SUKČIAVIMAS APSIMETANT ĮMONĖS VADOVYBE

Sukčiavimu, apsimetant įmonės vadovybe, apibūdinama situacija, kai darbuotojas, įgaliotas atlikti mokėjimus, apgaulės būdu priverčiamas apmokėti netikrą sąskaitą faktūrą arba atlikti neleistiną pavedimą iš įmonės banko sąskaitos.

KAIP TAI VYKSTA?

Sukčiai skambina arba siunčia el. laiškus, apsimesdami įmonės aukšto lygio vadovais, pvz., generaliniu direktoriumi arba finansų direktoriumi.

Jie gerai išmano organizacijos ypatybes.

Jie reikalauja atlikti skubų mokėjimą.

Vartojamos tokios frazės, kaip „Tai konfidencialu“, „Įmonė jumis pasitiki“ arba „Šiuo metu aš nepasiekiamas“.

Kalbama apie keblią situaciją, pvz., mokesčių patikrinimą, susijungimą, įsigijimą.

Dažnai prašoma atlikti tarptautinį pavedimą į sąskaitą ne Europos banke.

Darbuotojo prašoma nepaisyti įprastos mokėjimų tvirtinimo tvarkos.

Nurodymai, kaip elgtis, gali būti pateikti vėliau, per trečiąjį asmenį arba elektroniniu paštu.

Darbuotojo prašoma nepaisyti įprastos mokėjimų tvirtinimo tvarkos.

KADA REIKĖTŲ SUSIRŪPINTI?

- Nepageidaujamas el. laiškas/ telefono skambutis
- Tiesioginė užklausa iš vadovybės atstovo, su kuriuo įprastai nebendraujate
- Prašymas užtikrinti visišką konfidencialumą
- Spaudimas ir skubinimas
- Neįprastas prašymas, prieštaraujantis vidaus procedūroms
- Grasinimai arba neįprastas meilikavimas, pažadai apie atlygį

KĄ DARYTI?

ĮMONĖ

Žinokite apie esamą riziką ir užtikrinkite, kad **darbuotojai taip pat būtų apie ją informuoti**.

Skatinkite savo darbuotojus **apdairiai vertinti mokėjimo prašymus**.

Sukurkite vidinę mokėjimų tvarką ir jos laikykitės.

Sukurkite patikros tvarką el. paštu teikiamiems mokėjimo prašymams.

Sukurkite pranešimų tvarką sukčiavimo atvejams fiksuoti.

Peržiūrėkite informaciją, paskelbtą jūsų įmonės tinklalapyje, **venkite per didelio detalumo ir būkite apdairūs** socialiniuose tinkluose.

Atnaujinkite technines apsaugos priemones.

Informuokite policiją apie bandymus sukčiauti, net jei netapote apgaulės auka.

DARBUOTOJAS

Griežtai laikykitės mokėjimų ir pirkimų saugos procedūrų. **Nepraleiskite nė vieno žingsnio ir nepasiduokite spaudimui**.

Dirbdami su slapta informacija/ pinigų pervedimais, visada **atidžiai tikrinkite el. pašto adresus**.

Jei kyla abejonių dėl mokėjimo nurodymo, **pasitarkite su kompetentingu kolega**.

Niekada neatidarykite įtartinų nuorodų ar priedų, gautų el. paštu. Būkite ypač atsargūs tikrindami savo asmeninę pašto dėžutę įmonės kompiuteriuose.

Venkite per didelio detalumo ir būkite apdairūs socialiniuose tinkluose.

Venkite dalintis informacija apie įmonės organizacinę sandarą, saugumą ar tvarkas.

Sulaukę įtartino el. laiško arba skambučio, visada informuokite savo IT padalinį.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

SUKČIAVIMAS, SUSIJĘS SU INVESTAVIMU

Labiausiai paplitęs investicinio pobūdžio sukčiavimas yra susijęs su esą pelningomis investavimo galimybėmis, tokiomis kaip akcijos, obligacijos, kriptovaliutos, retieji metalai, investicijos į žemės sklypus užsienyje ar alternatyvius energijos šaltinius.

KADA REIKĖTŲ SUSIRŪPINTI?

