Pinigų plovimo prevencijos
kompetencijų centras

Sukčiavimo atvejų statistikos analizė

2024 m. III ketvirtis

2024 m.

2024 m. Q3 sukčiavimo atvejų statistikos analizė

Pinigų plovimo prevencijos kompetencijų centro statistinių duomenų teikėjai

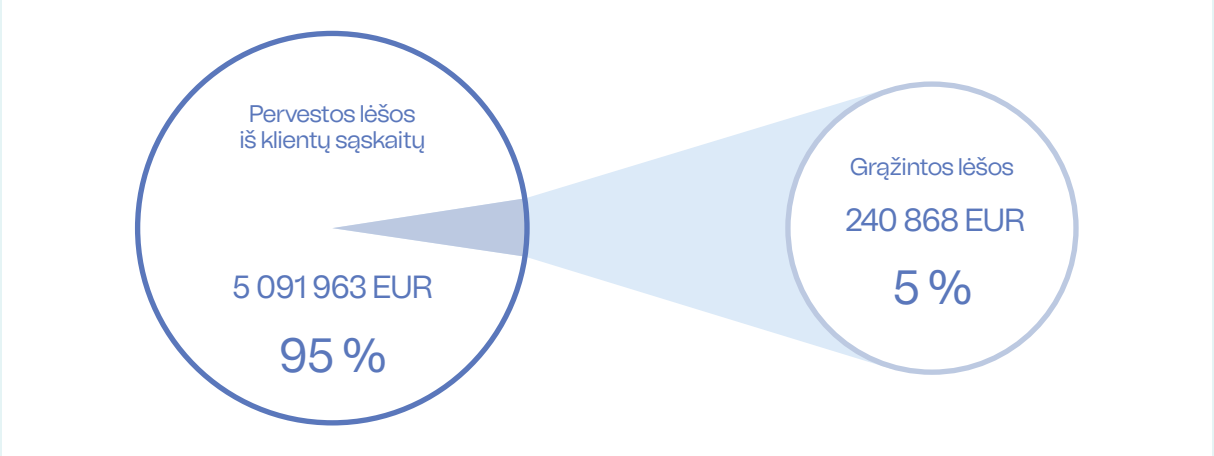
Pinigų plovimo prevencijos kompetencijų centras (toliau – PPPKC, Centras) pagal iš finansų įstaigų AB „Swedbank“, AB SEB banko, Revolut Bank, UAB, Luminor Bank AS Lietuvos skyriaus, AB Šiaulių banko, OP Corporate Bank plc. Lietuvos filialo, AS „Citadele banka“ Lietuvos filialo ir UAB URBO banko pateiktus duomenis atliko 2024 m. III ketvirčio (toliau – 2024 m. Q3, 2024 m. III ketvirtis, 2024 m. Q2, 2024 m. II ketvirtis, 2024 m. Q1, 2024 m. I ketvirtis) sukčiavimo atvejų statistikos analizę.

2024 m. Q3 finansinių sukčių aktyvumas

PPPKC pateikti duomenys rodo, kad 2024 m. III ketvirtį finansų įstaigos užfiksavo 2969 sukčiavimo incidentus. Finansų įstaigų klientų sukčiams pervestų lėšų suma viršijo 5 mln. Eur, iš šios sumos finansų įstaigos gyventojams sugrąžino virš 240 tūkst. Eur. Remiantis šiais duomenimis, realūs gyventojų nuostoliai, t. y. klientų prarastos lėšos – 4,8 mln. Eur.

Sukčiavimo būdu realiai patirti GYVENTOJŲ nuostoliai – 4,8 mln. EUR

2024 m. Q3



Lyginant 2024 m. Q1, Q2 ir Q3 sukčiavimo incidentų statistiką, matomas nuoseklus sukčiavimo atvejų mažėjimas. 2024 m. Q1 buvo fiksuota 3760 sukčiavimo atvejų, Q2 šių atvejų skaičius sumažėjo iki 3335, o Q3 buvo fiksuoti 2969 sukčiavimo incidentai. Lyginant Q1 su Q2, sukčiavimo atvejų skaičius sumažėjo 11,3 proc.

Analizuojant Q3 duomenis, sukčiavimų skaičius dar labiau sumažėjo – iki 2969 atvejų, tai sudaro papildomą 10,97 proc. kritimą lyginant su Q2. Per pirmuosius tris 2024 m. ketvirčius incidentų skaičius sumažėjo net 21,06 proc. Ši mažėjimo tendencija gali būti vertinama kaip aiškus finansų sektoriaus prevencinių priemonių veiksmingumo rodiklis, parodantis, kad taikomi metodai, efektyvi rizikų kontrolė, stebėsenos sistemų tobulinimas bei didesnis darbuotojų sąmoningumas prisideda prie sukčiavimo atvejų skaičių mažėjimo.

