VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ STUDIJŲ PROGRAMA

Naudotojo apsauga nuo duomenų viliojimo atakų

Users' protection against phishing attacks

Bakalauro baigiamasis darbas

Atliko: Domas Nemanius
Kamilė Samusiovaitė

Darbo vadovas: doc. dr. Kristina Lapin

Recenzentas: doc. dr. Vytautas Čyras

Vilnius – 2025

Padėka

Nuoširdžiai dėkojame Vilniaus universiteto Matematikos ir informatikos fakulteto Programų sistemų katedros docentei dr. Kristinai Lapin už vertingas konsultacijas, metodinius patarimus ir pagalbą rengiant bakalauro baigiamąjį darbą, mokslinį straipsnį bei ruošiant žodinius pranešimus, skaitytus VI konferencijoje „Lietuvos magistrantų informatikos ir IT tyrimai“ vykusioje 2025m. gegužės 13 dieną, bei 13-ojoje jaunųjų mokslininkų konferencijoje „Fizinių ir technologijos mokslų tarpdalykiniai tyrimai“ vykusioje 2025m. balandžio 11 dieną.

Taip pat reiškiame padėką alternatyviųjų maketų panaudojamumo testavimo ir kiekybinio tyrimo dalyviams už savanorišką įsitraukimą bei indėlį į šio darbo tyrimų rezultatus.

Galiausiai dėkojame Vilniaus universiteto Matematikos ir informatikos fakulteto dėstytojams ir visai akademinei bendruomenei – jų suteiktos žinios ir ugdytos kompetencijos buvo itin svarbios rengiant šį baigiamąjį bakalauro darbą.

Turinys

Santrauka

Šiame bakalauro darbe yra siekiama identifikuoti duomenų viliojimo atakų požymius naudotojo sąsajoje ir remiantis šiais požymiais sukurti projektavimo gaires kuriamai priemonei, skirtai apsaugoti naudotoją nuo duomenų viliojimo atakų. Atlikus literatūros analizę identifikuotas duomenų viliojimo atakos gyvavimo ciklas, išskirti atakų tipai ir identifikuoti požymiai naudotojo sąsajoje. Šie požymiai suskirstyti į dviejų tipų požymius: internetinių adresų (URL) ir internetinių svetainių. Toliau šiame darbe surinkti ir aprašyti įrankiai, skirti apsaugoti naudotoją nuo duomenų viliojimo atakų. Jakobo Nielseno euristikos pritaikytos formuluojant panaudojamumo kriterijus, taip pat suformuluoti diegimo ir techninių sprendimų kriterijai. Remiantis šiais kriterijais atliktas įrankių vertinimas, kuris atskleidė įrankių teigiamas savybes ir trūkumus. Remiantis darbo metu gautais rezultatais, suformuluotos projektavimo gairės bakalauro darbe kuriamai priemonei, kuri padėtų apsaugoti naudotoją nuo duomenų viliojimo atakų. Atsižvelgiant į projektavimo gaires darbe buvo kuriami alternatyvieji maketai ir atliekamas jų panaudojamumo testavimas. Po šio testavimo buvo atliktas ir kiekybinis tyrimas. Atsižvelgiant į panaudojamumo testavimo ir tyrimo rezultatus patikslintos projektavimo gairės, kuriomis remiantis sukurtas detalusis prototipas, galiausiai ir priemonė, skirta padėti apsaugoti naudotoją nuo duomenų viliojimo atakų.

Raktiniai žodžiai: duomenų viliojimas, duomenų viliojimo ataka, įrankių vertinimas, duomenų viliojimo atakos požymiai, panaudojamumas, diegimas.

Summary

This bachelor thesis aims to identify the features of phishing attacks in the user interface and, based on these features, to develop design guidelines for a tool to be developed to help protect the user against phishing attacks. Following a literature analysis, the lifecycle of a phishing attack was identified, as well as the types of attack and user interface features. These features were grouped into URL features and website user interface features. In the following, this paper collects and describes tools to protect the user against phishing attacks. Jacob Nielsen's heuristics were applied to formulate usability criteria, and criteria for deployment and technical solutions were also formulated. Based on these criteria, an evaluation of the tools was carried out, which revealed the strengths and weaknesses of the tools. Based on the results of the research, design guidelines were formulated for a tool to be developed in the Bachelor's thesis to protect the user against phishing attacks. Alternative layouts were developed according to the design guidelines and usability testing was carried out. This testing was followed by a quantitative study. Based on the results of usability testing and a quantitative study, design guidelines were refined, leading to the creation of a detailed prototype and, ultimately, a tool aimed at protecting users from phishing attacks.

Keywords: phishing, phishing attack, tools evaluation, phishing features, usability, deployment.