- Jums žadama greita grąža ir teigiama, kad investicija yra saugi.
- Pasiūlymas galioja tik ribotą laiką.
- Kai sulaukiate pasikartojančių nepageidaujamų skambučių.
- Pasiūlymas galioja tik jums ir jūsų yra prašoma juo nesidalinti.

KĄ DARYTI?

- Prieš perduodami pinigus ar investuodami, **visada pasikonsultuokite su pažįstamu ar savo banko finansininku.**
- **Atmeskite skambučius**, susijusius su investavimo galimybėmis.
- **Arsargiai vertinkite** pasiūlymus, žadančius saugias investicijas, garantuotą grąžą ar didelį pelną.
- **Nepamirškite, kad su sukčiavimu gali tekti susidurti ir ateityje.** Jei kartą jau investavote, susigundę apgaule, gali būti, kad ir ateityje sukčiai kreipsis į jus arba parduos jūsų duomenis kitiems nusikaltėliams.
- Jei įtariate sukčiavimą, **kreipkitės į policiją.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

SUKČIAVIMAS, SUSIJĘS SU SĄSKAITOMIS FAKTŪROMIS

KAIP TAI VYKSTA?

- Į verslo įmonę kreipiasi asmuo, apsimetantis tiekėjo/ paslaugų teikėjo/ kreditoriaus atstovu.
- Gali būti naudojami įvairūs būdai: telefonas, laiškai, el. paštas ir kt.
- Sukčius prašo pakeisti būsimų sąskaitų faktūrų apmokėjimo duomenis (t. y. gavėjo banko sąskaitos duomenis). Naujai pasiūlyta sąskaita priklauso sukčiui.

KĄ DARYTI?

ĮMONĖ

Užtikrinkite, kad **darbuotojai būtų informuoti** apie tokio pobūdžio sukčiavimą ir būdus, kaip jo išvengti.

Apmokykite darbuotojus, atsakingus už sąskaitų faktūrų apmokėjimą, **kaskart jas patikrinti**.

Įdiekite mokėjimo prašymų teisėtumo **patikrinimo procedūrą**.

Peržiūrėkite informaciją, paskelbtą jūsų įmonės tinklalapyje, ypač susijusią su sutartimis ir tiekėjais. Užtikrinkite, kad jūsų darbuotojai kuo mažiau pasisakytų apie įmonę savo socialinių tinklų paskyrose.

DARBUOTOJAS

Tikrinkite visas užklausas iš kreditorių, ypač kai šie prašo pakeisti jų banko sąskaitos duomenis būsimoms sąskaitoms faktūroms.

Mokėjimams, viršijantiems nustatytą limitą, įdiekite tikslios banko sąskaitos ir gavėjo **patvirtinimo procedūrą** (pvz., susitikimas su bendrove).

Nenaudokite kontaktinės informacijos iš laiško/ faksogramos/ el. laiško, kuriame prašoma ką nors pakeisti. Vietoje to naudokite duomenis **iš ankstesnio susirašinėjimo**.

Apmokėję sąskaitą faktūrą, **informuokite gavėją el. laišku.** Saugumui užtikrinti nurodykite gavėjo banko pavadinimą ir paskutinius keturis gavėjo banko sąskaitos skaitmenis.

Nustatykite **vieną kontaktų centrą** bendrovei, su kuria reguliariai atsiskaitote.

Apribokite informaciją apie savo darbdavį, kuria dalijatės socialiniuose tinkluose.

Kreipkitės į policiją, pastebėję bandymų sukčiauti, net jeigu netapote apgaulės auka.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

SUKČIAVIMAS APSIPERKANT INTERNETU

Apsiperkant internetu, neretai galima rasti patrauklių pasiūlymų, tačiau būkite atsargūs dėl galimo sukčiavimo.

KĄ DARYTI?

- Jei įmanoma, **naudokitės vietiniais mažmeninės prekybos tinklalapiais** – išspręsti iškilusias problemas bus tiesiog paprasčiau.
- **Atlikite savo tyrimą** – prieš pirkdami peržiūrėkite vertinimus.