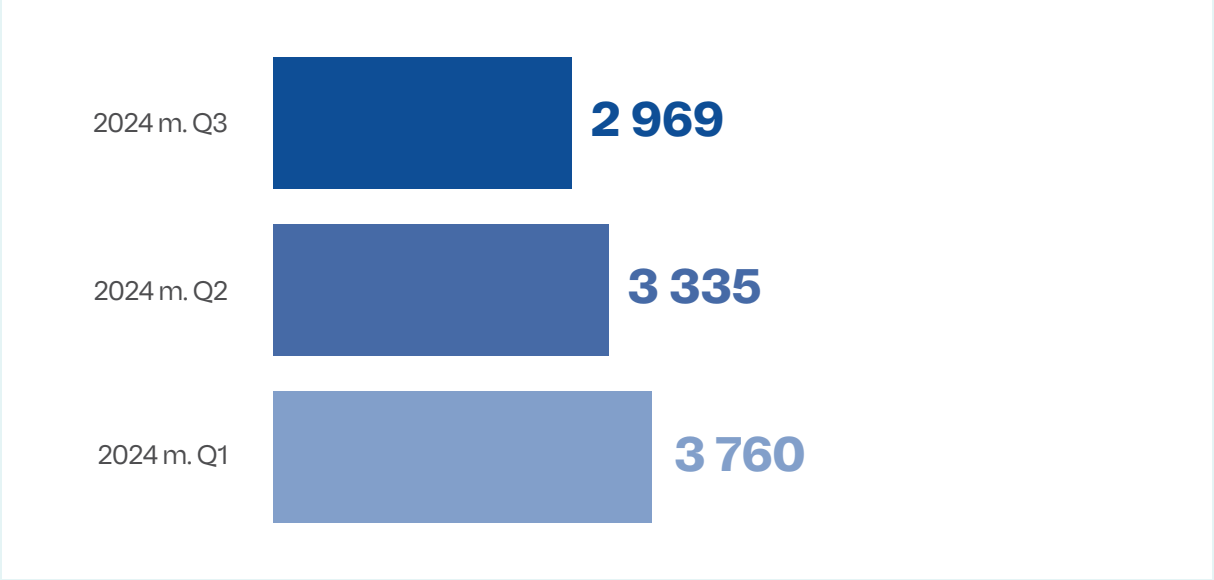
[1] Incidentų skaičius (vnt.) – sukčiavimo atvejai (epizodai, ne sukčiavimo būdu inicijuotos pavienės operacijos), kai klientas esamomis autorizavimo priemonėmis pasirašė ir inicijavo mokėjimą, kuris finansų įstaigos buvo sustabdytas / įvykdytas. Patikslinama, jog incidento vienetu laikomas atvejis, kai klientas dalyvauja tam tikroje sukčiavimo schemoje.

[2] Pervestos lėšos iš klientų sąskaitų – lėšos, išėjusios iš finansų įstaigos.

LYGINAMOJI ATASKAITA

Sukčiavimo incidentų skaičius

2024 m. Q1 vs 2024 m. Q2 vs 2024 m. Q3

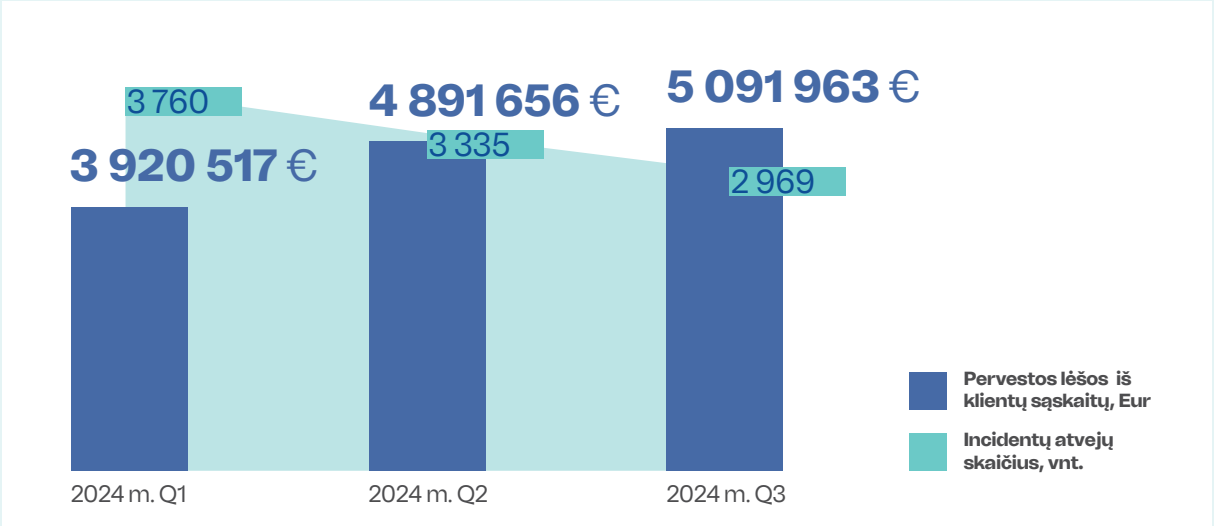


Nepaisant to, kad sukčiavimo incidentų skaičius 2024 m. mažėjo, gyventojų patiriami finansiniai nuostoliai nuolat auga, tai atskleidžia pavojingą paradoksą: nors sukčių atakų skaičius yra sumažėjęs, sukčių veiksmai tampa ženkliai efektyvesni.

2024 m. Q1 gyventojai sukčiams pervedė 3,9 mln. Eur, Q2 ši suma išaugo iki 4,8 mln. Eur, o 2024 m. Q3 pasiekė beveik 5,1 mln. Eur. Tai rodo, kad, nepaisant sumažėjusio incidentų skaičiaus (21 proc. mažėjimas nuo Q1 iki Q3), sukčiai sugeba padidinti vieno incidento finansinę žalą, todėl bendra prarastų pinigų suma augo daugiau nei 30 proc. Sukčiai tampa labiau rafinuoti ir taikosi į didesnes finansines sumas. Tai reiškia, kad net mažesnis sukčiavimo atvejų skaičius gali sukelti vis didesnius finansinius nuostolius.

Sukčiavimo statistika

2024 m.

