Pinigų plovimo prevencijos
kompetencijų centras

Sukčiavimo atvejų statistikos analizė

2024 m. II ketvirtis

2024 m.

2024 m. Q2 sukčiavimo atvejų statistikos analizė.

Pinigų plovimo prevencijos kompetencijų centro statistinių duomenų teikėjai

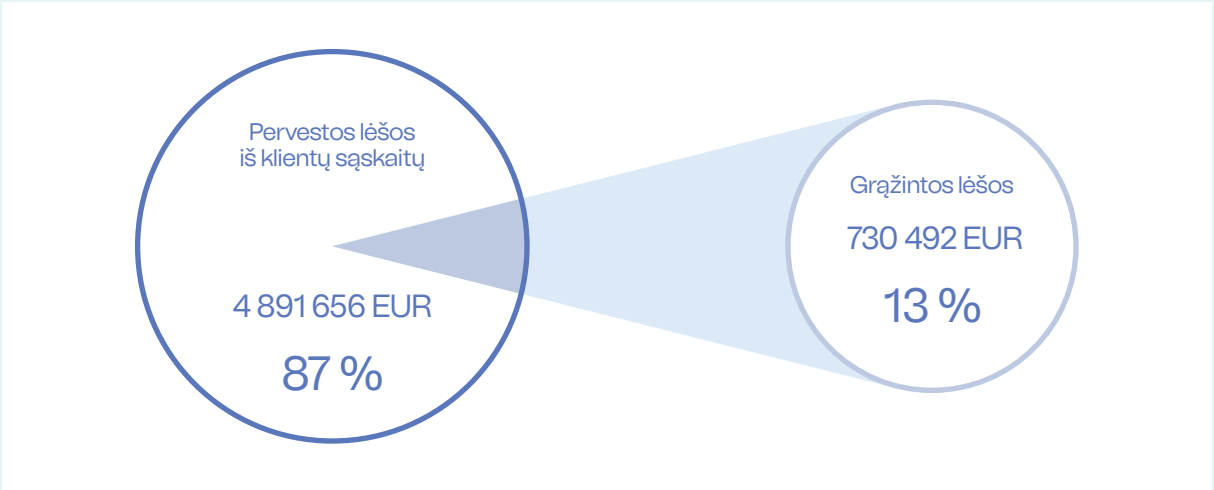
Pinigų plovimo prevencijos kompetencijų centras (toliau – PPPKC, Centras) pagal iš finansų įstaigų AB „Swedbank“, AB SEB banko, Revolut Bank, UAB, Luminor Bank AS Lietuvos skyriaus, AB Šiaulių banko, OP Corporate Bank plc. Lietuvos filialo, AS „Citadele banka“ Lietuvos filialo ir UAB URBO banko pateiktus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

2024 m. Q2 finansinių sukčių aktyvumas

PPPKC pateikti duomenys rodo, kad 2024 m. II ketvirtį finansų įstaigos užfiksavo 3 335 sukčiavimo incidentų[1]. Finansų įstaigų klientų sukčiams pervestų[2] lėšų suma siekė 4,8 mln. Eur, iš šios sumos finansų įstaigos gyventojams sugrąžino virš 730 tūkst. Eur. Remiantis šiais duomenimis, realūs gyventojų nuostoliai, t.y. klientų prarastos lėšos – 4,1 mln. Eur.

Sukčiavimo būdu realiai patirti GYVENTOJŲ nuostoliai – 4,1 mln. EUR

2024 m. Q2



Lyginant 2024 m. Q2 su 2024 m. Q1, šį ketvirtį sukčiavimo incidentų buvo fiksuota 11,3 proc. (425 atvejais) mažiau. 2024 m. Q2 fiksuota – 3335 sukčiavimo atvejų, o 2024 m. Q1 – 3760. Nors sukčiavimo atvejų skaičius šį ketvirtį buvo kiek mažesnis, tačiau finansų įstaigų klientų sukčiams pervestų lėšų suma buvo beveik 1 mln. Eur didesnė, nei 2024 m. Q1 – t.y. išaugo 5 proc.