- **Naudokitės kredito kortele.** Tokiu būdu turite daugiau galimybių susigrąžinti pinigus.
- **Atsiskaitykite tik saugiu būdu.** Prašoma tiesiogiai pervesti pinigus? Pagalvokite darkart!
- Mokėkite tik tada, kai esate prisijungę **prie saugaus interneto ryšio** – venkite nemokamų arba viešųjų bevielių tinklų.
- **Mokėkite tik iš saugaus įrenginio**. Reguliariai atnaujinkite operacinę sistemą ir saugos programinę įrangą.
- Saugokitės reklamų, siūlančių neįtikimas kainas ar stebuklingus gaminius. **Jei pasiūlymas skamba per daug gerai, kad būtų tiesa, greičiausiai taip ir yra**!
- Iškylantis langas, kuriame teigiama, kad laimėjote prizą? **Pagalvokite darkart**, galite laimėti nebent kenkėjišką programą.
- Nesulaukę užsakytos prekės, susisiekite su pardavėju. Jei šis neatsako, **kreipkitės į banką**.

Įtarę bet kokius bandymus sukčiauti, praneškite apie juos policijai netgi tuo atveju, jei netapote sukčių auka.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

APGAULINGI ELEKTRONINIAI LAIŠKAI IŠ BANKO

Apgaulingi el. laiškai iš banko – vienas iš duomenų vagystės būdų. Jais siekiama iš gavėjo išgauti asmeninę, finansų ir saugos informaciją.

KAIP TAI VYKSTA?

Šie el. laiškai:

gali atrodyti taip pat, kaip tikra banko korespondencija.

kopijuoja tikrų el. laiškų logotipus, maketą ir stilių.

prašo jūsų parsisiųsti pridedamą dokumentą arba paspausti ant nuorodos.

vartoja skubinančius posakius.

KĄ DARYTI?

- **Reguliariai atnaujinkite** savo programinę įrangą, įskaitant naršyklę, antivirusinę ir operacinę sistemą.
- Būkite ypač **budrūs**, jei „bankas“ el. paštu jūsų prašytų slapto pobūdžio informacijos (pvz., jūsų internetinės bankininkystės slaptažodžio).
- **Atidžiai peržiūrėkite el. laišką**: palyginkite siuntėjo adresą su ankstesniais tikrais pranešimais iš jūsų banko. Patikrinkite, ar nėra rašybos ir gramatikos klaidų.
- **Neatsakykite į įtartiną el. laišką**, verčiau persiųskite jį į savo banką, įrašę adresą patys.
- **Nespauskite ant pateiktų nuorodų ir neatsisiųskite priedų**, o įrašykite adresą savo naršyklėje.
- Kilus abejonėms, **pasitikrinkite** savo banko interneto svetainėje arba paskambinkite į banką.

Kibernetiniai nusikaltėliai vadovaujasi prielaida, kad žmonės yra užsiėmę; iš pirmo žvilgsnio šie elektroniniai laiškai atrodo tikroviški.

Saugokitės, kai naudojate mobilųjį įrenginį. Naudojantis telefonu arba planšete, gali būti sunkiau nustatyti bandymą sukčiauti.

#CyberScams

EUROPOL EC3 European Cybercrime Centre

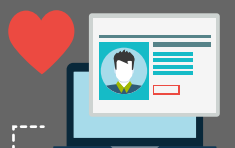
EBF European Banking Federation

LIETUVOS BANKŲ ASOCIACIJA

„ROMANTINIS“ SUKČIAVIMAS

Sukčiai ieško aukų pažinčių interneto svetainėse, tačiau kontaktui užmegzti taip pat gali pasinaudoti socialiniais tinklais ar elektroniniu paštu.

KADA REIKĖTŲ SUSIRŪPINTI?



Kai kažkas, su kuo neseniai susipažinote internete, prabyla apie savo stiprius jausmus jums ir prašo pradėti asmeninį susirašinėjimą.

Žinutės dažnai yra parašytos su klaidomis, jų turinys neaiškus.

Asmens paskyros informacija neatitinka to, ką jis jums sako.

Jūsų gali būti prašoma atsiųsti savo intymių nuotraukų arba vaizdo įrašų.

Pirmiausia siekiama pelnyti jūsų pasitikėjimą. Vėliau prašoma pinigų, dovanų ar jūsų banko sąskaitos/ kredito kortelės duomenų.

Nepervedę pinigų, galite sulaukti šantažo. Padarius pavedimą, pinigų bus prašoma daugiau.

TAPOTE AUKA?