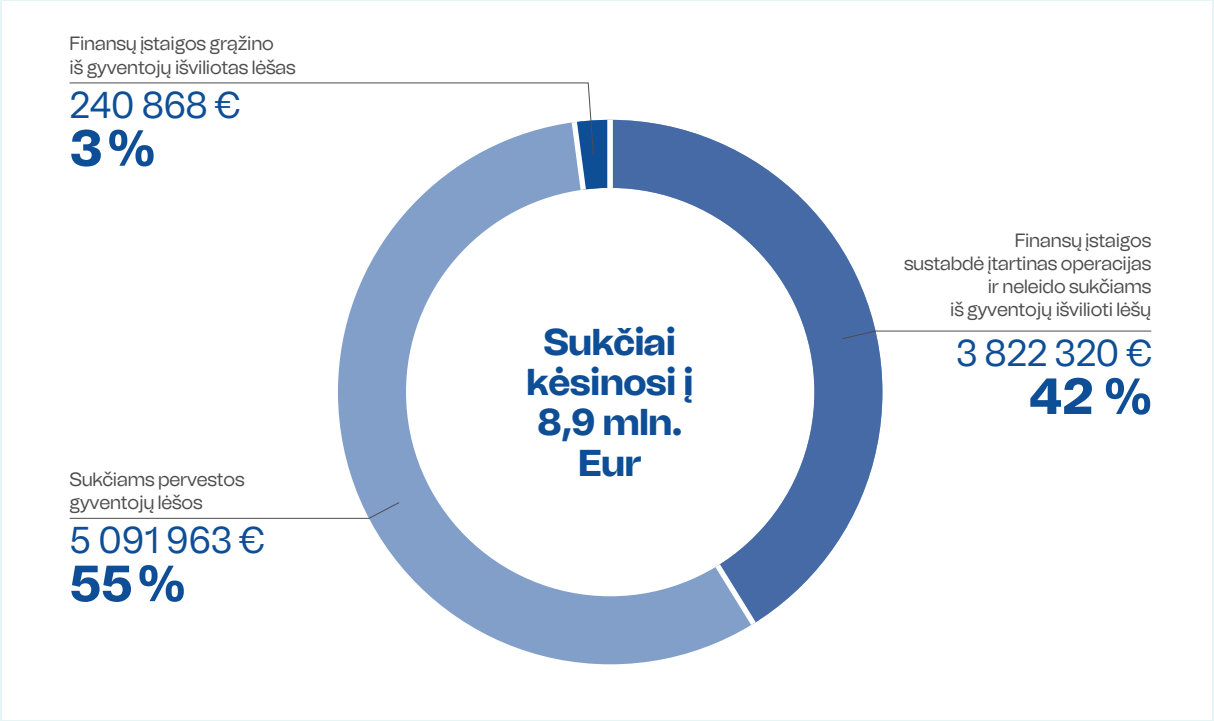


Tačiau, nepaisant sukčių atakų, pažymėtina, jog finansų įstaigos, taikydamos efektyvius prevencinius veiksmus ir toliau sėkmingai apsaugo šalies gyventojus ir įmones nuo reikšmingų finansinių nuostolių. 2024 m. III ketvirtį buvo sustabdyta 3,8 mln. Eur – tai 11,8 proc. daugiau nei 2024 m. II ketvirtį (kai buvo sustabdyta 3,4 mln. Eur) ir net 31 proc. daugiau nei 2024 m. I ketvirtį ketvirtį, kai buvo sustabdyta 2,9 mln. Eur suma.

Didėjantis sustabdytų lėšų skaičius indikuoja automatizuotų prevencijos sistemų efektyvumą ir specialistų greitą reagavimą į įtartinus sandorius.
Atkreiptinas dėmesys, kad tuo pat metu sukčių atakos tampa vis pavojingesnės. 2024 m. I ketvirtį sukčiai kėsinosi išvilioti 6,9 mln. Eur, o 2024 m. II ketvirtį ši suma išaugo iki 8,3 mln. Eur. 2024 m. III ketvirtį sukčių atakos dar labiau sustiprėjo, bendra sukčių siekiama išvilioti suma pasiekė 8,9 mln. Eur sumą.

Analizuojant 2024 metų trijų ketvirčių laikotarpį finansų įstaigų gyventojams sugrąžintų sukčiams jau pervestų lėšų rodiklį, stebima, kad lėšų grąžinimo dinamika buvo kintanti. Per 2024 m. Q1 finansų įstaigoms pavyko grąžinti 221 338 Eur, nors Q2 šis skaičius buvo išaugęs – iki 730 492 Eur, tačiau 2024 m. Q3 grąžintų lėšų suma, lyginant su 2024 m. Q2, reikšmingai sumažėjo iki 240 868 Eur.

Šis pokytis rodo, kad sukčiams prarastų lėšų grąžinimo sėkmė yra kintanti ir priklausanti nuo laiku bei koordinuotai atliktų finansinių įstaigų veiksmų.



SUKČIAVIMAI PAGAL TIPOLOGIJAS[3]

2024 m. III ketvirtis sukčiavimo srityje išsiskyrė itin didele sukčiams pervestų lėšų suma ir aiškiais sukčiavimo tipologijų skirtumais. Skirtingos sukčiavimo formos ir toliau paveikia daugybę Lietuvos gyventojų, o pervestų lėšų mastas rodo, kad sukčiai nuolat tobulina savo metodus, siekdami išvilioti vis didesnes pinigines lėšas.

[3] Susirašinėjimo el. paštu perėmimas (angl. Payment diversion fraud) – sukčiai įsilaužia į elektroninį susirašinėjimą tarp dviejų šalių ir sulaukę patogaus momento informuoja mokančią šalį apie pakeistą banko sąskaitą.

