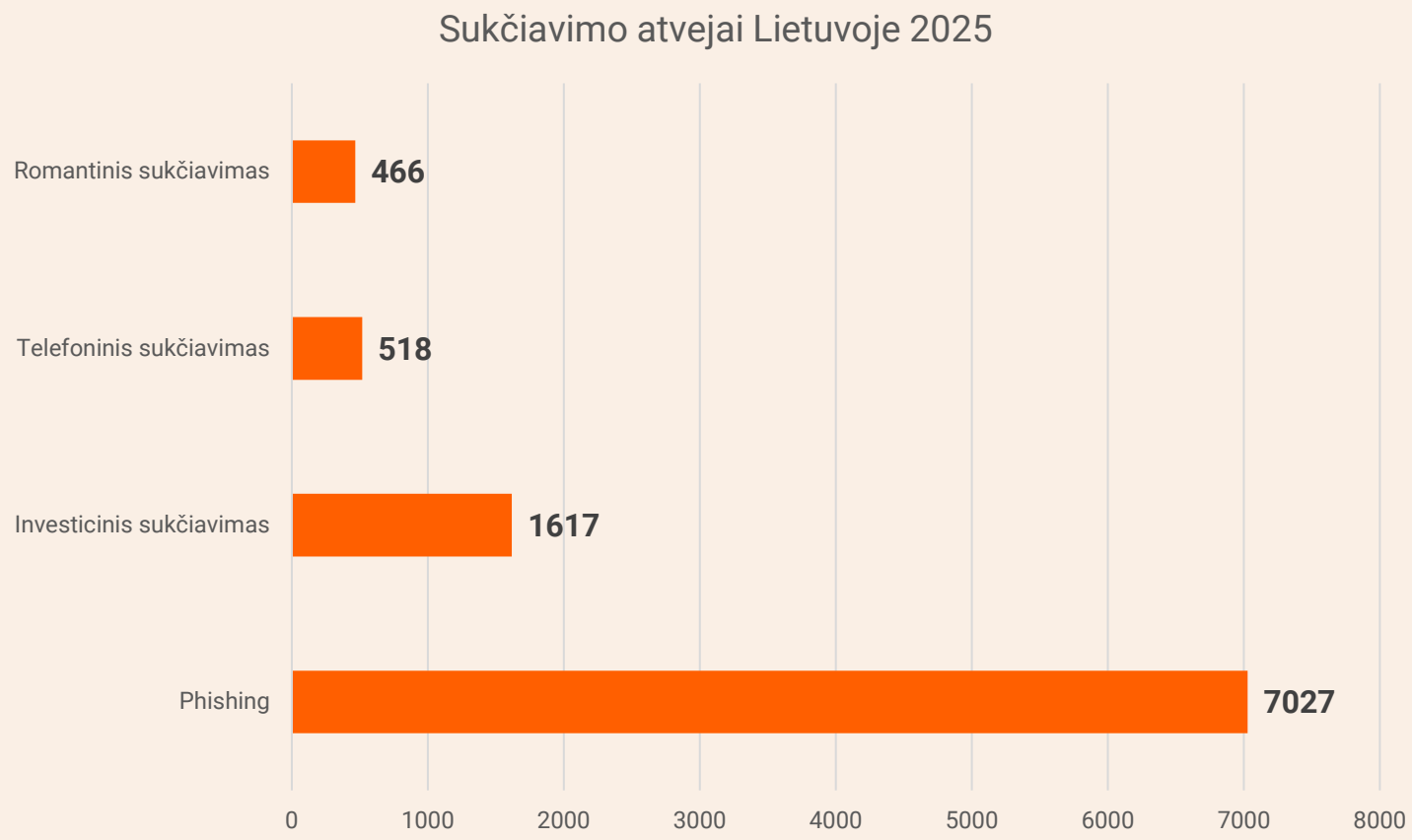
„*Red flags*“ finansų institucijoms: klientų elgesio indikatoriai ir operacijų modeliai

(Tipiniai sukčiavimo signalai realiuose atvejuose)