Nesijauskite nejaukiai!

Nedelsdami nutraukite bendravimą.

Jei įmanoma, išsaugokite visą komunikaciją, pavyzdžiui, susirašinėjimą.

Pateikite skundą policijai.

Praneškite apie situaciją svetainės, kurioje sukčius su jumis susisiekė pirmą kartą, administracijai.

Jeigu pateikėte savo sąskaitos informaciją, susisiekite su savo banku.

KĄ DARYTI?

- **Būkite labai atsargūs**, dalindamiesi asmenine informacija socialiniuose tinkluose ir pažinčių svetainėse.
- **Visada įvertinkite galimą riziką.** Sukčiai dirba ir geriausią reputaciją turinčiose svetainėse.
- **Išlikite ramūs** ir klausinėkite.
- **Atidžiai išanalizuokite** asmens nuotrauką ir paskyrą, patikrinkite, ar pateikti duomenys nėra naudojami ir kitur.
- **Atkreipkite** dėmesį į rašybos ir gramatikos klaidas, pasakojimo nenuoseklumą, tokius atsiprašymus, kaip „neveikia vaizdo kamera“ ir pan.
- **Nesidalinkite** jokia kompromituojančia informacija, kuri galėtų būti panaudota šantažui prieš jus.
- Sutarę susitikti asmeniškai, **praneškite savo šeimos nariams ir draugams**, kur einate.
- **Saugokitės prašymų pervesti pinigų.** Niekada nedarykite pavedimų, neteikite kredito kortelių, interneto bankininkystės duomenų ar asmeninių dokumentų kopijų.
- **Venkite išankstinių apmokėjimų menkai pažįstamiems asmenims**.
- **Neperveskite pinigų** už kitą asmenį: pinigų plovimas yra nusikaltimas.

EUROPOL EC3 European Cybercrime Centre

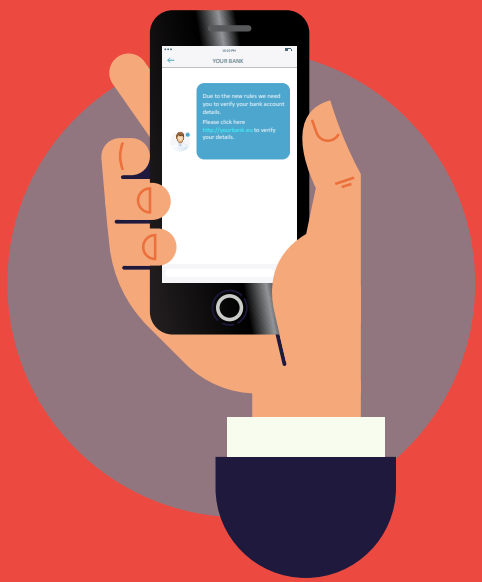
EBF European Banking Federation

LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

MELAGINGOS SMS ŽINUTĖS IŠ BANKO

Apgaulingomis trumposiomis SMS žinutėmis sukčiai bando išgauti asmeninę, finansinę ar saugos informaciją.



KAIP TAI VYKSTA?

Žinutėje paprastai prašoma paspausti ant nuorodos ar paskambinti telefonu, kad būtų „patikrinta“, „atnaujinta“ ar „pakartotinai aktyvuota“ jūsų sąskaita. Tačiau nuoroda nuveda į netikrą puslapį, o telefonu atsiliepia įmone apsimetantis sukčiautojas.

KĄ DARYTI?

- **Nespauskite ant nuorodų, priedų ar paveikslėlių,** kuriuos gaunate su nepageidaujamomis teksto žinutėmis, prieš tai neįsitikinę siuntėjo patikimumu.
- **Neskubėkite.** Užuot greitai atsakę, ramiai pasitikrinkite informaciją.
- **Niekada neatsakykite į tekstinę žinutę**, kurioje reikalaujama nurodyti PIN kodą, internetinės bankininkystės slaptažodį ar bet kuriuos kitus saugos duomenis.
- Jei manote, jog atsakėte į sukčių žinutę ir pateikėte savo asmeninę informaciją, **nedelsdami susisiekite su banku**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