Investicinis sukčiavimas (angl. Investment fraud) – sukčiai įkalbinėja klientus investuoti į egzotiškus investavimo instrumentus, nors iš tikrųjų nėra jokio investavimo, klientai perveda pinigus į sukčių kontroliuojamas sąskaitas.

Romantinis sukčiavimas (angl. Romance fraud) – sukčiai susiranda potencialias aukas per pažinčių svetaines, socialinius tinklus ir pan., užmezga romantinius santykius ir ilgainiui įtikina aukas pervesti pinigus į jų kontroliuojamas sąskaitas.

Telefoninis sukčiavimas (angl. Telephone fraud) – sukčiai apsimeta banko darbuotojais, policininkais ir pan. ir įtikina aukas atskleisti el. banko prisijungimo duomenis, patvirtinti sukčių atliekamus pavedimus ir pan.

Phishing'as (suklastotas SMS arba el. laiškas) (angl. Phishing fraud) – sukčiai siunčia suklastotus el. laiškus ar SMS žinutes, kurios atrodo panašios į banko ar kitų institucijų, siekdami gauti el. banko prisijungimo duomenis, prašo patvirtinti sukčių atliekamus pavedimus, t. t.

Netikras įmonės vadovas (angl. Fake CEO fraud) – sukčiai apsimeta įmonės vadovais skambindami telefonu ar siųsdami suklastotus el. laiškus ir įtikina atsakingus asmenis atlikti pavedimus į sukčių sąskaitas.

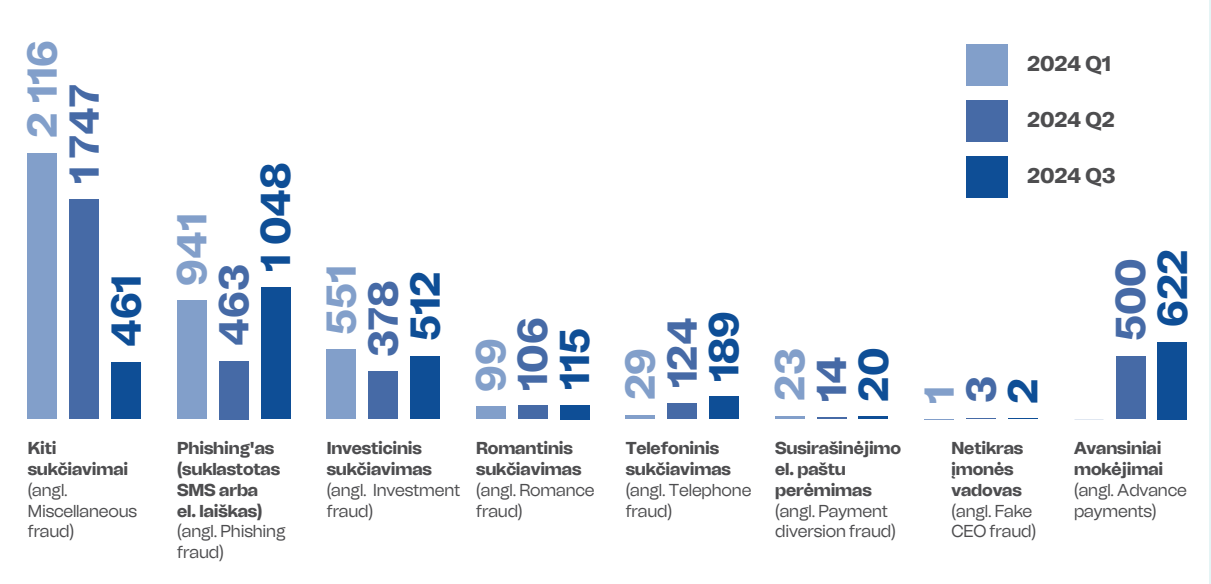
Avansiniai mokėjimai (angl. Advance payments) – mokėjimai pagal sukčių skelbimus internete apie neegzistuojančias prekes ar paslaugas, taip pat pateikiami fiktyvūs pavedimai už Booking / AirBnB platformų ribų ir pan.

Kiti sukčiavimai.

LYGINAMOJI ATASKAITA

Sukčiavimo tipologijos pagal incidentų skaičių, vnt.

2024 m. Q1 vs 2024 m. Q2 vs 2024 m. Q3



Analizuojant sukčiavimo mastą pagal pervestas lėšas, pastebima, kad kiekviena sukčiavimo tipologija pasižymi tiek specifiniu poveikiu gyventojams, tiek skirtingomis sukčių strategijomis. Pateikti duomenys įgalina mus geriau suprasti, kurios tipologijos yra pavojingiausios bei keliančios didžiausią žalą gyventojams. Taip pat pateikiama informacija gali padėti efektyviau kovoti su šiomis grėsmėmis.

Remiantis naujausiais duomenimis, 2024 m. liepos–rugsėjo mėnesiais dominuojantys sukčiavimo būdai, vertinant atvejų skaičių, buvo: *Phishing'as* (suklastotas SMS arba el. laiškas) (angl. Phishing fraud), kuris sudarė 1048 atvejus, ir „avansiniai mokėjimai" (angl. Advance payments), kurie sudarė 622 atvejus.

2024 m. Phishing'o sukčiavimo atvejų dinamika rodo reikšmingus svyravimus per pirmuosius tris metų ketvirčius. Q1 buvo fiksuota 941 Phishing'o incidentų, o Q2 šis skaičius ženkliai sumažėjo iki 463. Tačiau Q3 atakų skaičius smarkiai šoktelėjo iki 1048, grįždamas prie Q1 lygio ir net jį viršydamas.