[1] **Incidentų skaičius** (vnt.) – sukčiavimo atvejai (epizodai, ne sukčiavimo būdu inicijuotos pavienės operacijos), kuomet klientas esamomis autorizavimo priemonėmis pasirašė ir iniciavo 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

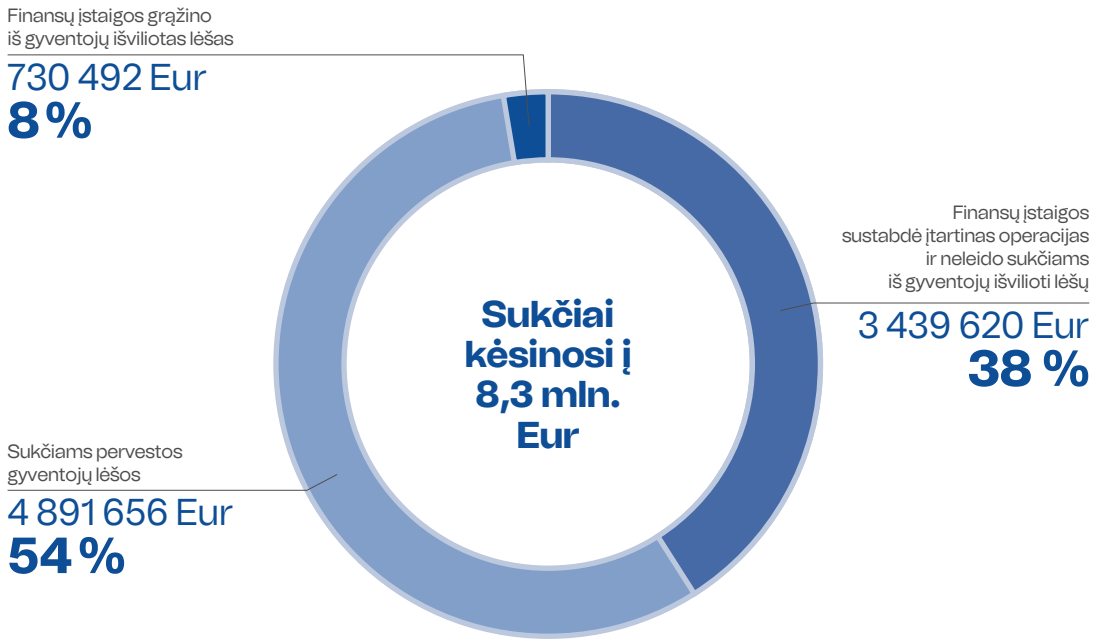
Sukčiavimo incidentų SKAIČIUS

2024 M. Q1 vs 2024 M. Q2

Finansų įstaigų taikomi proaktyvūs prevencijos veiksmai ir š.m. II ketvirtį padėjo apsaugoti šalies gyventojus ir įmonės nuo dar didesnių nuostolių – 2024 m. II ketv. sustabdyta 3,4 mln. Eur (17,2 proc. arba 500 tūkst. Eur daugiau nei 2024 m. Q2). Šios lėšos iš finansų įstaigų klientų sąskaitų neiškeliavo, nes buvo sustabdytos automatinių prevencijos sistemų bei prevencijos specialistų pastangomis.

Tokiu būdu buvo užkardyti sukčių nusikalstami veiksmai, kurie galėjo lemti daug didesnius nuostolius: bendra suma, kurią jie kėsinosi išvilioti, antrąjį šių metų ketvirtį siekė 8,3 mln. Eur – t.y. 1,5 mln. Eur daugiau nei 2024 m. Q1.

Kaip jau buvo minėta, šį ketvirtį finansų įstaigos gyventojams sugrąžino sukčiams jau pervestų 730 tūkst. Eur. Pastebima, jog lyginant su 2024 m. Q1, kuomet buvo sugrąžinta 221 tūkst. Eur, ši suma išaugo daugiau nei 3 kartus.