Įvadas

Tyrimo objektas. Bakalauro darbe analizuojamos duomenų viliojimo atakos (angl. *phishing attacks*). Šias atakas kibernetiniai nusikaltėliai realizuoja naudodami socialinės inžinerijos metodus. Duomenų vagystės atakos tradiciškai veikia siunčiant suklastotus elektroninius laiškus, imituojančius internetinius bankus, mokėjimo svetaines ar nukreipiant naudotojus į fiktyvius tinklalapius, kurie kruopščiai sukurti taip, kad atrodytų kaip tikrosios svetainės. Duomenų vagystės atakomis siekiama surinkti aukos jautrią ir asmeninę informaciją, tokią kaip: naudotojo vardas, slaptažodis ar finansiniai duomenys [AZ17].

Tyrimo aktualumas. Terminą „phishing“ pirmą kartą internete 1996 m. pavartojo įsilaužėlių grupė, kuri pavogė „America Online“ paskyras, apgaule privertusi naudotojus atskleisti savo slaptažodžius [GTJ+17]. Nuo to laiko atakų skaičius vis augo, 2016 metais siekė 1,2 milijono ir tai yra 65 % daugiau nei 2015 metais [BZL+21]. Remiantis naujausiu „Intersile Consulting Group, LLC“ atliktu tyrimu „Phishing Lanscape 2023: A Study of the Scope and Distribution of Phishing“, kuris buvo paskelbtas 2023 m. rugpjūčio 9 d., duomenų vagystės atakų skaičius per laikotarpį nuo 2022 m. gegužės iki 2023 m. balandžio išaugo 65 %, lyginant su ankstesniu tyrimo laikotarpiu, ir siekė 1,8 milijono unikalių atakų [Int23]. Ir nors kasmet atakų skaičius vis didėja, vyksta nuolatinės ginklavimosi varžybos tarp naujų sukčiavimo atakų ir joms atpažinti naudojamų apsaugos priemonių, juk nenuostabu, kad duomenų vagystės atakų rengėjai keičia sukčiavimo strategiją atsižvelgdami į tas pačias rekomendacijas ir gaires, kuriomis naudojasi apsaugos priemonių kūrėjai [DTH06; IWG+08].

Duomenų vagystės atakos labai pasikeitė nuo jų atsiradimo 1990-aisiais. Ankstyvosiose atakose kibernetiniai nusikaltėliai naudojo paprastas taktikas – suklastotus elektroninius laiškus, kuriuose naudotojai buvo raginami patvirtinti savo paskyras. Per pastaruosius kelis dešimtmečius duomenų vagystės atakos iš apgaulingų elektroninių laiškų siuntinėjimo išsivystė į sudėtingas ir daugialypes technikas, kurios remiasi psichologiniu manipuliavimu ir techniniais metodais, siekiant išgauti asmeninę informaciją [AHN+21].

Siekiant užtikrinti interneto naudotojų saugumą yra ieškoma įvairių kovos su duomenų viliojimo atakomis metodų: kuriami juodieji sąrašai kenkėjiškiems URL adresams, nagrinėjamos euristikos, leidžiančios sintetinti naujus URL adresus iš esamų juodojo sąrašo įrašų [PKK+10]. Pasitelkiami ir elektroninių laiškų klasifikavimo metodai pagal tam tikrus apgavikų nuolat naudojamus požymius, kuriais siekiama nukreipti auką į sukčiavimo svetaines. Ieškoma vizualinių panašumų interneto svetainėse, tikrinama svetainės lango struktūra, pavyzdžiui, ar logotipai ir grafinės piktogramos atsikartoja kiekviename naršyklės lange ir panašiai. Literatūroje siūlomi įvairūs sprendimai, kaip išvengti ir aptikti duomenų viliojimo atakas, tačiau kai tik atrandamas naujas būdas apsisaugoti nuo duomenų viliojimo atakų, apgavikai analizuoja pasiūlyto sprendimo pažeidžiamas vietas, jas randa, ir toliau sėkmingai vykdo duomenų viliojimo atakas [GAP18]. Remiantis 2024 metų rugpjūčio 4 dienos publikuoto tyrimo išvadomis, apsaugos nuo kibernetinių atakų ateitis priklausys nuo nuolat atnaujinamų dirbtinio intelekto metodų, siekiant neatsilikti nuo vis atsinaujinančių įsilaužėlių gudrybių [SAE+24].

Darbo tikslas – identifikuoti duomenų viliojimo atakų požymius naudotojo sąsajoje, siekiant

palengvinti naudotojo mokymąsi, atakų atpažinimą, sukurti projektavimo gaires bakalauro darbe kuriamai priemonei bei sukurti naršyklės įskiepį priemonę, kuri padėtų apsaugoti naudotoją nuo duomenų viliojimo atakų.