Šių incidentų rodiklio didėjimą galėjo lemti tai, kad, nors gyventojų sąmoningumas ir operatorių blokavimo priemonės padėjo sumažinti incidentus 2024 m. Q2, sukčiai vėl prisitaikė prie situacijos, pradėjo taikyti naujus sukčiavimo būdus ir strategijas tam, kad apgautų vartotojus.

Nepaisant to, kad Phishing'o sukčiavimo atvejų dinamika rodo reikšmingus svyravimus, sukčiams pervestų lėšų suma per tris ketvirčius išliko gana panaši. 2024 m. Q2 sukčiams buvo pervesta daugiau nei 320 tūkst. Eur, Q2 išviliotų sumų mastas siekė apie 280 tūkst. Eur, o Q3 beveik 390 tūkst. Eur, atitinkamai vidutinė išviliota suma siekė apie 370 Eur.

Kaip ir minėta, 2024 m. III ketvirčio „avansinių mokėjimų" (angl. Advance payments) sukčiavimų statistika rodo reikšmingą padidėjimą tiek incidentų skaičiumi, tiek pervestų lėšų suma. Q3 pervestų lėšų suma sudarė daugiau nei 600 tūkst. Eur, o vidutinė išviliota suma siekė 990 Eur. Palyginimui, Q2 fiksuota 500 incidentų, o pervestų lėšų suma buvo apie 260 tūkst. Eur, atitinkamai vidutinė suma siekė 500 Eur. Padidėjęs interneto naudojimas, ypač sezoninių pirkimų ir atostogų metu, galėjo būti lemiamas veiksnys, turėjęs įtakos avansinio sukčiavimo atvejų skaičiaus augimui.

Centras primena, kad 2024 m. II ketvirtį „avansinių mokėjimų" tipologija buvo išskirta į savarankišką kategoriją, siekiant geriau suprasti ir identifikuoti šio tipo sukčiavimo mastą, užtikrinant tikslesnę prevenciją ir efektyvesnę kovą su šiuo sukčiavimo būdu.

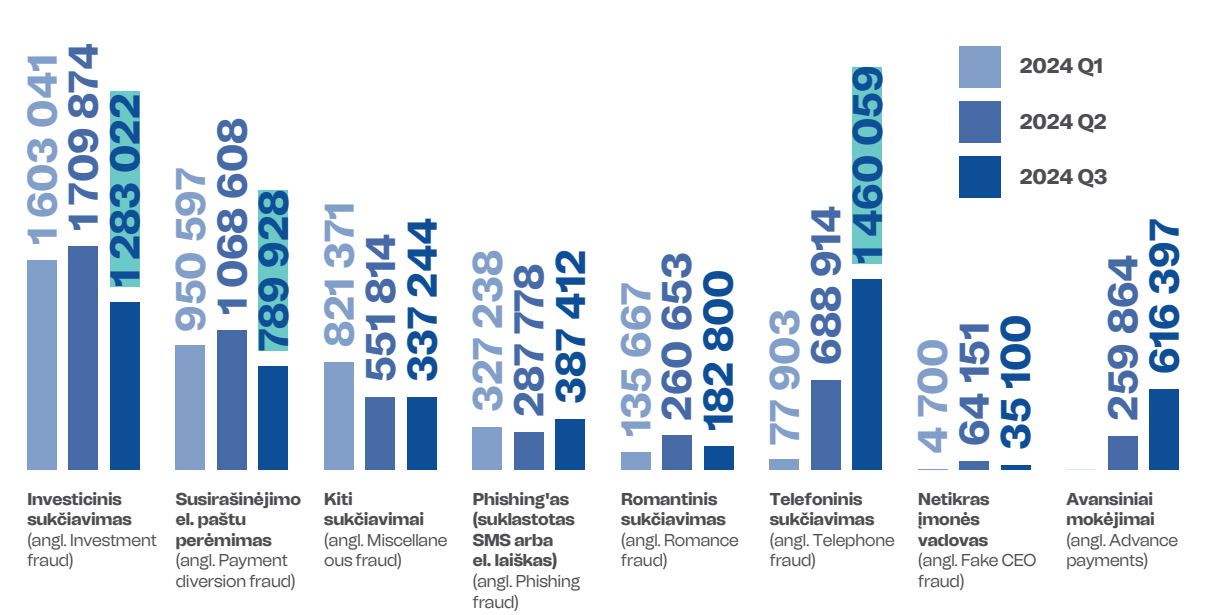
Ši sukčiavimo tipologija – tai sukčiavimo būdas, kai sukčiai deda į internetą skelbimus apie neegzistuojančias prekes ar paslaugas. Sukčiai už neegzistuojančią prekę ar paslaugą prašo mokėti avansu, tačiau prekė ar paslauga lieka nesuteikiama.

Siekiant išvengti tokio sukčiavimo, patariama labai gerai įvertinti gautus pasiūlymus, ypatingai tuos, kurie atrodo itin patrauklūs dėl kainos ir sąlygų, taip pat patariama nuodugniai tikrinti skelbimus, kalbėtis su paslaugos ar prekės teikėjais tiesiogiai, nenaudoti nepatikimų mokėjimo būdų ir vengti mokėti visą sumą iš anksto. Verta atsiminti, kad pasiūlymas, kuris skamba per gerai, kad būtų tiesa, greičiausiai toks ir nėra.

LYGINAMOJI ATASKAITA

Sukčiavimo tipologijos pagal iš gyventojų išviliotas lėšas, Eur

2024 m. Q1 vs 2024 m. Q2 vs 2024 m. Q3



Vertinant 2024 m. Q3 sukčiavimo tipologijas pagal sukčiams pervestas lėšas, matoma, kad telefoninis sukčiavimas, investicinis sukčiavimas ir susirašinėjimo el. paštu perėmimas buvo pavojingiausios sukčiavimo formos, kurių metu gyventojai ir įmonės patyrė didžiausius finansinius nuostolius.

