius jums paaiškins, jog sistemoje vyksta pakitimai, todėl jūs laikinai negalėsite naudotis savo banko sąskaita, kol neatnaujinsite duomenų.

Jie gali atsiųsti jums laišką pokalbio metu, kur paprašys jūsų prisijungti prie sistemos. Taip iš jūsų išvilioja prisijungimo prie jūsų elektroninės bankininkystės duomenis ir gali ištuštinti jūsų sąskaitą.

Taip pat yra buvę atvejų, kad apgauto žmogaus vardu pasiima greitąjį kreditą, tačiau „Credit24“ klientų patirties valdymo vadovė sako, jog šiandien to padaryti būtų neįmanoma dėl kelių priežasčių:

1. **Prieš suteikiant asmeniui naują kreditą, jis turi būti identifikuotas.** Tai padaryti galima dviem būdais: fizinis identifikavimas vietoje (pateikiant asmens dokumentą) ir identifikavimas nuotoliniu būdu.

„Kalbant apie internetines apgaules ir paskolos pasiėmimą internetu, tai net ir turint kito žmogaus dokumentą, kredito jūs pasiimti negalėsite. Nes viename iš žingsnių mes paprašysime identifikuoti savo tapatybę, nuskanuojat veidą telefonu, su specialia mūsų paruošta programėle, kurią turėsite atsisiųsti. Nuskenuoti nuotraukos – nepavyks. Todėl jau viename iš pirmųjų žingsnių sukčius nebepraeis kontrolės“, – teigia D. Stoškuvienė.

1. **Kontroliniai klausimai.** Naudojantis Lietuvoje prieinamais išoriniais registrais, paprastai yra suformuojami kontroliniai klausimai, į kuriuos gali atsakyti tik tas žmogus. Jie yra užduodami žmogui ir jeigu jam nepavyksta atsakyti į juos – paskola jam nebus suteikta.

„Tačiau pasitaiko ir taip, jog žmogumi būna pasinaudota iš artimos aplinkos: giminaičiai, draugai, kaimynai pasinaudoja žmogaus pažeidžiamumu dėl seno amžiaus ar neišmanymo ir paskatina žmogų pasiimti paskolą. Arba sužinoję visus jo prisijungimus ir slaptažodžius gali „padėti“ jam pasiimti paskolą. Tokių atvejų vis dar pasitaiko, todėl vienintelis patarimas čia – išlikti budriems ir nepateikti jokių asmeninių duomenų net ir artimai aplinkai“, – sako D. Stoškuvienė.

**Duomenų vagystė („phishing“)**

Paprastai tai reikiamo slaptažodžio „žvejyba“. Viskas prasideda nuo laiško jūsų elektroniniame pašte. Dažniausiai tai laiškas nuo jūsų banko. Laiške dažniausiai pranešama, neva reikia atnaujinti jūsų prisijungimus prie internetinės bankininkystės sistemos, nes buvo daryti pakeitimai. Taip pat jūsų gali paprašyti užpildyti klientų anketą, o už tai, kad skirsite savo laiko, dar gausite ir prizą.

Tik užpildę savo duomenis – jūs užkimbate. Visi jūsų asmeniniai duomenys ir prisijungimai prie elektroninės bankininkystės atitenka sukčiams, o jie veikia labai greitai. Gavę jūsų prisijungimus, jie jau būna pasiruošę specialią banko sąskaitą, į kurią pervedę jūsų pinigus, juos išgrynina.

Tačiau yra keli būdai, kaip atpažinti, jog tokie laiškai – apgavystė:

1. Nurodyta banko svetainė atrodo visiškai identiškai tikrajai, tačiau gerai įsižiūrėję, pastebėsite, jog žodyje trūksta raidės arba raidės yra apkeistos vietomis.
2. Jeigu laiške jūsų prašo pateikti jūsų asmeninius duomenis ar užpildyti anketą ir už tai galite laimėti prizą – tai tikras pavojaus signalas. Joks bankas niekada neprašys jūsų pateikti savo asmeninių duomenų mainais į prizus. Tuo labiau joks bankas niekada neprašys pateikti savo privačių prisijungimo duomenų.
3. Galiausiai, jei nesate tikri – visada galite paskambinti į savo banką ir pasiteirauti apie gautą laišką. Tik neskambinkite laiške nurodytu telefono numeriu, o patys susiraskite banko klientų aptarnavimo telefono numerį internete.

**Nepageidaujami laiškai „Trojos arklys“**

Bene dažniausiai pasitaikanti sukčiavimo forma, dar kitaip nepageidaujami laiškai vadinami „spam“. Tokie laiškai į gavėjo elektroninį paštą yra siunčiami labai dideliais kiekiais ir be gavėjo sutikimo. Dažniausiai tai reklaminio pobūdžio laiškai, tačiau pasitaiko ir vadinamųjų „Trojos arklių“.

Paprastai tokiuose laiškuose būna nuoroda, kurią skatinama atidaryti, o vos ją atidarius, virusas patenka į jūsų operacinę sistemą ir sugadina jūsų kompiuterį bei persiunčia tą patį „Trojos arklį“ visiems jūsų turimiems kontaktams.

Nuo šių laiškų apsisaugoti gana paprasta – tereikia neatidarinėti laiškų, gautų iš įtartinų siuntėjų, su kuriais niekada neturėjote nieko bendra, o gavus tokius laiškus žymėti juos kaip „nepageidaujamus“ (angl. Spam). Tokiu būdu, iš to siuntėjo gaunamas laiškas visada nukeliaus į nepageidaujamų laiškų aplanką ir jūs jo nebematysite.