Tyrimo uždaviniai:

1. išanalizuoti literatūrą, siekiant apžvelgti duomenų viliojimo atakų tipus bei identifikuoti atakos gyvavimo ciklo etapus, kuriuose jas galima atpažinti ir sustabdyti;
2. apžvelgti atakų tipus ir identifikuoti jų atpažinimo požymius naudotojo sąsajoje, skirtus apsaugoti naudotoją nuo duomenų viliojimo atakų;
3. suformuluoti kriterijus, kuriais remiantis bus įvertinti esami įrankiai, skirti apsaugoti naudotojus nuo duomenų viliojimo atakų;
4. remiantis įrankių vertinimo rezultatais suformuluoti projektavimo gaires bakalauro darbe kuriamai priemonei, skirtai apsaugoti naudotoją nuo duomenų viliojimo atakų;
5. remiantis projektavimo gairėmis sukurti alternatyviuosius maketus, kuriuose būtų išbandomi galimi sprendimai;
6. atlikti kiekybinį tyrimą, kurio tikslas išsiaiškinti, ar žmonės naudoja naršyklės įskiepius siekiant apsisaugoti nuo duomenų viliojimo atakų, kokios yra jų naudojimo ar nenaudojimo priežastys bei kaip būtų galima paskatinti tokių įrankių naudojimą siekiant didesnio kibernetinio saugumo;
7. remiantis tyrimo rezultatais bei alternatyviųjų maketų panaudojamumo testavimo rezultatais patikslinti suformuluotas projektavimo gaires;
8. remiantis patikslintomis projektavimo gairėmis sukurti detalųjį naršyklės įskiepio prototipą;
9. atsižvelgiant į detalųjį prototipą sukurti naršyklės įskiepį, kuris padėtų apsaugoti naudotoją nuo duomenų viliojimo atakų.

Teorinės darbo prielaidos ir metodika:

1. Literatūros apžvalga: Atliekama literatūros analizė, kurios metu analizuojamas duomenų viliojimo atakos procesas, tipai, požymiai bei įrankiai skirti apsaugoti naudotoją nuo duomenų viliojimo atakų. Taip pat remiantis moksline literatūra formuluojami kriterijai skirti vertinti įrankius, skirtus apsaugoti naudotoją nuo duomenų viliojimo atakų.
2. Euristinis vertinimas: remiantis suformuluotais panaudojamumo, diegimo bei techninių sprendimų kriterijais, atliekamas rastų įrankių, skirtų apsaugoti naudotoją nuo duomenų viliojimo atakų analitinis vertinimas.
3. Naudotojui palankus projektavimas (I etapas) skirtas užtikrinti kuriamos naudotojo sąsajos kokybę: remiantis įrankių vertinimo, pagal panaudojamumo kriterijus, rezultatais, gerosiomis praktikomis ir pastebėtais trūkumais, sukurti alternatyvieji maketai.
4. Panaudojamumo testavimas: atliekamas empirinis sukurtų maketų vertinimas su potencialiais naudotojais. Tyrimo metu analizuojamas maketų panaudojamumas, projektinių sprendimų efektyvumas ir renkama grįžtamoji informacija tolesniems patobulinimams.
5. Kiekybinis tyrimas: atliekamas tyrimas, siekiant išsiaiškinti esamą situaciją bei patikslinti projektavimo gaires.

6. Naudotojui palankus projektavimas (II etapas): remiantis patikslintomis projektavimo gairėmis bei alternatyviųjų maketų testavimo rezultatais, sukurtas detalusis prototipas, kuris tampa pagrindu kuriamam naršyklės plėtiniui.

Literatūros šaltiniai. Bakalauro darbas rašomas remiantis „Mokslinčius“ randama moksline literatūra. Ieškant literatūros šaltinių naudoti raktažodžiai, turintys žodį „*phishing*“. Efektyviausiai reikiamus šaltinius padėjo rasti raktažodžiai: „*phishing*“, „*phishing attack*“, „*phishing attack prevention tools*“, „*phishing detection*“. Peržiūrėta, bet nebūtinai naudota literatūra pateikiama prieduose (žr. 1 priedą). Naudoti šaltiniai pateikiami šaltinių skyriuje.

Darbo atlikimo aplinkybės. Panaudojamumo testavimas atliekamas tiesioginio kontakto būdu, susitinkant su testavimo dalyviais. Kiekybinis tyrimas atliekamas nuotoliniu būdu, dalyviai kviečiami užpildyti parengtą tyrimo anketą. Bakalauro baigiamasis darbas – grupinis. Įdėtas komandos narių darbo indėlis vienodas.

Naudojami instrumentai. Alternatyviajam bei detaliajam maketui kurti naudotas naudotojo sąsajos prototipų kūrimo įrankis „Figma“. „Google Chrome“ naršyklės plėtinio kūrimui taikytos šios technologijos:

1. „Microsoft“ sukurta integruota kūrimo aplinka „Visual Studio“.
2. Interpretuojamoji programavimo kalba „JavaScript“.
3. Žymėjimo kalba „HTML“.
4. Stilių aprašymo kalba „CSS“.
5. Programinė sąsaja „WHOIS API“, skirta domenų informacijos gavimui.
6. Programinė sąsaja „Google Safe Browsing API“, leidžianti tikrinti, ar URL arba IP adresas yra įtrauktas į žinomų nesaugių svetainių sąrašus.

Naršyklės plėtinio programinis kodas talpinamas viešoje „GitHub“ kodo saugykloje.