Telefoninis sukčiavimas padarė didžiausią žalą, nes per užfiksuotus 189 incidentus sukčiams pavyko išvilioti daugiau nei 1,46 mln. Eur. Telefoninio sukčiavimo statistika ir intensyvios skirtingų institucijų pastangos perspėti visuomenę patvirtina prielaidą, kad seniai žinoma taisyklė – neatskleisti savo bankinių duomenų nepažįstamiems asmenims – yra pamiršta.

2024 m. II ketvirtį buvo užfiksuotas staigus telefoninio sukčiavimo atvejų šuolis: incidentų skaičius išaugo nuo 29 iki 124, o išviliotų lėšų suma – nuo 80 tūkst. iki 688 tūkst. eurų. Šis reiškinys buvo vadinamas telefoninio sukčiavimo „renesansu".

Nors sukčiavimo atvejai, nukreipti į juridinius asmenis, nėra itin dažni, tačiau išviliotų lėšų suma išlieka ženkli. „Susirašinėjimo el. paštu perėmimo" (angl. Payment Diversion) sukčiavimo būdu 2024 m. Q1 ir Q2 metu išviliotų lėšų suma sudarė apie 2 mln. Eur, t. y. po 1 mln. Eur per ketvirtį. 2024 m. Q3 išviliotų lėšų suma sumažėjo iki 790 tūkst. Eur, buvo užfiksuoti 20 atvejai, o vidutinė nuostolio suma vienam atvejui siekė 39,5 tūkst. Eur.

Palyginimui, Q1 fiksuoti 23 incidentai, įmonės sukčiams pervedė daugiau nei 950 tūkst. Eur, o vidutinis nuostolis vienam atvejui siekė 41 tūkst. Eur, Q2 incidentų skaičius sumažėjo iki 14, pervestų lėšų suma išaugo iki 1,06 mln. Eur, tuomet vidutinė nuostolio suma siekė 76 tūkst. Eur.

Šie duomenys atskleidžia, kad taikydami susirašinėjimo el. pašto perėmimo sukčiavimo schemą, sukčiai nuolat taikosi prie įmonių saugumo sistemų, kuria vis įtikinamesnius bei sudėtingesnius klastojimo būdus. Padidėję nuostoliai per Q2 rodo, kad sukčiavimo schemos tampa labiau orientuotos į didesnes sumas, o ne tik į atvejų skaičių. Toks dinamiškas pokyčių modelis pabrėžia, kad įmonių apsaugos sistemos ir mechanizmai turi būti nuolatos peržiūrimi ir stiprinami.

Nepaisant to, kad romantinio sukčiavimo atvejų skaičius ir toliau palaipsniui didėjo, vidutinė išviliota suma sumažėjo: 2024 m. Q2 vidutiniškai vienas incidentas sukėlė apie 2 450 Eur nuostolį, o 2024 m. Q3 – apie 1 600 Eur nuostolį.

Netikras įmonės vadovas (angl. Fake CEO fraud) – sukčiai apsimeta įmonės vadovais skambindami telefonu ar siųsdami suklastotus el. laiškus ir įtikina atsakingus asmenis atlikti pavedimus į sukčių turimas sąskaitas.

Netikras įmonės vadovas (angl. Fake CEO fraud) – sukčiavimo metodas, taikomas juridiniams asmenims. Sukčiai dažniausiai apsimeta aukštas pareigas įmonėje užimančiais asmenimis, dažniausiai vadovais, ir skubos tvarka nurodo pervesti dideles pinigų sumas į tam tikras „naujas" ar „neatidėliotinas" sąskaitas. Šio sukčiavimo metu naudojamos psichologinės manipuliacijos, pabrėžiant tariamą skubumą ir autoritetą, siekiant sumažinti tikimybę, kad finansų departamentas ar įmonės darbuotojai pastebės apgaulę.

Nors tokių incidentų skaičius yra santykinai mažas ir per 2024 m. III ketvirtį išliko nepakitęs, jų metu padaroma finansinė žala gali būti labai didelė. 2024 m. III ketvirtis rodo, kad net vos du incidentai galėjo lemti reikšmingą 35 100 Eur nuostolį (vidutiniškai išviliota suma siekė apie 17 tūkst. Eur). Tai rodo, kad sukčiai, pasitelkę netikro įmonės vadovo metodiką, sėkmingai taikosi į įmones, iš kurių, deja, sukčiams pasiseka išvilioti dideles sumas.

2024 m. III ketvirtį „kitų sukčiavimų" (angl. Miscellaneous fraud) kategorijoje buvo fiksuotas 461 incidentas, o pervestų lėšų suma siekė daugiau kaip 330 tūkst. Eur. Palyginus su ankstesniais metų ketvirčiais, šių incidentų skaičius reikšmingai sumažėjo (Q1 – buvo fiksuota net 2 116 atvejų, Q2 – 1 747 atvejai). Šis drastiškas sumažėjimas gali būti paaiškinamas tuo, kad didžioji dauguma atvejų, kurie anksčiau buvo priskiriami „kitiems sukčiavimams", nuo Q2 buvo perklasifikuoti į aiškesnes sukčiavimo kategorijas, pavyzdžiui, į „avansinius mokėjimus" ir kt. Taigi, „kiti sukčiavimai" nebeliko „nematomame lauke", nes teikiami duomenys yra geriau segmentuojami pagal sukčiavimo pobūdį.