APGAULINGOS BANKŲ SVETAINĖS

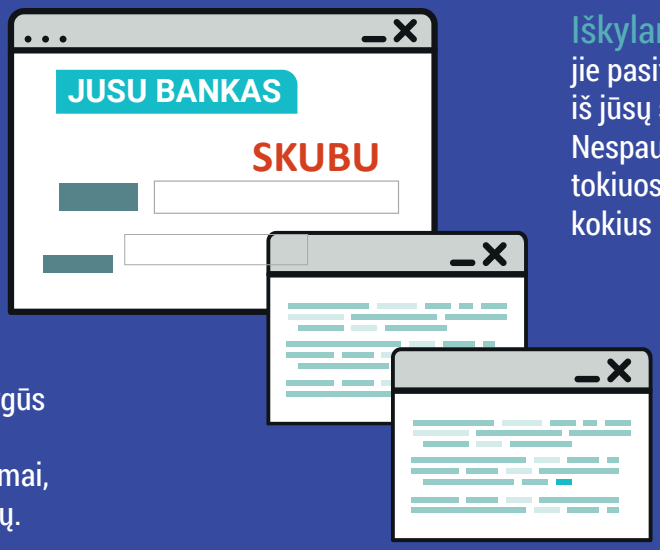
Melaginguose bankų laiškuose paprastai būna nuorodų į netikras bankų svetaines, kur jūsų bus prašoma atskleisti savo finansinę ir asmeninę informaciją.

KADA REIKĖTŲ SUSIRŪPINTI?

Melagingos bankų interneto svetainės atrodo beveik taip pat, kaip ir tikrų bankų. Dažnai jos turi ekrane iškylantį langą, kuriame prašoma įrašyti savo interneto bankininkystės prisijungimo duomenis. Tikri bankai tokių langų nenaudoja.

Šioms svetainėms paprastai būdinga:

Skubumas: tikrose svetainėse tokių žinučių nerasite.



Iškylantys langai: dažniausiai jie pasitelkiami, siekiant išgauti iš jūsų slaptą informaciją. Nespauskite ant jų ir venkite tokiuose languose rašyti bet kokius asmeninius duomenis.

Prastas dizainas: būkite atsargūs interneto svetainėse, kuriose akivaizdžiai matyti dizaino trūkumai, yra rašybos bei gramatikos klaidų.

KĄ DARYTI?

Niekada nespauskite į banko svetainę neva vedančių nuorodų, pateikiamų laiškuose.

Visada suveskite adresą rankiniu būdu arba naudokite jau susikurtą nuorodą iš savo žymių sąrašo.

Naudokite interneto naršyklę, kuri leidžia **blokuoti iškylančius langus.**

Jei bus kas nors tikrai svarbaus, jūsų bankas jus informuos žinute jūsų **internetinės bankininkystės paskyroje.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | LIETUVOS BANKŲ ASOCIACIJA

#CyberScams

MELAGINGI BANKO SKAMBUČIAI

Pasitelkę melagingus skambučius, sukčiai iš aukos siekia išgauti svarbią asmeninę, finansinę bei saugos informaciją arba išvilioti pinigus.

KĄ DARYTI?

- **Būkite apdairūs**, sulaukę nepageidaujamų telefono skambučių.
- **Užfiksuokite skambinančiojo numerį** ir pasakykite, kad perskambinsite.
- Norėdami patikrinti skambinančiojo tapatybę, p**aieškokite jo neva atstovaujamos organizacijos telefono numerio** ir susisiekite su ja tiesiogiai.
- **Netikrinkite skambinančiojo tapatybės, pasitelkę jo nurodytą telefono numerį** (tai gali būti fiktyvus numeris).
- Sukčiai gali rasti pagrindinę informaciją apie jus internete (pvz., socialiniuose tinkluose). **Nemanykite, kad skambinantysis asmuo yra tas, kuo prisistato**, vien todėl, kad jis šį tą apie jus žino.

- **Nesidalinkite** savo kredito ar debeto kortelės PIN kodu arba savo internetinės bankininkystės slaptažodžiu. Jūsų bankas niekada neprašys tokios informacijos.
- **Neperveskite** pinigų į kitą sąskaitą skambinančiojo prašymu. Jūsų bankas to niekada neprašys.
- Jei manote, kad skambutis yra melagingas, **praneškite savo bankui**.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

LIETUVOS BANKŲ ASOCIACIJA

#CyberScams