1. Duomenų viliojimo atakų apžvalga

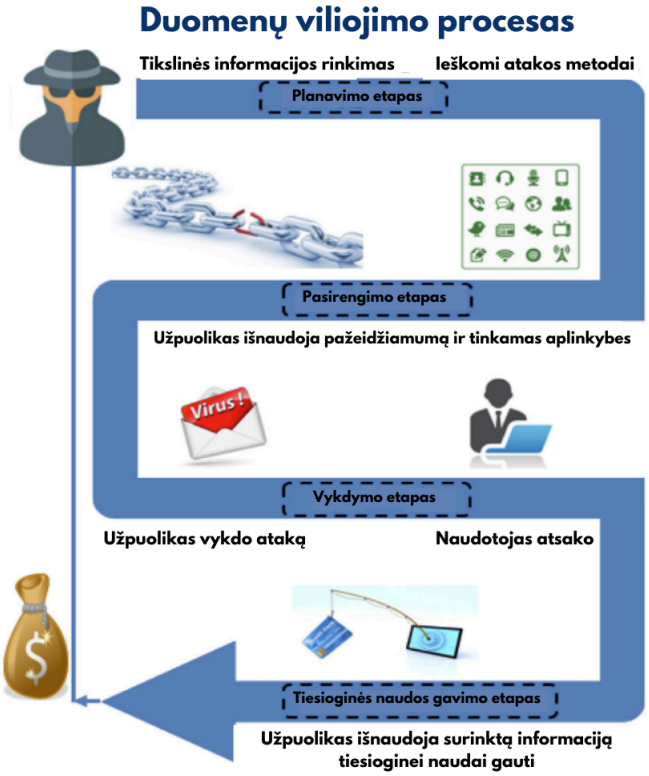
Šiame skyriuje apžvelgiamas duomenų viliojimo atakų procesas, duomenų viliojimo atakų tipai, siekiant identifikuoti požymius URL nuorodoje ir naudotojo sąsajoje. Taip pat apžvelgiamos duomenų viliojimo atakų pasekmės bei iššūkiai.

1.1. Duomenų viliojimo atakos

Duomenų viliojimo ataka (angl. *phishing attacks*) – tai sukčiavimo ataka, kai užpuolikas bando išvilioti interneto naudotojo asmeninę informaciją arba įgaliojimus, kad pasinaudojęs surinkta asmenine informacija gautų finansinės naudos. Duomenų viliojimo (angl. *phishing*) atakas galima palyginti su žvejyba (angl. *fishing*), suteikiant kiek kitokią prasmę. Atakos metu užpuolikas naudoja masalą (siunčia elektroninį laišką su įterpta nuoroda, nukreipiančią į apgaulingą svetainę), kad suvilioti interneto naudotojai atskleistų prisijungimo duomenis. Vieni anksčiausių programišių (angl. *hackers*) buvo žinomi kaip angl. *phreaks* (*phreak* yra asmuo, kuris įsilaužia į telefonų tinklus, kad galėtų skambinti nemokamai tarpmiestiniais telefono skambučiais arba pasiklausyti telefono linijų). Tad duomenų viliojimo atakų (angl. *phishing*) siejimas su „Phreaks“ ir yra priežastis, kodėl angliškame termine raidė „f“ pakeista į raides „ph“ [SC22].

1.2. Duomenų viliojimo procesas

Duomenų viliojimo atakos proceso eiga, paprastai susideda iš keturių etapų (žr. 1 paveikslą). Daugumoje atakų sukčiavimo procesas pradedamas renkant informaciją apie taikinį. Atakų organizatoriai renka informaciją apie aukas, kad jas suviliotų remdamiesi psichologiniu pažeidžiamumu. Renkama informacija gali būti bet kokia, pavyzdžiui, vardas, asmenų el.pašto adresai arba įmonės klientai. Į šį etapą taip pat įeina atakų metodų kūrimas, pavyzdžiui, suklastotų svetainių kūrimas. Priėmus sprendimą dėl taikinių ir surinkus informaciją apie juos, prasideda antrasis pasirengimo etapas, kurio metu programišiai pradeda rengti ataką ieškodami pažeidžiamumų, kuriais būtų galima pasinaudoti. Toliau seka atakos vykdymo etapas, kuriame naudojami atakos būdai grėsmei sukelti. Po aukos atsako užpuolikas įsilaužia į sistemą, kad surinktų naudotojo informaciją. Galiausiai seka tiesioginės naudos iš surinktų aukos duomenų gavimo etapas, kurio metu, apgavikai, panaudodami iš aukos surinktą informaciją, savinasi pinigus be naudotojų žinios, kuriuos naudoja pirkiniams įsigyti, finansuoti, arba parduoda surinktą informaciją juodojoje rinkoje [AHN+21].