Vidutinė suma, tenkanti vienam sukčiavimo incidentui 2024 m. Q3, siekė 731 Eur. Ši suma yra 231 Eur didesnė nei 2024 m. Q2, kai vidutinė išviliota suma sudarė 500 Eur. Pastebima, kad 2024 m. Q3 šio sukčiavimo incidentų skaičius sumažėjo, tačiau kiekvieno tokio atvejo patirta finansinė žala išaugo, nes sukčiai koncentravosi į mažesnį aukų skaičių, bet siekė išvilioti didesnes sumas.

Centras primena, kad sukčiai nuolat tobulina savo metodus, tapdami vis profesionalesni ir įtaigesni. Dažnai naudojamos emocinės manipuliacijos technikos, kai aukoms skambinama, apsimetant banko darbuotojais, teisėsaugos atstovais, „Google", „Meta" ar kt. autoritetingomis figūromis, siekiant sukurti pasitikėjimą arba sukelti skubos jausmą. Taip pat sukčiai vis geriau pritaiko technologines priemones, pavyzdžiui, skambina iš numerių, kurie atitinka tikrus institucijų numerius, taip sudarydami patikimumo įspūdį. Be to, gali būti naudojami dirbtinio intelekto įrankiai, siekiant imituoti balso toną arba manipuliuoti pokalbiais.

Policija, finansų įstaigos ir kitos valstybinės institucijos nuolat deda dideles pastangas, kad informuotų gyventojus apie įvairius sukčiavimo pavojus, susijusius su investicijomis, romantiniais santykiais ir kitais sukčių veiklos būdais, kurie gali apimti manipuliacijas internetu, pavyzdžiui: nuorodų siuntimą (phishingas) ir asmeninių duomenų ir PIN kodų atskleidimą.

Viešoje erdvėje nuolat girdimi perspėjimai, kad tokie skambučiai, kuriuose prašoma asmeninių duomenų, yra sukčiavimo schema, kuria yra siekiama išvilioti informaciją, gauti prieigą prie asmeninių banko sąskaitų ir jas ištuštinti.

! Atsižvelgdamas į tai, Centras dar kartą atkreipia dėmesį, kad valstybės institucijos, finansų įstaigos, policija tokios informacijos iš gyventojų niekada neprašo.

Nepaisant šių pastangų, sukčiavimo rodikliai ir toliau auga. Tai rodo, kad tiek visuomenės informavimo kampanijos, tiek finansinių institucijų apsaugos priemonės turi būti intensyvinamos arba turi būti ieškoma naujų efektyvių būdų didinti vartotojų atsparumą sukčiavimui. Svarbu kurti efektyvias prevencines priemones, kad būtų sumažintas gyventojų ir verslo subjektų pažeidžiamumas, apsaugojama nuo didėjančių finansinių nuostolių.

Išvados

- **Telefoninio sukčiavimo augimas:** telefoninis sukčiavimas tapo ypač pavojingas, su 189 incidentais ir nuostoliais, viršijančiais 1,46 mln. Eur. Šios tendencijos rodo, kad sukčiai sėkmingai manipuliuoja aukomis, o vidutinė prarasta suma per incidentą vienam gyventojui išaugo iki 7,7 tūkst. Eur.

- **Sukčiavimo incidentų mažėjimas:** 2024 m. III ketvirtį buvo fiksuoti 2 969 sukčiavimo atvejai. Tai rodo nuoseklų incidentų skaičiaus mažėjimą (21,06 proc. per tris ketvirčius). Tai taip pat gali būti vertinama kaip teigiama tendencija, rodanti efektyvesnes prevencijos priemones finansų sektoriuje.

- **Finansinių nuostolių augimas:** nors incidentų skaičius mažėja, gyventojų patirti finansiniai nuostoliai auga. Per pirmuosius tris metų ketvirčius nuostoliai išaugo daugiau nei 30 proc., pasiekė 4,8 mln. Eur. sumą Tai liudija, kad sukčiai tampa vis efektyvesni ir sugeba didinti vidutinę nuostolių sumą vienam gyventojui.

- **Prevencinių priemonių veiksmingumas:** 2024 m. III ketvirtį finansų institucijos sustabdė 3,8 mln. Eur, tai yra 11,8 proc. daugiau nei Q2 ir 31 proc. daugiau nei Q1. Tai rodo, kad finansų sektorius efektyviai reaguoja į grėsmes ir nuolat tobulina savo apsaugos sistemas.

- **Sukčiavimo tipologijų kaita:** 2024 m. Q3 dominuojantys sukčiavimo metodai yra phishing'as, avansiniai mokėjimai ir investicinis sukčiavimas. Phishing'o incidentų skaičius 2024 m. Q3 padidėjo iki 1048 (tai rodo didelį 126,3 proc. augimą 2024 m. Q2 ir 2024 m. Q3 laikotarpiu), o avansiniai mokėjimai šoktelėjo iki 622 atvejų (24,4 proc. didėjimas), investicinio sukčiavimo iki 512 (35,4 proc. augimą nuo Q2.). Šie duomenys atskleidžia sukčių prisitaikymą prie kintančių sąlygų ir liudija jų gebėjimą prisitaikyti, ir efektyviai reaguoti į taikomas saugumo priemones.

- **Investicinių sukčiavimų tendencijos:** investicinis sukčiavimas tapo didžiausią finansinę žalą sukeliančia sukčiavimo tipologija. Fiksuota 512 atvejų ir bendra prarastų lėšų suma siekė 1,3 mln. Eur. Sukčiai ir toliau taiko gerai pažįstamas manipuliavimo strategijas, siekdami užmegzti ilgalaikius santykius su aukomis.

