Pinigų plovimo prevencijos
kompetencijų centras

Sukčiavimo atvejų statistikos analizė

2024 m. IV ketvirtis

2024 m.

2024 m. Q4 sukčiavimo atvejų statistikos analizė

Pinigų plovimo prevencijos kompetencijų centro statistinių duomenų teikėjai

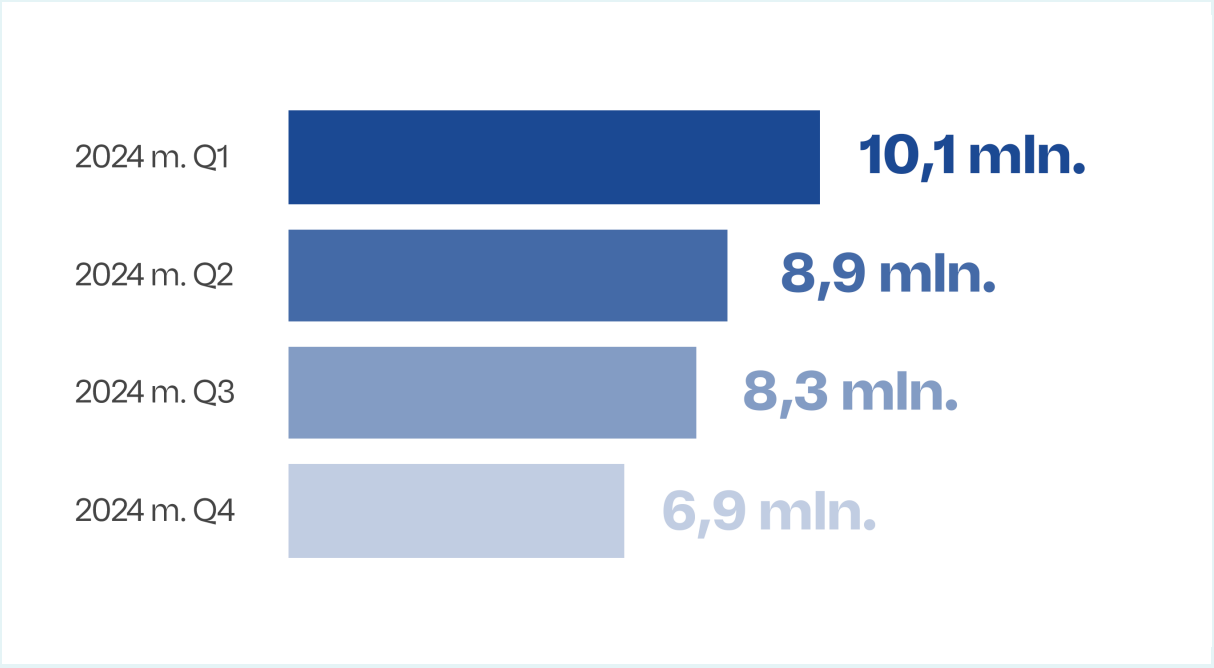
Pinigų plovimo prevencijos kompetencijos centras (toliau – PPPKC, Centras) pagal iš finansų įstaigų AB „Swedbank", Revolut Bank, AB SEB banko, UAB, Luminor Bank AS Lietuvos skyriaus, AB Šiaulių banko, OP Corporate Bank plc. Lietuvos filialo, AS „Citadele bankas" Lietuvos filialo ir UAB URBO banko pateiktus duomenis atliko 2024 m. IV ketvirčio (toliau – 2024 m. Q4, 2024 m. IV ketvirtis) sukčiavimo atvejų statistikos analizę.

2024 m. finansinių sukčių aktyvumas

PPPKC pateikti duomenys rodo, kad sukčių atakos tampa vis intensyvesnės ir pavojingesnės. Pirmąjį 2024 m. ketvirtį sukčiai kėsinosi išvilioti 6,9 mln. Eur, o antrąjį ketvirtį ši suma išaugo 20,1 proc. punktais, pasiekdama 8,3 mln. Eur. Trečiąjį ketvirtį sukčių atakos dar labiau sustiprėjo, bendra sukčių siekiama išvilioti suma pasiekė 8,9 mln. Eur. Tai atitinka 7,2 proc. punkto padidėjimą. Q4 ši suma perkopė Q3 ir siekė net 10,1 mln. Eur, o tai reiškia 13,5 proc. punkto augimą, palyginti su trečiuoju ketvirčiu.

Finansiniai sukčiai 2024 m. iš gyventojų ir įmonių siekė išvilioti 35 mln. Eur

2024 m. Q1 vs 2024 m. Q2 vs 2024 m. Q3 vs 2024 m. Q4



Apibendrinant 2024 m. IV ketvirtį, finansiniai sukčiai kėsinosi į 10,1 mln. Eur. Finansų įstaigos, taikydamos efektyvius prevencinius veiksmus, sustabdė ir neleido sukčiams pervesti beveik 4,8 mln. Eur.

Finansų įstaigos užfiksavo 3 627 sukčiavimo incidentus[1] , o sukčiams pervestų[2] lėšų suma viršijo 6,1 mln. Eur, iš šios sumos finansų įstaigos gyventojams sugrąžino virš 1,5 mln. eurų. Remiantis šiais duomenimis, realūs gyventojų nuostoliai, t. y. klientų prarastos lėšos – 4,6 mln. Eur.

Per visus 2024 m. ketvirčius, sukčiavimo atvejų skaičius svyravo. Q1 buvo fiksuota 3760 atvejų, Q2 – 3335, Q3 – 2969, ir Q4 – 3627. Nors pirmieji trys ketvirčiai parodė mažėjimo tendenciją, Q4 parodė aiškų incidentų šuolį – Q4 fiksuotas 22,2 proc. punktais didesnis sukčiavimo incidentų skaičius nei Q3 laikotarpiu.

