



NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS TAPATYBĖS VAGYSTĖS

2020 m. liepos 31 d.

Tapatybės vagystė suprantama, kaip asmens tapatybę identifikuojančių duomenų (pvz. mokėjimo ar kredito kortelės, Valstybinio socialinio draudimo pažymėjimo, paso ir pan.) panaudojimas nusikalstamai veikai vykdyti. Tapatybės vagystės auka galima tapti tiek fizinėje, tiek elektroninėje erdvėje, todėl bet koku atveju patiriamos vienokios ar kitokios neigiamos pasekmės. Elektroninėje erdvėje tapatybė iš esmės sutapatinama su prisijungimo vardu ir slaptažodžiu, bei visomis saugumo užtikrinimo priemonėmis, pavyzdžiui, skaitmeniniais sertifikatais ir kita. Atsižvelgiant į tai, kad su asmens duomenų tvarkymu susiduriame kiekvieną dieną (naudojamės bankomatu, mokame mokesčius, rašome prašymus, einame pas gydytoją, siunčiamės iš interneto informaciją, bendraujame socialiniuose tinkluose, užsiimame kita įvairia veikla), informacijos vertė yra akivaizdi, todėl privalu pasirūpinti savo duomenimis.

Ar tapatybės vagystės auka galima tapti vien tik talpinant informaciją internete?

Tapatybės vagystės auka galite tapti, net jei niekada nenaudojate kompiuterio. Nusikaltėliai gali gauti asmeninę informaciją (pvz. kreditinių kortelių numerius, telefonų numerius, sąskaitų numerius ir adresus), pavogdami jūsų piniginę, pasiklausydami telefoninių pokalbių, rausdamiesi po šiukšliadėžę ar nugvelbdami kvitą restorane, kuriame yra jūsų sąskaitos numeris. Jei vagis turi pakankamai informacijos, jis gali apsimesti kitu asmeniu norėdamas nusipirkti daiktų internetinėse parduotuvėse, atidaryti naujas sąskaitas ar kreiptis dėl paskolų.



Nusikaltėliams internetas padeda lengviau gauti asmeninius ir finansinius duomenis. Daugelis kompanijų ir kitų institucijų kaupia informaciją apie savo klientus duomenų bazėse. Jei vagis gauna prieigą prie tokios duomenų bazės, jis gali gauti informacijos apie daugelį žmonių vienu metu, o ne sutelkti dėmesį į vieną asmenį.

Kaip pasirenkamos aukos asmens tapatybės vagystėms?

Asmens tapatybės vagystės paprastai yra nusikaltimai dėl galimybės. Tai reiškia, kad dažniausiai jie nėra planuojami, o vykdomi spontaniškai, pastebėjus galimybę, todėl jūs galite nukentėti vien dėl to, kad informacija apie jus yra prieinama. Pavyzdžiui, vagys gali nusitaikyti į tam tikrų žmonių lengvai prieinamas, silpnai apsaugotas duomenų bazes, kuriose saugoma specifinė informacija. Jei jūsų informacija yra saugoma tokioje duomenų bazėje — galite tapti tapatybės vagystės auka. Be abejo, vyksta ir koordinuotos, tikslingos atakos, siekiant pavogti tam tikro asmens tapatybę. Vienas iš tapatybės vagystės pavyzdžių yra neseniai Krašto apsaugos ministrui iš suklastotos NATO pašto dėžutės nusikaltėlių siųstas laiškas, apsimitant NATO generaliniu sekretoriumi Jensu Stoltenbergu. Laiške informuojama, kad dėl siaučiančios pandemijos, su kurios valdymu „Krašto apsaugos ministerija nesusitvarko“, o „Lietuvos ligoninės perpildytos“ bus išvestas NATO karių kontingentas. Taip pasinaudojant žinomo žmogaus vardu nusikaltėliai galimai siekė supriešinti gyventojus ir destabilizuoti padėtį šalyje. Laiško autentiškumui abejonių sukėlė „laužyta“ anglų kalba parašytas tekstas, bei laiško antraštėje matomas serveris, iš kurio siųstas elektroninis laiškas.