Adomas Semeška

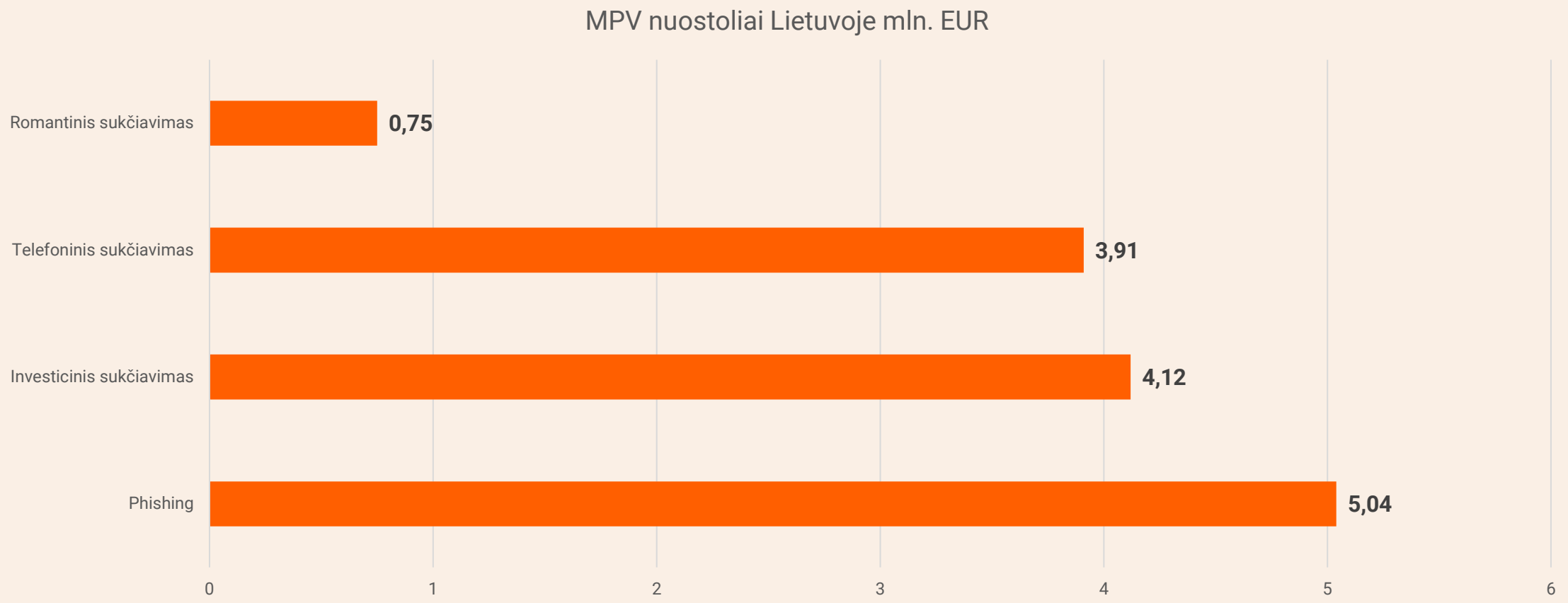
2026-04-15

Statistikos apžvalga 2025 metai



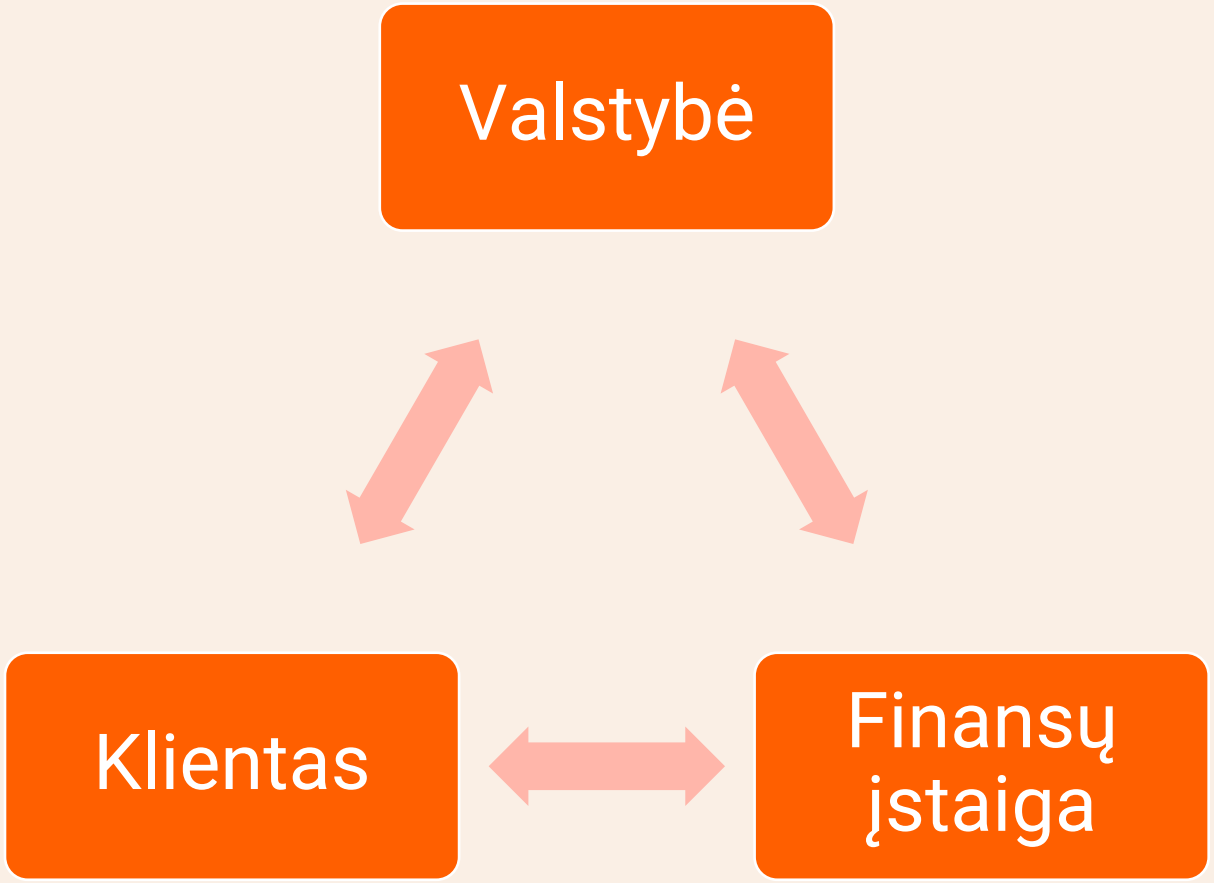
2024 – 13691 atvejis
2025 -15447 atvejis

Pagrindiniai sukčiavimo tipai



Duomenys iš: https://amlcenter.lt/wp-content/uploads/2026/02/0202.1-2025-metu-sukciavimo-atveju-statistikos-analize.pdf

Sukčiavimo prevencijos ekosistema – trys gynybos linijos



Sukčiavimo prevencijos ekosistema – trys gynybos linijos

Klientas

- Atpažįsta įtartinus pasiūlymus ir situacijas
- Niekam neatskleidžia savo asmeninių prisijungimų prie internetinės bankininkystės
- Atidžiai tvirtina savo mokėjimų nurodymus
- Tapęs sukčiavimo auka, nedelsdamas informuoja savo finansų įstaigą ir teisėsaugos institucijas

Finansų įstaiga

- Reaguoja į incidentus ir tobulina prevencijos modelius
- Stebi ir analizuoja operacijas bei klientų elgseną
- Kuria monitoringo scenarijus ir įgyvendina prevencinius veiksmus
- Konsultuoja klientą, ugdo finansinį raštingumą

Valstybė

- Kuria teisinę bazę bei ją prižiūri
- Prisideda prie klientų finansinio raštingumo ugdymo
- Kuruoja finansų įstaigų sukčiavimo prevencijos įgyvendinimo procesą
- Skatina finansų įstaigų tarpusavio bendradarbiavimą