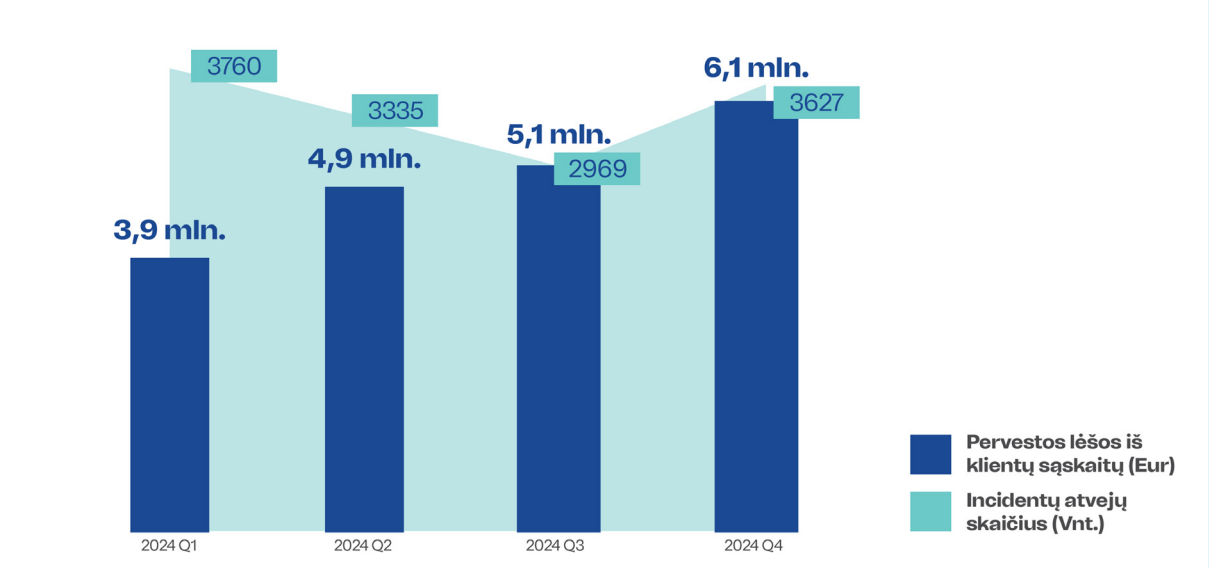
Šis augimas gali būti susijęs su sezoniniais pokyčiais, kadangi Q4 sutampa su šventiniu laikotarpiu, kuomet padidėja vartotojų aktyvumas, sukuriantis palankesnes sąlygas sukčiavimo veiksmams. Taip pat svarbu atkreipti dėmesį į technologinius veiksnius ir naujai atsirandančius sukčiavimo metodus, kurie galėjo lemti incidentų skaičiaus augimą.

Taigi, nors sezoniniai faktoriai turi reikšmės, vertėtų nepamiršti ir kovos su sukčiavimu fronte atsirandančių naujovių – sukčiai ne tik seka vartotojų įpročius, bet ir nuolat tobulina savo metodus. Todėl visuomenės švietimas ir prevencijos priemonės tampa ypatingai svarbios kovoje su nuolat kintančiais sukčiavimo būdais.

Svarbu paminėti, kad Q4 ketvirtį fiksuotas ne tik incidentų skaičiaus didėjimas, bet ir nuoseklus sukčiams pervestų lėšų augimas.

2024 m. Sukčiavimo atvejų statistika

Pervestos lėšos iš klientų sąskaitų (EUR), lyginant su incidentų atvejų skaičiumi



Augimas, stebimas nuo 3,9 mln. Eur per Q1 iki daugiau nei 6,1 mln. Eur per Q4, rodo 56,4 proc. punktų augimą. Tai žymiai viršija ankstesnį augimą tarp Q2 ir Q3, kuris sudarė tik 6,3 proc. Dramatiškas lėšų pervedimo augimas per Q4 gali būti susijęs su sukčių naudojamais sudėtingesniais apgaulės metodais, didesniu vartotojų aktyvumu bei galimu didesniu įsitraukimu į internetinę prekybą šventiniu laikotarpiu.

[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.

Be to, didėjanti lėšų pervedimo suma rodo ne tik augantį sukčių aktyvumą, bet ir didėjantį gyventojų pasitikėjimą elektroninėmis paslaugomis. Šią situaciją galėjo lemti sukčių prisitaikymas prie rinkos pokyčių ir gyventojų finansinių galimybių, pavyzdžiui, didesnių disponuojamų pajamų, lengvesnės prieigos prie kreditavimo, didėjančio įsitraukimo į investavimo bei elektroninės prekybos platformas.

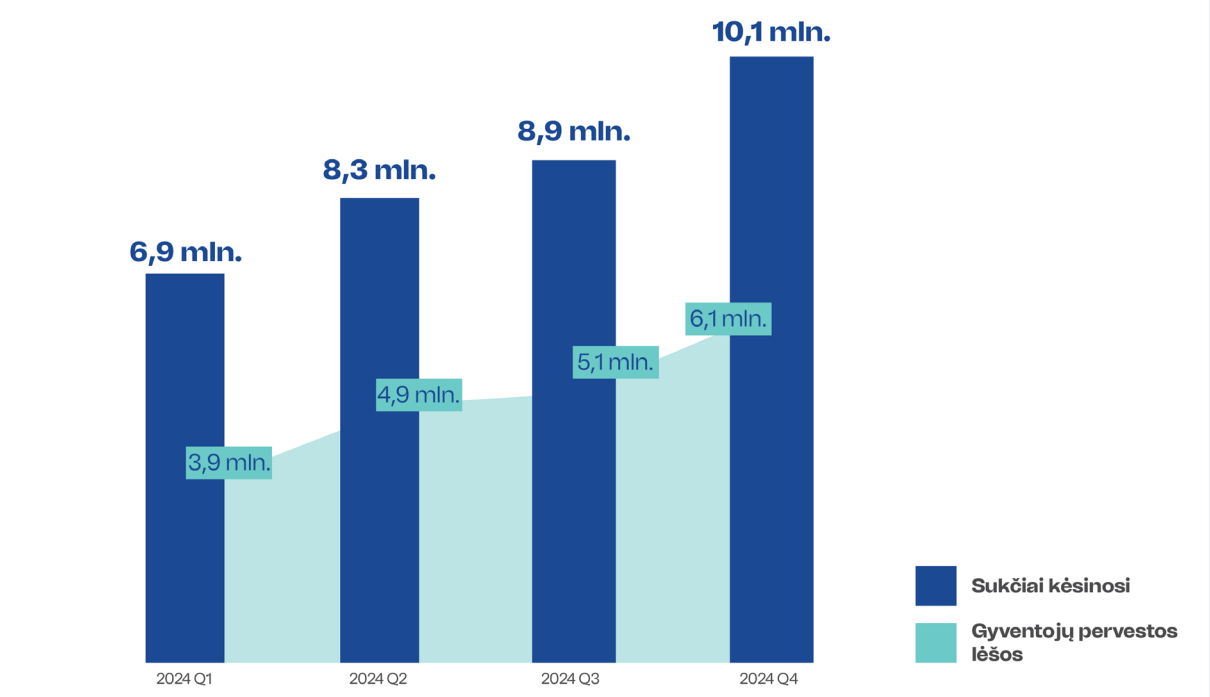
Dėl šių priežasčių, nepaisant incidentų skaičiaus mažėjimo pirmuosius tris ketvirčius, gyventojai vis dėlto patyrė didesnius finansinius nuostolius – tai indikuoja, kad sukčiai per metus sugebėjo pasiekti savo tikslus ir išnaudoti situaciją savo naudai.

Vis dėlto, nepaisant sukčių atakų, pažymėtina, jog finansų įstaigos toliau sėkmingai vykdė prevencinius veiksmus ir apsaugojo šalies gyventojus ir įmones nuo reikšmingų finansinių nuostolių.

Didėjantis sustabdytų lėšų skaičius indikuoja automatizuotų prevencijos sistemų efektyvumą ir greitą specialistų reagavimą į įtartinus sandorius: 2024 m. III ketvirtį buvo sustabdytos 3,8 mln. Eur suma – tai 11,8 proc. punktais daugiau nei antrąjį ketvirtį (kai buvo sustabdyta 3,4 mln. Eur) ir net 31 proc. punktais daugiau nei pirmąjį metų ketvirtį, kuomet buvo sustabdyta 2,9 mln. Eur suma. Q4 metu finansų įstaigos sustabdė 4,8 mln. Eur, o tai yra 26,3 proc. punktų augimas, lyginant su Q3 laikotarpiu.