SUKČIAVIMAI PAGAL TIPOLOGIJAS[3]

Remiantis naujausiais duomenimis, 2024 m. balandžio – birželio mėnesiais, dominuojantys sukčiavimo būdai, vertinant atvejų skaičių, buvo: „Kiti" (Miscellaneous fraud) sukčiavimai, kurie sudarė 1 747 atvejus, ir naujai išskirta tipologija „Avansiniai mokėjimai" (Advance payments), kuri sudarė 500 atvejų, o išviliotų lėšų mastas sudarė beveik 260 tūkst. Eur, atitinkamai vidutinė suma siekė 500 Eur.

Atkreiptinas dėmesys, kad 2024 m. Q1 „Kiti" sukčiavimai, kurie nebuvo priskirti aiškiai apibrėžtoms tipologijoms, sudarė 2116 atvejų, tarp kurių ir sukčiavimo atvejai, kuomet už būsimą prekę ar paslaugą prašoma atlikti avansinį mokėjimą.

Siekiant statistinio tikslumo, 2024 m. II ketvirtį, finansų įstaigos išskyrė ir Centrui pradėjo teikti duomenis, apie atskirą sukčiavimo tipologiją – „Avansiniai mokėjimai".

Ši sukčiavimo tipologija – tai sukčiavimo būdas, kuomet sukčiai talpina skelbimus internete apie neegzistuojančias prekes ar paslaugas. Sukčiai už neegzistuojančią prekę ar paslaugą prašo mokėti avansu, tačiau prekė ar paslauga nesuteikiama.

Atskyrus „Avansinių mokėjimų" tipologiją į savarankišką kategoriją, siekiama geriau suprasti ir identifikuoti šio sukčiavimo mastą, užtikrinti tikslesnę prevenciją ir efektyvesnę kovą su šiuo sukčiavimo būdu.

2024 m. II ketvirtį kiti, aktyviausiai taikyti sukčiavimo būdai, kuriuos taikant agresyviais veiksmais kėsinamasi į gyventojų turtą, vertinant atvejus, išlieka tie patys, kaip ir ankstesniais laikotarpiais: *Phishing'as* (suklastotas SMS arba el. laiškas) ir investicinis sukčiavimas (Investment fraud).

Šie sukčiavimo būdai stebimu laikotarpiu buvo dominuojantys ir reikalaujantys daugiausiai dėmesio.

Viena vertus, taikant *Phishing'o* metodą, kuomet duomenis bandoma išvilioti per SMS žinutes ar el. nuorodas, gyventojai atakuojami vis dar intensyviai, ir šio tipo atvejų fiksuota virš 463, tačiau praėjusį ketvirtį fiksuota kone 2 kartus daugiau *Phishing'o* incidentų – 941 atvejų.

Šio rodiklio mažėjimą galėjo lemti keli faktoriai – vienas jų, jog gyventojai tapo atidesni, kitas – Lietuvos ryšio operatoriai blokavo SMS, kurios neatitiko su turinio siuntėjais suderintų identifikacinių požymių. Tačiau Centro nuomone, vertinti šiuos skaičius dar labai anksti, reikėtų palaukti III ir IV ketvirčio rezultatų, kurie aiškiau identifikuos, kaip kinta situacija.

Phishing'o būdu išviliotų lėšų suma 2024 m. Q2 siekė 287 tūkst. Eur, taigi vidutinė išviliota suma – atitinkamai 621 Eur, kai praėjusį ketvirtį išviliotų lėšų suma siekė 320 tūkst. Eur, o vidutinė išviliota suma – 355 Eur. Taigi nors atvejų sumažėjo, tačiau vidutinė išviliota suma ūgtelėjo.

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

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

Romantinis sukčiavimas (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 (Telephone fraud) –Sukčiai apsimeta banko darbuotojais, policininkai ir pan. ir įtikina aukas atskleisti el.banko prisijungimo duomenus, patvirtinti sukčių atliekamus pavedimus ir pan.