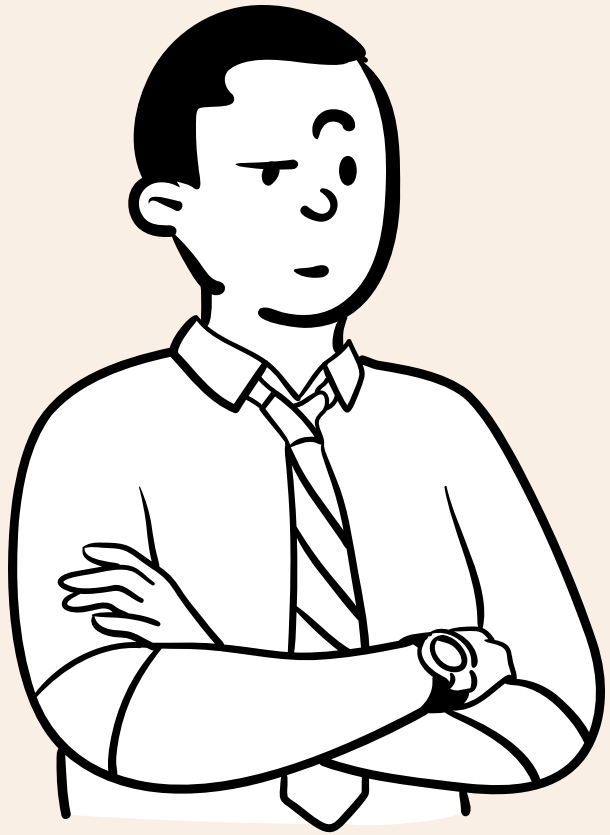
Konkrečių sukčiavimo atvejų apžvalga

Phishing atvejis – situacija kliento akimis

- Klientas pardavinėjo prekę internetinėje skelbimų platformoje
- Gavo žinutę / el. laišką su nuoroda, skirta apmokėjimui gauti iš pirkėjo
- Paspaudus nuorodą, buvo nukreiptas į internetinės bankininkystės puslapį
- Suvedė prisijungimo duomenis, patvirtino veiksmą, tačiau prisijungimas nepavyko
- Po kurio laiko mobiliojoje programėlėje pastebėjo mokėjimo operaciją, kurios pats neinicijavo

Phishing atvejis – situacija darbuotojo akimis

- Koks buvo realus finansinio veiksmo tikslas?
- Ar norint gauti apmokėjimą už prekę reikėjo jungtis prie internetinės bankininkystės?
- Ar situacijoje matomi socialinės inžinerijos požymiai?
- Ar laiko tarpai tarp veiksmų yra neįprasti?
- Ar tokia veiksnių seka būdinga kliento įprastam elgesiui?



Phishing atvejis – scenarijų kūrimas ir *„red flags“*

Elgsena

- Atliekami veiksmai neatitinka deklaruojamo tikslo
- Klientas autorizuoja veiksmus, kurių pasekmės jam nepalankios

Operacijos

- Mokėjimo operacijos, kurių klientas neinicijavo
- Neįprasti ar nauji gavėjai
- Mokėjimo operacijų sumos ar tipas neatitinka kliento istorijos

Kontekstas

- Trumpas laiko tarpas tarp prisijungimo ir finansinių veiksmų
- Klientui nebūdingi prisijungimai
- Nebūdingos mokėjimo operacijos detalės
- Nebūdingas lėšų gavėjo bankas

Phishing atvejis – scenarijų kūrimas ir „*red flags*“

Galimo scenarijaus pavyzdys:

- Klientui nebūdingas įrenginys
- Atlikta mokėjimo operacija naujam gavėjui kliento atžvilgiu
- Mokėjimo operacijos atlikimas per tam tikrą, greitą laiko periodą

Svarbu pabrėžti:

Kiekvieno naujo scenarijaus kūrimas, ypač deterministinio pobūdžio reikalauja atlikti išsamią klientų atliekamų mokėjimo operacijų analizę.