2024 m. Sukčiavimo atvejų statistika

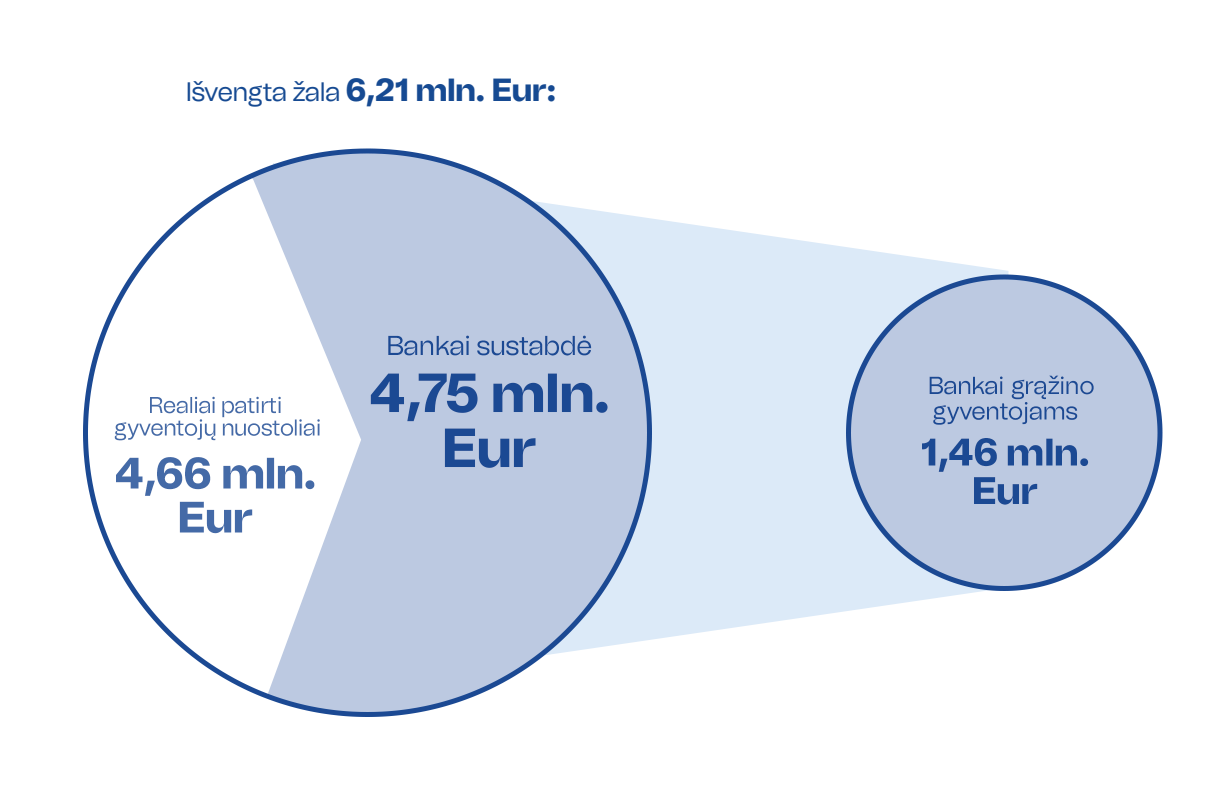
Finansiniai sukčiai pasikėsino į daugiau nei 35 mln. Eur, o gyventojų sukčiams pervestų lėšų suma viršijo 20 mln. Eur



2024 m. finansų įstaigų gyventojams sugrąžintų sukčiams pervestų lėšų rodiklis parodė kintančią dinamiką. Per pirmąjį ketvirtį finansų įstaigoms pavyko grąžinti 221 tūkst. Eur, Q2 šis skaičius išaugo ir viršijo 730 tūkst. Eur, Q3 grąžintų lėšų suma, lyginant su Q2, reikšmingai sumažėjo iki 241 tūkst. Eur, tačiau Q4 vėl buvo fiksuotas didelis sugrąžintų lėšų augimas, siekęs kone 1,5 mln. Eur.

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

Apibendrinant 2024 m. Q4 pervestų lėšų, finansų įstaigų sustabdytų lėšų ir grąžintų gyventojams lėšų rodiklius: sukčiai ketvirtąjį ketvirtį pasikėsino išvilioti net 10,1 mln. Eur, tačiau taikant sėkmingas prevencines priemones finansų įstaigoms pavyko gyventojams sugrąžinti daugiau nei 1,5 mln. Eur bei sustabdyti ir neleisti sukčiams įsisavinti beveik 4,8 mln. Eur. Tokiu būdu 2024 m. Q4 finansų įstaigos sumažino 52,5 proc. punktais realius gyventojų nuostolius nuo 10,1 mln. Eur iki 4,8 mln. Eur.



Iš viso 2024 m. finansiniai sukčiai pasikėsino į daugiau nei 35 mln. eurų, o sukčiavimo mastai išliko reikšminga grėsme tiek gyventojams, tiek verslui.

Praėjusiais metais gyventojų sukčiams pervestų lėšų suma viršijo 20 mln. eurų, tačiau finansų įstaigų prevenciniai veiksmai ir operatyvūs sprendimai leido sugrąžinti daugiau nei 2,6 mln. eurų. Dėl to realiai patirti gyventojų nuostoliai sumažėjo iki 17,3 mln. eurų. Tai rodo stiprėjančią finansų įstaigų kovą su sukčiavimu ir jų gebėjimą apsaugoti klientų lėšas.

Teigiama tendencija pastebima ir kalbant apie išvengtą žalą. Skaičiuojama, kad per 2024 m. finansų įstaigos sustabdė neteisėtus pervedimus, kurių vertė siekė 17,6 mln. eurų. Tai reiškia, kad pavyko išvengti daugiau nei pusės potencialiai prarastų lėšų. Šie rezultatai pabrėžia didėjantį dėmesį sukčiavimo prevencijai, gerėjančią institucijų tarpusavio sąveiką ir augantį visuomenės sąmoningumą apie finansinius nusikaltimus.

Nepaisant šių teigiamų pokyčių, sukčiavimo atvejų skaičius ir neblėstantis sukčių išradingumas išlieka iššūkiu, todėl būtina toliau stiprinti prevencines priemones, finansų įstaigų ir teisėsaugos institucijų bendradarbiavimą, bei tęsti visuomenės švietimą apie finansinio sukčiavimo grėsmes.

