VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ BAKALAURO STUDIJŲ PROGRAMA

Naudotojo apsauga nuo duomenų viliojimo atakų

Users' Protection Against Phishing Attacks

Bakalauro baigiamasis darbas

Atliko:	Miglė Micevičiūtė	(parašas)
Darbo vadovė:	doc. dr. Kristina Lapin	(parašas)
Darbo recenzentas:	doc. dr. Saulius Ragaišis	(parašas)

Vilnius – 2024

Santrauka

Bakalauro darbe yra tiriami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje, kuriais remiantis bus sukurtas naršyklės plėtinys, padedantis naudotojui atpažinti duomenų viliojimo atakas. Atlikus literatūros analizę apsibrėžiamas duomenų viliojimo procesas, išskiriami duomenų viliojimo atakų tipai. Apžvelgiami šiuo metu taikomi prevencijos būdai, jų privalumai bei trūkumai. Esamų duomenų viliojimo atakų prevencijų apžvalgoje išskiriami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje. Šie požymiai yra naudojami kuriant būsimos sistemos naudojimo scenarijus ir maketus. Įgyvendinant naudotojui palankią projektavimo metodiką, tiriama galimų projektinių sprendimų erdvė ir kuriami sprendimus iliustruojantys maketai. Toliau naudotojai yra įtraukiami į siūlomų sprendimų efektyvumo vertinimą. Atsižvelgiant į naudotojų pateiktas pastabas, yra išskiriami naudotojams palankūs projektiniai sprendimai ir yra projektuojamas „Google Chrome" naršyklės plėtinys, skirtas atpažinti duomenų viliojimo atakas pagal darbe surinktus duomenų viliojimo atpažinimo požymius. Analitiškai apžvelgiama kaip duomenų viliojimo atakas padengia sukurtas naršyklės plėtinys – ar visa duomenų viliojimo ataka yra padengiama. Sukurtas naršyklės plėtinys išbandytas ir ištestuotas naudotojų grupės ir buvo pastebėta, jog po plėtinio naudojimosi, duomenų viliojimo atakos yra geriau atpažįstamos – duomenų viliojimų atakų atpažinimas išaugo 20 %.

Raktiniai žodžiai: duomenų viliojimas, duomenų viliojimo atakos, prevencijos būdai, panaudojamumas, naršyklės plėtinys.

Summary

The bachelor thesis examines the features for recognizing phishing in the user interface, based on which a browser extension will be created to help users identify phishing attacks. After conducting a literature analysis, the process of phishing is defined, phishing attack types are identified. Overview of the methods of prevention currently used, their advantages, and disadvantages. In the existing phishing attack prevention methods evaluation, recognition signs for detecting phishing in the user interface are created. These signs then are used in creating scenarios for the future system, resulting in possible layouts. Applying user-centered design methodology users must be involved in decision-making to explore the space of project solutions and identify effective solutions. Users are further involved in the assessment of the effectiveness of the proposed solutions. Taking into account the comments provided by users and following user-centered design processes, a „Google Chrome" browser extension is developed to recognize phishing attacks based on the collected characteristics. Analytically reviewed how browser extension covers phishing attacks – whether the entire phishing attack is covered. The created browser extension is tested and evaluated by a group of users and it was observed that after using the browser extension, phishing attacks are better recognized – phishing attacks recognition increased by 20%.

Keywords: phishing, phishing attacks, prevention methods, usability, browser extension.

Turinys

Įvadas

Tyrimo objektas. Tyrime yra analizuojamos duomenų viliojimo atakos (angl. *phishing attacks*), kas yra vienas didžiausių kibernetinių nusikaltimų. Šios atakos yra pateikiamos elektroninių laiškų bei trumpųjų žinučių pavidalu, kurie kruopščiai sukuriami pavogti gavėjo jautrius duomenis (prisijungimo informacija, asmeniniai duomenys) arba instaliuoti kenkėjišką programą į kompiuterį [BR22]. Didžiausias dėmesys skiriamas atakoms, turinčioms vartotojo sąsają bei kaip apsaugoti naudotojus nuo šių atakų.

Tyrimo aktualumas. Kibernetinių nusikaltimų sukeliama žala auga kiekvienais metais. 2019 metais buvo patvirtinta, kad duomenų saugumo pažeidimų atvejų skaičius vis kyla. Socialinės inžinerijos atakų, tokių kaip duomenų viliojimas, skaičius šoktelėjo 8 % per vienerius metus, kenkėjiškų programų (angl. *malware*) šoktelėjo 11 %, o užšifruojančių ir išpirkos prašančių programų (angl. *ransomware*) skaičius šoktelėjo 21 % [ARJ+20].

Socialinės inžinerijos atakos yra manipuliavimo menas išgauti informaciją iš mažiau šias atakas suprantančio žmogaus [GSK16]. Duomenų viliojimo atakos yra populiariausias socialinės inžinerijos atakų tipas, kuomet duomenų vagis (angl. *phisher*) apgauna žmones maskuojantis kaip patikima įmonė [EBD+20]. Šių atakų skaičius pastoviai kilo nuo vėlyvų 2019 bei per COVID-19 pandemiją [ADP+21a], kuomet žmonės pradėjo dažniau naudotis elektroninėmis paslaugomis bei nuotolinėmis komunikavimo priemonėmis. Dažniausiai naudojamos elektroninės paslaugos yra elektroninė bankininkystė bei internetinės parduotuvės. Apgavikai naudojosi šia tendencija, todėl pradėjo siųsti elektroninius laiškus susijusius su pirkimais – pirkinio patvirtinimas, siuntos mokestis muitinėje su nuorodomis pervesti pinigus [ADP+21b]. Taip pat dažni pranešimai yra apie banko sąskaitos užblokavimą ar baudų susimokėjimą.

Kovojant su duomenų viliojimo atakomis yra kuriama daug įvairių veiksmingų priemonių su jomis susidoroti. Didžiausias dėmesys yra kreipiamas į naudotojų apmokymą, kaip atskirti tikrus elektroninius laiškus nuo duomenų viliojimo atakų [ADP+21b; JAB21], nes žmogus yra silpnoji grandis duomenų viliojimo atakų schemoje. Žmogus gali būti lengvai manipuliuojamas ir dažnai duomenų vagis naudoja psichologines, socialines ir technines silpnybes bandant išgauti norimą asmens jautrią informaciją [ADP+21b]. Taip pat vis dažniau sutinkamas metodas yra giliojo mokymosi bei mašininio mokymosi kuriami modeliai (angl. *deep learning and machine learning-based approach*), skirti analizuoti URL informaciją, teksto reikšmę bei jo interpretaciją, ir atpažinti ar tai tikras, ar apgavikų sukurtas internetinis puslapis. Modeliui paduodami įeities parametrai, pagal kuriuos yra atpažįstama puslapio ar elektroninio laiško autentiškumas [MAG+17]. Vis atnaujinamas būdas yra juodasis/baltasis sąrašai (angl. *blacklist/whitelist*), kuriuose yra saugomi žinomų apgavikų puslapių domenai ir su kokiu URL šie puslapiai buvo rasti, tačiau jei puslapis dar nėra sąraše, jis neapsaugos naudotojų [SAB+21]. Vizualiniu panašumu grindžiamo metodo (angl. *visual similarity-based approach*) esmė yra surasti vizualinius panašumus tarp tikros ir praneštos apgavikų svetainės [MKK08]. Tačiau mažiau dėmesio yra skiriama kokie internetinės svetainės bei adreso juostos bruožai gali parodyti, jog tai yra potenciali duomenų viliojimo ataka. Analizuojant esamus duomenų viliojimo atakų prevencijų būdus, šiame darbe yra renkami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje (angl. *user interface*), kurie naudojami naršyklės plėtinio

projektuotojų. Šie požymiai taip pat skirti naudotojams atpažinti duomenų viliojimo atakas kuriamos sistemos pagalba.

Darbo tikslas – ištirti duomenų viliojimo atpažinimo požymius vartotojo sąsajoje ir jais remiantis sukurti naršyklės plėtinį, padedantį naudotojui atpažinti duomenų viliojimo atakas.

Tyrimo uždaviniai:

1. Išanalizuoti literatūrą, siekiant apžvelgti duomenų viliojimo atakų tipus bei surinkti šiuo metu taikomus sprendimus apsaugoti naudotojus nuo atakų.
2. Remiantis surinktais duomenimis, išskirti duomenų viliojimo atpažinimo požymius vartotojo sąsajoje.
3. Pritaikyti požymius kuriant alternatyviuosius maketus, kuriuose bus išbandomi galimi sprendimai.
4. Įvertinti maketų panaudojamumą ir projektinių sprendimų veiksmingumą, bei remiantis vertinimo rezultatais, suprojektuoti detalųjį prototipą.
5. Sukurti naršyklės plėtinį ir atlikti apibendrinamąjį sprendimo vertinimą.

Teorinės darbo prielaidos ir metodika. Atliekama susijusios mokslinės literatūros analizė, kurioje yra analizuojamas duomenų viliojimo procesas, duomenų viliojimo atakų tipai bei atakų sėkmės priežastys. Taip pat yra apžvelgiami esami duomenų viliojimo atakų prevencijos būdai, iš kurių yra išskiriami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje. Įgyvendinant naudotojui palankią projektavimo (angl. *user-centered design*) metodiką, kuriami alternatyvieji maketai ir vykdomas formuojantis panaudojamumo testavimas su naudotojais. Naudotojai bus įtraukiami į sprendimų priėmimą, jog būtų ištirta įmanomų sprendimų erdvė ir būtų išskirtas efektyvus sprendimas. Formuojančio testavimo metu tiriamas sukurtų naršyklės plėtinio maketų panaudojamumas, projektinių sprendimų efektyvumas, renkama informacija apie patobulinimus. Apibendrinamojo analitinio vertinimo metu analizuojamas sukurto „Google Chrome“ naršyklės plėtinio atitikimas naudotojo poreikiams.

Literatūros šaltiniai. Nagrinėjama mokslinė literatūra, susijusi su duomenų vagystės procesu [ADP+21b], duomenų viliojimo atakų tipais [CPF+13; HTL09; SAB+21], atakų sėkmės priežastimis [ADP+21a; ADP+21b] bei esamais prevencijos būdais [AAD19; ASS20; JG17; KIJ13; RSG+21; ZYJ+14].

Darbo atlikimo aplinkybės. Bakalauro darbas rašomas remiantis „Google Scholar” randama moksline literatūra. Panaudojamumo testavimas su naudotojais atliekamas nuotoliniu būdu per „Zoom” platformą.

Naudojami instrumentai. Maketų kūrimui naudojamas vartotojo sąsajos prototipų kūrimo įrankis „Figma”, o „Google Chrome” naršyklės plėtiniui kurti naudojama JavaScript kalba. Naršyklės plėtinio kodas laikomas „Github” kodo repozitorijoje.

1. Duomenų viliojimo atakų apžvalga

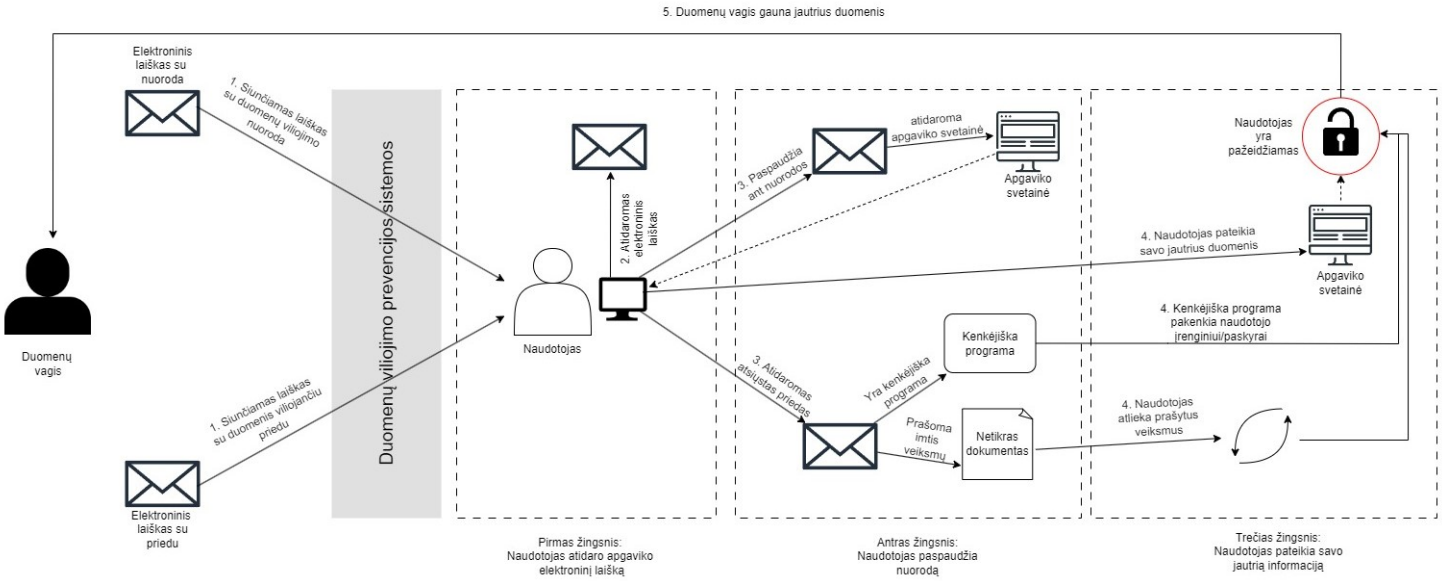
Šiame skyriuje yra apžvelgiamas duomenų viliojimo procesas, atakų tipai, apibrėžiamos šių atakų sėkmės priežastys. Tolimesniuose darbo skyriuose naudojamos tik tos duomenų viliojimo atakos, kurios turi vartotojo sąsają.

1.1. Duomenų viliojimo procesas

Duomenų viliojimo atakų tikslas yra surasti pasirinktos aukos silpnybes [GSK16] ir išgauti norimą jautrią informaciją. Informaciją apgavikai pateikia skirtingais būdais, pavyzdžiui elektroniniu laišku, telefono skambučiu ar trumpąja žinute (SMS).

Dažniausiai duomenų viliojimo procesas prasideda kai duomenų vagis išsiunčia apgaulingus elektroninius laiškus, kurie suvilioja auką. Elektroniniame laiške būna duomenų viliojimo nuoroda, ar priedas (arba abu). Elektroninis laiškas gali būti aptiktas ir sustabdytas duomenų viliojimo atakų prevencijos sistemos šiam laiškui dar nepasiekus gavėjo. Jei laiškas pasiekia gavėją sėkmingai, duomenų viliojimo procese atsiranda šie žingsniai [ADP+21b] (žr. 1 pav.):

1. Pirmasis duomenų viliojimo žingsnis yra kuomet naudotojas gauna ir potencialiai atidaro laišką, jei jam neužkerta kelio prevencijos sistemos.
2. Gavėjas paspaudžia ant nuorodos laiške ir/arba atidaro atsiųstą priedą. Paspaudus nuorodą, gavėjas yra nukreipiamas į duomenų viliojimo svetainę, kurioje duomenų vagis įvairiais būdais stengiasi apgauti savo auką ir išvilioti jos jautrią informaciją, pavyzdžiui banko prisijungimo duomenis. Priede gali būti kenkėjiška programa arba netikras dokumentas, prašantis aukos imtis veiksmų, pavyzdžiui sąskaita faktūra, kurioje prašoma pakeisti mokėjimo informaciją.
3. Paskutiniame žingsnyje gavėjas pateikia savo informaciją, atlieka prašomus veiksmus apgavikų svetainėje, Jei kenkėjiška programa, esanti priede, nėra aptinkama antivirusinės sistemos, pakenkiama naudotojo įrenginiui (kompiuteriui, telefonui) arba paskyrai (elektroninio laiško paskyrai, banko paskyrai).



1 pav. Duomenų viliojimo procesas, adaptuotas iš [ADP+21b] į lietuvių kalbą

Duomenų viliojimo atakos metu yra išnaudojamas naudotojo neišprusimas bei neatidumas, ir tai lemia sėkmingą duomenų viliojimo ataką. Didžiąją dalį laiškų užblokuoja prevencinės sistemos, tačiau likusius laiškus naudotojas turi atpažinti pats.

1.2. Duomenų viliojimo atakų tipai

Duomenų viliojimo atakų yra daug, tačiau galima išskirti pagrindinius jų tipus:

1. Apgaulinga duomenų viliojimo ataka (angl. *deceptive phishing*).
2. Personalizuotas duomenų viliojimas (angl. *spear phishing*).
3. Klonavimo duomenų viliojimo ataka (angl. *clone phishing*).
4. „Tarpininko“ duomenų viliojimo ataka (angl. *man in the middle*).
5. Nuorodos manipuliacijos/HTTP duomenų viliojimo ataka (angl. *link manipulation/HTTP phishing*).
6. SMS duomenų viliojimo ataka (angl. *smishing/SMS phishing*).
7. Balso duomenų viliojimo ataka (angl. *vishing/voice phishing*).

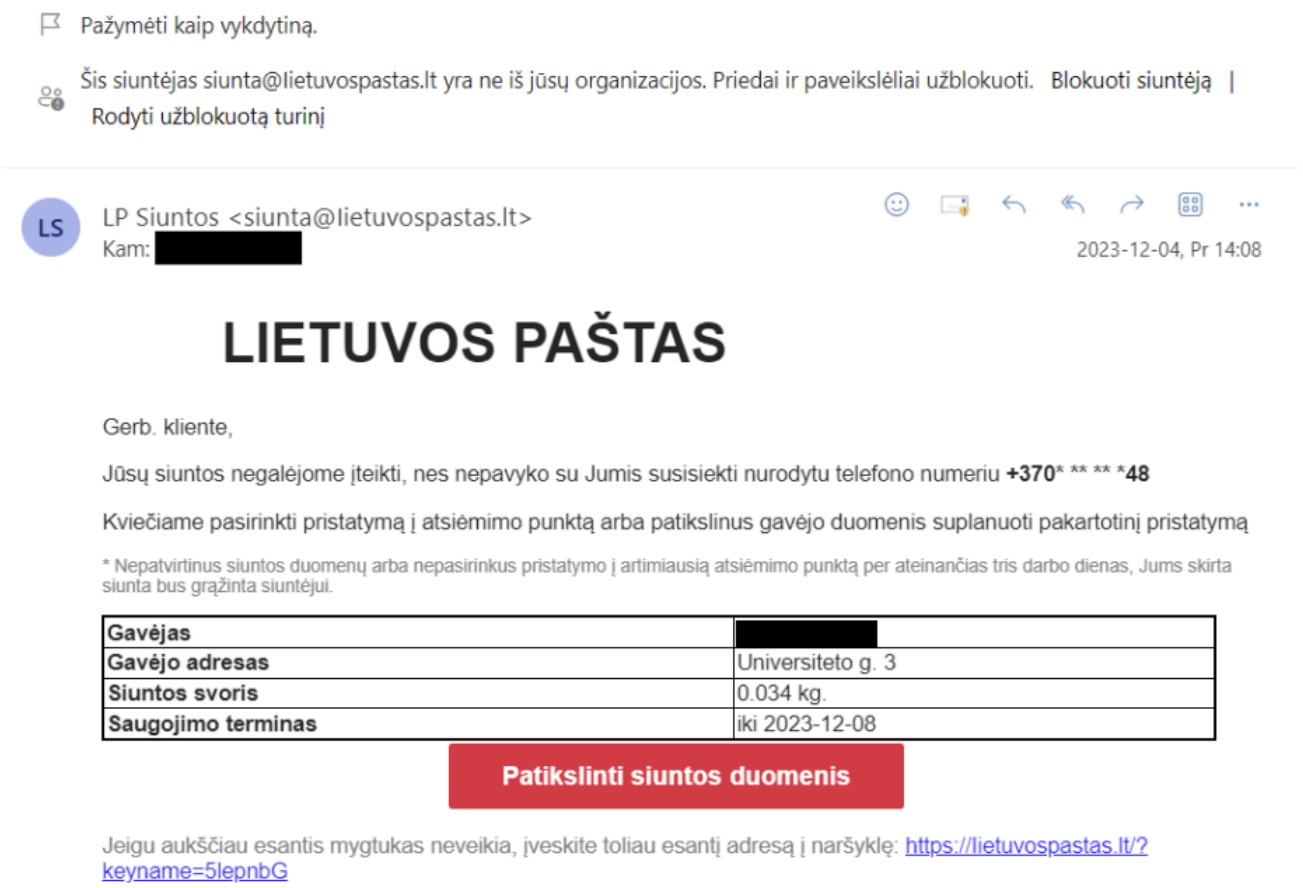
Kiekviena iš šių duomenų viliojimo atakų pasižymi skirtingomis savybėmis, atakavimo forma, kurias naudotojai turėtų žinoti, norėdami apsisaugoti nuo šių duomenų viliojimo atakų.

1.2.1. Apgaulinga duomenų viliojimo ataka

Dažniausias duomenų viliojimo atakų tipas – apgaulinga duomenų viliojimo ataka (angl. *deceptive phishing*). Šiame duomenų viliojimo atakų pobūdyje duomenų vagys (angl. *phishers*) apsimeta tam tikra korporacija (pvz. banku) ir stengiasi pavogti jautrius asmens ar prisijungimo duomenis skatinant naudotoją paspausti ant laiške esančios nuorodos [SAB+21]. Pasak Huang,

Tan bei Liu tyrimo [HTL09], visos apgaulingos duomenų viliojimo atakos telpa į vieną bendrą šabloną:

1. Apgavikas paruošia netikrą svetainę duomenų viliojimo atakai.
2. Apgavikas atsiunčia suklastotą elektroninį laišką, kuris yra skubus ir reikalaujantis, jog gavėjas paspaustų ant laiške esančios nuorodos.
3. Auka yra apgauta gautojo laiško kai paspaudžia ant nuorodos, nukreipiančios į suklastotą svetainę. Šis veiksmas paverčia auką pažeidžiama ir konfidenciali informacija gali būti nutekinta.
4. Konfidenciali informacija yra perduodama iš duomenų viliojimo serverio apgavikui.
5. Apgavikas naudojasi gauta informacija originalioje svetainėje, perima aukos tapatybę, jog galėtų gauti nelegalius finansinius privalumus.



2 pav. Pavyzdinis duomenų viliojimo laiškas

2 pav. yra matomas pavyzdinis duomenų viliojimo laiškas – gavėjas yra skatinamas paspausti mygtuką arba nuorodą, jog būtų atnaujinti gavėjo duomenys ir gaunama konfidenciali informacija. Mygtukas, esantis laiške, slepia nuorodą, į kurią bus nukreipiamas gavėjas, o apačioje esanti nuoroda yra matoma mažesniu šriftu ir neatkreipianti gavėjo dėmesio – raudonas mygtukas labiau patraukia gavėjo dėmesį.

1.2.2. Personalizuotas duomenų viliojimas

Personalizuotas duomenų viliojimas (angl. *spear phishing*) yra vienas dažnesnių atakų tipų. Šioje atakoje yra pasirenkama specifinė žmonių grupė vietoj didelio masto žmonių [BB13]. Dažnai personalizuotas duomenų viliojimas yra bandymas įsilaužti į sistemą ar organizaciją su tikslu, jog bus nutekinami jautrūs duomenys arba bus šnipinėjama pasirinkta sistema ar organizacija [CPF+13]. Apgavikai dažnai randa informaciją apie asmenį socialinėje medijoje ir taip gali sukurti personalizuotą pasirinktą komunikacijos metodą bei atrodyti autentiškai, pavyzdžiui elektroninis laiškas iš asmens darbovietės, kuriame prašoma atnaujinti asmeninę informaciją, paspaudus nuorodą, būtų nukreipiama į plagijuotą internetinę svetainę, kurioje būtų nutekinami duomenys [SAB+21].

1.2.3. Klonavimo duomenų viliojimo ataka

Klonavimo duomenų viliojimo atakoje (angl. *clone phishing*) apgavikas pasinaudoja korporacijų elektroninių laiškų šablonais ar nukopijuoja neseniai gautą elektroninį laišką, kuris turi priedą ir/arba nuorodą, paimami gavėjų elektroniniai paštai ir yra sukuriamas identiškas laiškas. Originaliame laiške buvusios nuorodos yra modifikuojamos, jog būtų nukreipiama į apgaviko svetainę [SAB+21]. Dažnai nuorodų pakeitimas yra sunkiai pastebimas, pavyzdžiui vietoj 0 (nulio) įdedama O (o didžioji). Jei originalus laiškas turėjo priedą, dažnai priedas yra užkrečiamas kenkėjiška programa (angl. *malware*) ar užšifruota ir išpirkos prašančia programa (angl. *ransomware*), jog būtų nutekinta informacija iš užkrėsto kompiuterio [BKS18].

1.2.4. „Tarpininko“ duomenų viliojimo ataka

„Tarpininko“ duomenų viliojimo atakoje (angl. *man in the middle*) apgavikas elgiasi kaip tarpininkas tarp laiško siuntėjo bei gavėjo. Apgavikas naudojasi tarpiniu serveriu, kuris yra tame pačiame tinklo segmente kaip ir gavėjas. Apgavikas perima visus duomenis iš siuntėjo ir užkrečia siunčiamą informaciją kenkėjiška programa. Gavėjas nepastebėjęs šios atakos gali ir toliau tęsti bendravimą su kita puse, nežinodamas apie tarpinį asmenį ir jog visa informacija patenka pas jį [SAB+21].

