

REKOMENDACIJOS IR PATARIMAI KAIP APSISAUGOTI NUO SUKČIŲ IR APSAUGOTI SAVO ASMENS DUOMENIS INTERNETE

(Informaciją parengtą ir atnaujintą kartu su Lietuvos Respublikos Valstybinės duomenų apsaugos inspekcijos, Pinigų plovimo prevencijos kompetencijų centro ir Krašto apsaugos ministerijos ekspertais)

2025 m. spalio 22 d.
Vilnius

Pastaruosius kelerius metus Lietuvos gyventojai itin dažnai sulaukia skambučių, kuriuose sukčiai apsimeta banko, telekomunikacijų operatoriais, „Google“ ar valstybinių institucijų darbuotojais ir įtikinėja jos perduoti slaptažodžius, pinigus ar net banko korteles. Šioms grėsmėms atremti Lietuvos Respublikos Krašto apsaugos ministerija formuoja kibernetinio saugumo politiką Lietuvoje, o jai pavaldus Nacionalinis kibernetinio saugumo centras yra atsakingas už vieningą kibernetinių incidentų valdymą valstybėje bei vykdo švietimo veiklą kibernetinio saugumo klausimais.

Kovojant su sukčiavimu internete praktiniais patarimais taip pat dalijasi Pinigų plovimo prevencijos kompetencijų centras ir Valstybinė duomenų apsaugos inspekcija. Šios institucijos pabrėžia, kad pirmasis žingsnis apsisaugant nuo sukčių – **mokėti juos atpažinti**.

KAIP ATPAŽINTI SUKČIUS?

Sukčiai iš užsienio vis geriau prisitaiko prie lietuviškos rinkos ir bando kalbėti lietuvių kalba, bet to dar negeba daryti kokybiškai. Dėl to pagrindiniu skiriamuoju bruožu galima laikyti „laužytą“ lietuvių kalbą ar perėjimą į rusų kalbą. Taip pat pastebima, kad sukčių reikalavimai būna nelogiški – apsimesdami banko darbuotojais, jie siūlosi atvažiuoti paimti banko kortelę, palaikyti grynusius pinigus ar atlikti grynųjų pinigų ekspertizę, taip pat jie siūlo lengvai uždirbti pinigų ar pelningai jos investuoti. Tikras bankas to niekada nedaro.

Pastaruoju metu Lietuvos gyventojams paskambinę sukčiai dažnai apsimeta telekomunikacijų atstovais. Skambučio metu jie bando įtikinti bendravimą tęsti kitose platformose – „WhatsApp“, „Telegram“ ar „Viber“. „Sukčiai taip pat itin dažnai skubina Lietuvos gyventojus atlikti veiksmus čia ir dabar, neva nėra laiko laukti. Siūlome niekada niekur neskubėti, nebijoti padėti ragelį ir atlikti prevencinius veiksmus“, – pataria Pinigų plovimo prevencijos kompetencijų centro ekspertė Ž. Kielienė.

GRĖSMĖS JŪSŲ DUOMENIMS INTERNETE.

Sukčiavimo skambučiai – tik viena iš daugelio grėsmių, su kuriomis susiduria Lietuvos gyventojai internete. Valstybinės duomenų apsaugos inspekcijos atstovai atkreipia dėmesį, kad šiandien Lietuvos gyventojų asmens duomenims kyla daugybė grėsmių, kurios nuolat kinta ir tampa vis sudėtingesnės.

Viena iš pagrindinių – kibernetinės atakos, kurių metu nusikaltėliai siekia pasisavinti vartotojų informaciją pasitelkdami sukčiavimo laiškus, kenkėjiškas programas ar įsilauždami į įvairių paslaugų teikėjų sistemas. Taip pat didelę riziką kelia socialinės inžinerijos metodai, kai Lietuvos gyventojai apgaulės būdu skatinami atskleisti savo asmens duomenis nusikaltėliams telefonu, el. paštu ar socialiniuose tinkluose. Pavojų kelia ir netinkamai apsaugotos paskyros, kai vartotojai renkasi silpnus slaptažodžius arba naudoja tą patį slaptažodį kelioms skirtingoms paskyroms.

DAŽNIAUSIOS LIETUVOS GYVENTOJŲ KLAIDOS.

Dažniausiai Lietuvos gyventojai patys netyčia prisideda prie savo asmens duomenų pažeidžiamumo. Viena iš pagrindinių klaidų – silpnų ir lengvai atspėjamų slaptažodžių naudojimas, pavyzdžiui, paprastų skaičių ar žodžių kombinacijų.

Dar viena dažna klaida – tas pats slaptažodis naudojamas kelioms paskyroms, todėl įsilaužus į vieną paskyrą gali būti pažeistos ir visos kitos. Taip pat Lietuvos gyventojai neretai neįjungia dviejų faktorių autentifikavimo, kuris gerokai padidintų paskyros apsaugą.

Kita dažnai pasitaikanti problema – neatsargus elgesys su el. laiškais ar nuorodomis, kai paspaudus ant įtartino pranešimo suteikiama prieiga sukčiams.

PAPRASTI, BET VEIKSMINGI PATARIMAI IR REKOMENDACIJOS.