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

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

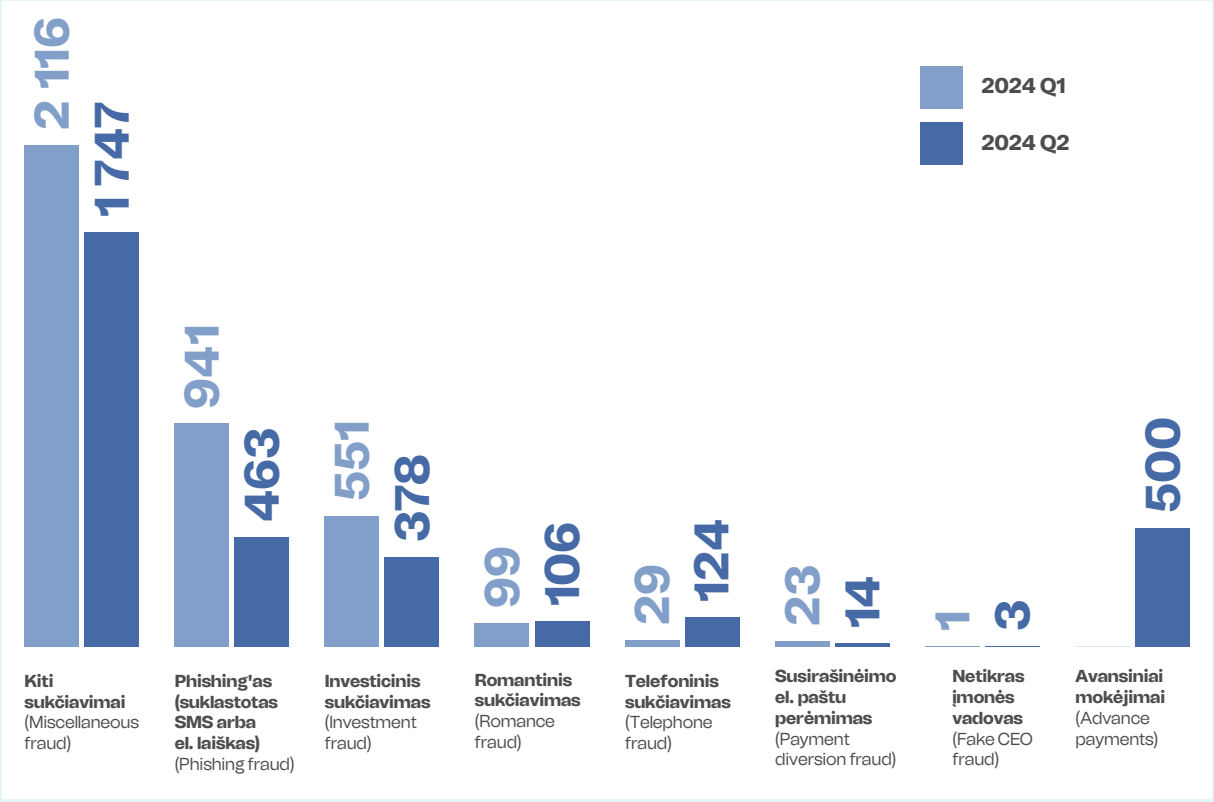
Avansiniai mokėjimai (Advance payments) – mokėjimai pagal sukčių skelbimus internete apie neegzistuojančias prekes ar paslaugas, taip pat pavedimai už Booking/AirBnB platformų ribų ir pan.

Kiti sukčiavimai.

LYGINAMOJI ATASKAITA

Sukčiavimo tipologijos pagal incidentų skaičių, vnt.