1.2.5. Nuorodos manipuliacijos/HTTP duomenų viliojimo ataka

Nuorodos manipuliacijos/HTTP duomenų viliojimo ataka (angl. *link manipulation/HTTP phishing*) dažnai yra kitų duomenų viliojimo atakų dalis, tačiau ne visada yra apsimetama tikra įmone. Apgavikas atsiunčia nuorodą į netikrą svetainę, kuri gali būti užkrėsta kenkėjiška programa. Nuoroda gali būti atsiųsta ne tik į elektroninį paštą, bet ir SMS pranešimus ar „Messenger“ platformą. Paspaudus nuorodą, vartotojas yra nuvedamas į klaidingą svetainę ir tuomet yra pasiekiami visi prisijungimo duomenys [SAB+21].

1.2.6. SMS duomenų viliojimo ataka

SMS duomenų viliojimo ataka (angl. *smishing/SMS phishing*) – tai atakų tipas, kuomet apgavikas siunčia telefoninius pranešimus. Dažniausiai apsimetama, jog pranešimas yra iš rimtos

korporacijos (pvz. banko), kuriame pranešama, jog gautas svarbus pranešimas į naudotojo paskyrą su nuoroda prisijungti ir perskaityti pranešimą [BB13]. Jei naudotojas paspaudžia nuorodą ir bando prisijungti prie savo paskyros, apgavikas gauna visus asmens prisijungimo duomenis.

1.2.7. Balso duomenų viliojimo ataka

Balso duomenų viliojimo ataka (angl. *vishing/voice phishing*) yra kuomet apgavikas skambina į vartotojo telefoną ir prašo jų asmeninės informacijos, pateikdami netikrą scenarijų kodėl tokia informacija yra šiuo metu reikalinga. Šios atakos yra sėkmingos, nes žmonės pasitiki telefonų skambučiais, taip pat didžioji dalis žmonių daugiau naudojasi telefonu nei renkasi komunikaciją elektroniniais laiškais [SAB+21].

1.3. Duomenų viliojimo atakų sėkmės priežastys

Duomenų vagys naudoja įvairias psichologines taktikas duomenų viliojimo procesui sukurti. Žmogus, kuris yra linkęs prie finansinių rizikų, dažnai tampa duomenų viliojimo potencialia auka [ADP+21a]. Technologijoms tobulėjant, tobulėja ir apgavikų būdai išgauti jautrius asmens duomenis. Nors yra keli technologiniai sprendimai užblokuoti duomenų viliojimo laiškus prieš jiems patenkant į elektroninių laiškų dėžutę, ne visada šie laiškai yra sėkmingai atpažįstami kaip apgavystė, todėl tai yra naudotojo darbas – nuspręsti koks laiškas jo dėžutėje yra bandymas išgauti jautrius duomenis, o kas yra tikras, nepadirbtas laiškas [ADP+21b]. Anot Abroshan, Devos, Poels ir Laermans tyrimų [ADP+21a; ADP+21b], žmogaus elgsena yra didžiausias duomenų viliojimo sėkmės faktorius. Jie išskyrė šiuos elgsenos faktorius:

1. **Rizikavimas** – naudotojo polinkis rizikuoti paveikia jo elgseną duomenų viliojimo procese. Naudotojai, kurie yra linkę priimti rizikingus finansinius sprendimus, yra labiau linkę spausti ant apgavikų atsiųstų nuorodų.
2. **Psichologiniai faktoriai** – naudotojo jaučiamas nerimas, stresas bei baimė paveikia jo elgseną duomenų viliojimo procese. Šie faktoriai labiausiai išryškėjo COVID-19 pandemijos metu, kuomet žmonės dažnai būdavo apgauti apgavikų elektroniniais laiškais apie COVID-19 virusą. Tyrimai rodo, jog nerimas ir baimė sukelia žemą užtikrintumo lygį bei žemą savikontrolę, dėl to aukštas nerimo lygis dažnai lemia sėkmingą duomenų viliojimo ataką.
3. **Priverstinis tikrinimo stresas** (angl. *compulsive checking stress*) paveikia naudotojo elgseną duomenų viliojimo procese. Naudotojas, jausdamas stresą, kompulsyviai tikrina ir ieško užtikrintumo spausdamas apgavikų nuorodas. Naudotojas, norėdamas sužinoti daugiau, nežiniomis nutekina savo jautrius duomenis.
4. **Demografiniai rodikliai** – iš demografinių rodiklių tokių kaip amžius, lytis bei išsilavinimas, naudotojo elgseną duomenų viliojimo atakoje daugiausia paveikia jo išsilavinimo lygis.

1.4. Apibendrinimas

Išanalizavus duomenų viliojimo atakas yra matoma, jog jų skaičius einant metams tik kyla ir jos vis labiau tobulėja, tačiau galima įžvelgti ir panašumų tarp jų.

Vienas didžiausių panašumų yra jog nuorodos manipuliacijos/HTTP duomenų viliojimo ataka yra dažnai kitų atakų dalis – yra atsiunčiamas laiškas su kenkėjiška programa ar nuoroda į apgavikų svetainę. Kitas panašumas yra jog klonavimo duomenų viliojimo ataka dažnai taip pat yra kitų dalis – plagijuojamas įmonės elektroninio laiško maketas, kuris naudojamas dažnai personalizuotame duomenų viliojime.

Žmogus yra silpnoji grandis duomenų viliojimo schemoje, todėl turi būti kreipiamas dėmesys į jų apmokymą atpažinti šias atakas. Išskyrus atakų tipus, atpažinimo procesas tampa paprastesnis dėl duomenų viliojimo atakose esančių panašumų. Tačiau yra svarbu atkreipti dėmesį, jog padarius sunkiai plagijuojamą vartotojo sąsają ar išskyrus duomenų viliojimo atpažinimo požymius, būtų galima palengvinti atpažinimo procesą.

Esminiai duomenų viliojimo atakų požymiai:

- Apgavikai apsimeta korporacijomis, jog galėtų pavogti asmens jautrius duomenis.
- Didžioji dalis duomenų viliojimo atakų turi plagijuotą vartotojo sąsają – naudotojai yra nukreipiami į suklastotas svetaines.
- Duomenų viliojimo aukos yra skubinamos atlikti veiksmus, lemiančius sėkmingą duomenų viliojimo ataką.

Toliau šiame darbe nagrinėjamos tik tos duomenų viliojimo atakos, kurios turi vartotojo sąsają, tai yra:

- apgaulinga duomenų viliojimo ataka,
- personalizuotas duomenų viliojimas,
- klonavimo duomenų viliojimo ataka bei
- nuorodos manipuliacijos ataka.

Šios duomenų viliojimo atakos yra toliau nagrinėjamos darbe bei yra ieškoma kaip apsaugoti naudotojus nuo šių atakų.

2. Duomenų viliojimo atakų prevencijų apžvalga

Šiame skyriuje yra apžvelgiami duomenų viliojimo atakų prevencijų būdai, nustatomi jų privalumai bei trūkumai atsižvelgiant į prevencijos būdų esminius principus, bei yra renkami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje.

Duomenų viliojimo prevencijos būdų esminiai principai:

P1. *Ilgaamžiškumas* – prevencijos būdo naudingumo trukmė.

P2. *Tikslumas* – prevencijos būdo tikslumas nustatant ar tai tikra, ar apgavikų svetainė.

Renkami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje indeksuojami *Gnr*. Jų identifikavimo numeris sukuriamas pagal vėliau priskiriamas požymių grupes, todėl identifikavimo numeriai nėra paeiliui.

2.1. Naudotojų apmokymai

Vienas iš pagrindinių būdų apsaugoti naudotojus nuo duomenų viliojimo atakų yra naudotojų apmokymas atpažinti duomenų viliojimą [CCR16; CPF+13]. Kadangi duomenų viliojimo atakoje žmogus dažniausiai lemia sėkmingą atakos pabaigą – apgavikas gauna duomenis – naudotojai yra apmokami atpažinti duomenų viliojimo pranešimus ir tuomet imtis atitinkamų veiksmų, pavyzdžiui pažymėti elektroninį laišką kaip potencialų duomenų viliojimą [KIJ13]. Naudotojų apmokymas atpažinti ir apsaugoti save nuo duomenų viliojimo atakų yra vienas svarbesnių aspektų kibernetiniame saugume. Tačiau dažnai naudotojai neatkreipia dėmesio į naršyklės siunčiamus perspėjimus, tokius kaip adreso juosta ar saugumo indikatoriai (SSL sertifikatas). Organizacijos stengiasi sukurti stilių, kuris būtų lengvai atpažįstamas jų naudotojų. Apgavikų svetainėse pasitaiko gramatinių klaidų ar vizualinių neatitikimų, pavyzdžiui kitoks dizaino išdėstymas ar kitokio šrifto panaudojimas. Apgavikams imituojant originalią svetainę dažnai kyla problemos naudojant lygiai tą patį šriftą. Internetinių svetainių dizaineriai šiek tiek modifikuoja šriftus, jog gautų unikalų šriftą, kurį būtų galima asocijuoti su vienu prekybiniu ženklu. Apgavikams yra sunku kopijuoti unikalų šriftą, nes jis yra saugomas ir sunkiai pasiekiamas (*G1*) [MBG+17].

Šio prevencijos būdo esminis trūkumas yra jog nenaudojamos žinios yra pamirštamos, todėl naudotojams reiktų periodiškų apmokymų. Žinių pamiršimas ir nenaudojimas skatina duomenų viliojimo atpažinimo tikslumo nuosmukį. Naudotojas gali būti atsargus, tačiau yra galimybė, jog naudotojas bus apgautas ir apsilankys apgaviko svetainėje, todėl dažnai yra pasitelkiami įvairūs programinės įrangos sprendimai, padedantys naudotojui atpažinti duomenų viliojimą ir jo išvengti [ASS20].

1 lentelė. Naudotojų apmokymo prevencijos būdo vertinimas pagal principus

Principas	Vertinimas
P1. Ilgaamžiškumas	- Žinios yra trumpalaikės, mokymai yra pamirštami. - Reikia periodiškų apmokymų žinioms palaikyti.
P2. Tikslumas	- Tikslumas krenta laikui bėgant, nes žinios yra trumpalaikės. - Periodiški apmokymai palaikytų pastovų tikslumo lygį.

1 lentelėje yra pateiktas naudotojų apmokymų prevencijos būdo vertinimas pagal išskirtus principus. Matoma, jog pirmasis prevencijos būdas yra ir trumpalaikis, ir netikslus. Nenaudojamos žinios neįsisavina, o pamirštos žinios nepadeda tiksliai nusakyti, ar tai yra duomenų viliojimo bandymas.

2.2. Juodasis/baltasis sąrašai

Juodasis/baltasis sąrašai (angl. *blacklist/whitelist*) yra dviejų prevencijos būdų sujungimas į vieną. Šis metodas yra naršyklėse kaip viena iš apsauginių priemonių nuo duomenų viliojimo [HTL09]. Baltojo sąrašo metode yra saugomas sąrašas saugių svetainių kartu su jų naudinga informacija. Bet kokia internetinė svetainė, kuri nėra šiame sąraše, yra laikoma įtartina. Jei naudotojas gauna laišką iš apgavikų, kuris yra susijęs su viena iš naudotojo saugių svetainių, naudotojui yra pranešama, jog šio URL detalės nesutampa su esančiomis baltajame sąraše [RGG17]. Esminis šio metodo minusas yra jog bet kokia internetinė svetainė, kurioje naudotojas apsilanko pirmą kartą, yra laikoma įtartina.

Juodasis sąrašas yra baltojo sąrašo priešingybė. Juodajame sąraše yra laikomos žinomos duomenų viliojimo svetainės bei jų informacija. Šie duomenys dažnai yra surenkami iš daug duomenų šaltinių [RGG17]. Nors šis metodas turi labai aukštą tikslumą, jis negali aptikti tų apgavikų puslapių, kurie turi trumpą gyvavimo laiką [ASS20]. Pagrindinis šio metodo minusas – jei svetainė nėra užblokuota juodajame sąraše kaip apgaulinga svetainė, ji nėra atpažįstama kaip duomenų viliojimo svetainė [HTL09]. Dažnai sąraše nebus visų duomenų viliojimo puslapių, nes naujai atsiradusiai svetainei reikia laiko, kol ji bus įtraukta į sąrašą. Naujai sukurta apgavikų svetainė juodajame sąraše atsiranda po dvylikos valandų nuo jos sukūrimo [JG17].

2 lentelė. Juodojo/baltojo sąrašų prevencijos būdo vertinimas pagal principus

Principas	Vertinimas
P1. Ilgaamžiškumas	+ Baltajame sąraše laikomos dažniausiai lankomos svetainės ir tai yra ilgaamžis dalykas, jei naudotojo lankomos svetainės retai/beveik nesikeičia. - Baltasis sąrašas trumpalaikis, jei naudotojo lankomos svetainės dažnai keičiasi ir nėra pastovumo. - Juodasis sąrašas nėra ilgaamžis, nes duomenų viliojimo svetainės nuolat kinta ir sąrašas turi būti nuolat naujinamas. Naujai atsiradusi duomenų viliojimo svetainė neiškart patenka į sąrašą.
P2. Tikslumas	- Baltojo sąrašo tikslumas nėra aukštas, nes visos internetinės svetainės, kuriose yra apsilankoma pirmą kartą, yra laikomos įtartinomis. - Juodojo sąrašo tikslumas aukštas, tačiau jis neatpažįsta trumpą gyvavimo ciklą turinčių internetinių svetainių ar naujų svetainių, dar neįtrauktų į sąrašą.

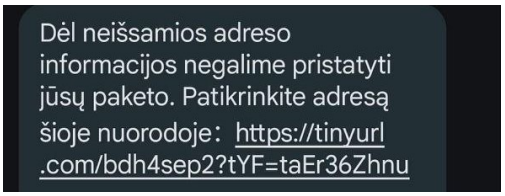
2 lentelėje yra pateiktas juodojo/baltojo sąrašų prevencijos būdo vertinimas pagal ilgaamžiškumą bei tikslumą. Baltasis sąrašas yra ilgaamžis, tačiau netikslus – reikia periodiškai atnaujinti

informaciją naudotojui, kad informacija būtų tiksli. Juodasis sąrašas yra tikslus, tačiau ne ilgaamžis – yra atpažįstamos duomenų viliojimo svetainės, jei jų gyvavimo ciklas nėra trumpas, bet reikia nuolat naujinti informaciją, jog būtų palaikomas prevencijos būdo tikslumas.

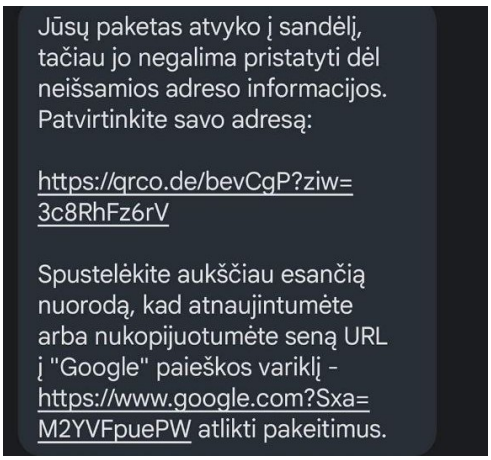
2.3. Mašininis mokymasis bei giliojo mokymosi modeliai

Mašininio mokymosi bei giliojo mokymosi sukurtais modeliais (angl. *deep learning and machine learning-based approach*) duomenų viliojimo svetainės yra atpažįstamos iš charakteristikų rinkinio ar savybių. Savybės yra ištraukiamos iš internetinio puslapio. Pasak šio prevencijos būdo, duomenų viliojimas yra struktūros atpažinimo problema, kuri gali būti išspręsta pasirenkant „teisingą“ savybių rinkinį ir „tinkamą“ atpažinimo algoritmą [WW13]. Dažnai šis metodas yra naudojamas analizuoti URL informaciją bei atitinkamas jų svetaines. URL informacija yra paimama iš adreso juostos ir yra analizuojama pagal pasirinktų savybių rinkinį. Dažniausiai yra tikrinama, ar nėra iškraipytas URL, pavyzdžiui, URL nuorodoje www.po1icija.lt raidė l (L mažoji) paverčiama į 1 (vienetą) *(G5)*. Yra išskiriami URL bruožai, kurie gali parodyti ar tai yra apgavikų svetainė [AAT14; FY21; RSG+21; ZYJ+14]:

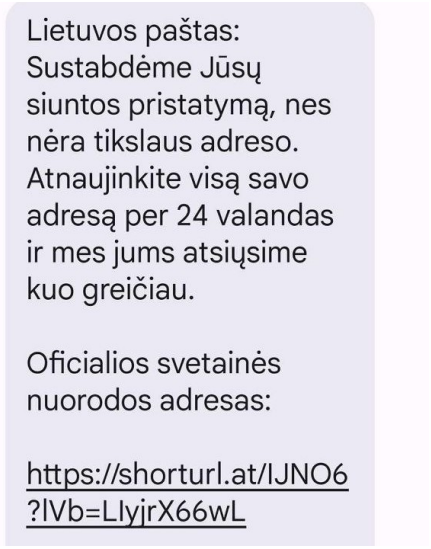
1. **URL ilgis** – dažnai ganėtinai ilgas URL reiškia, jog tai yra apgavikų svetainė, nes ilgoje nuorodoje gali būti paslėpti neįprasti simboliai ar iškraipytas URL su lengvai padirbamomis raidėmis. Nors nėra standartinio patikimo URL ilgio, tačiau yra laikoma, jog ilgesnis nei 54 simbolių URL turėtų būti traktuojamas kaip pavojingas (*G13*).
   Taip pat nuoroda gali būti sutrumpinta (nepilna), kas šiuo metu vis labiau populiarėja, jog būtų galima paprasčiau pasiekti internetinę svetainę. Dažnai apgavikai naudoja populiarius URL trumpintuvus (angl. *URL shortener*). Dažniausiai naudojami URL trumpintuvai šiuo metu yra matomi 3, 4, 5 bei 6 paveiksluose. Tai yra: *tinyurl.com*, *qrco.de*, *shorturl.at* bei *bit.ly* (*G14*).



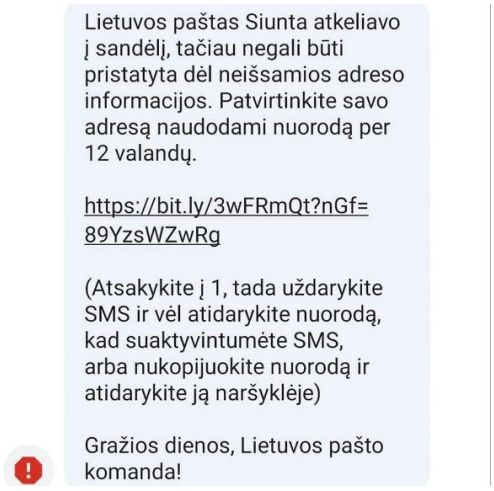
3 pav. Pirmasis pavyzdinis URL trumpintuvas



4 pav. Antrasis pavyzdinis URL trumpintuvas



5 pav. Trečiasis pavyzdinis URL trumpintuvas



6 pav. Ketvirtasis pavyzdinis URL trumpintuvas

2. **Aukščiausio lygio domenas** (angl. *TLD - top level domain*) – kartais sukčiai naudoja pigius aukščiausio lygio domenus, pavyzdžiui „xyz“ ar „info“. Pigių aukščiausio lygio

domenų naudojimas gali sufleruoti, jog tai yra duomenų viliojimo ataka. Šiuo metu dažniausiai naudojami pigūs aukščiausio lygio domenai yra: „xyz“, „info“, „cf“, „gq“, „ml“, „tk“, „ga“, „gd” *(G6)*.

Tačiau net ir „com“ gali kelti įtarimą, jei jis naudojamas lietuviškoje svetainėje. Pavyzdžiui, nuoroda „sebparama.com“, pranešanti, jog yra užblokuota jūsų paskyra yra puikus pavyzdys. „SEB“ bankas turi lietuvišką svetainę, o naudojamas „com“ ir žodis „parama“ taip pat sufleruoja, jog tai yra apgavikai *(G7)*. Kartais yra naudojama daugiau nei vienas aukščiausio lygio domenas, stengiantis paslėpti nuo naudotojų tikrąjį aukščiausio lygio domeną (*G8*).

3. **Neįprasti simboliai URL** – simboliai tokie kaip „ . “ „–“ dažnai yra naudojami keletą kartų apgavikų atsiųstose nuorodose. Jei URL šių simbolių skaičius viršija 3, tai gali sufleruoti jog svetainė yra sukurta apgavikų *(G9)*.

   Jei URL nuorodoje yra simbolis „@”, kuris nukreipia naudotoją į kitą svetainę, tai gali reikšti potencialią duomenų viliojimo ataką ir „@“ yra skaitomas kaip pavojingas simbolis. Pavyzdžiui www.swedbank.lt@netikra.lt nukreips į www.netikra.lt svetainę. Šis simbolis pasitaiko gan dažnai apgavikų atsiųstose nuorodose, nes naudotojui yra sunku atkreipti dėmesį į simbolį, slypintį nuorodos viduryje (*G10*).
4. **Saugumo protokolai** – SSL yra saugumo sluoksnis su duomenų užšifravimo technologijomis. Jei yra naudojamas SSL sertifikatas, nuorodos turi HTTPS protokolą. Jei svetainė neturi SSL sertifikato, yra naudojamas HTTP protokolas (*G11*).
5. **Netikras prisijungimas** – prisijungimo forma, kuri prašo jautrių duomenų, tačiau įvedus prisijungimo vardą bei slaptažodį negalima prisijungti arba įvesta informacija dingsta.
6. **Svetainės piktograma** (angl. *favicon*) – dauguma apgavikų svetainių neturi svetainės piktogramos, kurią turi originali svetainė (*G2*).
7. **IP adresas** – vietoj tekstinės nuorodos, nuoroda sudaryta iš IP adreso, pavyzdžiui http://110.75.2.128 (*G15*).
8. **Žodžių pridėjimas į URL** – prie originalios nuorodos yra pridedami papildomi žodžiai, dar vadinami priesagomis (angl. *suffix*) bei priešdėliais (angl. *prefix*). Pavyzdžiui, www.swedbank-netikra.lt yra ar www.saugus-swedbank.lt yra originalios svetainės nuorodos pakeitimas vienu pridėtiniu žodžiu bei simboliu „ – “. Dažniausi pridėti žodžiai – „saugus“, „patvirtinimas“, „nemokamas“, „išpardavimas“ ar „parama“ *(G12)*.
9. **Internetinės svetainės amžius** – jei internetinė svetainė yra „jaunesnė“ nei pusė metų, ji yra laikoma kaip rizikinga svetainė *(G16)*.

URL ilgis yra svarbus ir mobiliesiems įrenginiams, nes mažesniame ekrane nėra matoma visa nuoroda, o tik jos dalis. Apgavikai naudojasi šia problema ir dėl to dalis atakų yra nukreipiama į išmaniuosius telefonus [SZD+19].

Naudojantis giliojo mokymosi modeliais, galima atpažinti ar svetainė yra tikra, ar apgavikų ir iš svetainės vartotojo sąsajos. Modeliui yra paduodami kriterijai, pagal kuriuos bus vertinama, ar

svetainė yra tikra, ar tai yra duomenų viliojimo bandymas. Kelios dažnos problemos modernaus duomenų viliojimo [SMS+22]:

1. Modernūs duomenų viliojimo puslapiai dažnai apsimeta tam tikra korporacija, pavyzdžiui banku, siuntų tarnyba, tačiau ne visada yra plagijuojama originali vartotojo sąsaja, dažniausiai yra pasiimami tik aspektai iš originalios svetainės, pavyzdžiui logotipas ar spalvos.
2. Dažnai yra prašoma naudotojo įvesti savo asmeninius duomenis, įprastai tai būna keli įvedimo laukai ar išskleidžiamas sąrašas. Šios informacijos prašoma ne formoje, kaip dažnai yra daroma internetinėse svetainėse, o iššokančiame lange (angl. *pop-up window*) (*G3*).
3. Imituojant tikras svetaines, apgavikai sukūrė kelių puslapių procesą (angl. *multipage process*). Tai yra dažna praktika tikrose svetainėse, kuomet naudotojui yra pateikiamas trumpas paaiškinimas ir yra prašoma daugiau jautrios informacijos, tokios kaip mokėjimo informacija.
4. Yra pasitelkiamos modernios naudotojo verifikacijos sistemos, pavyzdžiui CAPTCHA.

Stengiantis spręsti šias problemas, buvo kuriamas giliojo mokymosi metodų šliužas (angl. *crawler*), kuris sekdamas duotus vartotojo sąsajos šablonus stengiasi pereiti prieš tai minėtas problemas ir atpažinti, ar svetainė yra tikra, ar ne. Šiame prevencijos būde yra pasinaudojama juodojo sąrašo metodu bei pasirinktomis euristikomis yra bandoma atpažinti, ar tai yra duomenų viliojimo bandymas. Didžiausias mašininio mokymosi bei giliojo mokymosi modelių pliusas palyginus su juodojo sąrašo metodu yra jog atpažinti svetainę galima realiu laiku, kuomet juodajame sąraše reikia laukti, kol apgavikų puslapis yra įtraukiamas į sąrašą. Šis metodas yra vienas iš tiksliausių būdų, padedančių atpažinti svetainių autentiškumą. Tačiau didžioji dalis šių modelių yra naudojama tik tyrimo tikslais ir jie nėra skirti viešam naudojamui [ASS20].