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

1.3. Duomenų viliojimo atakų tipai

Duomenų viliojimo atakų metu užpuolikai planuoja ir naudoja įvairius atakų tipus, atsižvelgdami į aplinkybes, kad atakos sėkmės tikimybė būtų kuo didesnė. Išanalizavus literatūrą išskiriami pagrindiniai atakų tipai:

1. Personalizuotas duomenų viliojimas (angl. *spear phishing*).
2. Klaidingus įvedimus panaudojantis duomenų viliojimas (angl. *typo squating*).
3. Apgaulingas duomenų viliojimas (angl. *deceptive phishing*).
4. Reklamomis pagrįstas duomenų viliojimas (angl. *advertisement-based phishing*).
5. SMS duomenų viliojimas (angl. *smishing*).
6. Nuorodų manipuliavimu pagrįstas duomenų viliojimas (angl. *link manipulation*).
7. Klaidingą tarimą panaudojantis duomenų viliojimas (angl. *sound squating*).

1.3.1. Personalizuotas duomenų viliojimas

Personalizuotas duomenų viliojimas (angl. *spear phishing*) yra vienas dažniausiai pasitaikančių atakos tipų. Šios atakos metu siunčiami elektroniniai laiškai su kenkėjiškomis programomis (angl. *malware*), paslėptomis už nuorodų ir priedų, kurie atrodo tarsi siunčiami patikimo šaltinio (pvz., patikimos ir gerai žinomos įmonės, darbovietės ar bendradarbio) [KLD+20]. Šios atakos metu dėmesys yra skiriamas konkrečiam asmeniui ar asmenų grupei. Užpuolikai renka informaciją apie aukas, kad siunčiamuose laiškuose turinys būtų kuo labiau pritaikytas aukoms. Laiške yra pateikiama surinkta specifinė informacija apie auką, pavyzdžiui, vardas, pavardė, darbovietė ar

pareigos. Socialinės medijos platformos, tokios kaip „Linkedin“, naudojamos rinkti informaciją personalizuotai duomenų viliojimo atakai [AAO+24]. Šios atakos metu siunčiamas turinys – stipriai suasmenintas, todėl aukai sunkiau atpažinti tokias atakas.

1.3.2. Klaidingus įvedimus panaudojantis duomenų viliojimas

Klaidingus įvedimus panaudojantis duomenų viliojimas (angl. *typo squating*), dar žinomas kaip URL užgrobimas, yra kibernetinės atakos forma, kai užpuolikai užregistruoja domenų vardus, panašius į populiarias ar gerai žinomas svetaines, bet turinčius rašybos klaidų. Šiose atakose užpuolikai pasinaudoja žmogiškosiomis klaidomis, kurios gali atsirasti įvedant svetainės adresą į naršyklę, pavyzdžiui, neteisingai įvestas ar praleistas simbolis arba sukeisti gretimi simboliai. Užpuolikai registruodami klaidingus domenų vardus, imituojančius tikras svetaines, siekia perimti interneto srautą iš naudotojų, kurie netyčia padaro klaidas vesdami svetainės adresą. Naudotojas, įvedęs klaidingą domeno vardą, yra nukreipiamas į apgaulingą svetainę, sukurtą pavogti asmeninę informaciją, platinti kenkėjišką programinę įrangą ar vykdyti kitą žalingą veiklą. Kadangi šiose atakose naudojami domenų vardai labai primena tuos, į kuriuos buvo norima patekti, naudotojas iš karto nesuvokia, kad pateko į kenkėjišką svetainę, kas dar labiau padidina tikimybę tapti atakos auka [AAO+24].

1.3.3. Apgaulingas duomenų viliojimas

Apgaulingo duomenų viliojimo (angl. *deceptive phishing*) metu užpuolikai apsimeta patikimais siuntėjais (žr. 2 paveikslą), pavyzdžiui, banku, elektronine parduotuve ar socialinės medijos svetaine ir išsiuntinėja tūkstančius elektroninių laiškų interneto naudotojams su raginimais ir įspėjimais kuo greičiau paspausti nuorodas. Nuorodos, esančios elektroniniame laiške, auką nukreipia į iš pirmo žvilgsnio autentiškas svetaines, vis dėlto, šios svetainės kruopščiai sukurtos siekiant pasisavinti aukos asmeninę informaciją [SC22].

2 pav. Apgaulingo duomenų viliojimo laiško pavyzdys

Aukščiau esančiame paveiksle (žr. 2 paveikslą) pateiktas Lietuvos pašto internetinėje svetainėje rastas apgaulingo duomenų viliojimo laiško pavyzdys. Laiško gavėjas yra skatinamas paspausti mygtuką, slepiantį nuorodą į internetinę svetainę, kurioje yra siekiama iš aukos išvilioti pinigus. Aukai siekiama sukelti skubumo jausmą, tikinant, kad siunta bus nepristatyta negavus mokėjimo už siuntimą per 48 valandas.

