*Pranešimas žiniasklaidai*

*2022 kovo 25**d.*

**Patarimai verslininkams: kaip užtikrinti savo pinigų saugumą**

**Nors daug yra kalbama apie sukčius, viliojančius pinigus iš individualių gyventojų, tačiau ir kiekvienas bankų paslaugomis besinaudojantis verslas gali tapti jų auka. Nepaisant to, kad finansinės įstaigos nuolat investuoja į aukščiausius saugumo standartus atitinkančias technologijas, tačiau pinigų saugumu privalo pasirūpinti ir patys verslininkai.**

„Internetiniai sukčiai ieško vis sumanesnių būdų, kaip išvilioti verslininkų prisijungimo prie internetinės bankininkystės kodus, atlikti jų pačių neinicijuotus mokėjimus. Todėl, kad ir kokios saugios bei patikimos būtų finansų įstaigų naudojamos apsaugos priemonėms, svarbu patiems visuomet išlikti budriems ir imtis visų įmanomų būdų lėšų apsaugojimui“, – sako skaitmeninio lietuviško kapitalo banko „SME Bank“ vadovas Mantvydas Štareika.

**Nelaikyti visų pinigų vienoje sąskaitoje ar finansinėje institucijoje**

Gerai žinoma, kad diversifikacija – esminis bet kokios investavimo strategijos veiksnys, apsaugantis portfelį nuo didelių nuostolių. Tačiau, pasak finansų eksperto, ta pati taisyklė pritaikoma ir bet kurio verslo banko sąskaitose turimiems pinigams.

„Finansų ekspertai verslams rekomenduoja savo pinigus diversifikuoti – turėti sąskaitas keliuose bankuose ir kiekvienoje jų laikyti po dalį įmonės turimų lėšų. Pavyzdžiui, Lietuvoje, iki 100 tūkst. eurų ribos, viename banke laikomos lėšos yra draudžiamos, todėl jų išskaidymas po kelis bankus verslininkams yra naudingas. Be to, taip užtikrinamas ir nuolatinis lėšų prieinamumas techninių darbų ar kitų nenumatytų aplinkybių atveju“, – pataria M. Štareika.

„SME Bank“ vadovas pateikia pavyzdį – galima turėti vieną einamąją sąskaitą, kurioje lėšos būtų skirtos planuojamiems įsipareigojimams padengti, ir kitą sąskaitą, kurioje saugiai laikomas lėšų rezervas.

**Įdarbinti ir apdrausti savo pinigus**

Kaip vieną iš galimų būdų dar geriau apsaugoti savo lėšas, finansų specialistas siūlo nelaikyti nenaudojamų lėšų rezervo sąskaitoje, o padėti terminuotąjį indėlį. Tai – konkrečios, indėlio sutarties sudarymo dieną nustatytos pinigų sumos laikymas banke pasirinktu laikotarpiu su galimybe įmonės pajamas padidinti banko mokamomis palūkanomis.

„Terminuotasis indėlis gali prisidėti prie pinigų saugumo banke. Pirmiausia, visi indėliai bankuose yra drausti. Antra – kol galioja sutarties terminas, sukauptas lėšas atsiimti galima tik ją nutraukus. Trečia, už kiekvieną indėlį mokamos nustatyto dydžio palūkanos, todėl pinigai dar ir įdarbinami. Sudarius sutartį su kas mėnesį mokamomis palūkanomis, net ir nutraukus sutartį neprarastumėte už ankstesnius mėnesius uždirbtų palūkanų“, – teigia M. Štareika.

Be to, kaip pabrėžia finansų specialistas, indėlio padėjimas į banką, kuriame nelaikomos einamosios lėšos, gali būti geras būdas lėšoms diversifikuoti. Taip pat tokiu būdu laikomoms lėšoms nėra taikomas mokestis klientui, kuris nuo tam tikros pinigų sumos yra taikomas įprastai sąskaitoje laikomoms lėšoms.

**Patvirtinti tapatybę naudojant vieną iš saugių autentifikavimo priemonių**

Šiuolaikinės finansų įstaigos privalo atitikti techninius reguliavimo standartus dėl griežto klientų autentiškumo patvirtinimo, taip užtikrindamos saugų klientų prisijungimą prie internetinės bankininkystės portalų.

Vis dėlto, laikytis saugumo rekomenduojama ir patiems klientams, prie internetinės bankininkystės jungiantis ir operacijas patvirtinant su asmens tapatybės patvirtinimo priemone „Smart-ID“ arba M. parašu. Abi šios priemonės atitinka aukščiausius saugumo reikalavimus, jomis paprasta bei patogu naudotis.