3 lentelė. Mašininio mokymosi bei giliojo mokymosi modelių prevencijos būdo vertinimas pagal principus

Principas	**Vertinimas**
P1. Ilgaamžiškumas	+ Modelio ilgaamžiškumas priklauso nuo jam paduotų savybių rinkinio. Parinkus gerą savybių rinkinį, šis prevencijos būdas gali būti laikomas ilgaamžiu, kol nepasikeičia duomenų viliojimo atakų bruožai.
P2. Tikslumas	+ Bene tiksliausias prevencijos būdas, jei atpažinti duomenų viliojimo atakas yra paduodamas tinkamas savybių rinkinys. + Atpažįsta duomenis viliojančias svetaines realiu laiku.

3 lentelėje pavaizduota mašininio bei giliojo mokymosi prevencijos būdo vertinimas pagal apsibrėžtus principus. Šis prevencijos būdas yra tiek tikslus, tiek ilgaamžis. Bet norint užtikrinti ilgaamžiškumą, turi būti pasirenkamas tinkamas savybių rinkinys modeliui apmokyti, o nuo to taip pat priklauso ir modelio tikslumas.

2.4. Vizualiniu panašumu grindžiamas metodas

Vizualiniu panašumu grindžiamas metodas (angl. *visual similarity-based approach*) skirtas atpažinti apgavikų sukurtas svetaines iš vartotojo sąsajos, nes dažnai plagijuotos svetainės yra vizualiai panašios ar netgi identiškos palyginus su originaliomis internetinėmis svetainėmis. Šiame prevencijos metode yra lyginama originalios internetinės svetainės vartotojo sąsaja su apgavikų svetainės vartotojo sąsaja, palyginimas vyksta pasirinkus kriterijus. Jei internetinės svetainės yra identiškos, jų URL skiriasi. Tačiau naudotojai ne visada atkreipia dėmesį į URL ar į SSL sertifikatą [JG17], kuris gali išduoti svetainės autentiškumą. Yra keletas skirtingų vizualiniu panašumu grindžiamo metodo variacijų – vieni labiau fokusuojasi į adreso juostą ir jame esančią informaciją, kiti – į internetinės svetainės vizualinį išdėstymą, joje esančio teksto bei paveikslėlių atributus.

Atpažinti ar tai tikra, ar apgavikų svetainė tipiškai yra naudojamos informatyvios įrankių juostos (angl. *toolbar*), kurios atpažįsta svetainės autentiškumą iš HTML kodo, tačiau šios įrankių juostos yra nepajėgios apsaugoti nuo aukšto lygio duomenų viliojimo [DDF+19]. Dažnai naudotojai neatkreipia dėmesio į įrankių juostų siunčiamus perspėjančius pranešimus. Apgavikų svetainės taip pat plagijuoja ir perspėjančius pranešimus juos šiek tiek iškreipdami. Nors naudotojai tokius iškreipimus pamato sunkiai, tačiau algoritmai tai greitai atpažįsta. Todėl atsirado siūlymas kurti detalesnius, labiau perspėjančius vartotojo sąsajos langus, kuriuose pranešama kas padeda atpažinti, jog tai yra potenciali ataka ir stengiamasi pamokyti naudotojus (*G4*) [AAD19]. Taip pat daugiau stengiamasi aptikti duomenų viliojimą atsižvelgiant į CSS kodą. Apgavikai dažnai paprasčiausiai tiesiogiai naudoja svetainės CSS kodą arba nukopijuoja CSS turinį ir išsaugo tai naujai sukurtame faile. Tačiau apgavikai tobulėja kartu su prevencijų būdais ir kuria kitokį CSS kodą analogiškam svetainės įvaizdžiui, todėl neužtenka stengtis atpažinti apgavikų svetaines tik iš kodo, skirto projektuoti vartotojo sąsają [MTL+17]. Reikia prisiminti, jog ne visada duomenų viliojimo svetainė yra identiška originaliai svetainei, kartais yra paimami tik keli aspektai, tokie kaip logotipas ar spalvos.

Naudojantis vizualinio panašumo grindžiamu metodu kartais taip pat yra naudojamas tapatybės nustatymo prevencijos būdas (angl. *identity-based*), kuris tikrina ar pavaizduota tapatybė, pavyzdžiui logotipas ar ženklo vardas, atitinka tikras internetinių svetainių tapatybes remiantis URL. Dažniausiai tai yra daroma pateikiant užklausas paieškos sistemai naudojantis logotipu ar ženklo raktiniais žodžiais, kad paieškos rezultatas nukreiptų į originalią internetinę svetainę. Nors tapatybės nustatymas yra efektyvus būdas surasti duomenų viliojimo svetaines, jo kombinacija kartu su vizualinio panašumo grindžiamu metodu kelia sudėtingumus atpažįstant ženklo internetinės svetainės tapatybę, todėl ši kombinacija prasčiau klasifikuoja originalias svetaines [TCY+23].

Šio prevencijos būdo trūkumai yra jog jei yra lyginama pagal internetinės svetainės vizualinį išdėstymą ir nėra žinoma originali svetainė (URL nėra esminis dalykas), tuomet yra žymiai sunkiau atpažinti apgavikų suprojektuotą internetinę svetainę. Kadangi apgavikai dažniausiai stengiasi padaryti kiek įmanoma panašią svetainę į originalią, kartais šiems metodams yra sunku atpažinti ar tai yra tikra svetainė tik iš vartotojo sąsajos [ZYJ+14].

4 lentelė. Vizualiniu panašumu grindžiamo metodo prevencijos būdo vertinimas pagal principus

Principas	Vertinimas
P1. Ilgaamžiškumas	- Duomenų vagys tobulėja ir vartotojo sąsają plagijuoja įvairiausiais būdais, todėl jei vagys sugeba apeiti kriterijus, keliamus CSS ir/ar HTML kodui, metodas nėra ilgaamžis.
P2. Tikslumas	- Jei stengiamasi atpažinti duomenis viliojančią svetainę tik iš vartotojo sąsajos elementų (neatsižvelgiama į URL), tikslumas yra žemas. - Vizualiniu panašumu grindžiamas metodas kartu su tapatybės nustatymu prastai klasifikuoja originalias svetaines. - Jei duomenis viliojančios svetainės vartotojo sąsaja nėra panaši į originalios svetainės, šis metodas nėra tikslus.

4 lentelėje pateiktas paskutinio prevencijos būdo – vizualiniu panašumu grindžiamo metodo – vertinimas pagal ilgaamžiškumą ir tikslumą. Prevencijos būdas nėra ilgaamžis ir nėra tikslus. Duomenų vagys lengvai plagijuoja vartotojo sąsają, todėl yra sunku pasakyti ar tai yra tikra, ar apgavikų svetainė.

2.5. Apibendrinimas

Peržvelgus esamus prevencijos būdus yra matoma, kad šiuo metu nėra vieno gero būdo apsaugoti naudotojus nuo duomenų viliojimo atakų, kurios turi vartotojo sąsają. Mašininio mokymosi bei giliojo mokymosi modelių rezultatai yra geriausi, tačiau tai priklauso nuo pasirinktų savybių rinkinio bei ar tas modelis bus skirtas ir pritaikytas viešam naudojimui, ar jis bus naudojamas tik moksliniams tyrimams plėtoti. 5 lentelėje yra pateikiama nagrinėtų prevencijos būdų palyginimo lentelė, joje matoma prevencijos būdų ilgaamžiškumo ir tikslumo vertinimai bei yra matomi jų privalumai bei trūkumai iš pasirinktų principų prizmės.

5 lentelė. Prevencijos būdų palyginimo lentelė

Prevencijos būdas	***P1. Ilgaamžiškumas***	***P2. Tikslumas***
Naudotojų apmokymai	Trumpalaikis — palaikyti žinioms reikia periodiškų apmokymų.	Žemas tikslumas — nenaudojamos žinios pamirštamos, kartu krenta ir tikslumo lygis.
Baltasis sąrašas	Baltasis sąrašas – ilgaamžis, jei naudotojo lankomų svetainių sąrašas retai kinta. Trumpalaikis, jei naudotojo lankomos svetainės nėra pastovios.	Žemas tikslumas – visos svetainės, kuriose yra apsilankoma pirmą kartą, laikomos pavojingomis.
Juodasis sąrašas	Juodasis sąrašas – trumpalaikis, nes duomenų viliojimo svetainių sąrašas nuolat kinta.	Aukštas tikslumas – greitai atpažįstamos pavojingos svetainės esančios sąraše, tačiau neatpažįsta svetainių, kurios nėra įtrauktos į sąrašą.
Mašininis mokymasis bei giliojo mokymosi modeliai	Ilgaamžis – jei yra pasirenkamas tinkamas savybių rinkinys.	Aukštas tikslumas – jei yra parenkamas tinkamas savybių rinkinys.
Vizualiniu panašumu grindžiamas metodas	Trumpalaikis – duomenų vagys prasmunka pro nustatytus kriterijus CSS bei HTML kodui.	Žemas tikslumas – apgavikų svetainės ne visada yra originalių svetainių kopijos ir neužtenka tik vartotojo sąsajos elementų, aprašytų HTML ir CSS kodu gauti gerą tikslumą

Nagrinėjant prevencijos būdus buvo renkami duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje – kokie aspektai yra iškraipomi vartotojo sąsajos lange ir į ką reiktų atsižvelgti internetinėse svetainėse.

Duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje:

G1. *Unikalus šriftas* – unikalus šriftas internetinėje svetainėje yra sunkiai padirbamas, todėl reiktų atkreipti dėmesį į šriftą, esantį internetinėje svetainėje.

G2. *Svetainės piktograma* – oficialios svetainės turi savo piktogramas, jos neturėjimas gali sufleruoti, jog svetainė yra netikra.

G3. *Netikras prisijungimas iššokančiame lange* – prisijungimo informacijos ar jautrių duomenų yra prašoma iššokančiame lange. Reiktų akcentuoti, jog iššokančiame lange yra pavojinga įvesti savo jautrius duomenis.

G4. *Perspėjantis langas* – vartotojo sąsajos langas, perspėjantis apie duomenų viliojimą kartu su pranešimu kas padeda atpažinti, jog tai yra ataka. Detalesnis pranešimas vartotojo sąsajos lange, o ne įrankių juostoje turėtų labiau atkreipti vartotojo dėmesį į perspėjimą.

G5. *Lengvai padirbamos raidės URL* – raidės, kurias galima pakeisti į kitus simbolius, turėtų būti akcentuojamos nuorodoje.

G6. *Pigus aukščiausio lygio domenas* – aukščiausio lygio domenas sufleruoja, ar tai yra tikra, ar apgavikų svetainė. Jei tai yra vienas pigių aukščiausio lygio domenų, tai gali reikšti, jog tai yra apgavikų svetainė.

G7. *Ne šalies aukščiausio lygio domenas* – jei naudojamas aukščiausio lygio domenas yra ne šalies kodo aukščiausio lygio domenas, tai gali sufleruoti, jog tai gali būti apgavikų svetainė, todėl turi būti atkreipiamas dėmesys ir į nuorodoje esantį aukščiausio lygio domeną.

G8. *Aukščiausio lygio domenų skaičius URL* – jei URL slypi daugiau nei vienas aukščiausio lygio domenas, tai sufleruoja, jog yra potenciali duomenų viliojimo ataka. Patikimų svetainių URL turi turėti tik vieną aukščiausio lygio domeną.

G9. *Neįprasti simboliai URL* – taškų bei brūkšnelių simbolių dažnas naudojimas turėtų būti akcentuojamas URL.

G10. *„@“ simbolis URL* – „@“ simbolis nuorodoje apgauna vartotoją, reiktų išryškinti nuorodoje tekstą, kuris eina po šio simbolio.

G11. *SSL sertifikatas* – sertifikatas nurodo, jog puslapis yra saugus. Jo nebuvimas gali nurodyti, jog tai yra duomenų viliojimo bandymas. Reiktų atkreipti dėmesį į šio sertifikato buvimą.

G12. *Priesagų bei priešdėlių pridėjimas URL* – prie egzistuojančio URL papildomų žodžių pridėjimas turėtų būti akcentuojamas naudotojui – pridedamas brūkšnelis ir papildomas žodis ne visada yra pastebimi adreso juostoje.

G13. *Ilgas URL* – nuorodos ilgis turėtų būti akcentuojamas, nes mažesniame ekrane, pavyzdžiui, išmanaus telefono, nėra matoma visa nuoroda, o ilgesnėje nuorodoje gali slypėti URL iškraipymai.

G14. *URL trumpintuvas* – apgavikai gali naudotis URL trumpintuvais, todėl reiktų atkreipti dėmesį į URL – ar nuorodoje nėra matomi populiarūs trumpintuvai.

G15. *IP adresas* – URL nuorodoje esantis IP adresas parodo, jog tai nėra oficiali svetainė. Vartotojų dėmesys turi būti atkreiptas į IP adresą esantį adreso juostoje.

G16. *Svetainės amžius* – nors tai nėra pastebimas dalykas, tačiau reiktų akcentuoti, jog nežinomų svetainių naudotojai turėtų vengti – kartais nežinoma svetainė gali reikšti, jog ji yra „jauna“ ir sukurta apgavikų.

6 lentelėje pateikti surinkti duomenų viliojimo atpažinimo požymiai, sugrupuoti į vartotojo sąsajos plagijavimo požymius, URL iškraipymo požymius bei taip pat į URL slėpimo požymius.

6 lentelė. Sugrupuoti duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje

Vartotojo sąsajos plagijavimo požymiai	**URL iškraipymo požymiai**	**URL slėpimo požymiai**
G1. Unikalus šriftas *G2.* Svetainės piktograma *G3.* Netikras prisijungimas iššokančiame lange *G4.* Perspėjantis langas	*G5.* Lengvai padirbamos raidės *G6.* Pigus aukščiausio lygio domenas *G7.* Ne šalies aukščiausio lygio domenas *G8.* Aukščiausio lygio domenų skaičius URL *G9.* Neįprasti simboliai URL *G10.* „@“ simbolis URL *G11.* SSL sertifikatas *G12.* Priesagų bei priešdėlių pridėjimas URL	*G13.* Ilgas URL *G14.* URL trumpintuvas *G15.* IP adresas *G16.* Svetainės amžius

3. Kuriamos sistemos aprašas

Šiame skyriuje yra aprašomi kuriamo naršyklės plėtinio scenarijai ir pateikiami maketai, kuriems atliktas formuojantis panaudojamumo testavimas ir pateikti testavimo rezultatai. Pasirinkta projektuoti naršyklės plėtinį, nes tai yra lengvai naudojamas įrankis – naudotojui nereikia mokytis kaip naudotis naujai gauta įranga, sistema parodo įspėjimus su paaiškinimais kodėl tai yra galimai pavojinga svetainė.

3.1. Plėtinio aprašas

Pagal išnagrinėtus prevencijos būdus bei darbe surinktus duomenų viliojimo atpažinimo požymius bus projektuojamas „Google Chrome“ naršyklės plėtinys (angl. *browser extension*), kuris bus pagalbinė priemonė naudotojui atpažinti duomenų viliojimo atakas. Plėtinys analizuos adreso juostoje esantį URL bei pateiks informaciją apie rastą potencialią duomenų viliojimo ataką.

Plėtinys įgyvendins išskirtą duomenų viliojimo atpažinimo požymį – perspėjantį langą (*G4*), kuriame bus pateikta kodėl nuoroda potencialiai pavojinga. Surinkti URL iškraipymo bei slėpimo požymiai bus naudojami atpažinti duomenų viliojimo atakas, turinčias vartotojo sąsają, bei bus pateikiama informacija naudotojui kaip atpažinti išskirtus duomenų viliojimo atpažinimo požymius. Išskirti požymiai skirti ne tik naršyklės plėtinio projektuotojams, bet taip pat ir naudotojams atpažinti duomenų viliojimo atakas.

3.2. Scenarijai

Naudotojui palankaus projektavimo procese visuose projektavimo etapuose naudotojas yra įtraukiamas į sprendimų priėmimą. Kuriami keli scenarijai, jog būtų palyginamas sprendimų efektyvumas ir būtų gaunamas kokybiškas rezultatas.

Scenarijuose yra norima atkreipti naudotojo dėmesį į URL slypinčią informaciją. Scenarijuose skiriasi informacijos išdėstymo stilius bei informacijos kiekis. Pirmame scenarijuje naudotojui matomas naršyklės langas su įspėjama informacija bei padidintu URL. Informacijos kiekis šiame scenarijuje didesnis – perspėjimai matomi prie padidinto URL bei išsiskleidžiančių langų, kuriuose iškart matomi rastų duomenų viliojimo atpažinimo požymių aprašymai. Antrasis scenarijus skirtas atpažinti tik duomenų viliojimo elektroninius laiškus, matomas šoninis naršyklės langas. Informacija perteikiama labiau koncentruotai – URL modifikuojamas toje vietoje, kurioje jis yra rastas, o išskleistas langas rodytų visą informaciją iškart.

Antrame scenarijuje optimizuojamas informacijos kiekis bei sutelkiamas dėmesys į vieną atakų tipą – elektroninius laiškus. Pirmasis scenarijus perteikia daugiau informacijos, naudojamas dažnesnis išdėstymo stilius bei atpažįstamos visos duomenų viliojimo atakos, turinčios vartotojo sąsają. Tikslas – patikrinti kuris iš šių sprendimų yra efektyvesnis naudotojui, kuriame naudotojas greičiau randa informaciją bei kuris maketas naudotojams atrodo patrauklesnis ir lengvesnis naudoti.

3.2.1. Pirmasis scenarijus

Pirmame žingsnyje naudotojas mato apgaviko elektroninį laišką, kuriame yra nuoroda ir ją paspaudžia. Antrame žingsnyje naršyklėje yra atidaromas vartotojo sąsajos langas, kuriame matoma:

- padidintas URL;
- priežastys, kodėl tai yra potencialiai pavojinga svetainė (lengvai padirbamos raidės (*G5*), neįprasti simboliai URL (*G9*) ir t.t.);
- apačioje kairėje esantis mygtukas „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“;
- apačioje dešinėje esantis mygtukas „Grįžti prie saugumo“.

Trečiame žingsnyje naudotojas detaliau peržiūri URL, jei kompiuterio pelytė yra virš pavojų keliančios vietos URL, toji vieta yra paryškinama kita spalva ir yra matomas mažas iššokantis pranešimas. Pranešimas nurodo kokia vieta nuorodoje yra iškraipyta, kelianti pavojų. Prie priežasčių, kodėl tai gali būti pavojinga svetainė, yra parašomas detalesnis aprašas (1–2 sakiniai). Ketvirtame žingsnyje naudotojas perskaito aprašą, detaliau paaiškinantį URL pavojingas dalis. Paspaudus „Daugiau“ yra pateikiamas panašių adresų sąrašas. Naudotojas gali paspausti „Grįžti prie saugumo“ ir yra nukreipiamas į pradinį naršyklės langą. Jei naudotojas paspaudžia „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“, jis yra nukreipiamas į potencialiai pavojingą svetainę.

3.2.2. Antrasis scenarijus

Pirmame žingsnyje naudotojas mato atidarytą elektroninio pašto dėžutę ir atidaro paskutinįjį gautą elektroninį laišką. Laiške yra nuoroda ir mygtukas, o mygtuke yra paslėpta nuoroda. Antrame žingsnyje naudotojas paspaudžia matomą nuorodą ar mygtuką ir yra analizuojama rasta nuoroda. Nuoroda yra modifikuojama – išryškinamos vietos, kurios potencialiai kelia pavojų bei yra matomas šoninis langas naršyklėje. Šoniniame lange yra matomos URL pavojų keliančių vietos bei paspaudus „Daugiau“, yra parodomi paaiškinimai kartu su panašiais URL adresais naudotojui susipažinti. Apačioje šoninio lango yra du mygtukai – kairėje „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“, kurį paspaudus naudotojas yra nukreipiamas į galimai pavojingą svetainę; dešinėje matomas „Pažymėti kaip šlamštą“ mygtukas, kuris pažymi laišką kaip šlamštą ir jis yra perkeliamas iš naudotojo pagrindinės pašto dėžutės į šlamšto skyrelį pašto dėžutėje.

3.3. Plėtinio maketai

Naršyklės plėtinio maketų kūrimui buvo naudojamas prototipų kūrimo įrankis „Figma“. Maketai[1] suprojektuoti pagal prieš tai aprašytus scenarijus. Pirmasis maketas įgyvendina pirmąjį scenarijų (žr. 3.2.1 Pirmasis scenarijus), antrasis maketas įgyvendina antrąjį scenarijų (žr. 3.2.2 Antrasis scenarijus). Maketuose buvo naudojamas apgaulingos duomenų atakos pavyzdys, kuris

[1]Pirmasis maketas – `https://www.figma.com/file/GdeoDulhjmbAQdOcCBUxSg/Kursiniomaketas-Nr.-1?type=design&node-id=0-1&mode=design`
Antrasis maketas – `https://www.figma.com/file/htwoWpY1hblkL2Fh9NC4Sh/Kursinio-maketas-Nr.-2?type=design&mode=design`

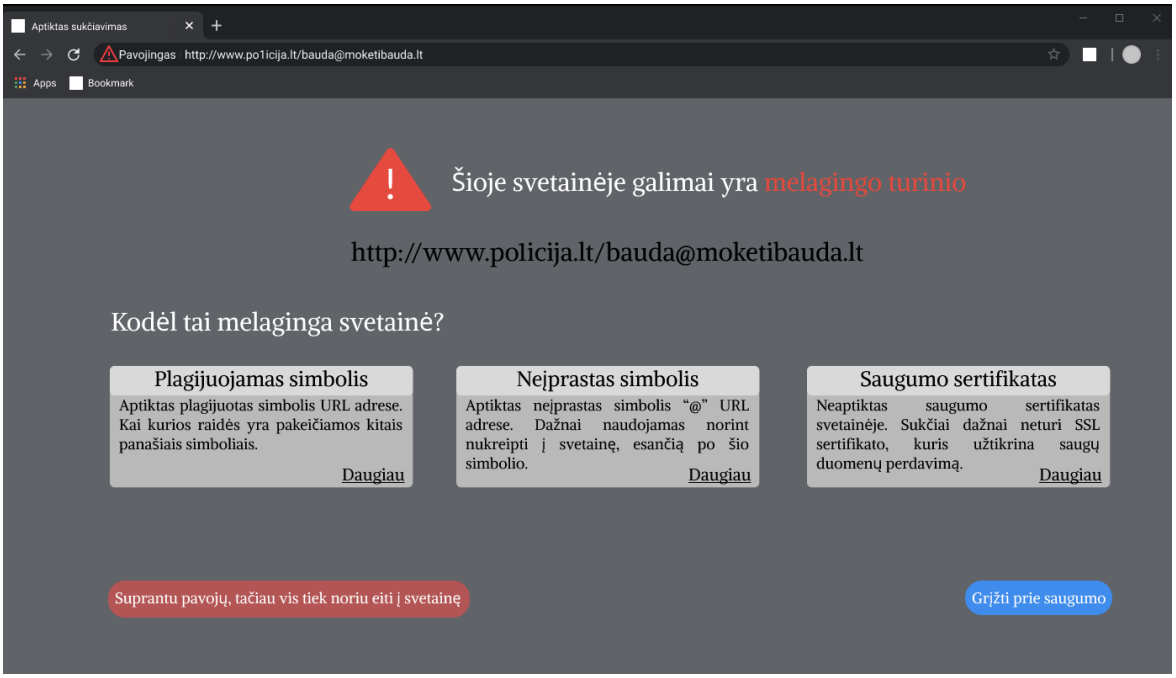
yra matomas 2 pav. Naudotojai gauna laiškus, kurie reikalauja naudotojo informacijos ir ji turi būti suteikiama paspaudus laiške esančią nuorodą. Pasirinkta maketus kurti su elektroninio laiško pavyzdžiu, nes tai yra dažniausias duomenų viliojimo atakų būdas orientuotas į kompiuterius. Darbe rinkti duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje naudojami tiek naršyklės plėtinio projektuotojo atpažinti duomenų viliojimo požymius, tiek supažindinti naudotojus su duomenų viliojimo požymiais.

Buvo sukurti du scenarijai, jog būtų tiriama galimų projektinių sprendimų erdvė kuriant maketus, siekiant įvertinti galimų sprendimų veiksmingumą. Ruošiantis panaudojamumo testavimui suformuluoti sėkmės kriterijai bei matai su užduotimis kiekvienam maketui. Formuojantis panaudojamumo testavimas su naudotojais leis pasirinkti veiksmingesnius sprendimus bei gauti grįžtamąjį ryšį apie maketus. Testavimo rezultatas – išrinkti geriausią iš dviejų maketų bei jį patobulinti.

3.3.1. Pirmasis maketas

Šiame skyriuje yra pateikiamas pirmasis maketas, kuriame yra įgyvendintas pirmasis scenarijus (žr. 3.2.1 skyrių).

Maketas pateikia visą informaciją atskirame lange, jog visas naudotojo dėmesys būtų sutelktas į perspėjimą. Padidintas URL padeda naudotojui rasti potencialiai pavojingas vietas, o išsiskleidžiantys elementai supažindina naudotoją su rastu duomenų viliojimo požymiu.



7 pav. Pirmojo maketo perspėjantis langas

Makete yra nagrinėjamas adreso juostoje esantis URL. Jei adreso juostoje esantis URL turi duomenų viliojimo bruožų, tuomet naudotojas mato naują vartotojo sąsajos langą, kuriame yra parodoma kodėl tai gali būti potenciali duomenų viliojimo ataka (žr. 7 pav.). Naudotojui pabraukus kompiuterine pelyte virš padidintos nuorodos, iššoktų mažas pranešimas su rastu duomenų viliojimo požymiu.