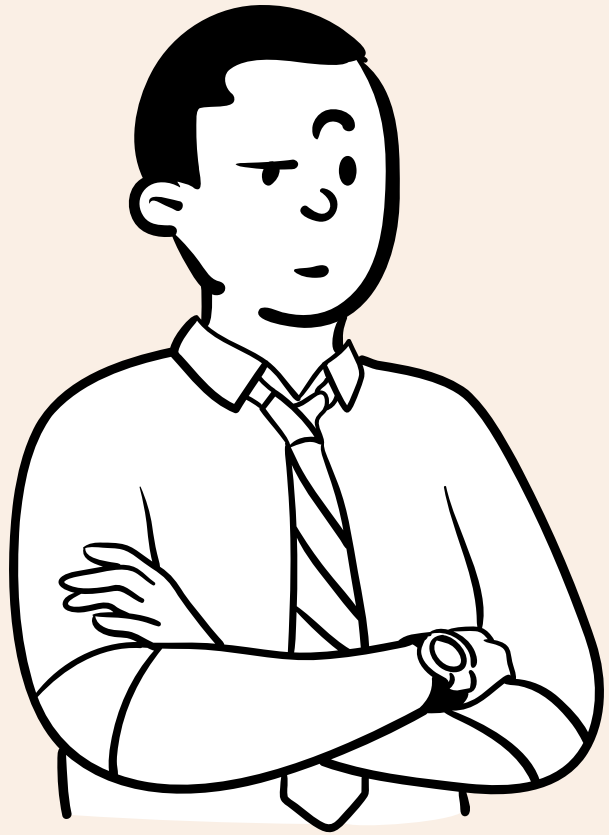
Phishing sukčiavimo atvejams taip pat rekomenduojama turėti „blogų“ sąskaitų sąrašą, į kurį būtų traukiamos visos su sukčiavimu susijusios sąskaitos, taip užkardant potencialius klientų nuostolius.

Investicinio sukčiavimo atvejis – situacija kliento akimis

- Klientas įstojo į *„sveikų finansų“* grupę socialiniuose tinkluose
- Grupėje pastebėjo pasiūlymus „įdarbinti pinigus“ ir gauti didelę grąžą
- Grupės „konsultantai“ pasiūlė investuoti į kriptovaliutas
- Klientas atliko mokėjimo operacijas į nurodytas sąskaitas, buvo skatinamas investuoti didesnes sumas ir kuo greičiau
- Po kurio laiko, prisijungęs prie socialinio tinklo, pastebėjo, kad *„sveikų finansų“* grupės nebėra

Investicinio sukčiavimo atvejis – situacija darbuotojo akimis

- Ar klientas gali aiškiai įvardinti naudojamus investicinius produktus?
- Ar kliento lėšos yra pervedamos į trečiųjų asmenų sąskaitas, ar į licencijuotą investicinę platformą?
- Ar kliento investavimo elgsena atitinka jo ankstesnę patirtį ir profilį?
- Ar „konsultantai“, konsultuojantys klientą, yra aiškiai identifikuoti ir patikrinami?



Investicinio sukčiavimo atvejis – scenarijų kūrimas ir *„red flags“*

Elgsena

- Klientas investuoja į produktus, kurių negali aiškiai įvardinti ar paaiškinti
- Sprendimai nukrypsta nuo kliento ankstesnio finansinio elgesio
- Investuojamos didėjančios sumos, reaguojant į „patarimus“
- Klientas priima sprendimus, kurių pasekmės jam finansiškai nepalankios

Operacijos

- Lėšos pervedamos į trečiųjų asmenų sąskaitas, kurių klientas negali įvardinti
- Pasikartojantys pavedimai su panašia logika
- Mokėjimo operacijų sumos ar dažnis neatitinka kliento istorijos
- Mokėjimai atliekami ne per investicinę platformą

Kontekstas

- Akcentuojama skuba ir „riboto laiko galimybės“
- Investavimo veiksmai vyksta po intensyvaus išorinio bendravimo
- Nėra aiškaus reguliuojamo investavimo kanalo
- Staigus ryšio su „konsultantais“ nutrūkimas

Investicinis sukčiavimas – scenarijų kūrimas ir *„red flags“*

Galimo scenarijaus pavyzdys:

- Vidutinis mėnesio mokėjimo operacijų skaičiaus išaugimas
- Ekrano dalijimasis vykdant mokėjimo operacijas
- Klientui nebūdingų mokėjimo detalių naudojimas