„Kadangi kodų kortelės ir PIN generatoriaus slaptažodžiai yra nurodyti kortelėje, pametus ją atskleidžiami visi kliento saugumo kodai, todėl sukčiams jais gali būti lengviau pasinaudoti. Tuo metu „Smart-ID“ programėlė arba M. parašas nesaugo kodų nei išmaniajame telefone ar planšetėje, nei serveriuose. Todėl net ir praradus telefoną, asmens duomenys liks saugūs“, – tikina M. Štareika.

„SME Bank“ vadovas primena, kad naudojantis „Smart-ID“ arba M. parašu reikėtų susikurti sudėtingus ir unikalius saugos kodus. Juose nepatariama naudoti asmeninių duomenų – telefono numerio, gimimo, asmens kodo fragmentų ar lengvai atspėjamų skaičių derinių. Taip pat kodus būtina reguliariai keisti bei su niekuo jais nesidalinti. Siekiant dar didesnio sąskaitų saugumo, finansų ekspertas pataria užtikrinti ir savo telefono, planšetės ir kitų išmaniųjų įrenginių saugumą.

„Be to, jeigu telefone netikėtai gavote M. parašo arba „Smart-ID“ kodą įvesti prašantį pranešimą, nors jūs nesijungėte prie banko ir neatlikote kitų operacijų, kuo skubiau informuokite savo banką. Taip padėsite apsaugoti ne tik savo, bet potencialiai ir kitų banko klientų lėšas“, – sako M. Štareika.

**Nuolat atnaujinti kontaktinę informaciją ir bendradarbiauti su finansų įstaigos darbuotojais**

Finansų ekspertas atkreipia dėmesį ir į nuolat atnaujinamos kontaktinės informacijos svarbą. Turėdamas naujausią ir tiksliausią informaciją apie savo klientus, bankas gali lengviau užtikrinti jų lėšų saugumą.

„Kiekvienas bankas turi klausimyną, kurį kartas nuo karto paprašo atnaujinti – pateikti informaciją apie gaunamas pajamas, turimus įsipareigojimus, esamą darbovietę bei nurodyti asmeninius duomenis. Tai suteikia galimybę bankui ateityje nedelsiant informuoti klientą apie finansines rizikas“, – sako „SME Bank“ vadovas.

Vis dėlto, finansų ekspertas primena, kad klientams skambinantys finansų įstaigų darbuotojai niekada neprašo klientų prisijungimų prie sąskaitos, taip pat nesiunčia trumpųjų žinučių, elektroninių laiškų su prisijungimo nuorodomis, kuriose reikia suvesti savo asmeninius duomenis ar pateikti kitą jautrią informaciją. Jungiantis prie interneto banko visada būtina patikrinti, ar interneto svetainės nuoroda yra teisinga.

**Išlikti budriems skaitant partnerių laiškus**

Pasak banko vadovo, bene dažniausia sukčių naudojama taktika verslininkams apgauti – įsiterpti į verslo partnerių elektroninį susirašinėjimą ir jų vardu nurodyti pinigus už prekes, paslaugas ar pan. sumokėti į apgavikų banko sąskaitos numerį. Verta pastebėti, kad neretai sukčių nurodama banko sąskaita yra kitos šalies banke. M. Štareikos teigimu, tokiu atveju susigrąžinti lėšas gali būti sunku.

„Vengdami tokių apgavysčių, ypač atidžiai skaitykite laiškus apie pakeistus partnerių banko rekvizitus, prašymus pervesti lėšas. Patartina investuoti į įmonės naudojamų IT sistemų saugumą, atidžiai patikrinti, iš kokio el. pašto adreso siųstas laiškas. Taip pat visada verta paskambinti partneriui telefonu – ne nurodytu naujame susirašinėjime, tačiau jau turėtu anksčiau arba paskelbtu oficialioje įmonės svetainėje“, – pataria finansų specialistas.

**Apie „SME Bank“**

Pirmasis lietuviško kapitalo neobankas „SME Bank“ orientuojasi į smulkų ir vidutinį verslą, kuriam skaitmeniniu būdu teikia ne tik kasdienes bankininkystės paslaugas, bet ir skolinimosi produktus. Europos Centrinio Banko licenciją turintis „SME Bank“ veiklą pradėjo vykdyti 2021 m. birželį, banko paslaugos yra prieinamos visose trijose Baltijos šalyse. Kartu su finansų technologijų startuoliu „SME Finance“, „SME Bank“ vienoje ekosistemoje valdo 200 mln. eurų finansavimo portfelį.

**Kontaktai žiniasklaidai**

Rūta Knyvienė

„SME Bank“ marketingo vadovė

[ruta.knyviene@smebank.lt](mailto:ruta.knyviene@smebank.lt)

+370 (683) 70522