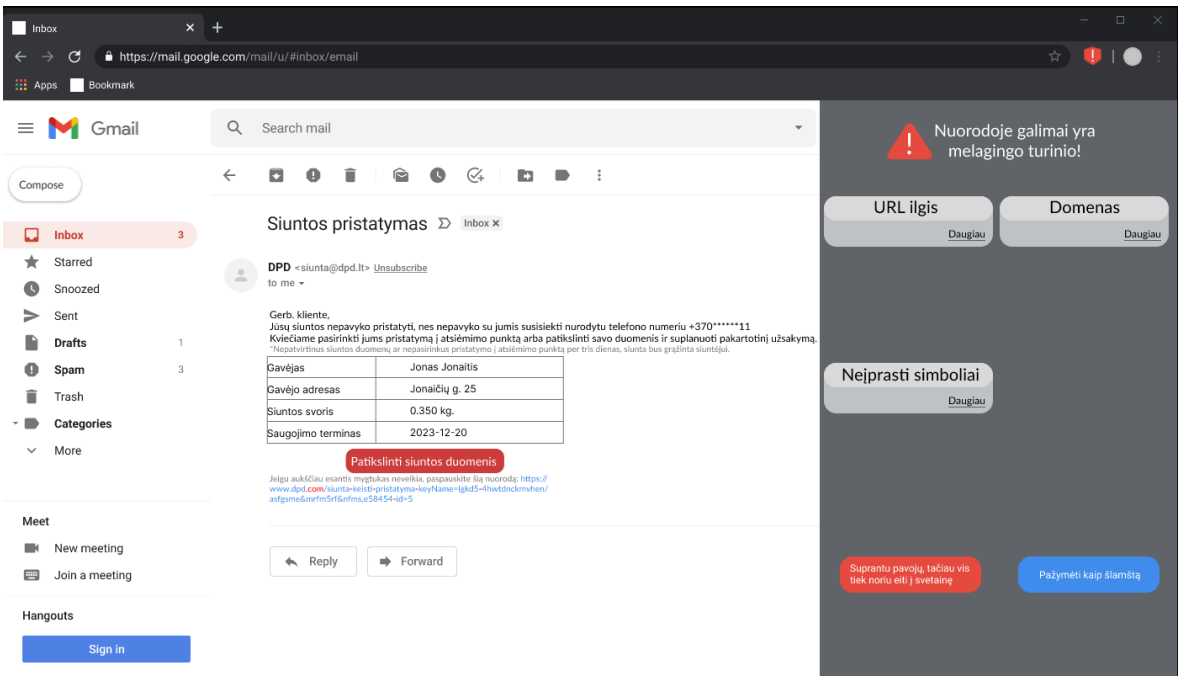
8 pav. Pirmojo maketo detalesnis perspėjimas

8 pav. yra pavaizduota galimų duomenų viliojimo priežasčių detalesni aprašai – prie paaiškinimų yra matomi kitų panašių svetainių pavyzdžiai.

3.3.2. Antrasis maketas

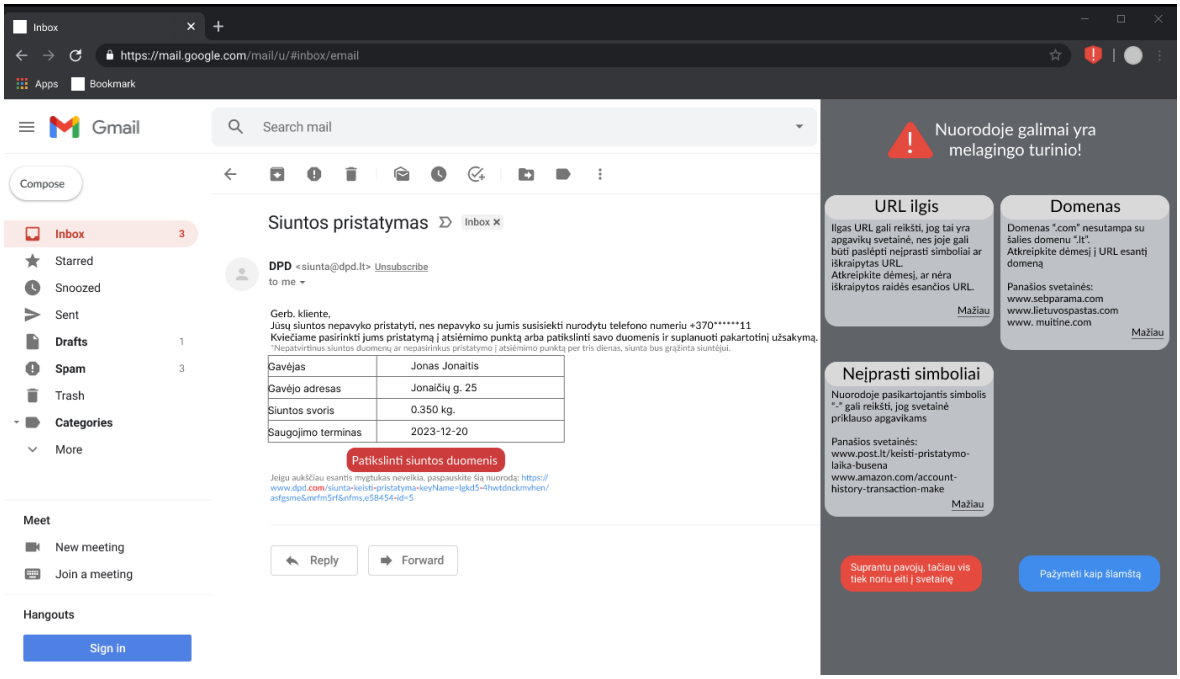
Šiame skyriuje yra pateiktas antrasis maketas, kuriame yra įgyvendintas antrasis scenarijus (žr. 3.2.2 skyrių).

Makete informacija pateikiama šoniniame lange, jog naudotojas galėtų matyti perspėjantį langą bei gautą laišką viename lange. Laiške esanti nuoroda yra modifikuojama ir atkreipiamas dėmesys į rastas pavojingas vietas, o šoniniame lange yra pateikiami detalūs paaiškinimai apie rastus duomenų viliojimo požymius.



9 pav. Antrojo maketo perspėjantis langas

Makete yra nagrinėjamas URL, į kurį ruošiamasi nukreipti naudotoją. Jei URL turi duomenų viliojimo bruožų, tuomet naudotojas mato naują vartotojo sąsajos langą dešiniame šone, kuriame yra parodoma kodėl svetainė yra laikoma pavojinga (žr. 9 pav.).



10 pav. Antrojo maketo detalesni perspėjimai

10 pav. yra pavaizduota kaip antrame makete atrodo detalesnis rastų duomenų viliojimo atpažinimo požymių aprašas – atsiranda paaiškinimas bei yra matomi kitų panašių svetainių pavyzdžiai.

3.4. Maketų testavimas

Šiame skyriuje yra atliekamas dviejų maketų panaudojamumo testavimas su naudotojais. Pirmasis maketas yra aprašytas 3.3.1 skyrelyje, antrasis maketas – 3.3.2 skyrelyje.

3.4.1. Testavimo tikslai

Maketų testavimo tikslas yra sužinoti kuris maketas yra patogesnis naudotojams – kuriame naudotojas sklandžiai pereina užduotis bei kuriame greičiau randama norima informacija.

3.4.2. Testavimo aplinka

Testavimas atliktas nuotoliniu būdu per „Zoom“ platformą. Testavimo pradžioje pateikiamas klausimynas – prašoma dalyvio charakteristikų ir užpildžius formą, nusiunčiamos maketų nuorodos. Dalyvis pasidalina savo ekranu ir atlieka užduotis kiekvienam maketui, o stebėtojas fiksuoja per kiek laiko bei paspaudimų užduotis sėkmingai užbaigiama.

Po testavimo dalyviai pateikia pastabas, pasiūlymus apie maketus ir pasako, kuris maketas labiau patiko, kokie yra maketų trūkumai.

3.4.3. Testavimo dalyviai

Viso testavimo metu laiką, paspaudimų skaičių bei gaunamas pastabas fiksuoja stebėtojas. Testavimas atliktas su 5 dalyviais. Kokybiniam tyrimui užtenka ir 5 dalyvių, nes po penkto dalyvio yra gaunami pakartotiniai pastebėjimai ir nėra nieko naujo sužinoma. Panaudojamumas yra kokybiškai ištestuojamas bei nėra švaistomi projekto resursai, kuriuos būtų galima panaudoti kituose testavimuose [Nie00; NL93]. Jog būtų užtikrintas panaudojamumo testavimo patikimumas, buvo parinkta įvairaus amžiaus bei IT naudojimo gebėjimų lygių dalyviai. IT gebėjimo lygis nustatomas su klausimynu, pateiktu 1 priedas, IT gebėjimo lygių paaiškinimas skyriuje. Kuo ilgiau yra naudojamos išvardintos technologijos bei kuo ilgiau yra naudojamas kompiuteris, tuo aukštesnis yra naudojimosi informacinėmis technologijomis lygis.

7 lentelėje yra pateikiama informacija apie dalyvius bei jų charakteristikas.

7 lentelė. Testavimo dalyvių charakteristikos

Dalyvio nr.	Amžius	Lytis	IT gebėjimo lygis	Ar žinote kas yra duomenų viliojimo atakos? Ar yra tekę susidurti su duomenų viliojimo atakomis?
1.	50	Moteris	Pradedančioji	Žino kas yra duomenų viliojimo atakos. Yra gavus elektroninius laiškus su pavojingomis nuorodomis.
2.	26	Moteris	Pažengusi	Žino kas yra duomenų viliojimo atakos. Yra susidūrus su jomis, tekę gauti skambučius bei SMS pranešimus.
3.	22	Vyras	Pažengęs	Žino duomenų viliojimo atakas. Yra gavęs SMS pranešimus bei elektroninius laiškus su pavojingomis nuorodomis.
4.	17	Moteris	Pradedančioji	Nežino termino duomenų viliojimas ar angliško „phishing“ termino. Pateikus pavyzdžius, pareiškė, jog žino apie šias atakas, tačiau nėra tekę susidurti asmeniškai.
5.	23	Vyras	Ekspertas	Žino apie duomenų viliojimo atakas. Yra gavęs elektroninius laiškus su pavojingomis nuorodomis.

3.4.4. Testavimo užduotys ir jų sėkmės kriterijai bei matai

Pagrindinė šio testavimo užduotis yra sėkmingai išspręsti duotas užduotis. Užduotis yra padalinta į žingsnius, jog būtų galima žinoti kur dalyviui sekasi puikiai, o kur jis sustoja ir nebežino kaip tęsti.

Kadangi maketai skiriasi, nors ir nežymiai, yra sudaromos skirtingos užduotys. Užduotys maketams yra pateiktos 8 bei 9 lentelėse. 8 lentelėje yra pateikiamos užduotys pirmajam maketui kartu su sėkmės kriterijais, 9 lentelėje pateikiamos užduotys bei sėkmės kriterijai antrajam maketui.

8 lentelė. Pirmojo maketo sėkmės kriterijai bei matai

Nr	Užduoties žingsniai	Sėkmės kriterijus	Sėkmės matas (sekundės arba paspaudimų skaičius)
1.	Paspausti ant nuorodos	Yra paspaudžiama laiške esanti nuoroda ir yra matomas perspėjimo langas	1 paspaudimas
2.	Peržiūrėti detalesnį perspėjimo aprašą	Paspaudžiama „Daugiau“ ant visų trijų perspėjimų	3 paspaudimai – kiekviena priežastis turi būti paspausta vieną kartą
3.	Peržvelgti URL esančias pavojingas vietas	Kompiuterio pelytė yra laikoma virš URL esančių pavojingų vietų ir yra matomas iššokantis pranešimas su perspėjimu	10 sekundžių
4.	Grįžti į saugų puslapį	Paspaudžiamas „Grįžti prie saugumo“ mygtukas	1 paspaudimas
5.	Nueiti į pavojingą puslapį	Paspaudžiama laiške esanti nuoroda. Atidaromas perspėjimo langas. Paspaudžiama „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“	2 paspaudimai

9 lentelė. Antrojo maketo sėkmės kriterijai bei matai

Nr	Užduoties žingsniai	Sėkmės kriterijus	Sėkmės matas (sekundės arba paspaudimų skaičius)
1.	Atidaryti elektroninį laišką	Yra atidaromas neperskaitytas elektroninis laiškas pašto dėžutėje	1 paspaudimas
2.	Paspausti ant mygtuko/nuorodos	Paspaudžiama „Patikslinti siuntos duomenis“ arba apačioje esanti nuoroda ir yra atidaromas perspėjantis šoninis langas	1 paspaudimas
3.	Peržiūrėti detalesnius perspėjimų aprašus	Prie kiekvieno perspėjimo, esančio šoniniame lange, paspaudžiamas mygtukas „Daugiau“	3 paspaudimai – kiekvienam perspėjimui po vieną paspaudimą
4.	Nueiti į pavojingą puslapį	Paspaudžiama „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“. Atidaromas pavojingos svetainės puslapis	1 paspaudimas
5.	Pažymėti laišką kaip brukalą	Atidaromas laiškas. Paspaudžiama mygtukas/nuoroda. Perspėjimo lange paspaudžiamas „Pažymėti kaip brukalą“. Iššokančiame lange paspaudžiamas „Pranešti apie šlamštą“	4 paspaudimai

3.4.5. Testavimo rezultatai

Visi dalyviai atliko užduotis sėkmingai. Tačiau iš gautų pastabų pastebėta, jog pirmas maketas dalyviams patiko labiau nei antras – panaudotas šriftas padėjo labiau pastebėti pavojingas vietas padidintoje nuorodoje bei detalūs perspėjimai perteikia informaciją.

Atlikus testavimą, dalyviai pateikė rekomendacijas kaip būtų galima patobulinti maketus:

1. Pasiūlyta perspėjimuose labiau koncentruotai pateikti informaciją – perspėjimas sudaromas iš vieno sakinio, bet paliekant pavyzdžius palyginimui. Informacijos kiekį pasirenka naudotojas – pirma mato tik duomenų viliojimo požymio pavadinimą, o išskleidus matytų paaiškinimą bei pavyzdinius URL.
2. Maži įspėjantys pranešimai prie pavojingų vietų nuorodoje turėtų būti matomi iškart, o ne perbraukus kompiuterio pelyte virš padidintos nuorodos.
3. Iššokantis langas būtų modernesnis sprendimas, labiau patinkantis naudotojams.
4. Pavojingas vietas URL iš karto paryškinti, jog naudotojas galėtų pastebėti pavojingas vietas ir į ką reiktų atkreipti dėmesį.

Po testavimo taip pat buvo priimti tokie sprendimai:

1. Jei nuorodoje yra „@“ simbolis, įspėjimo lange paryškinti nuorodos dalį, einančią po simbolio ir paklausti naudotojo, ar jis tikrai jungiasi prie minėtosios svetainės.
2. Nusprendus kurti iššokantį langą, pridėti papildomą vartotojo sąsajos langą. Lange būtų įspėjama jog rastas potencialus duomenų viliojimas, o išsami informacija randama iššokančiame lange. Perspėjimas skirtas naudotojams, turintiems reklamų blokavimo programą (angl. *ad blocker*) – norint pamatyti visą įspėjimą, reiktų išjungti reklamų blokavimo programą.

Testavimo dalyvių rezultatai yra pateikti 2 priede. Maketų testavimas skyriuje.

4. Naršyklės plėtinio įgyvendinimas

Šiame skyriuje yra aprašoma įgyvendinto naršyklės plėtinio funkciniai bei nefunkciniai reikalavimai, architektūra bei jos pagrindiniai komponentai. Naršyklės plėtinys sukurtas atsižvelgiant į 3 skyriuje aprašytus sistemos scenarijus.

4.1. Naršyklės plėtinio reikalavimai

4.1.1. Funkciniai reikalavimai

FR1. Sistema turi pateikti naudotojui perspėjantį langą aptikus duomenų viliojimo atpažinimo požymius.

FR2. Sistema padirbtas raides turi pakeisti į panašią raidę ir patikrinti, ar tokia internetinė svetainė egzistuoja.

FR3. Sistema turi patikrinti ar egzistuoja svetainė su šalies aukščiausio lygio domenu.

FR4. Sistema turi pateikti naudotojui URL, į kurį jis yra nukreipiamas su neįprastu simboliu „@“.

FR5. Sistema turi patikrinti, ar internetinė svetainė turi saugumo protokolą.

FR6. Sistema turi patikrinti ar nuorodoje nėra URL trumpintuvų, slepiančių tikrąją nuorodą.

FR7. Sistema turi patikrinti, ar nuorodoje nėra populiariausių pigių aukščiausio lygio domenų.

FR8. Sistema turi aptikti perteklinį neįprastų simbolių kiekį URL.

FR9. Sistema turi aptikti IP adresą, esantį URL.

FR10. Sistema turi patikrinti, ar nuorodos ilgis neviršija saugaus nuorodos ilgio.

FR11. Sistema turi aptikti populiariausius pridėtinius žodžius URL.

FR12. Sistema turi patikrinti, jog nėra daugiau nei vieno aukščiausio lygio domeno URL.

FR13. Sistema turi pateikti naudotojui paryškintas pavojingas vietas.

FR14. Sistema turi pateikti mažus pranešimus šalia pavojingos vietos.

FR15. Sistema turi pateikti detalų paaiškinimą bei pavyzdžius naudotojui.

10 lentelė. Duomenų viliojimo atpažinimo požymių vartotojo sąsajoje bei funkcinių reikalavimų atsekamumo matrica

	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16
FR1				X												
FR2					X											
FR3							X									
FR4										X						
FR5											X					
FR6														X		
FR7						X										
FR8									X							
FR9															X	
FR10													X			
FR11												X				
FR12								X								
FR13					X	X	X	X	X	X		X		X	X	
FR14					X	X	X			X		X		X	X	
FR15					X	X	X	X	X	X	X	X	X	X	X	

10 lentelėje pateikta duomenų viliojimo atpažinimo požymių vartotojo sąsajoje bei funkcinių reikalavimų atsekamumo matrica, kurioje matoma kokie požymiai įgyvendinti naršyklės plėtinyje. Vartotojo sąsajos plagijavimo požymiai (unikalus šriftas, svetainės piktograma, Netikras prisijungimas iššokančiame lange *(G1–G3)*) nėra įgyvendinti, nes jų negalima aptikti prieš atakos pradžią – naudotojas turi patekti į pavojingą svetainę, jog šie požymiai būtų aptikti. Svetainės amžius *(G16)* neįgyvendintas sistemoje, nes neužtenka URL, jog būtų patikrintas svetainės amžius.

4.1.2. Nefunkciniai reikalavimai

NFR1. Sistema turi veikti „Google Chrome“ naršyklėje.

NFR2. Sistemos duomenys saugomi lokalioje duomenų bazėje.

NFR3. Sistema turi veikti aptikus bent vieną duomenų viliojimo atpažinimo požymį.

NFR4. Vienu metu gali būti atidarytas tik vienas naršyklės plėtinio perspėjantis langas.

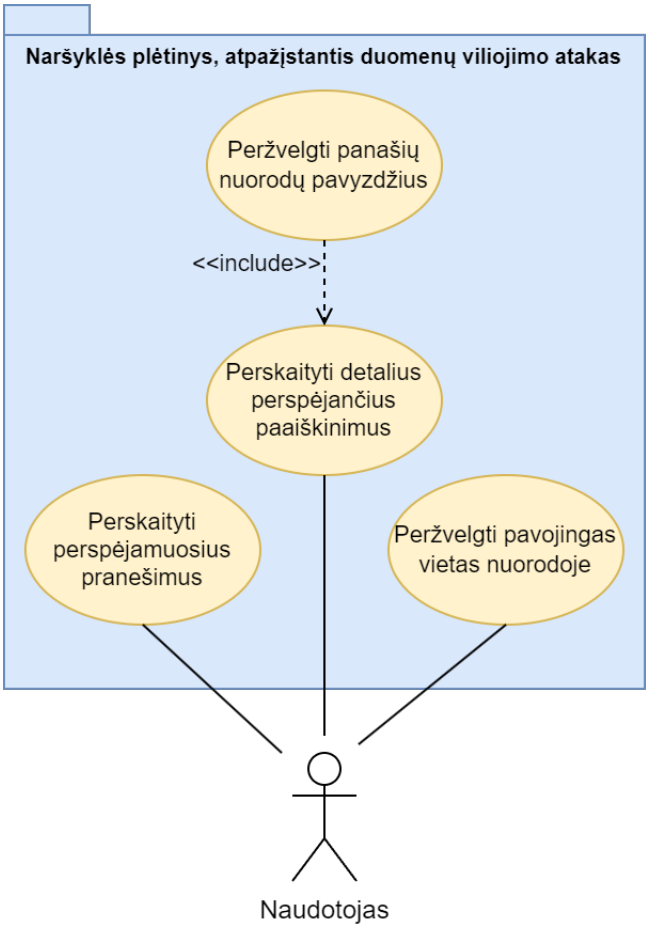
4.2. Naršyklės plėtinio architektūra

Šiame skyriuje yra pateikiama naršyklės plėtinio, skirto atpažinti duomenų viliojimo atakas „Google Chrome“ naršyklėje, architektūra naudojantis UML diagramomis.

4.2.1. Naudojimo atvejų diagrama

11 pav. yra pateikta naršyklės plėtinio naudojimo atvejų diagrama. Naudotojas gali perskaityti perspėjančius pranešimus, esančius šalia padidintos nuorodos naršyklės plėtinio lange.

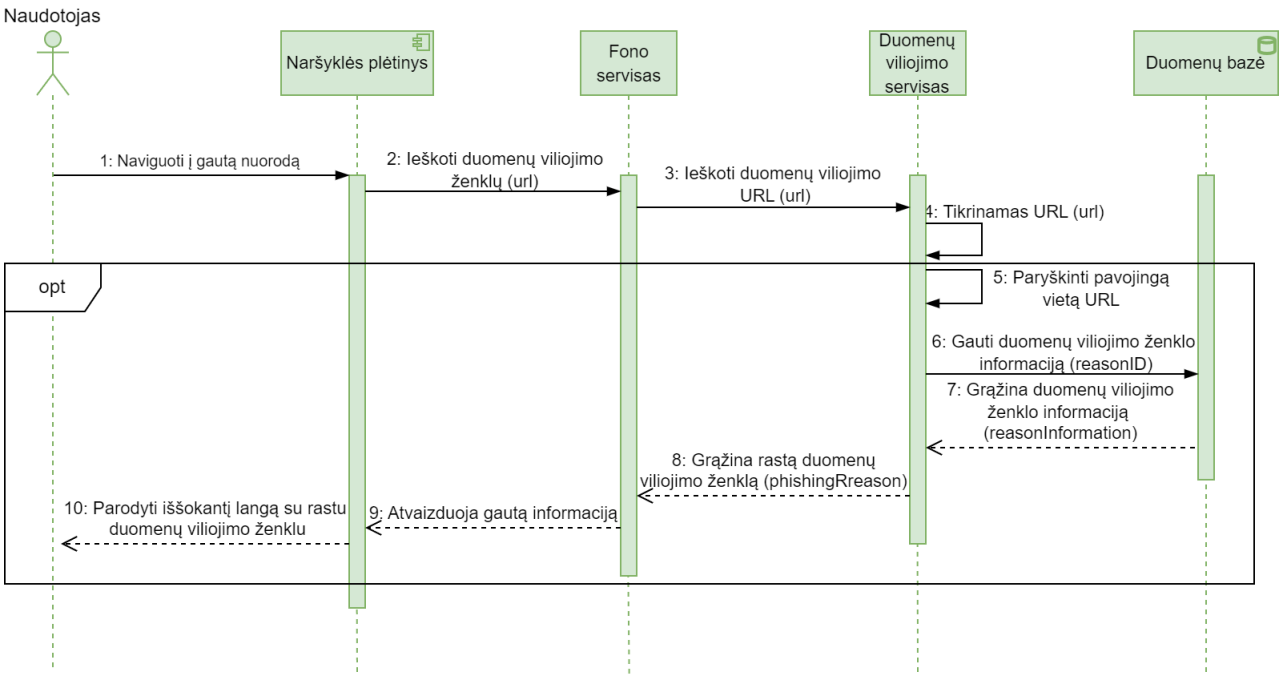
Padidintoje nuorodoje naudotojas taip pat gali peržvelgti pavojingas vietas, kurios yra paryškinamos. Naršyklės plėtinio naudotojas taip pat gali perskaityti detalius perspėjančius paaiškinimus, kuriuose yra pateikiama koks duomenų viliojimo atpažinimo požymis buvo rastas ir trumpas požymio paaiškinimas. Kuomet yra atidaromas detalus perspėjantis paaiškinimas, atsiranda galimybė pamatyti panašias nuorodas, kuriose yra rastas duomenų viliojimo požymis.



11 pav. Naudojimo atvejų diagrama

4.2.2. Sekų diagrama

12 pav. yra pavaizduota sekų diagrama bei sąveika tarp naudotojo, naršyklės plėtinio ir jo servisų – fono bei duomenų viliojimo servisų – bei duomenų bazės. Pirma, naudotojas bando patekti į svetainę. Naršyklės plėtinys perima šią informaciją ir kviečia fono servisą. Fono servisas nuskaito URL svetainės, į kurią naudotojas bando patekti, ir siunčia tai duomenų viliojimo servisui, jog būtų ieškoma ar URL yra paslėpti duomenų viliojimo požymiai. Jei yra randamas požymis, pavojinga URL vieta yra paryškinama, siunčiama užklausa į duombazę, jog būtų gaunama duomenų viliojimo ženklo informacija. Informacija yra grąžinama duomenų viliojimo servisui, kuris apdoroja gautą informaciją, siunčia ją fonui servisui. Fono servisas atvaizduoja gautąją informaciją ir naršyklės plėtinys parodo iššokantį langą su rastu duomenų viliojimo atpažinimo požymiu.