Svarbu pabrėžti:

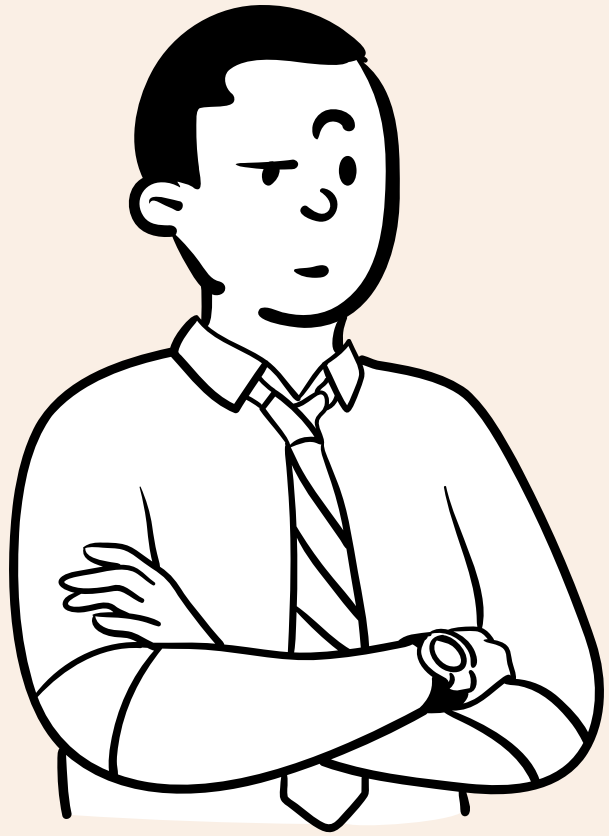
Kaip ir *phishing* sukčiavimo atvejams, taip pat ir investicinio sukčiavimo atvejams rekomenduojame turėti „blogų“ sąskaitų sąrašą, į kurį būtų traukiamos visos su šiuo sukčiavimu susijusios sąskaitos, taip užkardant potencialius klientų nuostolius.

Telefoninio sukčiavimo atvejis – situacija kliento akimis

- Klientui paskambino tretieji asmenys teigiantys prisistatantys populiarių paslaugų teikėjais
- Klientas informuojamas, kad yra galimai apgaudinėjamas ir peradresuojamas „policijos“ pareigūnams ar "banko" darbuotojams.
- Klientas, siekdamas apsaugoti lėšas, vykdo paskambinusių asmenų nurodymus
- Klientas supratęs, kad yra galimai apgaudinėjamas kreipiasi į policiją ir savo finansų įstaigą

Telefoninio sukčiavimo atvejis – situacija darbuotojo akimis

- Kodėl klientas atliko jam nebūdingo dydžio mokėjimo operaciją ir naujam lėšų gavėjui?
- Kodėl klientas daugiau nei įprastai prisijungia prie internetinės bankininkystės?
- Kodėl klientas pradėjo prisijunginėti prie internetinės bankininkystės iš skirtingų ir jam nebūdingų įrenginių?
- Kodėl klientas nutraukė sudarytas indėlių sutartis?



Telefoninio sukčiavimo atvejis – scenarijų kūrimas ir *„red flags“*

Elgsena

- Klientas, tikėdamas bendraujantis su oficialiais institucijų atstovais, pradeda vykdyti jų nurodymus
- Klientas staiga tampa labai aktyvus banko kanaluose (prisijungimai, veiksmai)
- Klientas nebendradarbiauja, nenoriai teikia informaciją apie atliktas operacijas

Operacijos

- Lėšos pervedamos į trečiųjų asmenų sąskaitas
- Mokėjimo operacijų sumos ar dažnis nebūdingi klientui
- Nutraukiami indėliai, imami vartojimo kreditai
- Kliento sąskaitoje galima identifikuoti lėšų tranzitiškumą

Kontekstas

- Klientas yra atskiriamas nuo artimųjų bei finansų įstaigos
- Klientas spaudžiamas čia ir dabar atlikti veiksmus, siekiant „apsaugoti“ jį ir jo lėšas
- Klientas negali iki galo detaliai paaiškinti savo atliekamų veiksmų