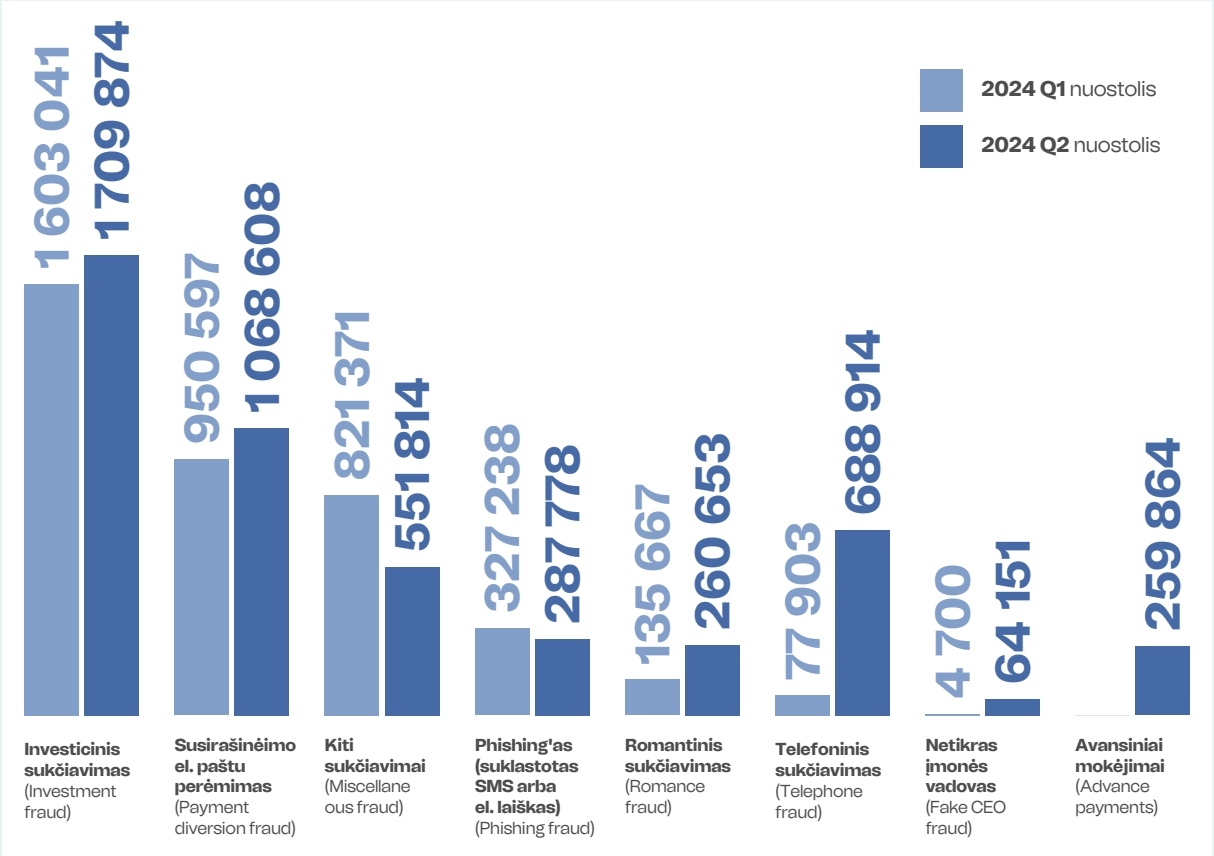
2024 M. Q1 vs 2024 M. Q2



LYGINAMOJI ATASKAITA

Sukčiavimo tipologijos pagal iš gyventojų išviliotas lėšas, Eur

2024 M. Q1 vs 2024 M. Q2



Nors ir investicinio sukčiavimo atvejų 2024 m. Q2 ketvirtį fiksuota mažiau – 378 atvejai, tačiau atkreiptinas dėmesys, kad investicinis sukčiavimas tarp visų sukčiavimo tipologijų, vertinant mastą pagal išviliotas lėšas, ir toliau sudaro didžiausią patirtą gyventojų nuostolį.

Mastas, skaičiuojant investicinio sukčiavimo būdu išviliotas lėšas, auga: per minėtą laikotarpį iš gyventojų išviliota net 1,7 mln. Eur, o vidutinė išviliota suma sudarė daugiau nei 4 500 Eur, tuo tarpu 2024 m. Q1 fiksuota 551 atvejis, kai iš gyventojų buvo išviliota net 1,6 mln., vidutiniškai 3 200 Eur vienam gyventojui.

Investicinio sukčiavimo schema visada reikalaus daug laiko, sukčių įdirbio išlaikant „aukos" dėmesį.

Vadinamas „investavimas" dažniausiai prasideda nuo mažos sumos, nuo aukos ir sukčiaus santykių ir pasitikėjimo kūrimo. Auka sulaukia netikėto „investicijų eksperto" skambučio, kuris vėliau atsiunčia nuorodą į „investavimo platformą", joje matomi grafikai. Grafikuose vaizduojama, kaip investicijos neva augs ir generuos neįtikėtinai didelį pelną.