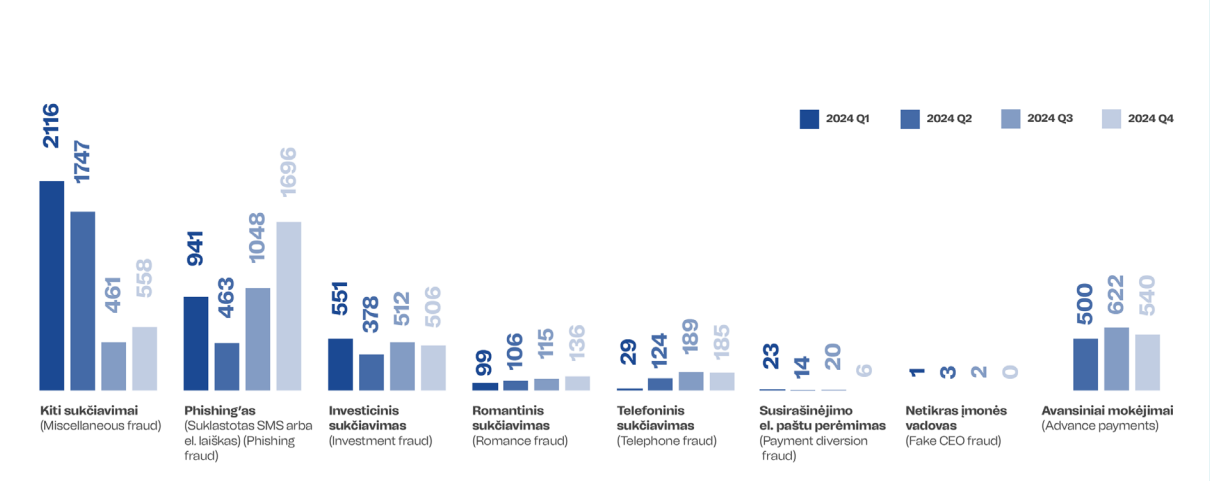
SUKČIAVIMAI PAGAL TIPOLOGIJAS[3]

2024 m. IV ketvirtis sukčiavimo srityje vėl parodė ryškius pokyčius, ypač vertinant pervestų lėšų sumas ir sukčiavimo tipologijas. Šis ketvirtis išsiskyrė dideliu sukčių aktyvumu – jie pasitelkė naujausius metodus, pavyzdžiui, sukūrė fiktyvų e. sveikatos portalą, apsimetinėjo mobiliojo ryšio operatoriais ar finansų įstaigų atstovais. Finansiniai nusikaltėliai ne tik pasiekė rekordinius rodiklius, bet ir kėlė vis didesnę grėsmę tiek gyventojams, tiek verslui.

Q4 metu padidėjęs sukčiavimo atvejų skaičius rodo, kad sukčiai toliau ieškojo naujų galimybių, prisitaikydami prie kintančių rinkos sąlygų. Puikiai išvystytos socialinės inžinerijos strategijos, apimančios netikrus pasiūlymus, infiltruotus skambučius ir Phishing'ą, lėmė sukčiavimo atvejų augimą.

[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.

2024 m. LYGINAMOJI ATASKAITA
Sukčiavimo tipologijos pagal incidentų skaičių, vnt.
2024 m. Q1 vs 2024 m. Q2 vs 2024 m. Q3 vs 2024 m. Q4

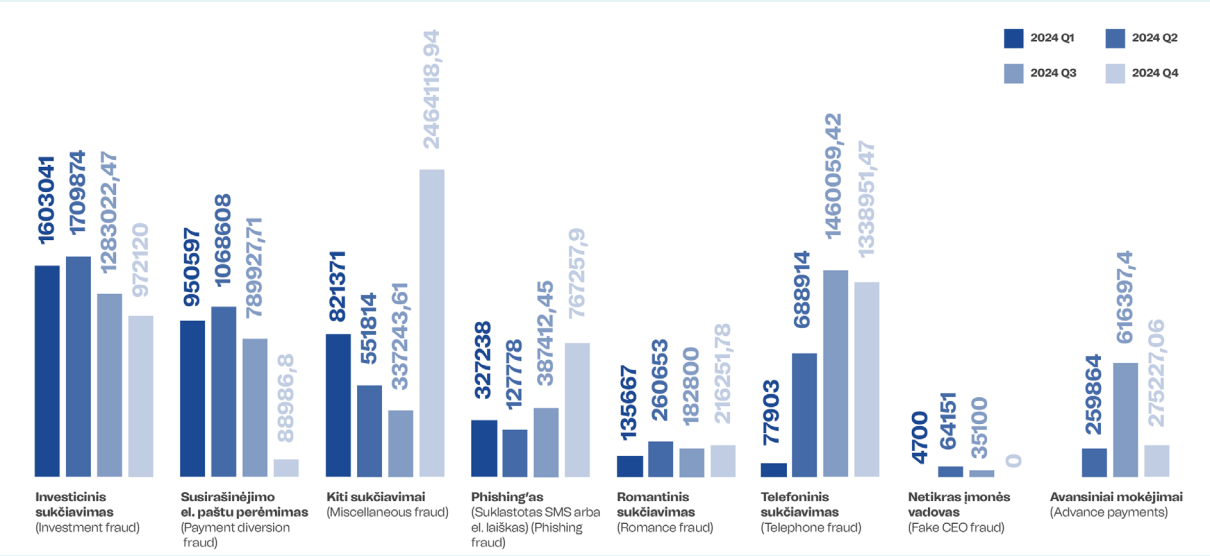


Analizuojant finansinių nusikaltimų mastą pagal pervestas lėšas, pastebima, kad kiekviena sukčiavimo tipologija pasižymi specifiniu poveikiu gyventojams ir skirtingomis pinigų išviliojimo strategijomis. Pateikti duomenys leidžia geriau suprasti, kurios tipologijos yra pavojingiausios ir daro didžiausią žalą. Pateikiama informacija gali padėti efektyviau kovoti su šiomis grėsmėmis.

Remiantis naujausiais duomenimis, 2024 m. spalio – gruodžio mėnesiais, dominuojantys sukčiavimo būdai, **vertinant atvejų skaičių**, buvo: **„Phishing'as"** (suklastotas SMS arba el. laiškas) (angl. Phishing fraud), kurie sudarė 1696 atvejus, „Kiti sukčiavimai", kurie sudarė 558 atvejus ir „Avansiniai mokėjimai" (angl. Advance payments), kurie sudarė 540 atvejus.

Vertinant Q4 sukčiavimo tipologijas **pagal pervestas lėšas,** matoma, kad „Kiti sukčiavimai", kurie sudarė 2,5 mln. Eur, „Telefoninis sukčiavimas", kurio mastas siekė beveik 1,3 mln. Eur ir „Investicinis sukčiavimas", kai pervestų sukčiams lėšų suma sudarė beveik 1 mln. Eur buvo pavojingiausios sukčiavimo formos, kurių metu gyventojai patyrė didžiausius finansinius nuostolius.

2024 m. LYGINAMOJI ATASKAITA
Sukčiavimo tipologijos pagal iš gyventojų išviliotas lėšas, Eur
2024 m. Q1 vs 2024 m. Q2 vs 2024 m. Q3 vs 2024 m. Q4



2024 m. IV ketvirtis sukčiavimo srityje parodė stiprėjantį **Phishing'o** incidentų augimą, kuris tapo reikšminga problema tiek gyventojams, tiek finansų institucijoms.