SECRETARY GENERAL
LE SECRÉTAIRE GÉNÉRAL
Jens Stoltenberg

SG(2020)0095

21 April 2020

Dear Mr. Raimundas Karoblis,

I would like to inform you about the decision to withdraw NATO troops from Lithuania in May 2020. This decision has been made due to the epidemic is now entering a more serious and complex period. The number of infected with COVID-19 NATO soldiers in Lithuania has been rising constantly.

Military medics assessed the situation in Lithuania. In accordance with the report, the situation with COVID-19 spread within the NATO enhanced Forward Presence Battle Group in Lithuania is catastrophic.

This state of affairs resulted from failure of the Lithuanian Ministry of Defence to take necessary measures to combat the spread of coronavirus. It is reported that hospitals in Lithuania are overwhelmed, short-staffed and ill-equipped as the outbreak continues.

At the moment, it is impossible to predict how widespread coronavirus will be among NATO military in Lithuania. NATO's focus is on how to save lives. So we will continue to work with Lithuania using other forms of cooperation.

I very much appreciate your attempts to restrain the spread of the COVID-19 and Lithuania's fulfilment of obligations within NATO.

Yours Sincerely,

Jens Stoltenberg

His Excellency
Mr Raimundas Karoblis
The Minister of National Defence of the Republic of Lithuania
Vilnius



Kaip žinoti, kad jūsų tapatybė pavogta?

Privačius klientų duomenis saugančios bendrovės pastebėjusios įsilaužimą ir galimą informacijos vagystę dažniausiai apie tai informuoja visuomenę, tačiau neretai po įsilaužimo praeina tam tikras laiko tarpas, kai pati bendrovė apie jį sužino, arba jis gali likti visai nepastebėtas. Todėl turėtumėte atkreipti dėmesį į atsiradusią neįprastą veiklą jūsų paskyroje, pavyzdžiui prisijungimą prie jos iš kitos šalies. NKSC yra išleidęs informacinį biuletinį apie socialinio tinklo Facebook paskyros saugumą. Jį galima perskaityti: https://www.nksc.lt/doc/biuleteniai/NKSC%20Facebook%20Biuletenis_2018-04-09.pdf

Toliau pateikiami požymiai, kurie gali reikšti, kad kažkas pasiekė jūsų informaciją:

- neįprasti ar nepaaiškinami jūsų sąskaitų mokesčiai
- mokesčiai už sąskaitas, produktus ar paslaugas, kurių nepirkote
- reguliarių sąskaitų ar laiškų negavimas
- naujos, keistos sąskaitos, rodomos jūsų kredito ataskaitoje
- netikėtas kredito kortelės atmetimas
- neaiškūs laiškai, pranešimai ir žinutės iš jūsų socialinių tinklų paskyrų

Ką daryti, kai jūsų tapatybė pavogiama?

Jei manote, kad susidūrėte su asmens tapatybės vagyste, turėtume apie tai kuo greičiau pranešti atitinkamoms institucijoms:

Į Policiją reikėtų kreiptis, jei įtariate, kad:

- Iš banko sąskaitos dingo pinigai
- Kažkas veikė jūsų vardu su suklastotais dokumentais
- Buvo įsilaužta į elektroninio pašto dėžutę
- Buvo paimtas greitis kreditas jūsų vardu
- Kažkas sukčiauja naudodamasis jūsų arba kitų asmenų duomenimis
- Kažkas neteisėtai naudojami jūsų mokėjimo kortelės duomenimis
- jūsų vardu buvo įsigytos prekės ar paslaugos, kurių jūs nepirkote

Į Vartotojų teisių apsaugos tarnybą (VVTAT) galite kreiptis jei manote, kad:

- Kažkas sumokėjo už prekes ar paslaugas, pasinaudodamas jūsų mokėjimo kortele, tačiau bankas ar kita finansų įstaiga nesutiko išspręsti problemos jums palankiu būdu



- Jūsų vardu paimtas vartojimo kreditas, tačiau finansų įstaiga nesutiko išspręsti problemos jums palankiu būdu

Į Valstybinę duomenų apsaugos inspekciją (VDAI) galite kreiptis jei įtariate, kad:

- Tiesioginės rinkodaros pranešimai siunčiami arba reklaminiai skambučiai daromi be jūsų išankstinio sutikimo, jus atakuoja kitokio pobūdžio nepageidaujami elektroniniai laiškai
- Jūsų asmens duomenys yra tvarkomi neteisėtai, perteklinai ar netinkamai
- Duomenų valdytojas nenori įgyvendinti jūsų, kaip duomenų subjekto, teisių (nepaaiškina duomenų tvarkymo teisėtumo, nereaguoja į jūsų prašymus)
- Elektroninių ryšių tinkluose yra įvykęs asmens duomenų saugumo pažeidimas

Į teismą kreipiatės, jei:

- Norite tam tikrus neteisėtus veiksmus, kurie užtraukia administracinę atsakomybę, skųsti tiesiogiai teismui
- Ketinate prisiesti turtinę ir neturtinę žalą

Svarbu: tais atvejais, kai skundas nėra susijęs su baudžiamąja atsakomybe, t. y. nėra kreiptasi į policiją, galite kreiptis ne į konkretų vieną priežiūros subjektą, bet į kelis. Kartais konkrečią situaciją pagal kompetenciją galėtų nagrinėti net kelios institucijos.

Į Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos (NKSC), jei manote, kad:

- Įvyko saugumo incidentas elektroninių ryšių tinkluose, ypač kai yra potenciali rizika tinklo funkcionalumui ar duomenų saugumui. NKSC atliks tyrimą ir pateiks rekomendacijas panašių incidentų užkardymui ateityje.

Į Ryšių reguliavimo tarnybą (RRT) galite kreiptis dėl tinklų ir informacijos saugumo, t.y. manote, kad jūsų interneto paslaugų teikėjas arba mobilus ryšio operatorius neįgyvendina tinkamų techninių ir organizacinių priemonių savo teikiamų paslaugų saugumui ir vientisumui užtikrinti.



Kaip išvengti tapatybės vagystės elektroninėje erdvėje?

Deja, neįmanoma garantuoti, kad netapsite tapatybės vagystės auka. Tačiau yra būdų, kaip sumažinti tokią riziką:

- Užsiimkite verslu su patikimomis įmonėmis - prieš pateikdami bet kokią asmeninę ar finansinę informaciją įsitikinkite, kad bendraujate su patikima, įsitvirtinusia įmone. Kai kurie užpuolikai gali bandyti jus apgauti sukurdami apgaulingas interneto svetaines, kurios atrodo teisėtos, todėl prieš pateikdami bet kokią informaciją turėtumėte patikrinti jų legitimumą. Prekes pirkite tik iš patikimų elektroninių parduotuvių. Kaip atpažinti suklastotą elektroninę parduotuvę galima susipažinti: <https://www.nksc.lt/doc/biuleteniai/2018-11-21%20Kaip%20atpažinti%20suklastota%20elektronine%20parduotuve.pdf>
- Naudokitės saugos funkcijomis – saugumo lygis pakyla, jei naudojami slaptažodžiai ir kitos saugos priemonės. Naudokite kelių žingsnių autentifikavimą, jei tai įmanoma. Apie slaptažodžių saugumą skaitykite čia: https://www.nksc.lt/doc/biuleteniai/NKSC_Slaptazodziu_saugumo_biuletenis.pdf
- Patikrinkite privatumo politiką - teikdami informaciją imkitės atsargumo priemonių ir būtinai patikrinkite paskelbtas privatumo politikas, kad pamatytumėte, kaip įmonė naudos jūsų duomenis. Daugelis kompanijų leidžia klientams prašyti, kad jų duomenimis nebūtų dalijamasi su kitomis įmonėmis.
- Būkite atidūs, kokią informaciją skelbiate - užpuolikai gali surinkti informaciją iš įvairių šaltinių. Venkite skelbti asmeninius duomenis viešuose forumuose ir socialiniuose tinkluose.
- Naudokite ir prižiūrėkite antivirusinę programinę įrangą bei ugniasienę. Apsaugokite save nuo virusų ir kitokių kenkėjiškų programų, kurios gali pavogti ar pakeisti jūsų asmeninio kompiuterio duomenis ir padaryti juos pažeidžiamus.
- Sekite savo paskyrų veiklą - atkreipkite dėmesį į savo pareiškimus ir kasmet patikrinkite kredito ataskaitą. Kartą per dvylika mėnesių turite teisę gauti nemokamą kiekvienos iš pagrindinių kredito ataskaitas teikiančių bendrovių kredito ataskaitos kopiją.