Tik per ilgesnį laiką, kuris gali trukti ir kelis mėnesius (tai visada priklauso nuo aukos elgesio, finansinio statuso ar galimybių gauti pinigines lėšas), auka pradės investuoti daugiau. Tik po tam tikro laiko tariamos „investicijos" ženkliai padidėja ir padažnėja, auka jau pasitiki savo „finansų konsultantu" – sukčiumi, tampa „bičiuliais".

Aukos pradeda „investuoti" vis daugiau ir daugiau pinigų, o jei lėšų nebeturi, sukčiai, naudodami psichologinį spaudimą, ragina aukas pasiimti greitąjį kreditą ar pasiskolinti lėšų iš giminaičių ar pažįstamų žmonių.

Sukčius tiek užvaldo auką, manipuliuoja ja, naudoja psichologinį spaudimą, kad auka pradeda slėpti nuo artimųjų lėšų poreikį investicijoms, taip pat slepia savo „sėkmę" nuo artimos aplinkos, o finansų įstaigoms pradėjus teirautis apie neįprastas operacijas, sukčių pamokyta, auka neatskleidžia visos tiesos apie bankinių pavedimų paskirtį, nes jau yra įtikinta sukčių apie milžinišką finansinę grąžą, didelius turtus, o finansų įstaigos įvardijamos kaip nepatikimos.

Po „sėkmingo investavimo" lėšų susigrąžinti nebepavyksta, kadangi paprašius išmokėti lėšas „finansų ekspertai" staiga pradingsta. Tačiau sukčiams pradingus, atsiranda tariamieji „gelbėtojai", kurie puikiai žinodami situaciją, susisiekia su auka, prisistato policijos ar kitos institucijos atstovais ir nurodo, kad gali pagelbėti susigrąžinti lėšas ar kad sukčiai yra sulaikyti, tačiau reikia „tik" susimokėti papildomus „administracinius" mokesčius. Gavus „administracinius mokesčius" tokie „gelbėtojai" dingsta. Tokiu būdu išviliojamos ženkliai didesnės sumos.

Antroje vietoje pagal išviliotas lėšas – „Susirašinėjimo el. paštu perėmimas" (Payment Diversion). 2024 m. Q1 ir Q2 išviliotų lėšų suma sudarė apie 2 mln. Eur, t.y. po 1 mln. Eur per ketvirtį. Sukčiai, pasitelkę šį sukčiavimo metodą, atakuoja juridinius asmenis. Jiems pateikiamos suklastotos sąskaitos – faktūros arba „verslo partneriai" nurodo „naujas sąskaitas" skubiems pavedimams. Šis sukčiavimo būdas, kaip ir „Netikras įmonės vadovas" (Fake CEO), yra dažniausiai taikomi metodai juridinių asmenų atžvilgiu.

Nors, atvejai, kai sukčiai kėsinasi į juridinį asmenį nėra dažni – 2024 m. Q2 fiksuoti 17 atvejų (3 iš jų – „Netikras įmonės vadovas" ir 14 – „Susirašinėjimo el. paštu perėmimas"), o 2024 m. Q1 – 24 atvejai, t.y. 7 atvejais daugiau nei šį ketvirtį, tačiau išviliotų lėšų suma yra ženkli.

2024 m. Q2 sukčiai iš bendrovių, taikant abi „Susirašinėjimo el. paštu perėmimo" ir „Netikras įmonės vadovo" schemas, kartu sudėjus vidutiniškai išviliojo 66 tūkst. Eur, o 2024 m. Q1 vidutiniškai, iš vieno juridinio asmens, išviliota daugiau kaip 39 tūkst. Eur.

Apgaule užvaldyti juridinio asmens lėšas nėra spontaniškas sukčiavimas – tai yra specifinis metodas, reikalaujantis laiko ir įžvalgų, kadangi sukčiai, prieš pasikėsindami į juridinio asmens finansus, turi išanalizuoti bendrovės struktūrą, procesus, susipažinti su vidine korespondencija, siekia išsiaiškinti įmonės vadovo bendravimo stilių. Ir kai tik sukčiai perpranta bendrovės modelį, struktūrą, pasirūpina, kad apgaulingi laiškai ir bendravimas su atsakingais asmenimis būtų kuo tikroviškesni ir tokiu savo elgesiu paskatina auką pervesti įmonės lėšas į neva patikimo partnerio ar vadovo banko sąskaitą arba imituoja įmonės vadovo „nurodymus".