Palyginus su ankstesniais ketvirčiais, IV ketvirtis demonstruoja didesnį incidentų skaičių ir padidėjusią išviliotų lėšų sumą. Pavyzdžiui, Q1 buvo fiksuotas 941 „Phishing'o" incidentas (išviliotų lėšų suma siekė daugiau nei 320 tūkst. Eur), Q2 šis skaičius sumažėjo iki 463 (išviliotų lėšų suma nukrito iki 280 tūkst. Eur), Q3 atakų skaičius smarkiai šoktelėjo iki 1 048 (išviliotų lėšų suma išaugo iki 390 tūkst. Eur) – tai rodo aiškiai svyruojančią dinamiką. Tačiau Q4 fiksuoti 1 696 atvejai (išviliotų lėšų suma daugiau nei 767 tūkst. Eur) atskleidžia net 61,5 proc. punktų augimą, lyginant su Q3, ir rodo didelį incidentų skaičių, kai išviliota suma vidutiniškai siekė daugiau nei 450 Eur.

Šis augimas susijęs su sukčių gebėjimu prisitaikyti prie naujų saugumo priemonių ir vartotojų elgsenos pokyčių. Pavyzdžiui, sukčiai naudoja netikrus interneto puslapius, imituojančius oficialias svetaines – vienu ryškiausių pavyzdžių tapo netikros eSveikata platformos sukūrimas. Taip pat, norėdami išvilioti asmeninius duomenis, pavyzdžiui, prisijungimo informaciją, sukčiai siunčia elektroninius laiškus, teigdami, kad vartotojo sąskaitai kilo pavojus, todėl būtina kuo skubiau atnaujinti duomenis.

2024 m. Q4 „Kiti sukčiavimai" (angl. Miscellaneous fraud) buvo fiksuoti 558 incidentai, o sukčiams pervestos lėšos atskleidžia ryškų augimą, kai bendra sukčiavimo suma pasiekė net 2,5 mln. Eur. Tai yra ženklus šuolis, lyginant su ankstesniais ketvirčiais: Q3 sukčiavimai sudarė 337 tūkst. Eur, Q2 – 500 tūkst. Eur, o Q1 – 820 tūkst. Eur. Dėl vykstančių procesų šio augimo priežastys dar nėra tiksliai nustatytos.

Šis augimas rodo, kad nors „kiti sukčiavimai" pagal atvejų skaičių išliko stabiliai dideli, smarkiai išaugo pervestų lėšų suma. Centras atkreipia dėmesį, kad „kiti sukčiavimai" apima įvairius sukčiavimo metodus, kurie nepatenka į aiškiai apibrėžtas tipologijas. Dėl sukčiavimo sudėtingumo, Q4 nebuvo galimybės identifikuoti tikslios tipologijos, kuri nulėmė tokį aukštą „kiti sukčiavimai" rodiklį.

Telefoninis sukčiavimas 2024 m. IV ketvirtį ir toliau kėlė didelę grėsmę, nes buvo užfiksuoti 185 incidentai, kurių metu sukčiams pavyko išvilioti net 1,3 mln. Eur, o vidutinė išviliota suma siekė 7 200 Eur. Šie skaičiai atskleidžia, kaip telefoniniai sukčiai geba sumaniai manipuliuoti žmonių pasitikėjimu.

Analizuojant 2024 m. „Telefoninio sukčiavimo" tendencijas, akivaizdu, kad po fiksuoto atvejų šuolio II ketvirtyje, kuomet incidentų skaičius šoktelėjo iki 124 ir išviliotos lėšos sudarė net 688 tūkst. Eur, Q4 duomenys patvirtina, kad grėsmė nesumažėjo. Nepaisant institucijų pastangų perspėti visuomenę, skaičiai ir toliau rodo įspūdingą incidentų skaičiaus stabilumą.

Q3 užfiksuoti 189 incidentai ir daugiau nei 1,46 mln. Eur. Sukčiams patikėtų lėšų suma aiškiai parodo, kad telefoninis sukčiavimas daro didžiausią žalą ir išlieka aktualia problema, rodančia, jog seniai žinoma taisyklė „neatskleisti savo bankinių duomenų nepažįstamiems asmenims", vis dar nėra įsisąmoninta.

2024 m. Q4 **„Investicinio sukčiavimo"** statistika rodo, kad situacija išliko stabili – buvo užfiksuoti 506 investicinio sukčiavimo atvejai, o bendra išviliotų lėšų suma apie 1 mln. Eur (vidutinė išviliota suma – 1 900 Eur). Tai liudija, jog sukčiai ir toliau efektyviai naudojasi gyventojų pasitikėjimu, manipuliuoja emocijomis tam, kad užvaldytų jų turimas lėšas.

Palyginus su Q3, kuomet fiksuota 512 atvejų ir bendra prarastų lėšų suma siekė 1,3 mln. Eur, Q4 duomenys rodo nedidelį incidentų mažėjimą, tačiau išviliotų lėšų suma išlieka didelė.

Šios tendencijos pabrėžia būtinybę stiprinti gyventojų švietimą ir informuotumą apie galimus

sukčiavimo metodus, ypatingai didelį dėmesį skiriant investicinio sukčiavimo tipologijos temai.

Centras ragina gyventojus, ieškančius būdų sėkmingai investuoti, būti ypač atsargiems ir atsakingiems, kai kalbama apie investicijas. Norint investuoti, būtina rinktis patikimus ir patvirtintus finansų tarpininkus, siekiant apsaugoti savo finansines lėšas ir išvengti nemalonių situacijų.

„Romantinis sukčiavimas“ remiasi emociniais ryšiais, kuriuos sukčiai išnaudoja manipuliuodami aukomis. 2024 m. Q4 atvejų skaičius ir toliau palaipsniui didėjo, kai minėtu laikotarpiu buvo fiksuoti 136 atvejai, bendra pervestų lėšų suma viršijo 200 tūkst. Eur, o vidutinė išviliota suma atitinkamai siekė apie 1 500 Eur.

Q1 sukčiams buvo pervesta daugiau nei 135 tūkst. Eur, kai atvejų skaičius siekė 99 incidentus, Q2 – virš 260 tūkst. Eur, atvejų skaičiui augant iki 106 incidentų, Q3 – beveik 183 tūkst. Eur, kai incidentų fiksuota 115.

Romantiniai sukčiai dažnai palieka aukas ne tik su finansiniais nuostoliais, bet ir gilia emocine žala. Emocinis aspektas šiame sukčiavime vaidina lemiamą vaidmenį, todėl aukos tampa ypač pažeidžiamos. Dėl šios priežasties, realus romantinio sukčiavimo aukų skaičius gali būti gerokai didesnis nei fiksuoja finansų įstaigos ar policija.

„Avansinių sukčiavimų“ atvejų skaičius Q4 siekė 540, o bendra pervestų lėšų suma mažėjo iki 275 tūkst. Eur, vidutinė išviliota pinigų suma siekė 510 Eur.