12 pav. Sekų diagrama

4.2.3. Techninis įgyvendinimas

Naršyklės plėtinys sukurtas „Google Chrome“ naršyklei, su JavaScript kalba, duomenys saugomi IndexedDB duomenų bazėje.

Sukurtas naršyklės plėtinys, paleidimo instrukcija ir demonstracinis video yra pasiekiami 3 priedas, Įgyvendintas naršyklės plėtinys priedų skyriuje.

4.3. Įgyvendinti naršyklės plėtinio komponentai

Šiame skyrelyje yra aprašomi įgyvendinti naršyklės plėtinio komponentai bei jų veikimas.

4.3.1. URL tikrinimas

Naršyklės plėtinio darbas prasideda nuo URL, į kurį bando patekti naudotojas, nagrinėjimo. URL yra ieškoma duomenų viliojimo atpažinimo požymių, kurie buvo renkami 2 skyriuje, duomenų viliojimo atakų prevencijų apžvalgoje. Naršyklės plėtinyje įgyvendinti tie duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje, kurie yra susiję su URL bei kuriuos galima aptikti prieš naudotojui patenkant į potencialiai pavojingą svetainę. Naršyklės plėtinys yra skirtas sukoncentruoti dėmesį į patį URL, kuriame galima aptikti daugiausia duomenų viliojimo požymių. Įgyvendinti duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje:

G4. *Perspėjantis langas.*
G5. *Lengvai padirbamos raidės URL.*
G6. *Pigus aukščiausio lygio domenas.*
G7. *Ne šalies aukščiausio lygio domenas.*
G8. *Aukščiausio lygio domenų skaičius URL.*

G9. *Neįprasti simboliai URL.*

G10. *„@“ simbolis URL.*

G11. *SSL sertifikatas.*

G12. *Priesagų bei priešdėlių pridėjimas URL.*

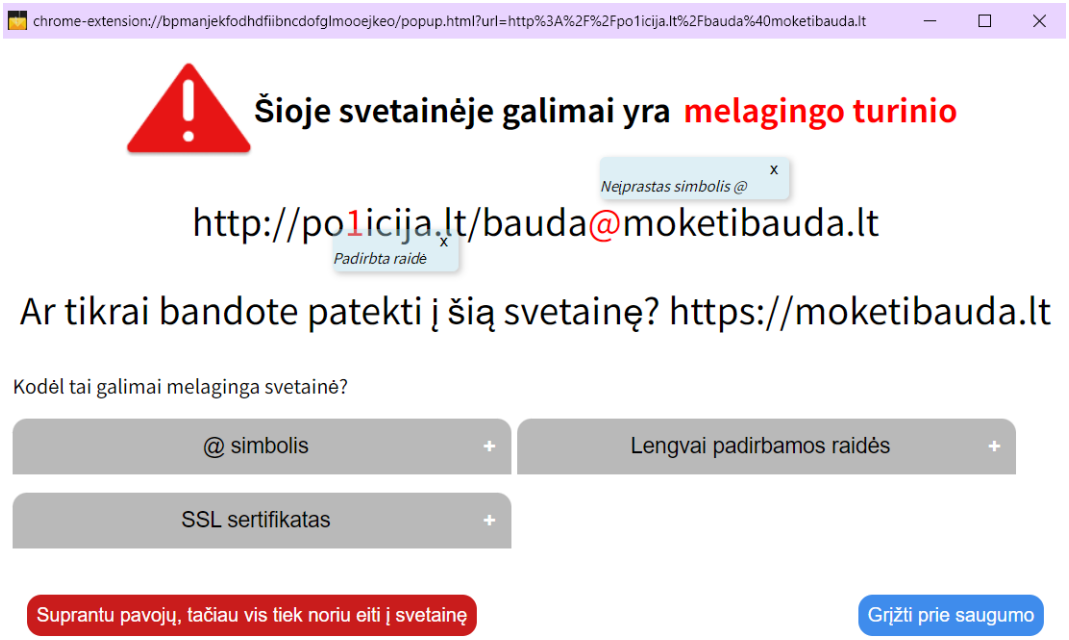
G13. *Ilgas URL.*

G14. *URL trumpintuvas.*

G15. *IP adresas.*

Naudotojo dėmesys naršyklės plėtinyje yra patraukiamas į adreso juostoje esantį URL, nes daug duomenų viliojimo požymių slypi būtent šioje vietoje. Aptikus duomenų viliojimo požymį URL, naudotojas yra apsaugomas nuo duomenų viliojimo atakos prieš jai įvykstant – į galimai pavojingą svetainę naudotojas nepatenka. Įgyvendinti visi duomenų viliojimo požymiai, esantys URL iškraipymo grupėje. URL slėpimo požymių grupėje nėra įgyvendintas svetainės amžius požymis (*G16*), nes kuriamas naršyklės plėtinys neturi prieigos prie tokios informacijos bei naudotojas tokios informacijos pats negalėtų pastebėti. Vartotojo sąsajos plagijavimo požymių grupėje įgyvendintas tik vienas požymis – perspėjantis langas (*G4*). Likusios gairės nebuvo įgyvendintos, nes jos gali būti aptiktos tik tuomet, kai naudotojas yra jau patekęs į galimai pavojingą svetainę ir duomenų viliojimo ataka galimai jau įvykdyta sėkmingai.

4.3.2. Perspėjantis langas



13 pav. Naršyklės plėtinio iššokantis langas

Naršyklės plėtinys, radęs bent vieną duomenų viliojimo atpažinimo požymį, parodo naudotojui iššokantį perspėjantį langą su paaiškinimais kodėl ši svetainė gali būti potencialiai pavojinga svetainė. Naršyklės plėtinio veikimo metu galima matyti tik vieną perspėjantį iššokantį langą –

neišjungus esamo lango, nebus matomas naujas perspėjimo langas. Taip yra siekiama sumažinti iššokančių langų skaičių bei skatinti naudotoją sukoncentruoti dėmesį į vieną perspėjimą.

13 pav. yra matomas pavyzdinis naršyklės plėtinio perspėjantis langas. Naudotojas yra perspėjamas, jog svetainė, į kurią bandoma patekti, galimai turi melagingo turinio. Viršuje yra pateiktas padidintas URL, į kurį naudotojas bando patekti. Vietos, kurios gali reikšti duomenų viliojimo ataką, yra paryškinamos raudona spalva bei šalia yra pateikiami maži pranešimai, kurie pasako koks duomenų viliojimo atpažinimo požymis yra rastas. Pavyzdžiui, šalia „1“ (vieneto) yra pateiktas pranešimas „Padirbta raidė“, nes raidė „l“ (L mažoji) buvo pakeista į skaičių „1“.

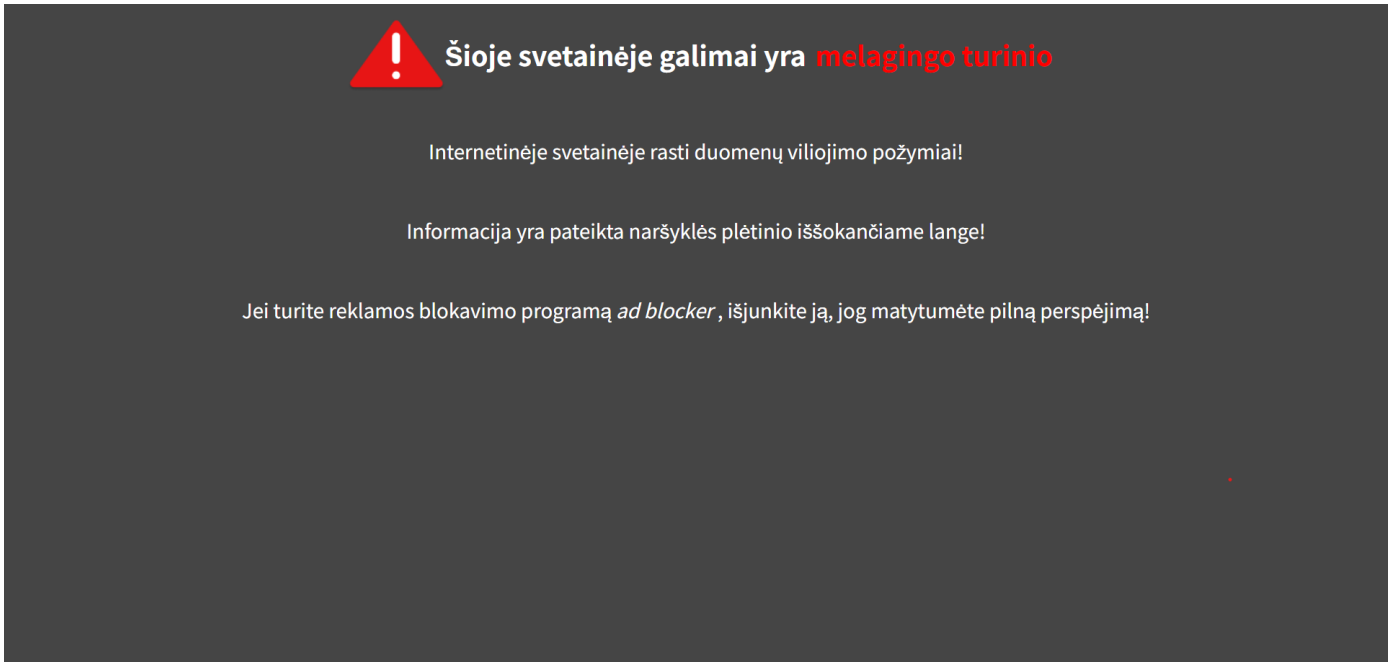
Jei URL yra randama padirbta raidė, pakeitus padirbtą raidę į panašią raidę ir radus originalią svetainę, naudotojui lange pateikiama „Ar nenorite patekti į šią svetainę?“ su rastu URL. Taip yra tikrinama ar egzistuoja svetainė su šalies aukščiausio lygio domenu ir radus tokią svetainę, informacija pateikiama naudotojui. Jei URL yra „@“ simbolis, naudotojui yra pateikiama URL dalis, einanti po šio simbolio ir paklausiama, ar naudotojas nori patekti į tą svetainę.

Žemiau yra pateikiami išsiskleidžiantys elementai, kuriuose yra matoma rastų duomenų viliojimo atpažinimo požymių pavadinimai. Kuomet naudotojas paspaus „+“ mygtuką, yra matomas turinys, pavaizduotas 14 pav. Kiekvienas duomenų viliojimo požymis yra pateikiamas su trumpu paaiškinimu – kas buvo aptikta URL, kodėl tai gali būti pavojinga. Duomenų viliojimo atpažinimo požymiai, kuriems įmanoma pateikti panašių URL pavyzdžius, po trumpais paaiškinimais yra pateikiama po 3–4 pavyzdinius URL naudotojui susipažinti.

Naudotojui iššokančiame lange yra matomi du pasirinkimai – „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“ bei „Grįžti prie saugumo“. Paspaudus raudonąjį „Suprantu pavojų, tačiau vis tiek noriu eiti į svetainę“ mygtuką, naudotojas yra nukreipiamas į svetainę, į kurią ir bandė patekti. O paspaudus mėlynąjį „Grįžti prie saugumo“ mygtuką, naudotojas yra grąžinamas į puslapį, kuriame naudotojas buvo prieš bandymą patekti į potencialiai pavojingą svetainę.

14 pav. Naršyklės plėtinio iššokantis langas su išskleistas perspėjimais

Naršyklės plėtinys atidarytame naršyklės lange pateikia įspėjantį langą, jog yra rasti duomenų viliojimo požymiai. 15 pav. yra matoma, jog naudotojas yra perspėjamas apie rastus duomenų viliojimo požymius, matomus iššokančiame lange. Taip pat perspėjama, jog reklamos blokavimo programa turi būti išjungta, kad naršyklės plėtinys veiktų tinkamai.



15 pav. Naršyklės plėtinio langas, nurodantis jog informacija randama iššokančiame lange

5. Apibendrinamasis analitinis vertinimas

Šiame skyriuje yra aprašomas analitinis tyrimas – peržvelgiama kokias duomenų viliojimo atakas sukurtas naršyklės plėtinys padengia bei gali atpažinti.

Su naudotojais atliktas duomenų viliojimo atakas atpažinti padedančio naršyklės plėtinio efektyvumo tyrimas, kurio metu pateikiamas klausimynas prieš ir po naršyklės plėtinio naudojimo.

5.1. Analitinis tyrimas

11 lentelėje pateikta darbe tiriamų duomenų viliojimo atakų tipai ir kaip jie yra atpažįstami naudojantis sukurtu naršyklės plėtiniu. Trys tipai – „Tarpininko“, SMS bei balso duomenų viliojimo atakos – nėra atpažįstamos. „Tarpininko“ duomenų viliojimo ataka neturi vartotojo sąsajos bei joje nėra siunčiamas URL naudotojui, todėl ši ataka nėra aptinkama. SMS bei balso duomenų viliojimo atakos yra orientuotos į mobilųjį telefoną, ir nors SMS atakose naudotojai gali gauti pavojingas nuorodas, plėtinys yra sukurtas kompiuterio „Google Chrome“ naršyklei ir jis neapima apsaugos nuo duomenų viliojimo atakų mobiliuosiuose telefonuose.

Kiti tipai – personalizuotas duomenų viliojimas, apgaulinga duomenų viliojimo, klonavimo, nuorodos manipuliacijos atakos – yra atpažįstamos sukurto naršyklės plėtinio. Personalizuotas duomenų viliojimas nėra pilnai atpažįstamas – jei ataka orientuota į mobilųjį telefoną, naudotojas nebus apsaugotas. Klonavimo duomenų atakoje elektroniniame laiške pasitaikantys pavojingi priedai taip pat nėra atpažįstami. Naršyklės plėtinyje įgyvendinti URL iškraipymo bei URL slėpimo požymiai atpažįsta pavojingas nuorodas, esančias elektroniniuose laiškuose. Naudotojui bandant patekti į pavojingą svetainę, kelią sustabdo naršyklės plėtinys su perspėjančiu langu bei paaiškinimais apie rastus duomenų viliojimo atpažinimo požymius.

11 lentelė. Duomenų viliojimo atakų atpažinimas sukurto naršyklės plėtinio pagalba

Duomenų viliojimo atakų tipas	Duomenų viliojimo atakos atpažinimas
Apgaulinga duomenų viliojimo ataka	Ataka yra atpažįstama – nagrinėjamas URL, kurį paspaudžia naudotojas elektroniniame laiške.
Personalizuotas duomenų viliojimas	Ataka yra atpažįstama, jei pasirinktas komunikacijos būdas turi vartotojo sąsają (elektroninis laiškas). Jei pasirinkta komunikuoti telefonu, ataka neatpažįstama.
Klonavimo duomenų viliojimo ataka	Ataka yra atpažįstama – nagrinėjama nuoroda laiške, jei naudotojas paspaudžia ant nuorodos. Pavojingi priedai neatpažįstami.
„Tarpininko“ duomenų viliojimo ataka	Ataka nėra atpažįstama – neturi vartotojo sąsajos.
Nuorodos manipuliacijos/HTTP duomenų viliojimo ataka	Ataka yra atpažįstama – nagrinėjami visi URL, į kuriuos bando patekti naudotojas.
SMS duomenų viliojimo ataka	Ataka nėra atpažįstama – neturi vartotojo sąsajos.
Balso duomenų viliojimo ataka	Ataka nėra atpažįstama – neturi vartotojo sąsajos.

5.2. Duomenų viliojimo atakas atpažįstančio naršyklės plėtinio efektyvumo tyrimas

5.2.1. Tyrimo tikslas

Tyrimo tikslas – palyginti dalyvių žinias apie duomenų viliojimo atakas prieš ir po naršyklės plėtinio naudojimosi. Kadangi naudotojų apmokymai yra pamirštami – tai yra trumpalaikis prevencijos būdas, kurio tikslumas krenta su pamirštamomis žiniomis – sukurtas naršyklės plėtinys atliktų periodiškų apmokymų paskirtį. Radus duomenų viliojimo požymį URL, iššokantis langas primintų naudotojui apie aptiktą požymį ir žinios būtų atnaujinamos. Siekiama sužinoti ar sukurtas naršyklės plėtinys padeda įsisavinti jame pateikiamą informaciją bei ar padeda atpažinti duomenų viliojimo atpažinimo požymius URL.

5.2.2. Tyrimo eiga

Tyrimo etapai:

1. Pateikiamas klausimynas apie duomenų viliojimo atakų atpažinimą. Dalyviai turėjo pažymėti ar pateiktas elektroninis laiškas yra įtartinas, neįtartinas ar dalyvis negali atsakyti.
2. Po kelių dienų – naršyklės plėtinio išbandymas bei susipažinimas su pateiktais testiniais URL. Naršyklės plėtinys buvo siunčiamas tyrimo dalyviams, kartu su instrukcija kaip įdiegti ir pasileisti sistemą. Testiniuose URL dalyviai susipažino su įgyvendintais duomenų viliojimo atpažinimo požymiais.
3. Kelios dienos po naršyklės plėtinio panaudojimo pakartotinai pateikiamas klausimynas apie duomenų viliojimo atakų atpažinimą. Pakartotinio klausimyno tikslas nustatyti, ar dalyviai geriau atpažįsta duomenų viliojimo požymius, esančius URL.

5.2.3. Tyrimo dalyviai

Tyrime dalyvavo 7 dalyviai, jų charakteristikos matomos 12 lentelėje. Tyrimui pasirinkti dalyviai yra įvairaus amžiaus bei IT gebėjimų lygių. Pasirinkta įvairus amžiaus bei IT gebėjimo lygių dalyviai, jog būtų užtikrintas tyrimo patikimumas. IT gebėjimo lygis nustatomas su klausimynu, pateiktu 1 priedas, IT gebėjimo lygių paaiškinimas skyriuje. Kuo didesnė patirtis su išvardintomis technologijomis bei kuo dažniau yra naudojamas kompiuteris, tuo aukštesnis yra naudojimosi informacinėmis technologijomis lygis. Kadangi tai yra kokybinis tyrimas, jam užtenka iki 10 dalyvių, nes turint daugiau dalyvių, įžvalgos yra pakartotinos ir naujų įžvalgų skaičius krenta sulig kiekvienu dalyviu [Nie00; NL93].

12 lentelė. Tyrimo dalyvių charakteristikos

Dalyvio nr.	Amžius	Lytis	IT gebėjimo lygis
1.	27	Moteris	Pažengusi
2.	51	Vyras	Pradedantysis
3.	33	Vyras	Pažengęs
4.	22	Moteris	Ekspertas
5.	51	Moteris	Pradedančioji
6.	22	Vyras	Pažengęs
7.	23	Vyras	Ekspertas

5.2.4. Tyrimo klausimynas

Tyrimo klausimyne dalyviams pateikta 12 skirtingų elektroninių laiškų bei trumpųjų žinučių. Dalyviams reikėjo nuspręsti, ar matomi pranešimai yra įtartini, ar neįtartini. Tyrime naudotas klausimynas yra matomas 4 priedas, Naršyklės plėtinio efektyvumo tyrimo klausimynas priede.

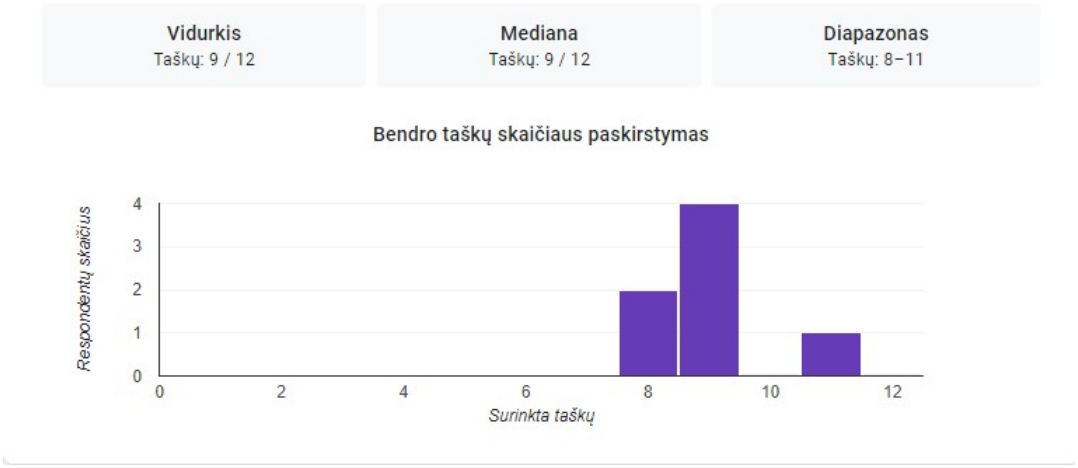
Klausimyne duomenų viliojimo laiškų pavyzdžių buvo 8, tai yra – pirmas, antras, penktas, šeštas, septintas, aštuntas, dešimtas, dvyliktas. Likę laiškai – trečias, ketvirtas, devintas, vienuoliktas – yra patikimi.

5.2.5. Tyrimo rezultatai

16 pav. pateikti klausimyno rezultatai prieš naršyklės plėtinio panaudojimą. Matoma, jog nė vienas dalyvis gerai neatpažino visų laiškų, tačiau visi dalyviai didžiąją dalį laiškų identifikavo teisingai. Daugiausiai neteisingai atsakyti klausimai yra pirmas, trečias bei šeštas klausimai. Penki dalyviai klydo ir atsakė, jog pirmas laiškas yra patikimas, nors tai yra duomenų viliojimo atakos laiškas. Trečia laišką trys dalyviai pažymėjo kaip įtartiną, vienas pažymėjo kad nežino, tačiau šis laiškas yra patikimas. Šeštąjį laišką trys pažymėjo kaip neįtartiną, vienas pažymėjo jog negali atsakyti, tačiau šis laiškas buvo vienas iš duomenų viliojimo atakų pavyzdžių.

Kelis laiškus visi dalyviai atpažino teisingai. Antrąjį, septintąjį bei dešimtąjį visi dalyviai pažino kaip duomenų viliojimo atakos laišką. Iš patikimų laiškų, vienintelis devintasis laiškas buvo teisingai atpažintas kaip patikimas laiškas.

Visi rezultatai yra matomi 5 priedas, Klausimyno rezultatai prieš naršyklės plėtinio panaudojimą skyriuje.



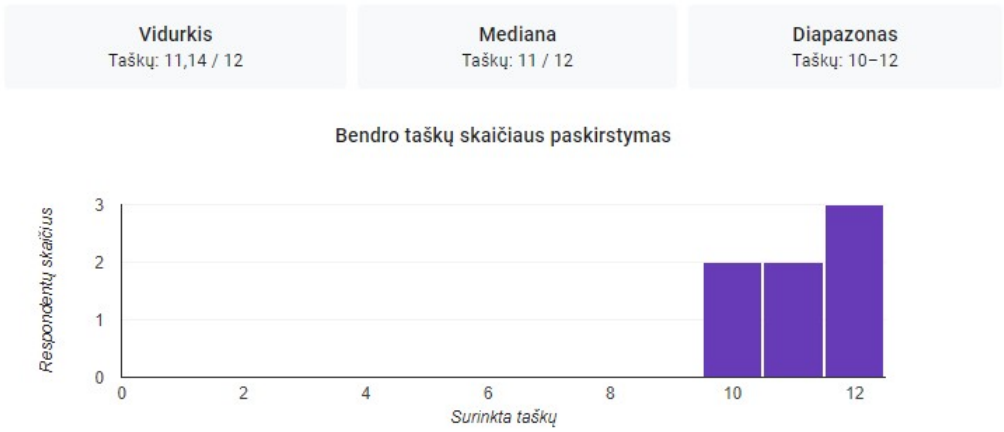
16 pav. Klausimyno rezultatai prieš naršyklės plėtinio panaudojimą

Po naršyklės plėtinio naudojimo pakartotinai pateiktas toks pat klausimynas, skirtas įvertinti, ar pasikeitė rezultatai.

17 pav. pateikti klausimyno rezultatai po naršyklės plėtinio panaudojimo. Visi dalyviai antrą, penktą, šeštą, septintą, aštuntą, dešimtą bei dvyliktą atpažino kaip duomenų viliojimo laiškus. Teisingai atpažinti patikimi laiškai buvo ketvirtas ir devintas.

Daugiausia klaidų yra pirmame laiške – trys iš septynių dalyvių pažymėjo laišką kaip patikimą. Du dalyviai trečią laišką pažymėjo kaip įtartiną, nors tai yra patikimo laiško pavyzdys. Trys dalyviai visus laiškus identifikavo tinkamai.

Visi pakartotinio klausimyno rezultatai yra 6 priedas, Klausimyno rezultatai po naršyklės plėtinio panaudojimo skyriuje.