Š.m. antrąjį ketvirtį fiksuotas telefoninio sukčiavimo „renesansas“. 2024 m. II ketvirčio duomenys rodo, jog telefoninio sukčiavimo atvejai šoko iki 124 incidentų, o išviliotų lėšų suma sudarė net 688 tūkst. Eur., tai vidutiniškai sudarė virš 5,5 tūkst. Eur per atvejį, kai tuo tarpu 2024 m. Q1 incidentų skaičius sudarė 29, o išviliotų lėšų suma sudarė apie 80 tūkst., o vidutinė suma sudarė 2,6 tūkst. Eur.

Tai yra ženklus šio ketvirčio išviliotų lėšų šuolis ir signalizuoja, kad sukčiai yra labai aktyvūs ir naudoja seniai visiems žinomas sukčiavimo schemas.

Šį sezoną gyventojai sulaukė skambučių iš neva „Google“, „Meta“, bankų arba policijos atstovų, kurie iš gyventojų išviliojo interneto banko prisijungimo duomenis. Naudojant šį sukčiavimo metodą, sukčiai įtikino aukas atiduoti jiems savo prieigas prie banko sąskaitų, bankines korteles ir prisijungimus ir net įsidrąsino atvykti į aukos namus jų paimti – tokiu būdu gyventojai prarado asmenines lėšas.

Centras, balandžio mėn. sulaukęs informacijos apie šį sukčiavimo būdą iš finansų įstaigų, nedelsiant informavo visuomenę apie sukčius ir jų skambučius. Aktyviai apie šį sukčiavimo metodą nuolat perspėja tiek policija, tiek finansų įstaigos, tačiau akivaizdu, kad nepaisant visų pastangų, nukentėjusiųjų yra labai daug, o išviliotų lėšų skaičiai nepalieka abejingų.

Tiek statistiniai telefoninio sukčiavimo augimą atskleidžiantys rodikliai, tiek intensyvios skirtingų institucijų pastangos perspėti visuomenę apie šį sukčiavimo būdą, patvirtinta, kad gerokai primiršta, atrodė, jau išmokta, taisyklė – neatskleisti savo bankinių duomenų skambinantiems asmenims, kurie apsimesdami valstybės institucijų, bankų darbuotojais, bendrauja išskirtinai tik rusų kalba, mėgina su pašnekovu užmegzti kontaktą ir manipuliuodami jautriomis detalėmis bando išvilioti asmens mokėjimo duomenis.

Policija, finansų įstaigos ir kitos valstybinės institucijos deda daug pastangų ir nuolat perspėja gyventojus, kad bankinių prisijungimo duomenų, PIN kodų niekam negalima atskleisti ar perduoti, kad tokio skambučio motyvas – išvilioti duomenis, gauti asmens mokėjimo kortelę su slaptažodžiais, užvaldyti banko sąskaitas ir jas ištuštinti.

! Atsižvelgiant į tai, Centras dar kartą atkreipia dėmesį ir pabrėžia, jog valstybės institucijos, finansų įstaigos, policija tokios informacijos iš gyventojų niekada neprašo.

2024 m. II ketvirtį taip pat vertintos romantinio sukčiavimo, su kuriuo susiduria gyventojai, kitimo tendencijos. Deja, lyginant š.m. Q1 ir Q2, stebimas tiek atvejų, tiek išviliotų lėšų augimas: fiksuoti 106 atvejai (2024 m. Q1 – 99 atvejai), tačiau išviliotų lėšų mastas šoko drastiškai – 2 kartus ir 2024 m. Q2 sudarė daugiau kaip 260 tūkst., kai 2024 m. Q1 išviliotų lėšų suma sudarė apie 135 tūkst. Eur.

Romantinių sukčių metodika išlieka ta pati: pastarieji susikuria netikras anketas su netikromis nuotraukomis, „liūdnomis“ ir netikromis istorijomis, taikosi į 40–70 metų amžiaus moterų ir vyrų grupes, kurie yra vieniši ir tikisi sutikti turtingą, empatišką gyvenimo draugą.