Palyginus su Q3, kuriame buvo fiksuoti 622 incidentai, o bendra pervestų lėšų suma viršijo 600 tūkst. Eur, Q4 rodo tam tikrą pervestų lėšų sumažėjimą. Q3 vidutinė išviliota suma siekė 990 Eur, o didesnis incidentų skaičius šiuo laikotarpiu parodė didelį sukčių aktyvumą ir efektyvumą.

Q2 situacija atrodė dar labiau palanki sukčiams – tuomet fiksuota net 500 incidentų, o pervestų lėšų suma buvo apie 260 tūkst. Eur. Tai rodo, kad Q2 sukčiai sugebėjo užvaldyti mažiau lėšų nei Q3 ir Q4 laikotarpiais.

Augantis interneto naudojimas, ypač sezoninių pirkimų ir atostogų metu, galėjo būti lemiamas veiksnys, turėjęs įtakos avansinių sukčiavimų atvejų skaičiaus augimui.

Ši sukčiavimo tipologija – tai sukčiavimo būdas, kuomet sukčiai įkelia skelbimus internete apie neegzistuojančias prekes ar paslaugas. Sukčiai už neegzistuojančią prekę ar paslaugą prašo mokėti avansiniu būdu, tačiau prekė ar paslauga lieka nesuteikta.

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

Nors sukčiavimo atvejai, nukreipti į juridinius asmenis, nėra itin dažni, tačiau išviliotų lėšų sumos gali būti ženklios:
„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 – sukčiavimo metodas, taikomas juridinių asmenų atžvilgiu. Sukčiai skubos tvarka nurodo pervesti dideles pinigų sumas į sukčių valdomas bankines sąskaitas.

Šio sukčiavimo metu naudojamos psichologinės manipuliacijos, pabrėžiant tariamą skubumą ir autoritetą, taip siekiant sumažinti tikimybę susivokti ir pastebėti sukčių apgaulę.

Nors tokių incidentų skaičius yra santykinai mažas ir per 2024 m. Q4 tokių sukčiavimo atvejų fiksuota nebuvo, tačiau verta įsidėmėti, kad pakliuvus į sukčių pinkles, finansinė žala gali būti labai didelė. III ketvirtis rodė, kad vos 2 incidentai galėjo lemti reikšmingą 35 100 Eur nuostolį (vidutiniškai išviliota suma siekė apie 17 tūkst. Eur). Tai rodo, kad sukčiai, pasitelkę „Fake CEO fraud" metodiką, taikosi į įmones, iš kurių tikisi išvilioti reikšmingas pinigų sumas.

Taip pat 2024 m. IV ketvirtis parodė pagerėjusią situaciją ir **„Susirašinėjimo el. paštu perėmimo"** (angl. Payment Diversion) sukčiavimo srityje. Šiuo laikotarpiu fiksuoti 6 atvejai, o išviliotų lėšų suma sudarė 90 tūkst. Eur.

Šis ženklus pagerėjimas gali būti didėjančio įmonių budrumo, geresnės apsaugos ir darbuotojų mokymų rezultatas.

Centro duomenimis, Q1, Q2 ir Q3 fiksuoti žymiai didesni juridinių asmenų finansiniai nuostoliai: Q1 per 23 incidentus išviliota daugiau nei 950 tūkst. Eur (vidutinė suma siekė 41 tūkst. Eur), o Q2 incidentų skaičius sumažėjo iki 14, tačiau bendra pervestų lėšų suma išaugo iki 1,06 mln. Eur (vidutinė suma siekė 76 tūkst. Eur). Q3 per 20 incidentų pervesta 790 tūkst. Eur, o vidutinę nuostolio sumą Q3 sudarė 39,5 tūkst. Eur.

Šie duomenys atskleidžia, kad sukčiai, taikydami šį „Susirašinėjimo el. paštu perėmimo" sukčiavimo būdą, nuolat prisitaiko prie įmonių saugumo sistemų, kurdami vis įtikinamesnius ir sudėtingesnius dokumentų bei elektroninių paštų klastojimo būdus.
Stebint šias sukčiavimo tendencijas, akivaizdu, kad nė vienas juridinis asmuo nėra apsaugotas nuo sukčių atakų.

Incidentų skaičių ir masto kaita rodo, kad sukčiai nepasiduoda ir nuolat atakuoja, ieškodami silpnų vietų organizacijų saugumo sistemose. Siekiant to išvengti, svarbu nuolat organizuoti darbuotojų mokymus, kaip atpažinti sukčiavimo schemas. Toks pasirengimas ir budrumas gali padėti užkirsti kelią potencialiems nuostoliams ir sustiprinti organizacijų apsaugą nuo sukčiavimo grėsmių.

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, abonentinio ryšio operatoriais, „Google", „Meta" įgaliotiniais ar kitomis 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 sukurdami patikimumo įspūdį. Jie gali naudoti dirbtinio intelekto įrankius, siekiant imituoti balso toną arba klaidinti pašnekovą.

Policija, finansų įstaigos ir kitos valstybinės institucijos nuolat stengiasi informuoti gyventojus apie įvairius sukčiavimo pavojus, susijusius su investicijomis, romantiniais santykiais ir kitais sukčių veiklos būdais, kurie gali apimti manipuliacijas internetu, tokias kaip spaudimas nuorodoms (phishing'as) ir asmeninių duomenų bei PIN kodų atskleidimas.

Viešojoje erdvėje nuolat girdimi perspėjimai, kad skambučiai, kuriais prašoma atskleisti asmeninius duomenis, yra sukčiavimo schema, kuria siekiama išvilioti informaciją, gauti prieigą prie asmeninių banko sąskaitų ir jas ištuštinti.

Nepaisant šių pastangų, sukčiavimo rodikliai ir toliau auga. Tai rodo, kad tiek visuomenės informavimo kampanijos, tiek finansinių institucijų apsaugos priemonės turi būti intensyvinamos arba ieškoma naujų efektyvių būdų didinti vartotojų atsparumą sukčiavimui.

Svarbu kurti efektyvias prevencines priemones, kad būtų sumažintas gyventojų ir verslo subjektų pažeidžiamumas, apsaugoma nuo didėjančių finansinių nuostolių.

! Atsižvelgiant į tai, Centras dar kartą atkreipia dėmesį ir pabrėžia, jog valstybės institucijos, finansų įstaigos, policija niekuomet nereikalauja gyventojų pateikti jautrią informaciją ar asmeninius duomenis.

Išvados

2024 m. sukčiavimo tendencijos: pokyčiai, pamokos ir iššūkiai

2024-ieji dar kartą priminė, kaip sparčiai vystosi sukčiavimo metodai ir kokias problemas jie kelia tiek gyventojams, tiek finansų institucijoms. Analizuojant šių metų duomenis, pastebėta, kad didėja ne tik sukčių aktyvumas, bet ir jų gebėjimas prisitaikyti prie technologinių naujovių bei rinkos pokyčių. Tokie iššūkiai kelia klausimą: ar ši kova su sukčiais taps nuolatine lenktynių su laiku dalimi?