Telefoninis sukčiavimas– scenarijų kūrimas ir *„red flags“*

Galimo scenarijaus pavyzdys:

- Mokėjimo operacija naujam gavėjui
- Padidėjęs aktyvumas internetinėje bankininkystėje
- Nebūdingai ilgos internetinės bankininkystės prisijungimo sesijos
- Tam tikras klientų segmentas

Svarbu pabrėžti:

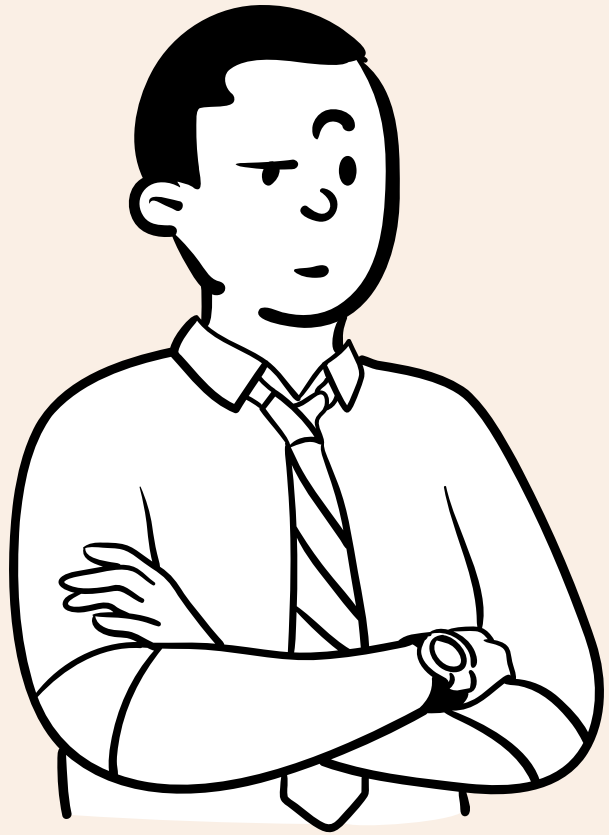
Telefoninio sukčiavimo požymių identifikavimas yra sudėtingas procesas, reikalaujantis kelių skirtingų scenarijų taikymo. Jų efektyvumas priklauso nuo scenarijų kūrėjų pasirinkto modelio bei finansų įstaigos tolerancijos *„false positive“* įspėjimų kiekiui.

Romantinio sukčiavimo atvejis – situacija kliento akimis

- Klientas socialiniuose tinkluose susipažįsta su „žinomu turkų aktoriumi“
- Užsimezga bendravimas trunkantis keletą mėnesių, susitariama, kad naujas pažįstamas atvyks į Lietuvą
- Prieš atvykimą, naują pažįstamą ištinka nelaimė – jis patenka į avariją ir yra užblokuojamos jo finansinės lėšos,
- Klientas nusprendžia padėti draugui, kuris paprašo atlikti mokėjimo operaciją jo pažįstamam asmeniui

Romantinio sukčiavimo atvejis – situacija darbuotojo akimis

- Kodėl klientas pradėjo vykdyti mokėjimus naujiems, jam iki šiol nebūdingiems gavėjams?
- Kodėl klientas teigia pirkęs prekes ar paslaugas, tačiau negali jų detalizuoti ar pateikti tai pagrindžiančių dokumentų?
- Kodėl, paklausus apie galimą trečiųjų asmenų įtaką mokėjimams, klientas pyksta ar atsisako komentuoti?