Siekiant apsaugoti savo asmens duomenis internete, visų pirma svarbu elgtis sąmoningai ir atsakingai. Lietuvos Respublikos Valstybinės duomenų apsaugos inspekcijos, Pinigų plovimo prevencijos kompetencijų centro ir Krašto apsaugos ministerijos ekspertai **rekomenduoja**:

1. Tikrinkite informaciją – jeigu gaunate pasiūlymą investuoti ar įsidarbinti, pasidomėkite įmone ar investavimo platforma, atsiliepimais, patikimumu. Kartu atsiminkite – jeigu tai skamba per gerai, kad būtų tiesa, ko gero, taip ir yra.

2. Sulaukėte „rusakalbio eksperto“ skambučio – dėkite ragelį, ignoruokite ir netęskite pokalbio.

3. Neskubėkite – sukčiai dažniausiai spaudžia priimti sprendimą čia ir dabar. Laikas patikslinti informaciją gali išgelbėti jus nuo nuostolių.

4. Neperduokite jokių savo asmens duomenų ir banko duomenų tretiesiems asmenims.

Niekada nesutikite atidaryti sąskaitos banke „kitam žmogui“.

5. Būkite ypač atsargūs su lengvais darbo pasiūlymais, kurie reikalauja pervesti ar „tvarkyti“ jūsų pinigus.

Tai dažnas būdas pritraukti Lietuvos gyventojus tapti – pinigų plovimo tarpininkais nusikaltėliams.

6. Naudokite tik oficialius kanalus – jeigu kyla abejonų dėl pateiktos informacijos ar pasiūlymų, kreipkitės į savo banką ar policiją oficialiais kontaktais, o ne tais, kuriuos nurodė sukčiai. Sukčiai visada stengiasi pereiti į kitus komunikacijos kanalus, pavyzdžiui, Viber, Telegram ar WhatsApp. Niekada to nedarykite.

7. Dalinkitės patirtimi – jeigu tapote bandymo jus apgauti liudininku, informuokite savo artimuosius, banką ir policiją oficialiais kontaktais.

8. Kaip apsaugoti savo duomenis internete?

Valstybinės duomenų apsaugos inspekcijos specialistai taip pat rekomenduoja naudoti stiprius, unikalius slaptažodžius kiekvienai paskyrai bei pasitelkti slaptažodžių tvarkykles. Svarbu įjungti dviejų faktorių autentifikavimą, nes tai suteikia papildomą saugumo sluoksnį net ir tuo atveju, jei slaptažodis būtų pavogtas.

9. Kas yra dviejų faktorių autentifikavimas?

Dviejų faktorių autentifikavimas (*trumpinamas 2FA*) – tai papildomas saugumo žingsnis, padedantis apsaugoti jūsų paskyrą net tuo atveju, jei kas nors sužinotų jūsų slaptažodį.

Paprastai prisijungiant prie paskyros reikia įvesti tik slaptažodį, bet su 2FA prisijungimas vyksta dviem žingsniais. Pirmas žingsnis – kaip įprasta, įvedate savo slaptažodį. Antras žingsnis – sistema paprašo dar vieno patvirtinimo, pavyzdžiui, įvesti kodo, atsiųsto SMS žinute į jūsų telefoną, patvirtinti prisijungimą specialioje programėlėje arba naudoti elektroninį raktą ar biometrinių patvirtinimą (pavyzdžiui, piršto antspaudą).

Tai reiškia, kad net jei sukčiai sužinotų jūsų slaptažodį, jie vis tiek negalėtų prisijungti prie jūsų paskyros, nes neturėtų to antro žingsnio – jūsų telefono ar kito patvirtinimo būdo. Paprastai tariant, tai kaip durys su dviem užraktais: vienas – jūsų slaptažodis, o antras – kodas ar patvirtinimas, kurį turite tik jūs.

10. Papildomos apsaugos priemonės.

Valstybinė duomenų apsaugos inspekcija rekomenduoja reguliariai atnaujinti savo įrenginių operacines sistemas bei programas, kad būtų ištaisytos saugumo spragos. Taip pat būtina būti atsargiems su gaunamais el.laiškais ir nuorodomis – neatdaryti įtartinų priedų ar nepatikrintų svetainių.

Dalijantis asmenine informacija reikėtų apsvarstyti, ar ji tikrai būtina, ir ją teikti tik patikimiems šaltiniams. Galiausiai verta peržiūrėti privatumo nustatymus socialiniuose tinkluose bei kitose interneto platformose, kad būtų aišku, kokie duomenys ir kam yra matomi.

Tokios priemonės gali žymiai sumažinti jums riziką tapti asmens duomenų vagystės ar neteisėto jų panaudojimo auka. Būdami budresni ir atsakingesni skaitmeninėje erdvėje, galite apsaugoti ne tik save, bet ir savo artimuosius nuo finansinių nuostolių bei asmens duomenų vagysčių.

Pagarbiai



Josifas Lovkys

Teisininkas -konsultantas

UAB „EB teisė ir konsultacijos“

Ukmergės g. 369A, 8 a., LT-12142, Vilnius

Mob. +370 698 11214

El. paštas: dap@eblaw.lt