Šiemet sukčiavimai pasiekė rekordines aukštumas, sukčiai siekė išvilioti 35 mln. Eur, o realiai pervesta buvo daugiau nei 20 mln. Eur. Ypač ryškiai išaugo sukčiavimo atvejų skaičius paskutinį metų ketvirtį, kai tiek incidentų, tiek pervestų lėšų suma smarkiai padidėjo.

Tai rodo, kad šventinį laikotarpį ir didesnį vartotojų aktyvumą internete sukčiai išnaudoja savo naudai. Nors sezoniniai svyravimai nėra naujiena, jų mastas kelia susirūpinimą dėl didesnio visuomenės pažeidžiamumo, ypač impulsyvių sprendimų priėmimo metu.

Svarbu paminėti, kad sukčių metodai tampa vis sudėtingesni. Metų viduryje fiksuotas sumažėjęs „phishing" atvejų skaičius paskutiniame ketvirtyje ypač išaugo ir pasiekė rekordines aukštumas. Tai rodo, kad sukčiai ne tik stengiasi pasiekti masinį efektą, bet ir geba manipuliuoti žmonių pasitikėjimu, taikydami socialinės inžinerijos principus. Sukčių atpažinimas tampa vis sudėtingesnis - jei anksčiau sukčius išduodavo gramatinės klaidos ar nelietuviški telefono numeriai, šiandien šie požymiai - aptinkami vis rečiau.

Nors elektroninių laiškų ar netikrų svetainių kūrimas jau tapo įprasta praktika, dabar sukčiai dažnai naudoja personalizuotas atakas, pritaikytas kiekvienai potencialiai aukai.

Finansų institucijų vaidmuo šiame kontekste taip pat buvo itin svarbus. 2024 m. joms pavyko sustabdyti 15 mln. Eur vertės sukčiavimo bandymų – tai rodo ne tik inovatyvius techninius sprendimus, bet ir pagerintą institucijų koordinavimą. Tačiau ketvirto ketvirčio sukčiavimo masto augimas net 26,3 proc. punktais, lyginant su ankstesniu, rodo, kad sukčiai tampa vis išradingesni ir atkaklesni.

Taigi, kova su sukčiavimu duoda vis daugiau teigiamų rezultatų – nors grėsmė išlieka, finansų įstaigos vis sėkmingiau užkerta kelią neteisėtiems pervedimams. Duomenys rodo, kad 2024 m. finansų įstaigoms pavyko apsaugoti ir sustabdyti beveik dvigubai didesnę sukčiams pervestą lėšų sumą, palyginti su 2023 m., kai buvo sustabdyta 7,9 mln. eurų.

Džiugina ir gyventojams grąžintų lėšų dinamika, ypač paskutiniame metų ketvirtyje, kai jiems buvo sugrąžinta 1,5 mln. Eur. Tai rodo, kad finansų institucijos reaguoja greitai, o visuomenė tampa atsakingesne, pranešdama apie sukčiavimo atvejus. Tačiau negalima ignoruoti fakto, kad išvilioti pinigai rodo vis dar nepakankamą gyventojų sąmoningumą ir atsparumą tokio pobūdžio sukčiavimo atakoms.

Kalbant apie sukčiavimo tipus, išlieka trys pagrindinės kryptys: „investicinis sukčiavimas", „telefoniniai sukčiavimai" ir „kiti sukčiavimai". Investiciniai sukčiavimai rodo, kad žmonės vis dar linkę pasitikėti „per gerai, kad būtų tiesa" pasiūlymais, todėl svarbu didinti visuomenės finansinį raštingumą ir gerinti informacijos sklaidą.

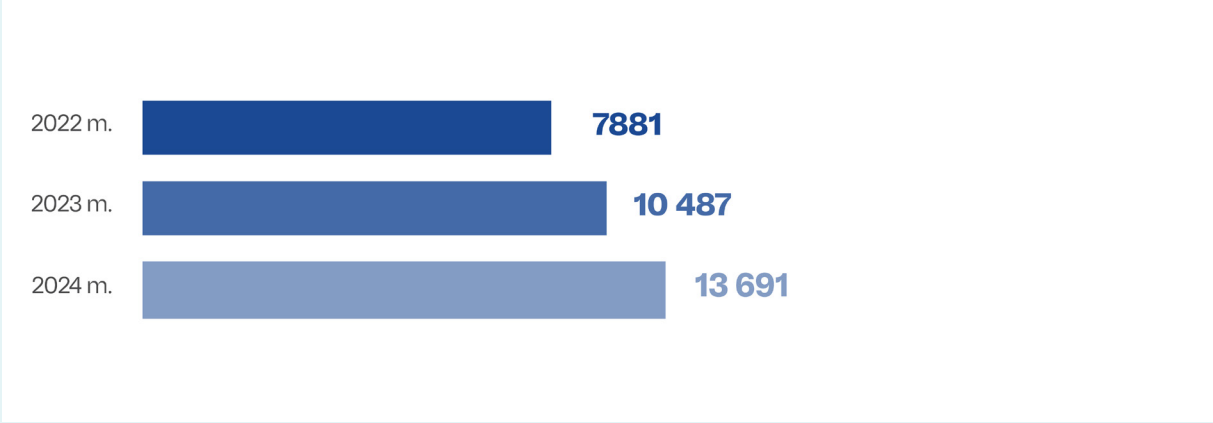
2024 metai išryškino sukčiavimo metodų evoliuciją – sukčiai tapo greitesni, kūrybiškesni ir technologiniu požiūriu pažangesni, o visuomenė vis dar dažnai atsilieka nuo šių pokyčių. Didėjantis sukčiams pervestų lėšų mastas, nepaisant visų pastangų tai užkardyti, kelia susirūpinimą. Tai rodo, kad vien technologiniai sprendimai nesugeba kovoti su sukčiavimu – reikalingas ir visuomenės švietimas, prevencinės kampanijos bei bendras atsparumo didinimas.

Apibendrinant, 2024 m. dar kartą patvirtino, kad kovos su sukčiavimu tikslas nėra vien tik technologijų ar įstatymų leidėjų uždavinys – tai turi būti bendras visuomenės ir institucijų darbas. Kiekvienas žmogus turi suprasti, kad saugumas internete prasideda nuo atsargumo ir gebėjimo atpažinti grėsmes. Tik tokiu būdu galime sukurti aplinką, kurioje sukčiai neturės galimybės pasipelnyti.