Romantinio sukčiavimo atvejis – scenarijų kūrimas ir *„red flags“*

Elgsena

- Klientas atlieka finansinius veiksmus, motyvuotus emociniu ryšiu.
- Klientas vengia detalizuoti atliekamas mokėjimų operacijas
- Klientas pateikia paaiškinimus, kuriais siekia uždaryti diskusiją, o ne pagrįsti sprendimus

Operacijos

- Kliento sprendimai nukrypsta nuo jam įprastų mokėjimo operacijų
- Klientui nebūdingų mokėjimų operacijų sumos ar dažnis palaipsniui didėja

Kontekstas

- Klientas su sukčiumi užmezga ilgalaikį emocinį ryšį
- Užsitikrinus pasitikėjimą klientas įstumiamas į emocinį spaudimą sukeliančias situacijas
- Klientas yra prašomas neinformuoti artimųjų ir banko apie „santykius“
- Klientui nepripažįsta tapęs sukčiavimo auka

Romantinis sukčiavimas– scenarijų kūrimas ir *„red flags“*

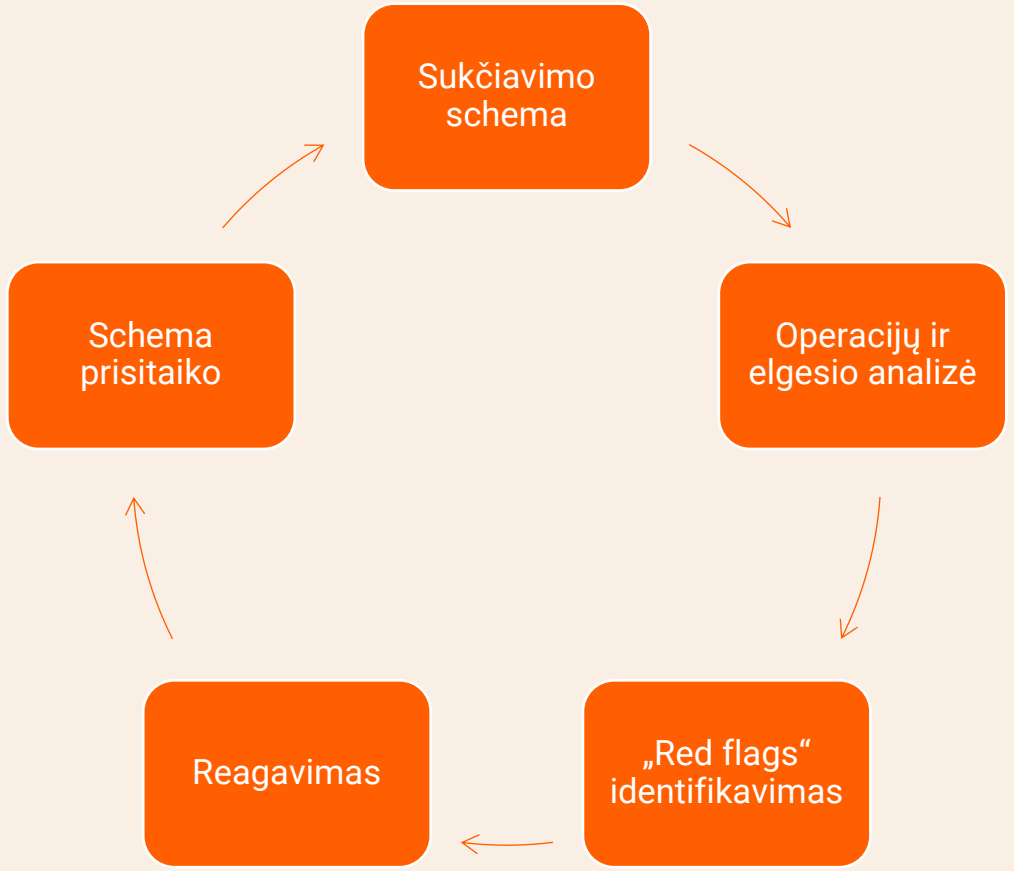
Galimo scenarijaus pavyzdys:

- Tam tikras klientų segmentas
- Tam tikros mokėjimo operacijos detalės
- Mokėjimo operacijos nuo tam tikros sumos

Svarbu pabrėžti:

Kaip ir *phishing* sukčiavimo atvejams, taip pat ir romantinio sukčiavimo atvejams rekomenduojame turėti „blogų“ sąskaitų sąrašą, į kurį būtų traukiamos visos su šiuo sukčiavimu susijusios sąskaitos, taip užkardant potencialius klientų nuostolius.

Sukčiavimo schemos kinta – *„Red flags“* kartojasi




Swedbank
SINCE 1820