1.3.4. Reklamomis pagrįstas duomenų viliojimas

Reklamomis pagrįsto duomenų viliojimo (angl. *advertisement-based phishing*) metu užpuolikai, vietoje to, kad siuntinėtų elektroninius laiškus dideliam kiekiui interneto naudotojų, reklamuoja kenkėjiškas svetaines paieškos varikliuose (angl. *search engine*). Šiais laikais internetas yra puiki platforma reklamoms. Daugelis įmonių internete reklamuoja naujus produktus ir paslaugas. Tačiau užpuolikai taip pat neatsilieka ir išnaudoja šias galimybes reklamuodami savo kenkėjiškas svetaines paieškos varikliuose, tikėdamiesi nukreipti potencialias aukas į kenkėjiškus interneto tinklalapius. Kai interneto naudotojas ieško tam tikrų raktažodžių, paieškos variklis parodo rezultatus, tarp kurių yra ir reklamos. Šios reklamos yra rodomos paieškos rezultatų viršuje arba tam tikrame puslapyje kaip iššokantis langas (angl. *pop-up*). Dauguma naudotojų paspaudžia aukščiausiai paieškos variklio pateiktą rezultatą, nepatikrinę adreso. Tai juos nukreipia į iš pirmo žvilgsnio nekenkėjišką svetainę, kuri reikalauja aukos prisijungimo ar kitų jautrių duomenų [SC22].

1.3.5. SMS duomenų viliojimas

Trumpųjų žinučių paslaugos (angl. *Short Message Service*, toliau SMS) duomenų viliojimo (angl. *smishing*) metu užpuolikai apsimeta patikimais siuntėjais, pavyzdžiui, pažįstamu asmeniu, banku, telefono paslaugų operatoriumi ar siuntas pristatančia bendrove ir siunčia SMS žinutes su nuorodomis, kurios nukreipia į kruopščiai padirbtas interneto svetaines. Auka gali sulaukti žinutės su tekstu „Interneto banke turite naują neperžiūrėtą pranešimą. Prisijunkite prie savo paskyros peržiūrėti“. Auka, paspaudusi SMS žinutėje pateiktą nuorodą, yra nukreipiama į apgaulingą svetainę, sukurtą pavogti asmeninę informaciją. Aukai bandant prisijungti prie savo paskyros, prisijungimo duomenys atitenka užpuolikui [AAO+24; SC22].

1.3.6. Nuorodų manipuliavimu pagrįstas duomenų viliojimas

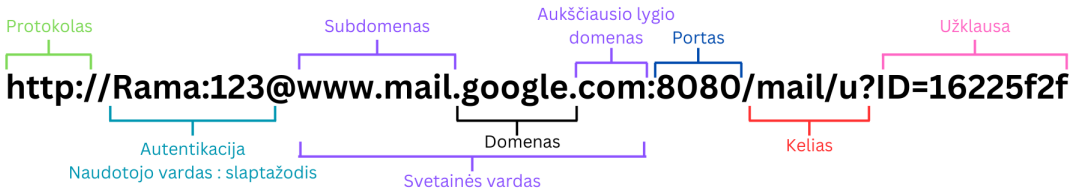
Nuorodų manipuliavimas (angl. *link manipulation*) yra kitų duomenų viliojimo atakų sudėtinė dalis. Užpuolikai nuorodas, skirtas aukas nukreipti į apgaulingas svetaines slepia naudodami hipertekstą. Aukai neužvedus pelės žymeklio ant hiperteksto ir neįsitikinus adreso autentiškumu, atsiranda rizika būti nukreiptai į užpuoliko kruopščiai sukurtą svetainę, skirtą išvilioti jautriems duomenims [AAO+24].

1.3.7. Klaidingą tarimą panaudojantis duomenų viliojimas

Klaidingą tarimą panaudojantis duomenų viliojimas (angl. *sound squating*) yra kibernetinės atakos forma, kai užpuolikai užregistruoja domenų vardus, kurie skamba panašiai kaip tikrieji

domenai, į kuriuos naudotojas bando patekti. Tokie domenai turės rašybos klaidų, sukeistų vietomis raidžių arba turės skirtingą galūnę, lyginant su tikruoju domenu, bet tariant naudotojui balsu skambės beveik identiškai. Šios duomenų viliojimo atakos tikslas išnaudoti naudotojo galimas rašybos klaidas, atsirandančias dėl panašiai skambančių žodžių. Naudotojui patekus į apgaulingą svetainę, atsiranda rizika atskleisti savo jautrius duomenis ar nukentėti finansiškai [AAO+24].

1.4. Duomenų viliojimo atakų požymiai URL nuorodoje



3 pav. URL pavyzdys, su pažymėtais standartiniais komponentais, adaptuotas iš [ARV19] į lietuvių kalbą

Apžvelgus duomenų viliojimo atakų tipus, aiškiai matoma, kad viena pagrindinių sudedamųjų dalių – URL nuorodos, nukreipiančios į užpuolikų padirbtas svetaines, skirtas išvilioti aukos jautrius duomenis. Kadangi svetainių URL adresai yra unikalūs, užpuolikams neįmanoma panaudoti tikrųjų svetainių adresų, pavyzdžiui, „facebook.com“, tad užpuolikai kuria adresus, panašius į tikruosius („facebok.com“, „blogis.com/facebook“). Analizuojant URL adresą (žr. 3 paveikslą) galima aptikti požymius, kurie indikuoja apie potencialiai duomenų viliojimo atakoms sukurtas interneto svetaines [AAT14; ARV19; LYC+19; MTM12]:

UP.1 **IP adresas**. URL nuorodoje vietoje domeno vardo naudojamas IP adresas yra vienas iš indikatorių, kad svetainė, kurią bandoma pasiekti, galimai yra skirta duomenų viliojimo atakai. IP adresas URL nuorodoje gali atrodyti taip: „http://91.131.11.211/~facebook/login“.