2024 m. III ketvirtis atskleidė, kad sukčiai sėkmingai pritaiko įvairius metodus, siekdami didelio finansinio pelno, o svarbiausia, rizika kyla tiek gyventojams, tiek verslui. Šios sukčiavimo tipologijos padeda suprasti, kuriose srityse reikėtų stiprinti prevencines priemones bei gerinti visuomenės ir įmonių informuotumą apie galimus pavojus. Švietimas apie rizikas, susijusias su telefoniniais skambučiais, investicijomis ir el. paštu, yra būtinas, todėl Centras ir toliau didins vartotojų sąmoningumą apie sukčiavimo metodus, siekiant sumažinti aukų skaičių.

REKOMENDACIJOS GYVENTOJAMS

Gyventojai raginami būti atidūs užmezgant romantinius santykius socialiniuose tinkluose. Būtina suvokti rizikas, susijusias su romantiniu sukčiavimu. Svarbu būti atsargiam ir kritiškai vertinti internetinius pažinčių profilius, vengti greitai atskleisti asmeninę informaciją ar finansinius duomenis, taip pat kritiškai vertinti pernelyg skubotus ar emocionalius prašymus dėl pinigų pervedimo ar kitos pagalbos. Rekomenduojama pasitikrinti galimus partnerio duomenis ir ieškoti ženklų, kurie gali rodyti sukčiavimo pavojų.

Tikslinga ir toliau tęsti prevencinį visuomenės švietimą. Nuolat, pasitelkiant masinio informavimo priemones, supažindinti gyventojus su naujomis sukčiavimo tipologijomis. Taip pat svarbu priminti apie esamas sukčiavimo tipologijas, tendencijas ir sukčių taikomus metodus.

Darbas su tikslinėmis grupėmis bei nuolatinė informacijos sklaida skatins gyventojus būti sumanius ir išgirdus telefono ragelyje „Google" atstovu ar banko darbuotoju prisistatantį asmenį pasakyti „stop", nutraukti pokalbį. Tai sumažins sukčių galimybes pasisavinti gyventojų lėšas. Taip pat skatins gyventojus suklusti, būti įžvalgesniems ir nespausti neaiškių nuorodų ir taip apsaugoti savo asmens duomenis, prisijungimus prie elektroninės bankininkystės bei asmenines lėšas. Svarbus kritinis mąstymas gavus išskirtinį pasiūlymą „tik JUMS" užsiimti investavimo veikla (prekiauti valiutomis, tauriaisiais metalais, žaliavomis ir kita). Investiciniai sukčiai manipuliuoja noru greitai ir lengvai užsidirbti ir praturtėti esant labai mažai rizikai.

REKOMENDACIJOS JURIDINIAMS ASMENIMS

Centras atkreipia juridinių asmenų dėmesį į tai, kad organizacijos, siekdamos apsisaugoti nuo sukčiavimo atvejų, pavyzdžiui: „netikras vadovas" (angl. Fake CEO) ar „susirašinėjimo el. paštu perėmimas" (angl. Payment Diversion), turėtų darbuotojams organizuoti reguliarius mokymus apie dažniausiai pasitaikančius sukčiavimo būdus ir kaip juos atpažinti.

Įmonėms pravartu turėti parengtą veiksmų planą, kaip reaguoti į sukčiavimo atvejus. Siekdamos efektyvios prevencijos, bendrovės turėtų griežtinti vidines procedūras, kuriose būtų nustatytos aiškios taisyklės, kada ir kaip gali būti keičiami mokėjimų gavėjų banko duomenys. Be kita ko, rekomenduojama atlikti periodiškus mokėjimų auditus bei naujinti programinę įrangą ir operacines sistemas.

Bendraudami su klientais, įmonės darbuotojai turėtų išlaikyti atidumą, o prireikus – taikyti atsargumo priemones: tikrinti naujų tiekėjų ir klientų tapatybę bei jų kontaktinę informaciją, naudoti oficialius komunikacijos kanalus bei kreiptis į žinomus kontaktinius asmenis.

Ypatingai svarbu, kad prieš vykdydami stambius arba neįprastus mokėjus, juos atliekantys specialistai užtikrintų vadovo tapatybės patvirtinimą telefonu arba kitomis bendrovės naudojamomis identifikavimo priemonėmis, taip pat taikytų griežtas finansinių operacijų procedūras (dvigubas patvirtinimo procesas dideliems mokėjimams).

Be to, labai svarbu atkreipti dėmesį į tai, kad sukčiai vis dažniau pasitelkia dirbtiniu intelektu (angl. Artificial Intelligence) grįstas priemones tam, kad sukurtų įtikinamas, apgaulingas sukčiavimo schemas. Viena tokių taktikų – vadovo atvaizdo suklastojimas vaizdo skambučio metu, kai yra panaudojami dirbtiniu intelektu generuojami ir modifikuojami vaizdai ir balsai siekiant imituoti teisėtus įmonės atstovus. Tokiu būdu yra sukuriama patikimumo iliuzija, kuria siekiama lengviau manipuliuoti aukomis.

Dėl šių technologijų pažangos atsakingi įmonėse dirbantys asmenys turėtų imtis veiksmų, kad šviestų darbuotojus apie tai, kaip atpažinti tokius sukčiavimo atvejus ir užtikrinti, kad būtų taikomi griežti patvirtinimo procesai, pvz., naudojant antrąjį identifikavimo šaltinį ar kitus saugumo protokolus.

Minėtų priemonių taikymas padės apsaugoti juridinį asmenį nuo sukčiavimo ir lėšų praradimo bei užtikrins saugų finansinių operacijų vykdymą.