17 pav. Klausimyno rezultatai po naršyklės plėtinio panaudojimo

13 lentelė. Tyrimo dalyvių detalūs rezultatai

Dalyvio nr.	Klausimyno rezultatai prieš plėtinio panaudojimą	Klausimyno rezultatai po plėtinio panaudojimo
1.	9 teisingai iš 12	12 teisingai iš 12
2.	8 teisingai iš 12	10 teisingai iš 12
3.	9 teisingai iš 12	11 teisingai iš 12
4.	9 teisingai iš 12	12 teisingai iš 12
5.	8 teisingai iš 12	10 teisingai iš 12
6.	9 teisingai iš 12	11 teisingai iš 12
7.	11 teisingai iš 12	12 teisingai iš 12

13 lentelėje yra matomi galutiniai rezultatai. Iš rezultatų matoma, jog sukurtas naršyklės plėtinys padeda įsisavinti žinias apie duomenų viliojimo atpažinimo požymius – duomenų viliojimo atakų atpažinimas išaugo 20 %. Galima teigti, jog „Google Chrome“ naršyklės plėtinys padeda naudotojams geriau atpažinti duomenų viliojimo atakas pagal surinktus duomenų viliojimo atpažinimo požymius bei radus duomenų viliojimo požymį nuorodoje, primins naudotojui apie aptiktą požymį.

Apibendrinant tyrimo rezultatus, galima teigti, jog naršyklės plėtinys padeda įsisavinti duomenų viliojimo atpažinimo požymius, nes atpažinimo lygis išaugo 20 %.

5.3. Tolimesni darbai

1. Naršyklės plėtinį praplėsti į kitas populiarias naršykles, kaip „Firefox“, „Safari“ bei „Opera“.
2. Sukurti naršyklės plėtinio atitikmenį išmaniajam telefonui – telefono programėlė, atpažįstanti duomenų viliojimo atakas, gaunamas trumpąją žinute (SMS).
3. Jog būtų mažesnis naudotojo veiksmų skaičius, ieškoti pavojingų nuorodų puslapyje – perspėjantis langas iššoktų su perspėjimu apie rastą pavojingą nuorodą, esančią svetainėje. Taip būtų apsaugomas naudotojas nuo nuorodos paspaudimo.

Rezultatai

Darbe analizuojama duomenų viliojimo atakų tipai bei prevencijos būdai. Darbo tikslas – ištirti duomenų viliojimo atpažinimo požymius vartotojo sąsajoje, remiantis kuriais sukurti naršyklės plėtinį, padedantį naudotojui atpažinti duomenų viliojimo atakas.

Darbo metu pasiekti šie rezultatai:

1. Mokslinės literatūros analizės metu išskirtos duomenų viliojimo atakos, kurias galima atpažinti vartotojo sąsajoje. Surinktų atakų rinkinys – apgaulinga duomenų viliojimo ataka, personalizuotas duomenų viliojimas, klonavimo duomenų viliojimo ataka bei nuorodos manipuliacijos ataka.
2. Esamų prevencijos būdų privalumų ir trūkumų palyginimas ilgaamžiškumo bei tikslumo principų požiūriu.
3. Surinkti duomenų viliojimo atpažinimo požymiai vartotojo sąsajoje, kurie sugrupuoti į vartotojo sąsajos plagijavimo, URL iškraipymo bei URL slėpimo požymius.
4. Sukurtas „Google Chrome" naršyklės plėtinys, padedantis naudotojui atpažinti duomenų viliojimo atakas pagal darbo metu surinktus duomenų viliojimo atpažinimo požymius. Sukurtas plėtinys padeda naudotojui atpažinti duomenų viliojimo atakas bei naudotojas yra apmokamas pats atpažinti šias atakas.

Išvados

1. Išnagrinėjus duomenų viliojimo atakas pastebėta, jog didžioji dalis jų turi vartotojo sąsają, kuri yra plagijuota duomenų vagies. Todėl nuspręsta kurti naršyklės plėtinį, padedantį atpažinti duomenų viliojimą iš URL, esančio adreso juostoje.
2. Apžvelgus duomenų viliojimo atakų prevencijos būdus pastebėta, jog esamų prevencijos būdų – naudotojų apmokymų, juodojo/baltojo sąrašo, mašininio mokymosi bei giliojo mokymosi modelių bei vizualiniu panašumu grindžiamo metodo – nepakanka. Dalis jų nepaaiškina naudotojui kodėl tai yra potencialiai pavojingos svetainės ir į ką naudotojas turi atkreipti dėmesį, jog apsisaugoti nuo duomenų viliojimo atakų.
3. Išanalizavus surinktus duomenų viliojimo atpažinimo požymius vartotojo sąsajoje pastebėta jog jie susiję su vartotojo sąsajos plagijavimu, URL iškraipymu bei URL slėpimu.
4. Panaudojamumo testavimo metu pastebėta, jog struktūrizuotas informacijos pateikimas bei pavojingų vietų išryškinimas padeda naudotojams greičiau rasti aktualią informaciją.
5. Atlikus tyrimą apie duomenų viliojimo atakas pastebėta, jog po sukurto naršyklės plėtinio naudojimosi, naudotojai sugeba geriau atpažinti duomenų viliojimo atakas – atpažinimas išaugo 20 % – ir geriau įsimena į kokias URL vietas reikia atkreipti dėmesį.

Šaltiniai

[AAD19] J. Aneke, C. Ardito, G. Desolda. "Designing an intelligent user interface for preventing phishing attacks". *IFIP Conference on Human-Computer Interaction*. 2019.

[AAT14] N. Abdelhamid, A. Ayesh, F. Thabtah. "Phishing detection based associative classification data mining." *Expert Systems with Applications 41(13)*. 2014, p. 5948–5959.

[ADP+21a] H. Abroshan, J. Devos, G. Poels, E. Laermans. "Covid-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic." *Ieee Access 9*. 2021, p. 121916–121929.

[ADP+21b] H. Abroshan, J. Devos, G. Poels, E. Laermans. "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process." *IEEE Access 9*. 2021, p. 44928–44949.

[ARJ+20] M. R. Arabia-Obedoza, G. Rodriguez, A. Johnston, F. Salahdine, N. Kaabouch. Social engineering attacks a reconnaissance synthesis analysis. *2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. 2020, p. 0843–0848.

[ASS20] S. Apandi, J. Sallim, R. Sidek. "Types of anti-phishing solutions for phishing attack. IOP Conference Series." *IOP Conference Series: Materials Science and Engineering. Vol. 769. No. 1*. 2020.

[BB13] M. N. Banu, S. M. Banu. "A Comprehensive Study of Phishing Attacks." *International Journal of Computer Science and Information Technologies 4.6*. 2013, p. 783–786.

[BKS18] V. Bhavsar, A. Kadlak, S. Sharma. "Study on Phishing Attacks." *International Journal of Computer Applications 182.33*. 2018, p. 27–29.

[BR22] S. Baki, M. V. Rakesh. "Sixteen Years of Phishing User Studies: What Have We Learned?" *IEEE Transactions on Dependable and Secure Computing 20.2*. 2022, p. 1200–1212.

[CCR16] J. A. Chaudhry, S. A. Chaudhry, R. G. Rittenhouse. "Phishing Attacks and Defenses." *International journal of security and its applications 10.1*. 2016, p. 247–256.

[CPF+13] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, M. E. Johnson. "Going spear phishing: Exploring embedded training and awareness." *IEEE security and privacy 12.1*. 2013, p. 28–38.

[DDF+19] G. Desolda, F. Di Nocera, L. Ferro, R. Lanzilotti, P. Maggi, A. Marrella. "Alerting users about phishing attacks." *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*. 2019.

[EBD+20] A. El Aassal, S. Baki, A. Das, R. M. Verma. "An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs." *IEEE Access 8*. 2020, p. 22170–22192.

[FY21] H. Faris, S. Yazid. "Phishing web page detection methods: URL and HTML features detection." *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*. 2021.

[GSK16] S. Gupta, A. Singhal, A. Kapoor. "A literature survey on social engineering attacks: Phishing attack." *2016 international conference on computing, communication and automation (ICCCA)*. 2016.

[HTL09] H. Huang, J. Tan, L. Liu. "Countermeasure techniques for deceptive phishing attack." *2009 International Conference on New Trends in Information and Service Science*. 2009.

[JAB21] A. Jayatilaka, N. A. G. Arachchilage, M. A. Babar. "Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors." *arXiv preprint arXiv:2108.04766*. 2021.

[JG17] A. K. Jain, B. B. Gupta. "Phishing detection: analysis of visual similarity based approaches." *Security and Communication Networks 2017*. 2017.

[KIJ13] M. Khonji, Y. Iraqi, A. Jones. "Phishing detection: a literature survey." *IEEE Communications Surveys and Tutorials 15.4*. 2013, p. 2091–2121.

[MAG+17] S. Marchal, G. Armano, T. Gröndahl, K. Saari, N. Singh, N. Asokan. "Off-the-hook: An efficient and usable client-side phishing prevention application." *IEEE Transactions on Computers 66.10*. 2017, p. 1717–1733.

[MBG+17] M. M. Moreno-Fernández, F. Blanco, P. Garaizar, H. Matute. "Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud." *Computers in Human Behavior 69*. 2017, p. 421–436.

[MKK08] E. Medvet, E. Kirda, C. Kruegel. "Visual-similarity-based phishing detection." *Proceedings of the 4th international conference on Security and privacy in communication netowrks*. 2008, p. 1–6.

[MTL+17] J. Mao, W. Tian, P. Li, T. Wei, Z. Liang. "Phishing-alarm: Robust and efficient phishing detection via page component similarity." *IEEE Access 5*. 2017, p. 17020–17030.

[Nie00] J. Nielsen. "Why you only need to test with 5 users." 2000, p. 1–4.

[NL93] J. Nielsen, T. K. Landauer. "A mathematical model of the finding of usability problems." *Proceedings of the INTERACT'93 and CHI'93 conference on Human factors in computing systems*. 1993, p. 206–213.

[RGG17] G. Ramesh, J. Gupta, P. G. Gamya. "Identification of phishing webpages and its target domains by analyzing the feign relationship." *Journal of Information Security and Applications 35*. 2017, p. 75–84.

[RSG+21] S. S. Ravindra, S. J. Sanjay, S. N. A. Gulzar, K. Pallavi. "Phishing Website Detection Based on URL." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (USRCSEIT) 7.3*. 2021, p. 589–594.

[SAB+21] A. Sadiq, M. Anwar, R. A. Butt, F. Masud, M. K. Shahzad, S. Naseem, M. Younas. "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0." *Human behavior and emerging technologies 3.5*. 2021, p. 854–864.

[SMS+22] K. Subramani, W. Melicher, O. Starov, P. Vadrevu, R. Perdisci. "PhishInPatterns: measuring elicited user interactions at scale on phishing websites." *Proceedings of the 22nd ACM Internet Measurement Conference*. 2022, p. 589–604.

[SZD+19] H. Shahriar, C. Zhang, S. Dunn, R. Bronte, A. Sahlan, K. Tarmissi. "Mobile anti-phishing: Approaches and challenges." *Information Security Journal: A Global Perspective 28.6*. 2019, p. 178–193.

[TCY+23] C. C. L. Tan, K. L. Chiew, K. S. Yong, Y. Sebastian, J. C. M. Than, W. K. Tiong. "Hybrid phishing detection using joint visual and textual identity." *Expert systems with applications 220*. 2023.

[WW13] S. Wedyan, F. Wedyan. "An Associative Classification Data Mining Approach for Detecting Phishing Websites." *Journal of Emerging Trends in Computing and Information Sciences 4.12*. 2013.

[ZYJ+14] D. Zhang, Z. Yan, H. Jiang, T. Kim. "A domain-feature enhanced classification model for the detection of Chinese phishing e-Business websites." *Information and Management, 51(7)*. 2014, p. 845–853.

Priedai

1 priedas

IT gebėjimo lygių paaiškinimas

Informacinių technologijų gebėjimo lygių paaiškinimas:

- Pradedantysis – reikia papildomos pagalbos naudojantis programine įranga iki kol taps pažengusiu.
- Pažengęs – žino kur ieškoti reikalingos informacijos apie programinę įrangą, motyvuoti mokytis daugiau, tačiau reikia prieigos prie patarimų sklandžiam naudojimui.
- Ekspertas – informacinės technologijos nekelia jokių sunkumų, vertina naujas, galingas funkcijas.

Dalyvio klausimynas

A. INFORMACINIŲ TECHNOLOGIJŲ PATIRTIS

1. Kiek turite patirties su šiomis sistemomis:

	0-6 mėnesiai	6 mėnesiai – 1 metai	1-3 metai	Daugiau nei 3 metai
Teksto doroklius (pvz. Word)	☐	☐	☐	☐
Skaičiuokles (pvz. Excel)	☐	☐	☐	☐
Pristatymų rengimo priemones (pvz. Power Point)	☐	☐	☐	☐
Paveikslėlių apdorojimo priemones (pvz. Photoshop, Corel Draw)	☐	☐	☐	☐
Kita	☐	☐	☐	☐

2. Kiek laiko vidutiniškai per dieną naudojatės kompiuteriu?

2.1. Namuose:
☐ Mažiau negu 1 valandą
☐ 1-3 valandas
☐ 4-6 valandas
☐ Daugiau negu 6 valandas

2.2. Darbe:
☐ Mažiau negu 1 valandą
☐ 1-3 valandas
☐ 4-6 valandas
☐ Daugiau negu 6 valandas

3. Kam naudojate kompiuterius? (galimi keli variantai)

☐ Programavimui ☐ Darbo reikalais ☐ Duomenims saugoti
☐ Laisvalaikiui ☐ Dokumentams kurti ☐ Kita (įrašyti): _____

18 pav. IT gebėjimo lygio nustatymo klausimynas

2 priedas
Maketų testavimas

14 lentelė. Pirmojo maketo testavimo rezultatai

Pirmasis maketas					
Dalyvio nr.	1.	2.	3.	4.	5.
1 užduotis	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas
2 užduotis	3 paspaudimai	3 paspaudimai	3 paspaudimai	3 paspaudimai	3 paspaudimai
3 užduotis	20 sekundžių	30 sekundžių	8 sekundės	5 sekundės	15 sekundžių
4 užduotis	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas
5 užduotis	3 paspaudimai	3 paspaudimai	2 paspaudimai	2 paspaudimai	2 paspaudimai
Papildomi komentarai	Patogiau, kai įspėjimai yra matomi per visą ekraną, dažnai neatkreipia dėmesio į informaciją, kai ji yra šone ar apačioje. Norėtų, jog pranešimai su perspėjimais prie nuorodos būtų rodomi iškart, o ne tik perbraukus pelyte.	Naudotas šriftas padeda pamatyti pavojingus simbolius adreso juostoje - 1 vietoj l. Šis maketas yra patogesnis naudoti. Patiko, jog yra atskiras langas su perspėjimais. Pavojingos vietos nuorodoje galėtų būti išryškintos iškart, o ne tik perbraukus virš jų kompiuterio pelyte.	Patiko informacijos kiekis, parodoma jog kyla pavojus, kuris reikalauja vartotojo dėmesio ir papildomo atsakingumo. Norėtų, jog informacija būtų pateikta labiau koncentruotai: jei žmogui sunku sutelkti dėmesį, jis neskaitys viso perspėjimo. Labiau būtų linkęs naudoti šį maketą.	Patiko detalūs paaiškinimai. Mano, jog pranešimas prie nuorodoje esančios pavojingos vietos turi būti matomas iškart. Maketo paaiškinimai atrodė paprastesni, lengviau suprantami - nuoroda viršuje padeda matyti nuorodos keliamą pavojų.	Nepatiko kad yra vartotojo sąsajos langas per visą kompiuterio ekraną. Norėtų modernesnio sprendimo, kaip pavyzdį pateikė iššokantį langą. Patinka perspėjimų stilius, detalūs paaiškinimai.

15 lentelė. Antrojo maketo testavimo rezultatai

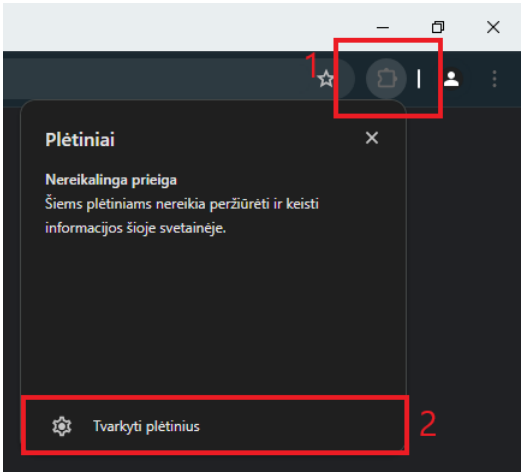
Antrasis maketas					
Dalyvio nr.	1.	2.	3.	4.	5.
1 užduotis	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas
2 užduotis	1 paspaudimas	1 paspaudimas	2 paspaudimai	1 paspaudimas	1 paspaudimas
3 užduotis	4 paspaudimai	4 paspaudimai	3 paspaudimai	3 paspaudimai	3 paspaudimai
4 užduotis	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas	1 paspaudimas
5 užduotis	4 paspaudimai	4 paspaudimai	4 paspaudimai	4 paspaudimai	4 paspaudimai
Papildomi komentarai	Sunku įskaityti šoniniame lange matomus perspėjimus – reiktų didinti šriftą. Laiško pažymėjimas kaip šlamštą nepatiko, nes nuoroda gali būti paimta nebūtinai iš laiško. Raudonų nuorodos elementų nepastebėjo.	Geriau perspėjimas apačioje arba per visą ekraną, nėra pratusi matyti šoniniame lange. Galima daryti iššokantį langą. Jog nuoroda yra modifikuojama laiške – nuspalvinamos pavojingos vietos – neatkreipė dėmesio.	Patiko, kad siūloma iškart imtis priemonių – pažymėti laišką kaip brukalą. Nepatiko, jog mažame lange yra daug informacijos – perspėjimų informacija kartu su laišku buvo per daug painu ir tapo neaišku, kas yra problema.	Lengvai matoma informacija, įspėjimai gerai paaiškina kodėl nuoroda galimai pavojinga. Norėtų, jog informacija būtų perteik-iama taip - naudotojas pats pasirinktų kada matyti visą infor-maciją bei pavyzdines nuorodas. Vizualiai, šis maketas patiko labiau – šoninis langas pasirodė modernesnis bei įdomesnis.	Labiau patiko šoninio lango maketas. Abiejuose patiko kad neleidžia iškart patekti į pavojingą svetainę. Labiau būtų linkęs naudoti naudoti antrąjį maketą.

3 priedas

Įgyvendintas naršyklės plėtinys

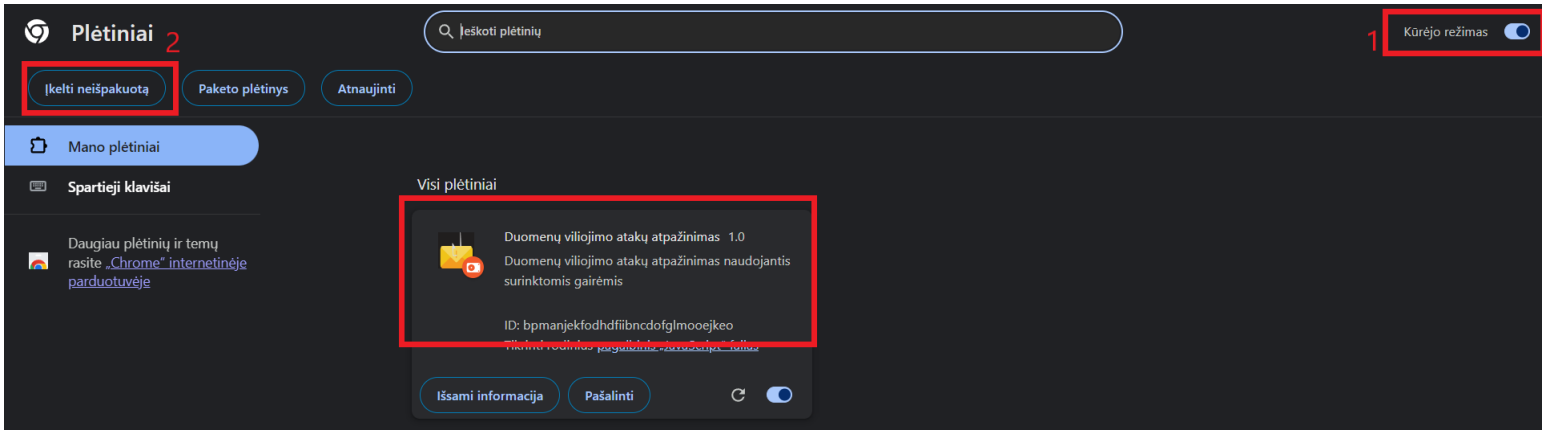
Įgyvendinto naršyklės plėtinio kodą galima rasti čia:
`https://github.com/MigleMic/Phishing-browser-extension`
Įgyvendinto naršyklės plėtinio demonstracinis vaizdo įrašas yra pasiekiamas su nuoroda: `https://drive.google.com/file/d/1tVk66kkiOZnZWw2nXp8MSWdSvXQXHPWS/view?usp=drive_link`
Naršyklės plėtinio įdiegimas ir paleidimas:

1. Atidaryti nuorodą:
   `https://drive.google.com/drive/u/1/folders/1AZKlQ2__ggoNapqY4UmvzXJ5RfIXdc8H`
2. Atsisiųsti PhishingExtension.zip;
3. Išarchyvuoti PhishingExtension.zip;
4. Atidaryti „Google Chrome" naršyklę;
5. Paspausti ant „Plėtiniai" ir tuomet „Tvarkyti plėtinius" (19 pav.) arba „Nustatymai" ir tada „Plėtiniai", jei nematote plėtinio ženkliuko;



19 pav. „Google Chrome" naršyklės plėtiniai

6. Įjungti „Kūrėjo režimą", paspausti „Įkelti neišpakuotą". Suraskite išarchyvuotą PhishingExtension failą ir įkelkite. Įkėlus sėkmingai, turėtumėte matyti naršyklės plėtinį sąraše (20 pav.).



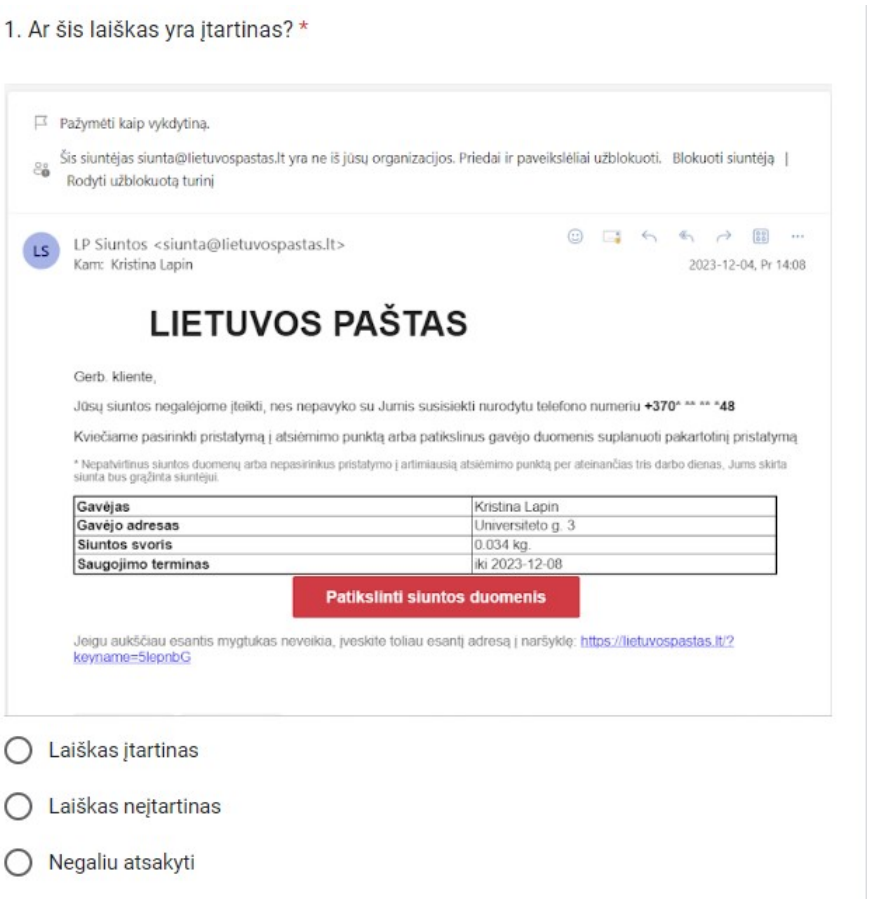
20 pav. Naršyklės plėtinio pridėjimas

7. Jei turite reklamos blokavimo programą, išjunkite. Ji gali blokuoti naršyklės plėtinio iššokantį langą.

8. „sampleURLs” kataloge esantis „testURLs.html” failas turi pavyzdinius URL, kuriuos galite panagrinėti detaliau su naršyklės plėtiniu. Atidarykite „testURLs.html” „Google Chrome” naršyklėje ir susipažinkite su visais įgyvendintais duomenų viliojimo atpažinimo požymiais.