Sukčių sukurtos istorijos yra tipinės, turinčios kelis scenarijus, tačiau visos priverčia aukas pasijausti reikalingas, mylimas. Aukos apipilamos pažadais, nušviečiama šviesi ir laiminga ateitis su pasiturinčiu Amerikos kilmės kariškiu, turtingu našliu ar našle, ar kt. išgalvota asmenybe. Sukčiai įžvelgia aukų geranoriškumą, dosnumą, priverčia aukas susižavėti jais ir manipuliuodami išvilioja iš gyventojų nemenkas sumas.

Išvados

- **Finansiniai sukčiai iš Lietuvos gyventojų ir įmonių antrąjį šių metų ketvirtį kėsinosi išvilioti 8,3 mln. Eur – t.y. 1,5 mln. Eur daugiau nei 2024 m. Q1. Eur. Tačiau finansų įstaigų dėka dalies sukčiavimo atvejų sukeliamų finansinių nuostolių buvo išvengta, kai finansų įstaigos 2024 m. Q2 sustabdė daugiau kaip 3,4 mln. Eur. Taip pat, finansų įstaigoms pavyko grąžinti klientams sukčių išviliotas pinigines lėšas, kurių suma siekė virš 730 tūkst. Eur., t.y. 3 kartus daugiau nei 2024 m. Q1.**

- **2024 m. II ketvirtį finansų įstaigoms pavyko sustabdyti 38 proc. sukčiavimo metu bandytų išvilioti lėšų, tačiau bendras antrojo ketvirčio incidentų skaičius, nors ir mažesnis nei praėjusį ketvirtį, išliko aukštas ir siekė 3335 fiksuotų atvejų rodiklį. Finansų įstaigų klientų realūs nuostoliai augo ir sudarė daugiau kaip 4,1 mln. Eur, kai praėjusį ketvirtį užfiksuota 3760 sukčiavimo incidentų, o realūs nuostoliai siekė 3,7 mln. Eur.**

- **Nustatyta, kad 2024 m. dominuojantys sukčiavimo būdai, vertinant atvejų skaičių, išlieka suklastotas SMS arba el. laiškas (Phishing fraud) ir investicinis sukčiavimas bei naujai atskira sukčiavimo tipologija „Avansiniai mokėjimai“.**

- **Vertinant tipologijas pagal išviliotas lėšas – investicinis sukčiavimas ir „Susirašinėjimo el. paštu perėmimas“ (Payment diversion fraud).**

- **2024 m. Q2 užfiksuotas ženklus telefoninio sukčiavimo atvejų šuolis. Šis sukčiavimas vėl tapo populiarus prasidėjus „Google“ atstovais apsimetančių sukčių skambučių bangai. Incidentų skaičius sudarė net 124 atvejus, o išviliotų lėšų suma sudarė daugiau kaip 688 tūkst. Eur, kai atitinkamai 2024 m. Q1 incidentų skaičius sudarė 29, o išviliotų lėšų suma siekė apie 80 tūkst. Eur.**

REKOMENDACIJOS GYVENTOJAMS

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 prisistatančiu asmeniu pasakyti „Stop", nutraukti pokalbį. Tai sumažins sukčių galimybes nusavinti gyventojų lėšas. Taip pat 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.

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, o taip pat būti 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.

REKOMENDACIJOS JURIDINIAMS ASMENIMS

Centras atkreipia juridinių asmenų dėmesį į tai, kad organizacijos, siekdamos apsisaugoti nuo sukčiavimo atvejų, tokių kaip „Netikras vadovas" (Fake CEO) ar „Susirašinėjimo el. paštu perėmimas" (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, jog prieš vykdant stambius arba neįprastus mokėjus, juos atliekantys specialistai užtikrintų vadovo tapatybės patvirtinimą telefonu ar kitomis bendrovės naudojamomis identifikavimo priemonėmis, o taip pat taikytų griežtas finansinių operacijų procedūras (dvigubas patvirtinimo procesas dideliems mokėjimams).

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