2022 – 2024 m. APŽVALGA

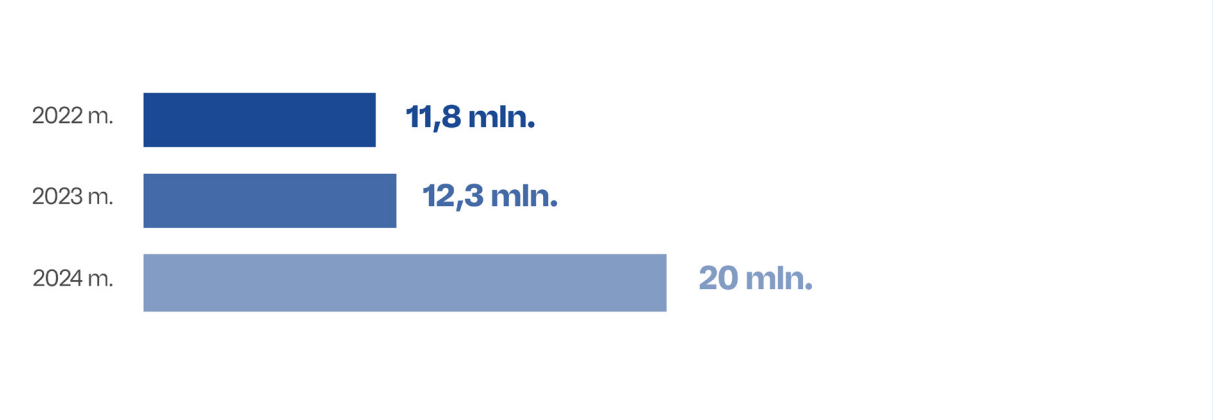
Nuo 2022 m. iki 2024 m. fiksuotų sukčiavimo atvejų augimas buvo itin spartus, vertinant tiek išviliotų lėšų sumą, tiek bendrą atvejų skaičių. 2022 m. užfiksuotas 7 881 sukčiavimo atvejis, tačiau 2023 m. šis skaičius šoktelėjo iki 10 487. Dar ryškesnis augimas pastebimas 2024 m., kuomet sukčiavimo atvejų skaičius pasiekė net 13 691.

Sukčiavimo atvejų dinamika (VNT.)



Šis greitas augimas tiesiogiai atitinka ir finansinių pervedimų dinamiką: 2022 m. pervesta 11,8 mln. Eur, 2023 m. – 12,3 mln. Eur, o 2024 m. – net 20 mln. Eur. Tai rodo, kad ne tik daugėja sukčiavimo atvejų, bet ir didėja šių operacijų mastas. Didėjantis sukčiavimo atvejų skaičius ir išviliotų pinigų kiekis išryškina problemas tiek kibernetinio saugumo, tiek visuomenės atsparumo bei informavimo srityse.

Pervestų lėšų dinamika (EUR)



Galima numanyti, kad viena iš priežasčių – sukčių metodų tobulėjimas ir pasaulyje didėjantys sukčiavimo mastai[4]. Tuo tarpu žmonės lieka pažeidžiami dėl mažo sąmoningumo ir per menko dėmesio asmeninių duomenų saugumui.

Ši statistika tik dar kartą pabrėžia, kokia svarbi yra investicija į pažangesnes saugumo technologijas ir aktyvesnį visuomenės švietimą apie sukčiavimo grėsmes. Jei ši tendencija nesikeis, galime tikėtis, kad sukčiavimo mastas ir toliau palaipsniui didės.

2025 metų prognozės – žvelgiant į pastaruosius trejus metus ir stebint spartų sukčiavimo atvejų augimą, galima numatyti tam tikras tendencijas, kurios greičiausiai formuos ateitį.

Technologijos ir sukčiavimas:

2025 m. sukčiai, tikėtina, vis dažniau naudosis pažangiomis technologijomis – dirbtiniu intelektu (DI), automatizuotais įrankiais ir kibernetinėmis atakomis. DI ir mašininio mokymosi algoritmai padės kurti vis įtikinamesnius apgaulingus pranešimus, o automatizuoti procesai leis greičiau ir efektyviau vykdyti nusikaltimus. Kibernetinis saugumas taps dar svarbesnis, nes atsiras naujų grėsmių, tokių kaip naudojimasis angl. deepfake technologijomis, siekiant kurti įtikinamus sukčiavimo scenarijus.

Momentiniai mokėjimai ir jų poveikis sukčiavimui:

Nepaisant to, kad sukčiavimo atvejų skaičius ir toliau auga, momentinių mokėjimų populiarėjimas gali turėti reikšmingos įtakos šiam procesui. Šie mokėjimai leidžia atlikti greitus pervedimus, kurie įvykdomi akimirksniu. Nors šis mokėjimo būdas suteikia patogumą ir efektyvumą, jis taip pat sukuria palankias sąlygas sukčiams.

Kibernetinė grėsmė ir visuomenės saugumas:

Su skaitmeninėmis technologijomis susijusios saugumo problemos neapsiribos tik finansinėmis institucijomis. Kibernetinis saugumas taps svarbus ne tik verslui, bet ir kasdieniam vartotojui, nes sukčiai vis dažniau naudos socialinės inžinerijos metodus ir savo naudai išnaudoja technologines spragas finansiniams nusikaltimams vykdyti. Taps dar svarbiau informuoti ir šviesti visuomenę apie saugumą, skatinant valdžios institucijas ir privačias įmones daugiau investuoti į švietimą, prevenciją ir technologines inovacijas, nes sukčiai vis dažniau naudos socialinės inžinerijos metodus ir savo naudai išnaudos technologines spragas finansiniams nusikaltimams vykdyti. Taps dar svarbiau informuoti ir šviesti visuomenę apie saugumą, skatinant valdžios institucijas ir privačias įmones daugiau investuoti į švietimą, prevenciją ir technologines inovacijas.

Sukčiavimas „socialinėse medijose“ ir mobiliosiose platformose:

Atsižvelgiant į tai, kad socialinės medijos ir mobiliosios aplikacijos tampa vis svarbesnės kasdieniame gyvenime, 2025 m. tikėtina, kad sukčiavimo atvejai šiose platformose dažnės. Sukčiai naudosis tiek nuomonės formuotojais (angl. influencers), tiek vartotojų elgesio duomenimis, kad sukurtų personalizuotas ir įtikinamas apgaules.

[4] INTERPOL Global Financial Fraud Assessment

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, o taip pat kritiškai vertinti pernelyg skubotus ar emocionalius prašymus dėl pinigų pervedimo bei kitos materialios pagalbos. Rekomenduojama tikrinti 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" (angl. Fake CEO) ar „Susirašinėjimo el. paštu perėmimas" (angl. Payment Diversion), turėtų organizuoti darbuotojams reguliarius mokymus apie dažniausiai pasitaikančius sukčiavimo būdus ir jų atpažinimą.

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. Taip pat, rekomenduojama atlikti periodinius mokėjimų auditus, nuolat 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 arba kitomis bendrovės naudojamomis identifikavimo priemonėmis, o taip pat, taikytų griežtas finansinių operacijų procedūras (dvigubas patvirtinimo procesas dideliems mokėjimams).

Ne mažiau 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 gali būti vadovo atvaizdo suklastojimas vaizdo skambučio metu, kuomet panaudojami dirbtiniu intelektu sugeneruoti vaizdai ir balsas, siekiant imituoti teisėtus įmonės atstovus. Tokiu būdu sukuriama patikimumo iliuzija, kuria siekiama lengviau manipuliuoti aukomis.

Dėl šių technologijų pažangos, atsakingi įmonėse dirbantys asmenys turėtų imtis veiksmų tam, 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 vykdymo procesą.