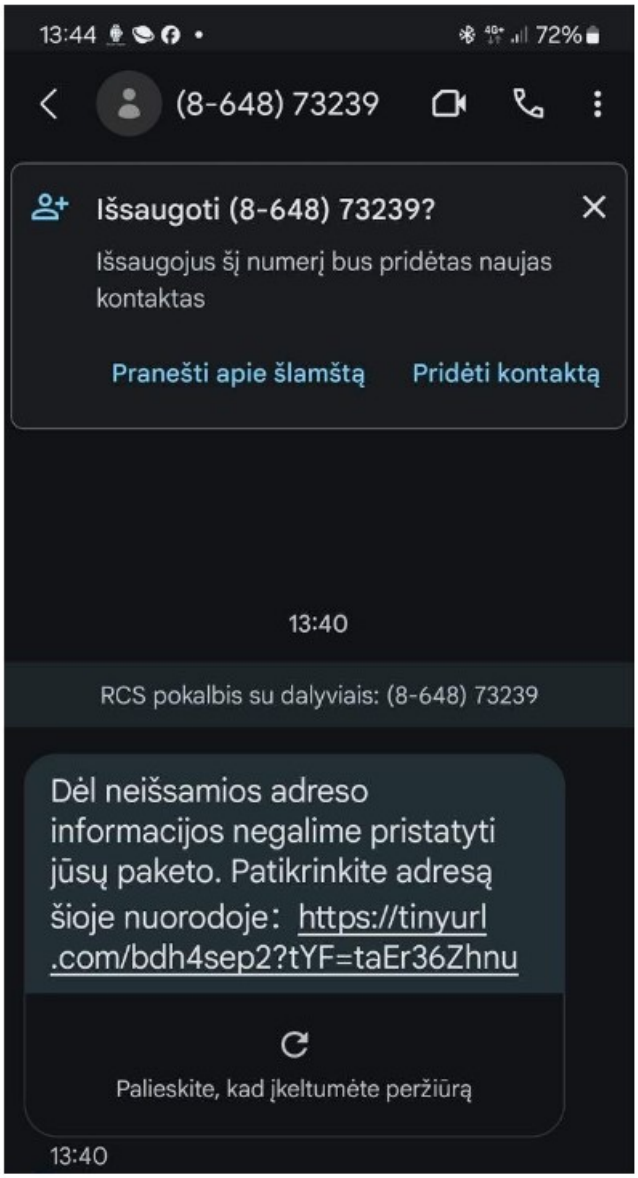
4 priedas

Naršyklės plėtinio efektyvumo tyrimo klausimynas



21 pav. Tyrimo pirmas klausimas

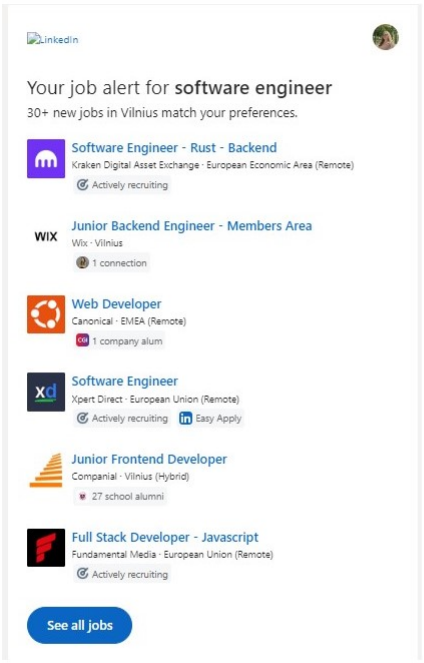
2. Ar šis laiškas yra įtartinas? *



- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

22 pav. Tyrimo antras klausimas

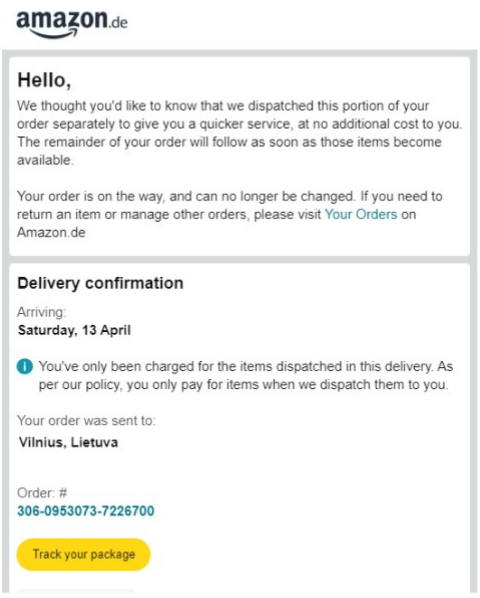
3. Ar šis laiškas yra įtartinas? *



- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

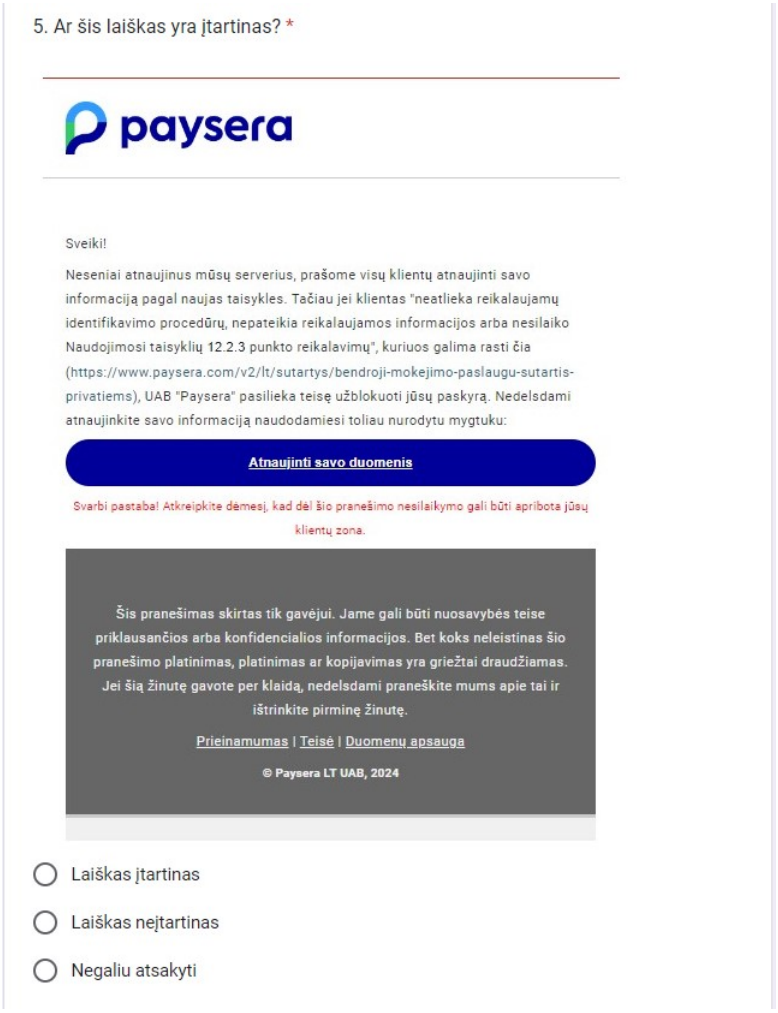
23 pav. Tyrimo trečias klausimas

4. Ar šis laiškas yra įtartinas? *

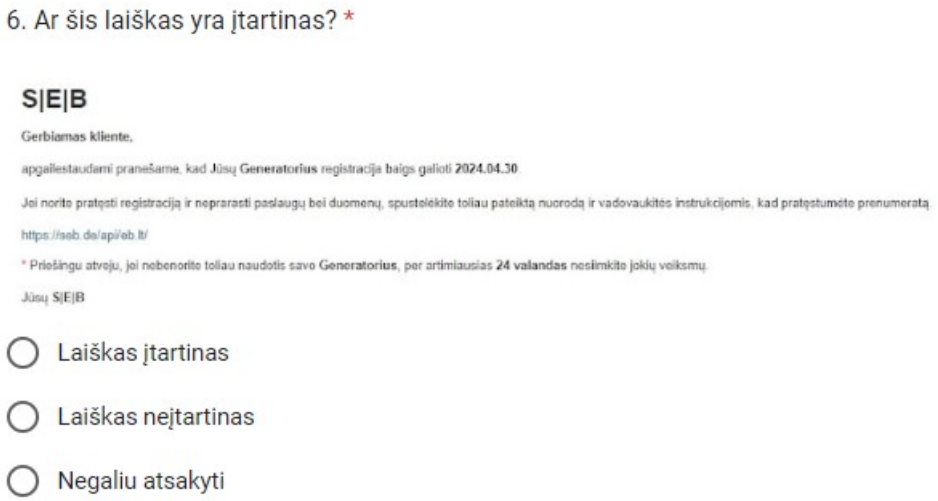


- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

24 pav. Tyrimo ketvirtas klausimas

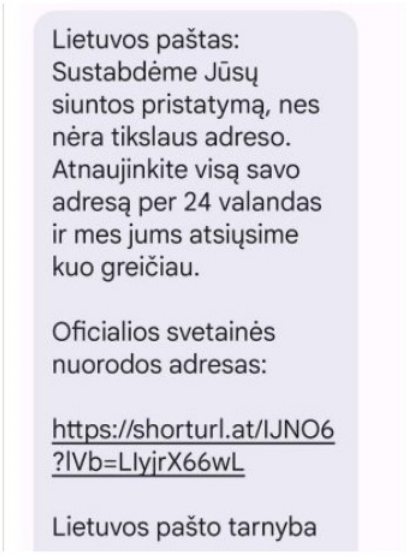


25 pav. Tyrimo penktas klausimas



26 pav. Tyrimo šeštas klausimas

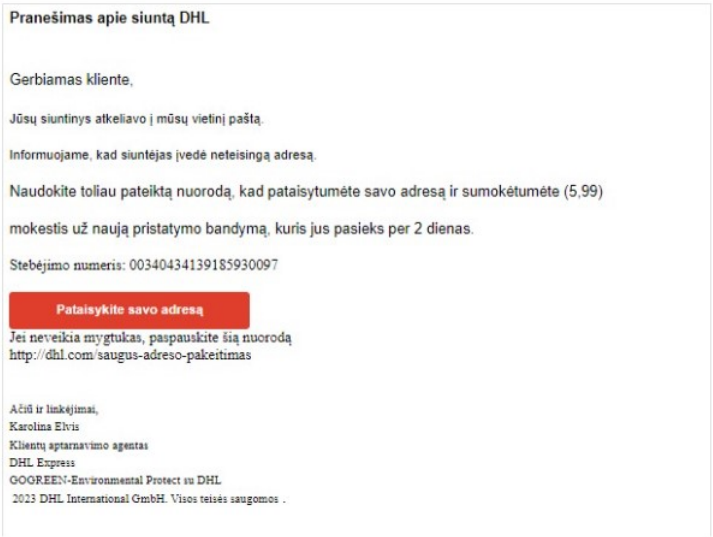
7. Ar šis laiškas yra įtartinas? *



- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

27 pav. Tyrimo septintas klausimas

8. Ar šis laiškas yra įtartinas? *



- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

28 pav. Tyrimo aštuntas klausimas

9. Ar šis laiškas įtartinas? *

Labas,

Primename, jog siunta JJFI63864910006163434, skyrelio nr. 23 vis dar laukia Smartpost Itella paštomate Maxima XX Žirmūnai, Tuskulėnų g. 66, Vilnius, iki 09.05.

Norėdami atidaryti dureles: spauskite C 361493 OK

Iki,

Smartpost Itella

Linkėjimai,
Smartpost Itella

- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

29 pav. Tyrimo devintas klausimas

10. Ar šis laiškas įtartinas? *

Luminor

Gerbiamas kliente,

Nuo 2024 m. sausio 3 d. nebegalėsite naudotis savo kortele
jei nesate aktyvavę naujos internetinės saugumo sistemos.
Naujasis saugumo tinklas - tai sprendimas, užtikrinantis didesnį saugumą ir patikimą veikimą

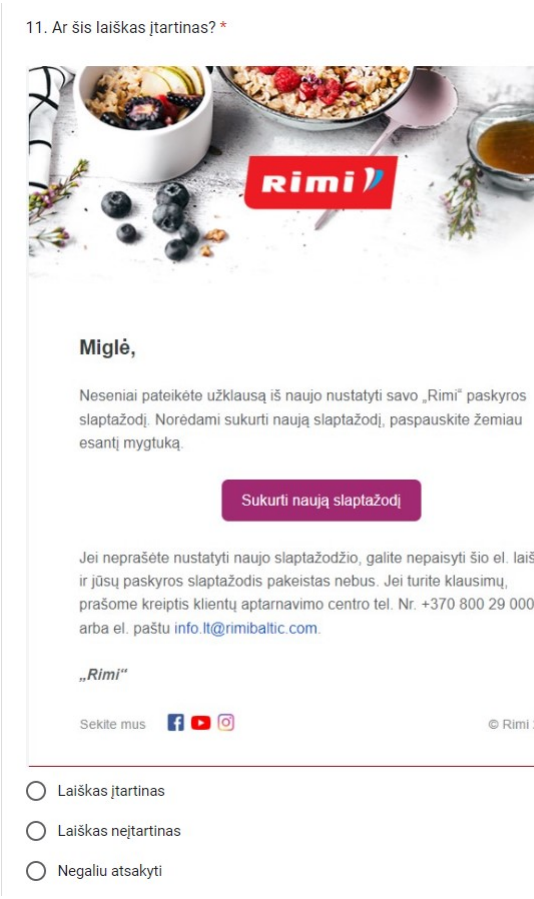
Naujos apsaugos sistemos įjungimas, https://luminor.lt/ijungti-apsaugos-sistema@box.info

PASTABA: Jei pranešimas atsidūrė nepageidaujamų laiškų aplanke, pažymėkite jį kaip nepageidaujamą, kaip ne šlamštą. Tai tik sistemos klaida

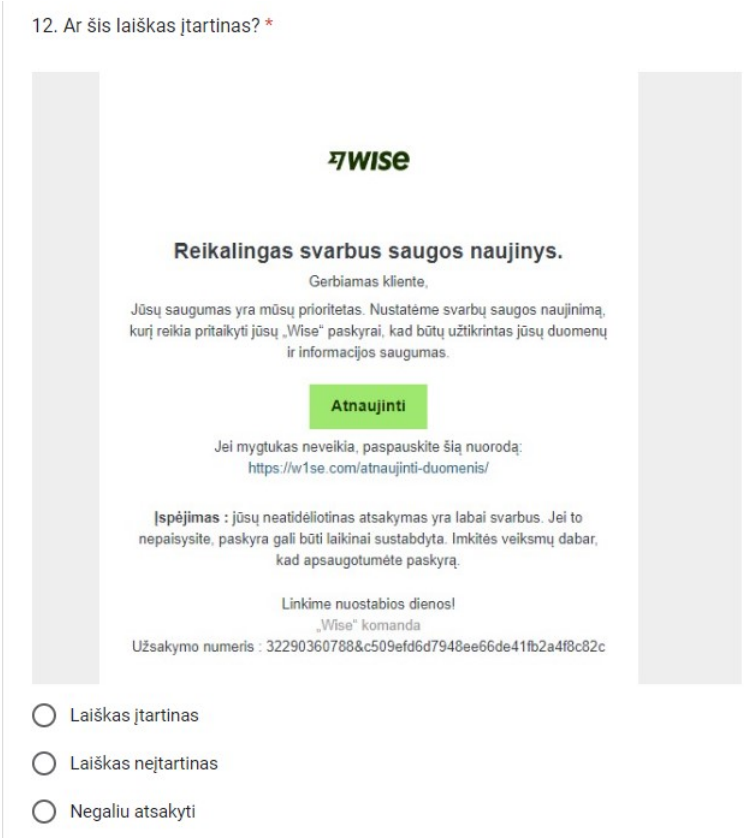
Malonūs linkėjimai,
Luminor

- ◯ Laiškas įtartinas
- ◯ Laiškas neįtartinas
- ◯ Negaliu atsakyti

30 pav. Tyrimo dešimtas klausimas



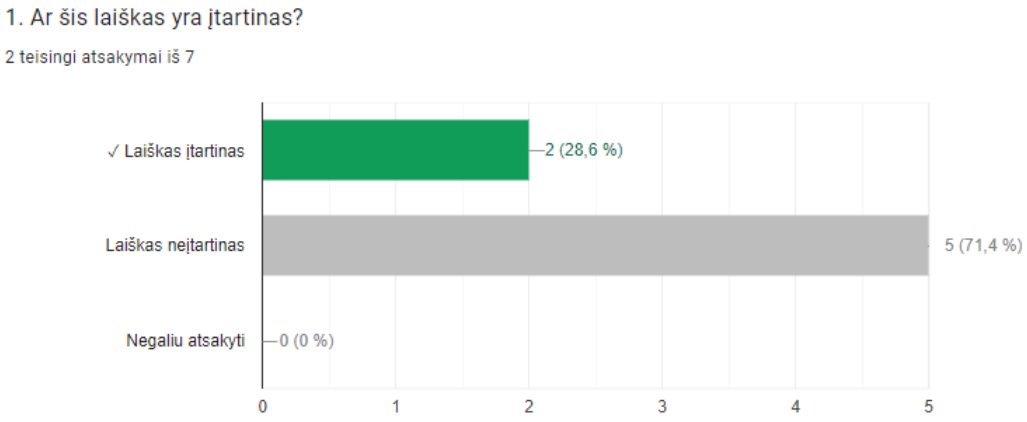
31 pav. Tyrimo vienuoliktas klausimas



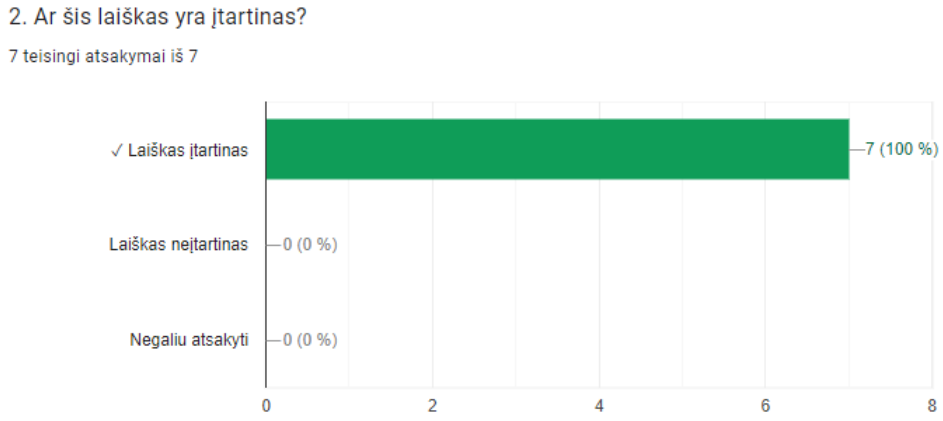
32 pav. Tyrimo dvyliktas klausimas

5 priedas

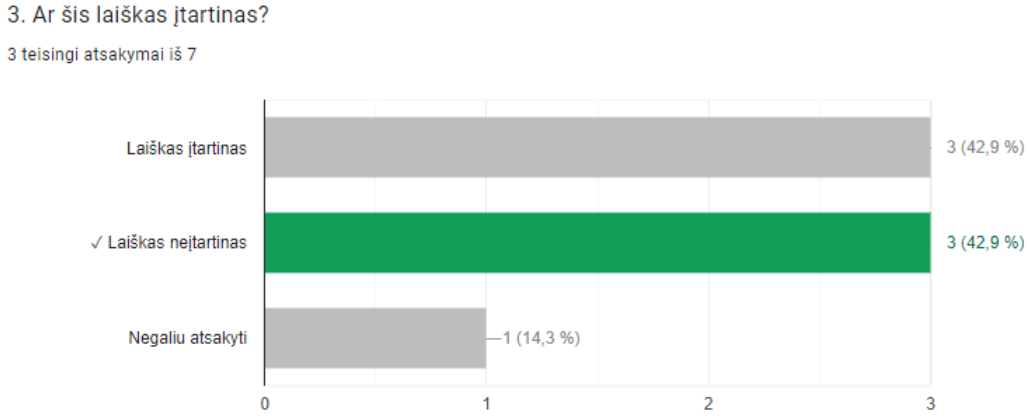
Klausimyno rezultatai prieš naršyklės plėtinio panaudojimą



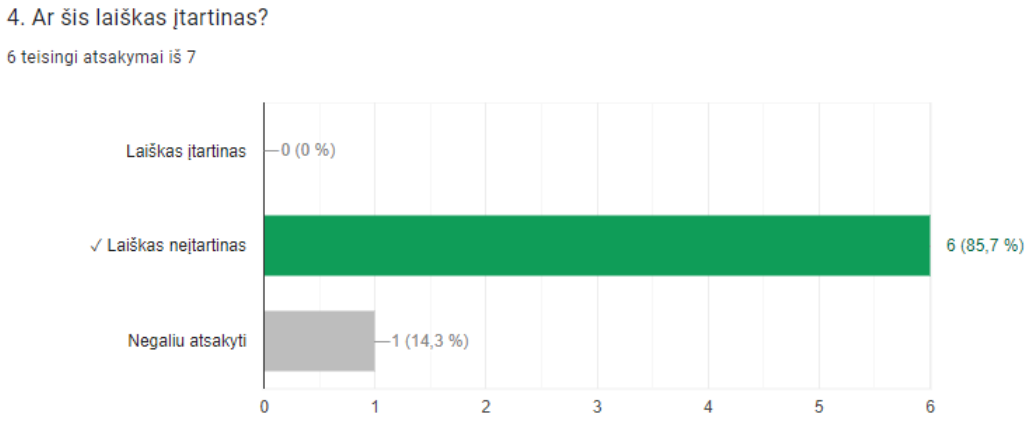
33 pav. Pirmo klausimo rezultatai prieš plėtinio panaudojimą



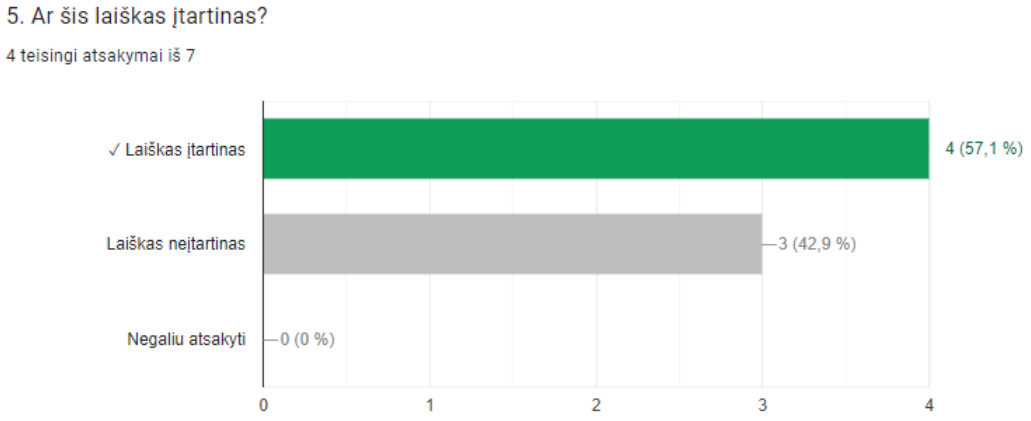
34 pav. Antro klausimo rezultatai prieš plėtinio panaudojimą



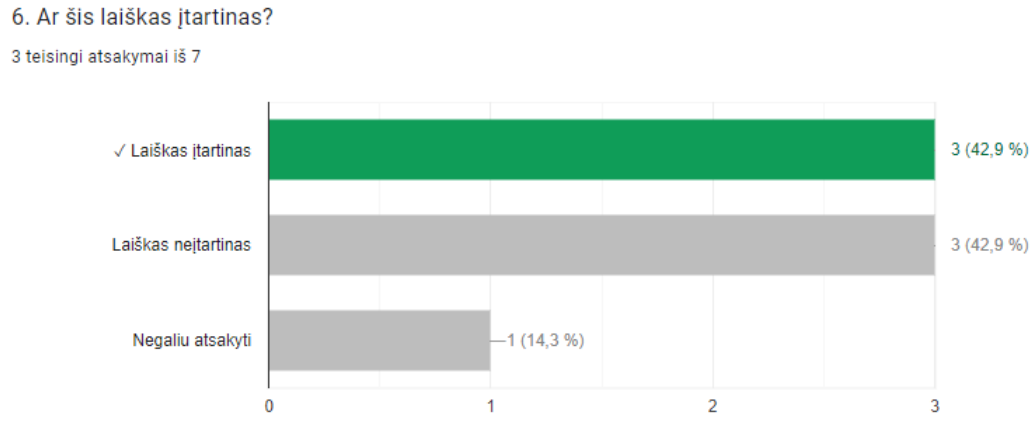
35 pav. Trečio klausimo rezultatai prieš plėtinio panaudojimą



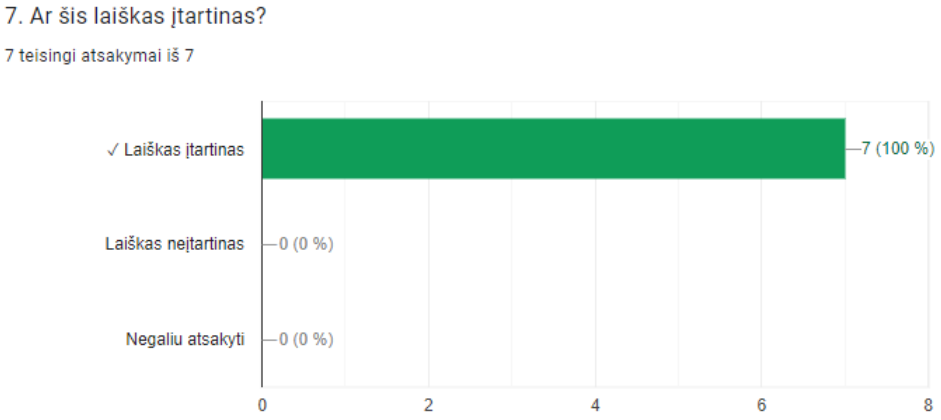
36 pav. Ketvirto klausimo rezultatai prieš plėtinio panaudojimą