UP.2 **Ilgas URL adresas**. Užpuolikai stengiasi paslėpti įtartiną URL nuorodos dalį, naudodami ilgus URL adresus. Nėra patikimo standarto, kuris nurodytų, nuo kokio ilgio URL nuoroda klasifikuojama kaip įtartina, bet [MTM12] siūlo, kad jeigu URL ilgis viršija 54 simbolius, tokią URL nuorodą galima laikyti įtartina.

UP.3 **URL nuoroda, turinti @ simbolį**. URL nuorodoje įterptas simbolis „@“ priverčia interneto naršyklę ignoruoti viską prieš šį simbolį ir nuvedą į URL adresą, nurodytą po jo. Pavyzdžiui, URL nuoroda „https://facebook.com@blogis.com/“ nuvestų į interneto svetainę „https://blogis.com/“.

UP.4 **URL nuorodoje priešdėlis ar priesaga atskirti simboliu „-“**. Brūkšnys yra labai retai naudojamas tikruose URL adresuose, tad užpuolikai, pasinaudodami „-“, URL nuorodos domeno dalyje stengiasi užregistruoti domenų vardus, kuo panašesnius į tikruosius, pavyzdžiui, užregistruodami domeną „www.pay-pal.com“, siekia suklaidinti auką ir priversti patikėti, kad lankosi tikrojoje finansinių paslaugų svetainėje „www.paypal.com“. Taip pat neretai prie tikrųjų domenų vardų prideda priesagas (angl.

suffix) bei priešdėlius (angl. *prefix*). Užpuolikai, stengdamiesi suklaidinti potencialias aukas, gali užregistruoti domenų vardus pasinaudodami priešdėliais ar priesagomis, pavyzdžiui, „www.luminor-mokejimas.lt“, „www.bankas-luminor.lt“. Vieni dažniausiai priesagoms ir priešdėliams naudojami žodžiai: „Saugu“, „Mokėjimas“, „Paskyra“, „Patvirtinti“, „Užsakymas“.

UP.5 **Subdomeno naudojimas URL adrese**. Užpuolikų dar viena taikoma strategija – naudojami subdomenai URL nuorodoje siekiant suklaidinti potencialias aukas. Straipsnyje [MTM12] siūloma URL adresus, kurie turi 3 taškus (vieną subdomeną) URL nuorodoje klasifikuoti kaip įtartinus, o turinčius 4 taškus (du subdomenus) – kaip duomenų viliojimo atakoms naudojamus.

UP.6 **Netikras ar nenaudojamas HTTPS protokolas**. HTTPS – tai saugesnė HTTP protokolo versija, kuri padeda užtikrinti svetainės lankytojų duomenų šifravimą ir apsaugo nuo galimos duomenų vagystės. HTTPS protokolo buvimas indikuoja, kad naudotojas greičiausiai prisijungęs prie patikimos svetainės. Vis dėlto užpuolikai gali naudoti suklastotą HTTPS protokolą, kad apgautų potencialias aukas. Todėl svarbu įsitikinti, ar HTTPS protokolui reikalingą SSL sertifikatą išdavė patikima sertifikavimo institucija.

UP.7 **Domeno vardo amžius**. Duomenų vagystės atakoms naudojami domenų vardai egzistuoja labai trumpą laiką, tad domenai, kurie užregistruoti anksčiau nei prieš 6 mėnesius – klasifikuojami kaip įtartini. „WHOIS“ yra užklausų protokolas, kuris pateikia 48 savybes apie užklaustą domeno vardą, tarp jų ir kada domenas užregistruotas, atnaujintas bei kada baigia galioti.

UP.8 **Homoglifai domenų varduose**. Homoglifais vadinami simboliai ar simbolių junginiai, kurie vizualiai iš pirmo žvilgsnio labai panašūs į kitus simbolius. Keletas pavyzdžių: „rn“ gali susilieti ir atrodyti panašiai kaip „m“, „vv“ gali atrodyti panašiai kaip „w“, „cl“ panašu į „d“, „5“ į „S“, „B“ į „8“, simboliai „l“ (mažoji L), „I“ (didžioji I), „1“ (vienetas) gali būti maišomi tarpusavyje. Užpuolikai, pasinaudodami šia vizualine apgaule, registruoja domenų vardus, panašius į patikimų įmonių ar interneto svetainių domenus, siekdami juos panaudoti duomenų viliojimo atakų metu.