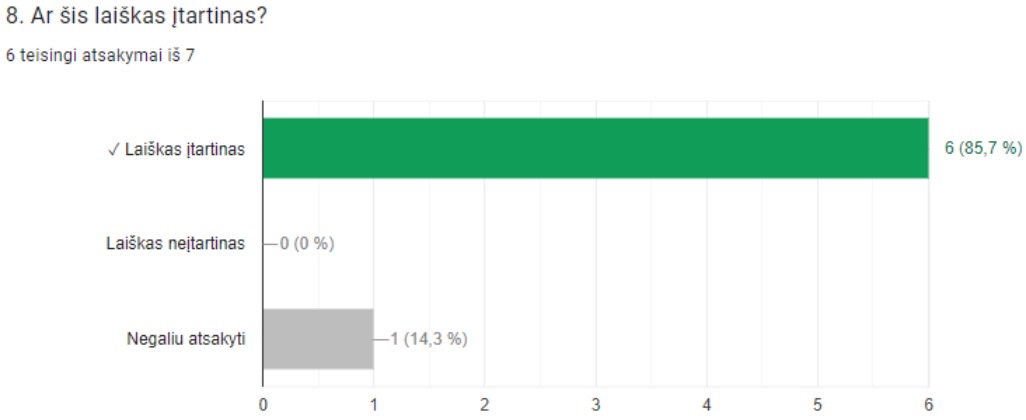
37 pav. Penkto klausimo rezultatai prieš plėtinio panaudojimą



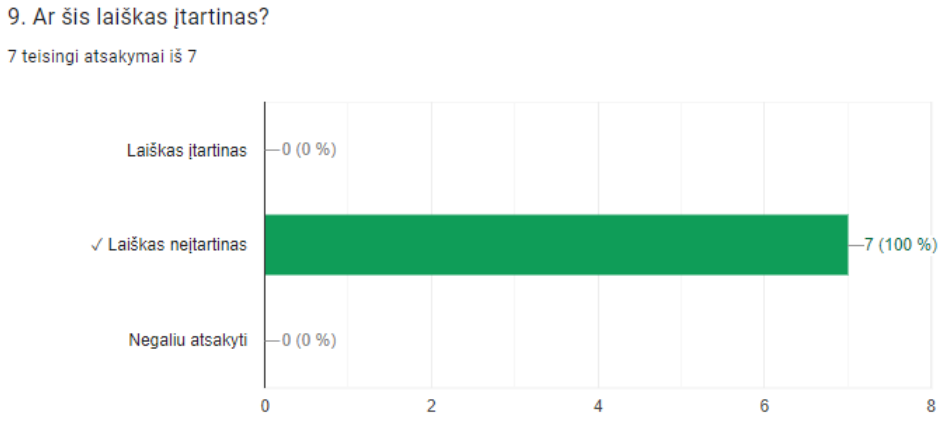
38 pav. Šešto klausimo rezultatai prieš plėtinio panaudojimą



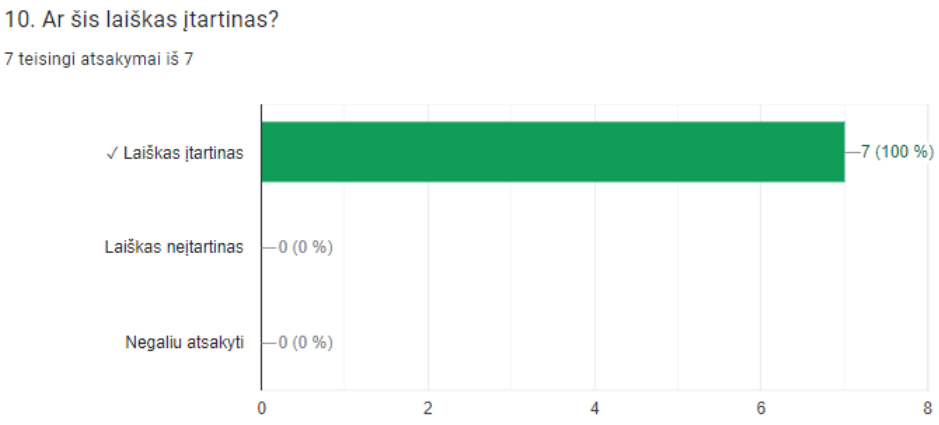
39 pav. Septinto klausimo rezultatai prieš plėtinio panaudojimą



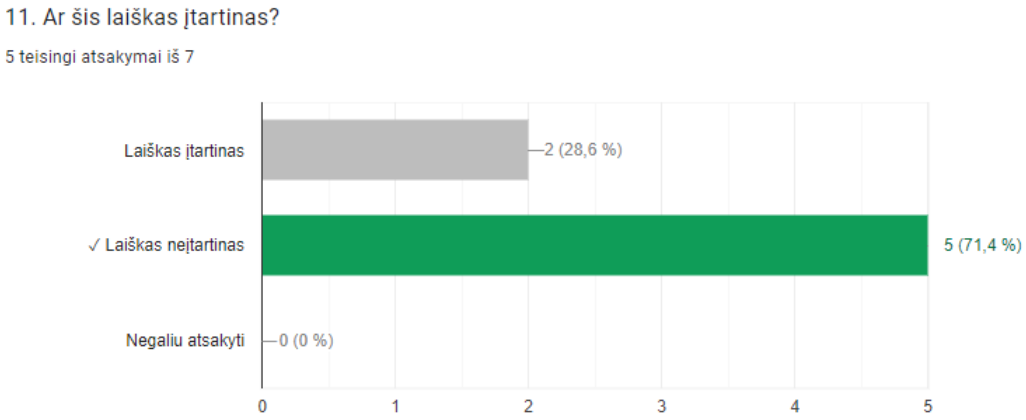
40 pav. Aštunto klausimo rezultatai prieš plėtinio panaudojimą



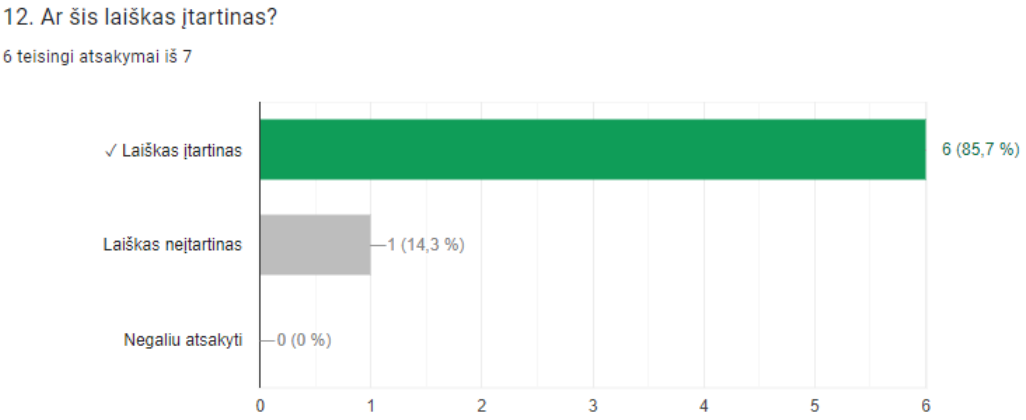
41 pav. Devinto klausimo rezultatai prieš plėtinio panaudojimą



42 pav. Dešimto klausimo rezultatai prieš plėtinio panaudojimą



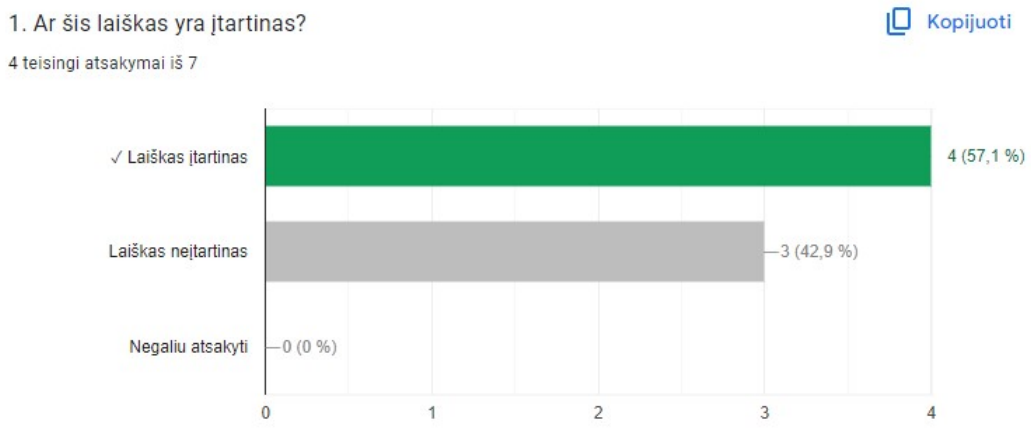
43 pav. Vienuolikto klausimo rezultatai prieš plėtinio panaudojimą



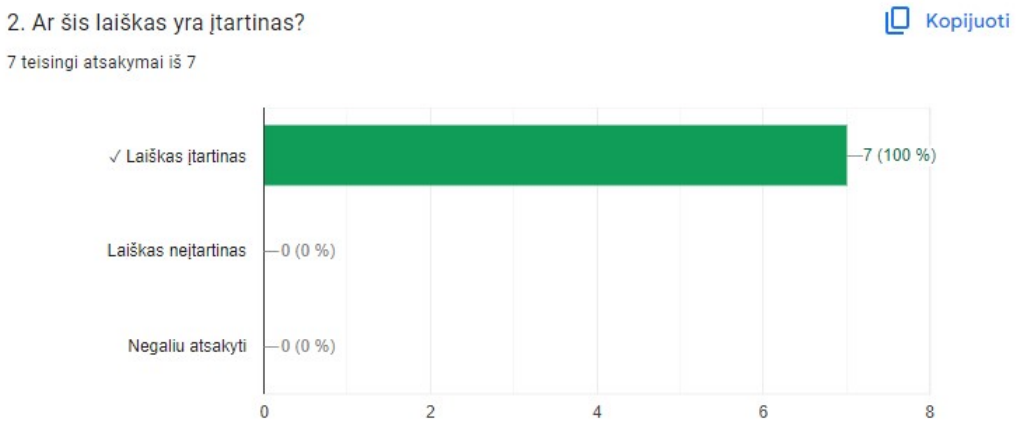
44 pav. Dvylikto klausimo rezultatai prieš plėtinio panaudojimą

6 priedas

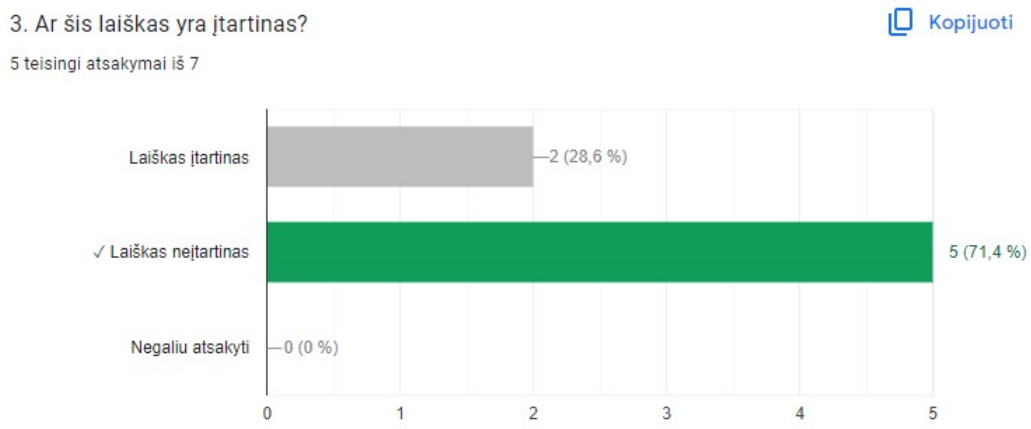
Klausimyno rezultatai po naršyklės plėtinio panaudojimo



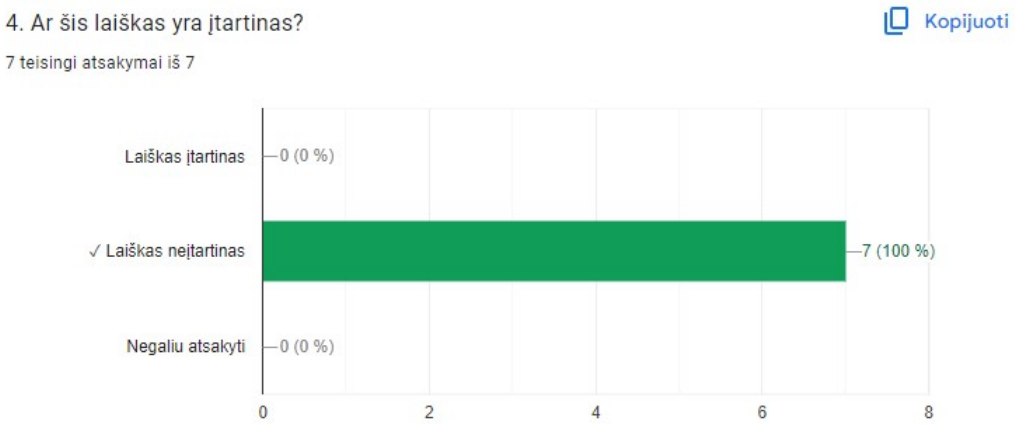
45 pav. Pirmo klausimo rezultatai po plėtinio panaudojimo



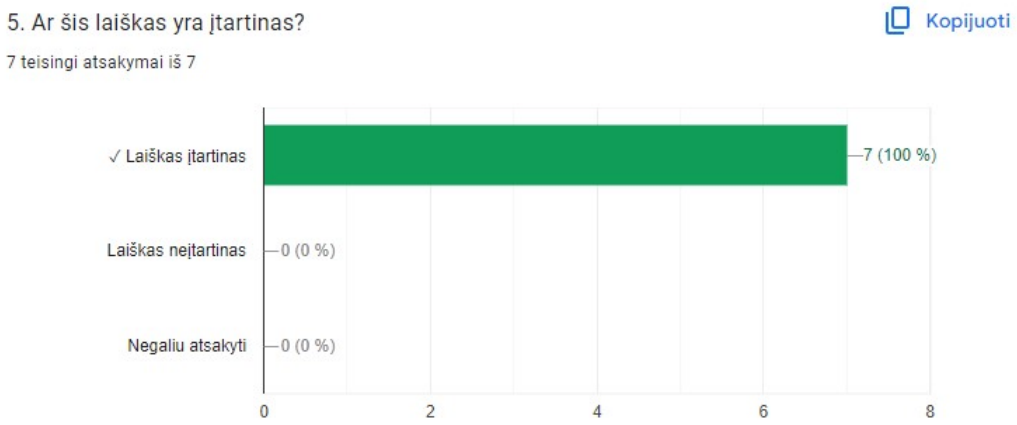
46 pav. Antro klausimo rezultatai po plėtinio panaudojimo



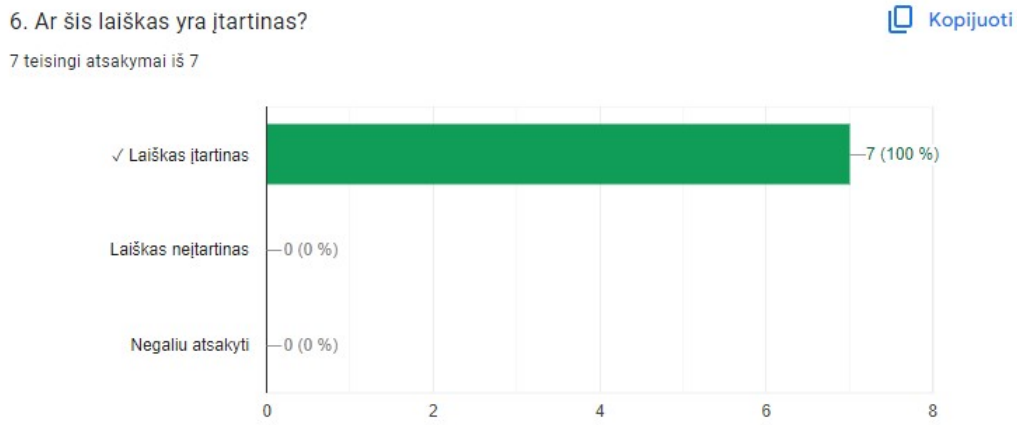
47 pav. Trečio klausimo rezultatai po plėtinio panaudojimo



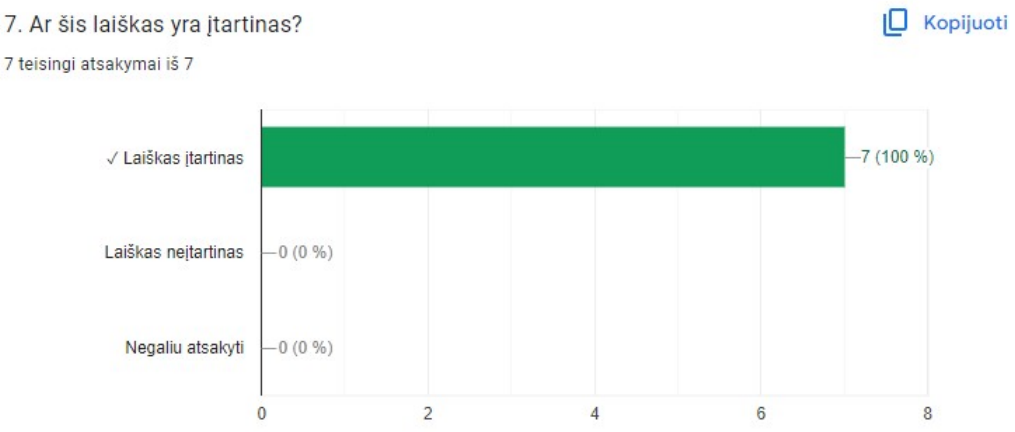
48 pav. Ketvirto klausimo rezultatai po plėtinio panaudojimo



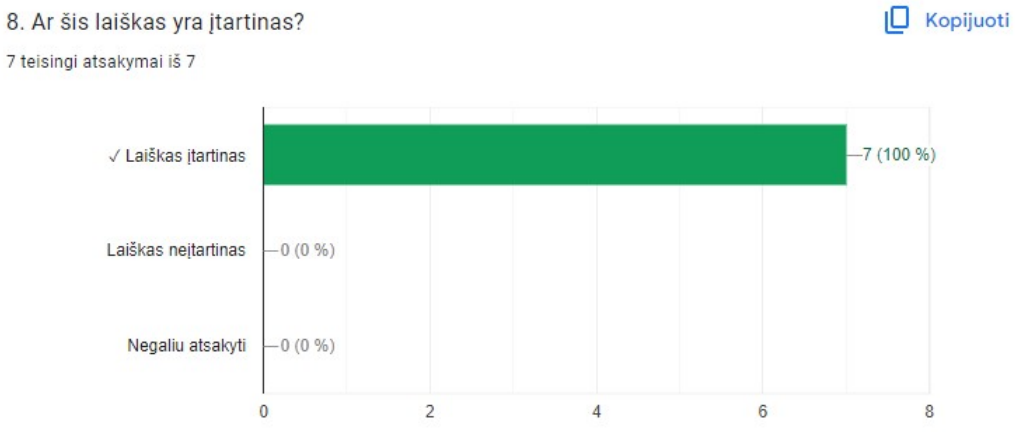
49 pav. Penkto klausimo rezultatai po plėtinio panaudojimo



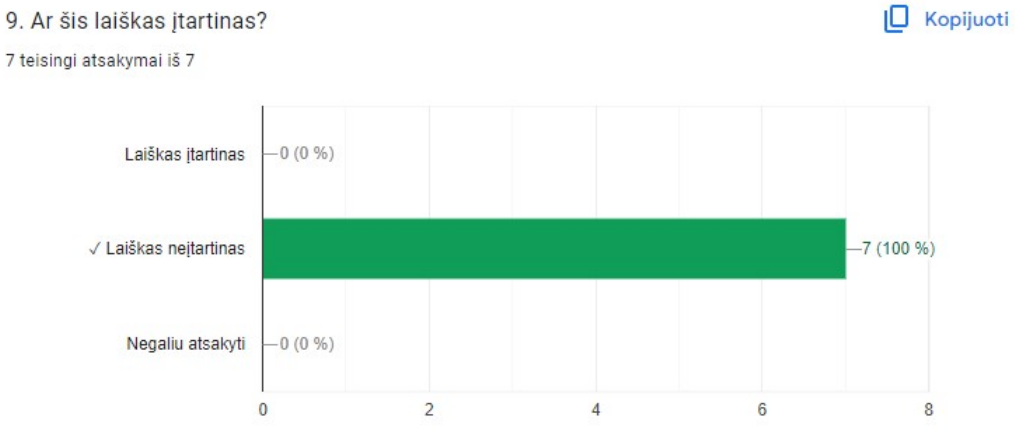
50 pav. Šešto klausimo rezultatai po plėtinio panaudojimo



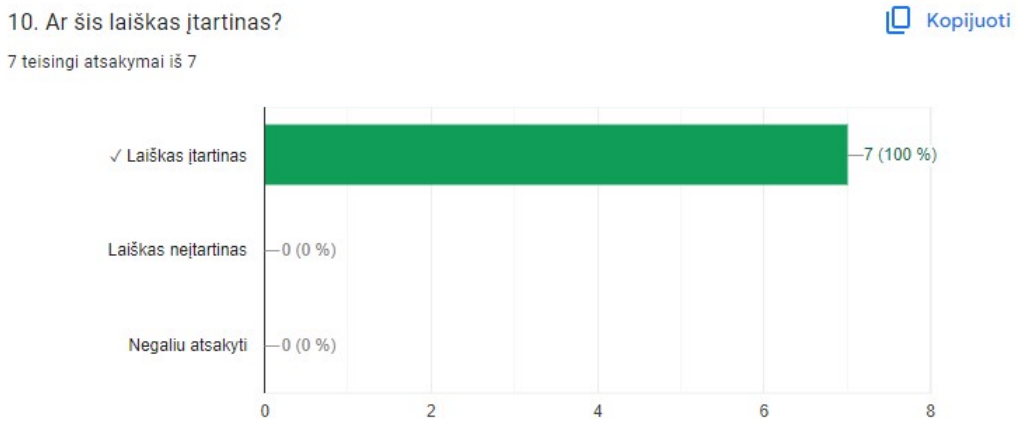
51 pav. Septinto klausimo rezultatai po plėtinio panaudojimo



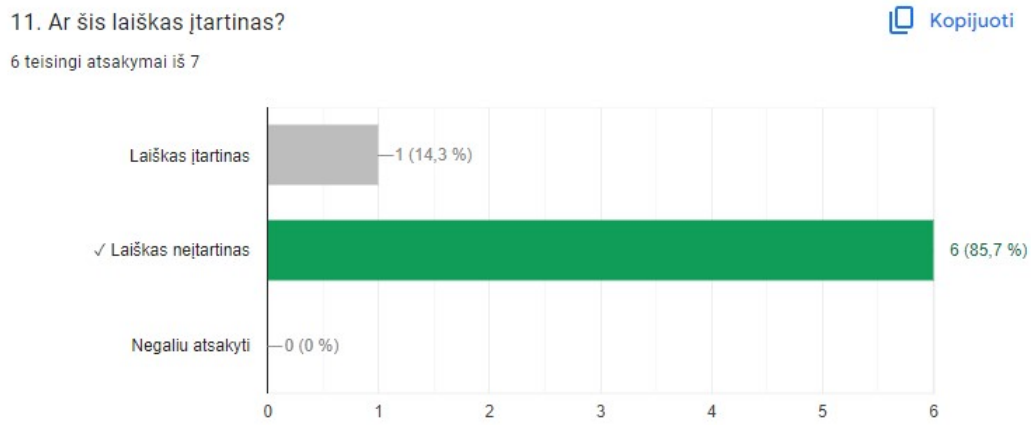
52 pav. Aštunto klausimo rezultatai po plėtinio panaudojimo



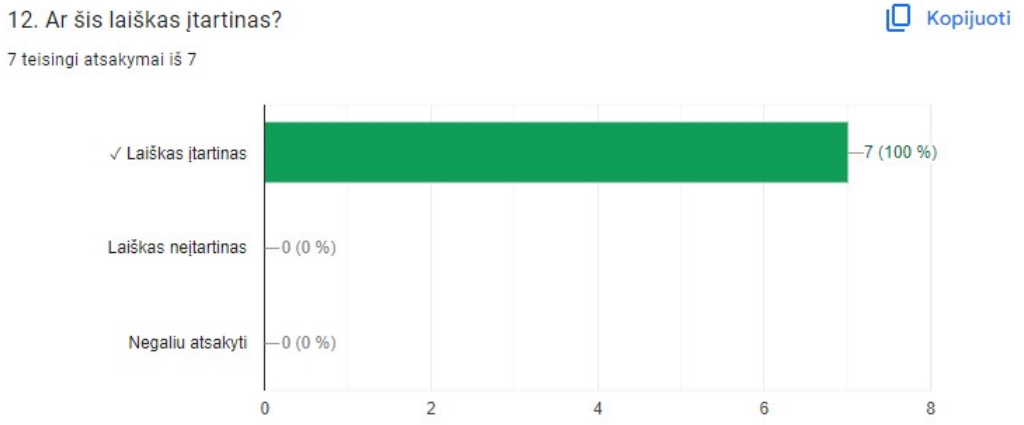
53 pav. Devinto klausimo rezultatai po plėtinio panaudojimo



54 pav. Dešimto klausimo rezultatai po plėtinio panaudojimo



55 pav. Vienuolikto klausimo rezultatai po plėtinio panaudojimo



56 pav. Dvylikto klausimo rezultatai po plėtinio panaudojimo