UP.9 **Nestandartiniai aukščiausio lygio domenai**. Aukščiausio lygio domenai skirstomi į dvi kategorijas: šalies kodo, pavyzdžiui Lietuvos „.lt“ ir bendrinius, pavyzdžiui, „.com“, skirtas įmonėms, „.org“, skirtas nepelno siekiančioms organizacijoms, „.gov“, skirtas vyriausybinėms organizacijoms. Vienas iš požymių, indikuojančių apie potencialią duomenų viliojimo ataką, yra šalies kodo aukščiausio lygio domenas, kuris nesutampa su domeną užregistravusio subjekto šalimi, pavyzdžiui, lankantis lietuviškoje svetainėje, kuri naudoja ne Lietuvos aukščiausio lygio domeną „.lt“, naudotojas turėtų būti atsargesnis ir įsitikinti, ar lankosi tikrojoje internetinėje svetainėje. Šią informaciją taip pat galima sužinoti naudojant jau anksčiau minėtą „WHOIS“ užklausų protokolą.

1.5. Duomenų viliojimo atakų požymiai internetinių svetainių naudotojo sąsajoje

Apžvelgę duomenų atakų tipus ir atakos požymius URL nuorodoje, matome, kad paskutinė duomenų viliojimo atakos dalis, kurioje dalyvauja naudotojas – internetinės svetainės, į kurias potencialios aukos yra nukreipiamos po to, kai paspaudžia ant užpuolikų atsiųstų URL nuorodų. Šiame etape užpuolikų tikslas – surinkti aukos jautrią informaciją, tad užpuolikai kuria svetaines, kuo panašesnes į autentiškas, žymių bei patikimų įmonių ar paslaugų tiekėjų. Gera žinia ta, kad plagijuotose interneto svetainėse galima aptikti požymių, kurie indikuoja apie potencialias duomenų viliojimo atakas [AAT14; LYC+19; MTM12]:

SP.1 **Prisijungimas iššokančiame lange**. Užpuolikai naudoja iššokančius langus (angl. *pop-up window*), kuriuose aukų prašo įvesti jautrią informaciją. Autentiškose svetainėse tai retai naudojama praktika, tad tai yra vienas iš indikatorių apie potencialią duomenų viliojimo ataką.

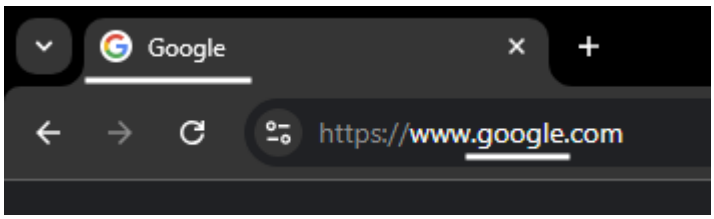
SP.2 **Raginimai ar įspėjimai kuo greičiau atlikti veiksmus**. Duomenų viliojimo atakos metu užpuolikai naudotoją laiko silpnąja grandimi (angl. *weaklink*), tad svetainėse naudoja tekstą, raginantį kuo greičiau atlikti veiksmus, kurių neatlikus gali būti neigiamos pasekmės, taip siekiant aukai sukelti stresą ir skubumo jausmą. Vienas iš pavyzdžių – naudotojas gali būti skubinamas prisijungti prie savo paskyros, kad patvirtintų savo duomenis, o to neatlikus per tam tikrą laiką, jo paskyra bus užblokuota. Naudotojai, pastebėję skubinimus, turėtų būti atidesni ir įsitikinti, ar lankosi autentiškoje svetainėje, nes tai vienas iš požymių, indikuojančių apie potencialią duomenų viliojimo ataką.

SP.3 **Neaktyvios nuorodos internetinėje svetainėje**. Užpuolikai, kurdami internetines svetaines duomenų viliojimo atakoms, siekia, kad jos atrodytų kuo panašiau į autentiškas svetaines, tad prideda nuorodų į kitus šios svetainės puslapius. Vis dėlto šios nuorodos būna neaktyvios. Pastebėję, kad internetinėje svetainėje yra neaktyvių nuorodų, naudotojai turėtų būti atsargesni, nes tai vienas iš padirbtos svetainės požymių.

SP.4 **Dešiniojo pelės mygtuko išjungimas**. Užpuolikai, naudodami „JavaScript“, išjungia dešiniojo pelės mygtuko paspaudimo funkciją, kad neleistų naudotojams peržiūrėti bei išsaugoti svetainės šaltinio kodo.

SP.5 **Puslapio pavadinimo ir domeno vardo nesutapimas**. Paprastai internetinės svetainės pavadinimas (angl. *website title*) ir domeno vardai sutampa. Jei internetinės svetainės pavadinimas ir domeno vardas nesutampa, tikėtina, kad tai duomenų viliojimo atakai sukurta svetainė (žr. 4 paveikslą). Pavyzdžiui, internetinės svetainės „www.google.com“ tiek domenas, tiek svetainės pavadinimas yra „google“.

SP.6 **Nuorodų slėpimas naudojant hipertekstą**. Užpuolikai naudoja hipertekstą, siekdami paslėpti nuorodas, skirtas aukas nukreipti į apgaulingas svetaines. Užpuolikai tikisi, kad auka neužves pelės žymeklio ant hiperteksto, nepatikrins URL adreso ir atsidurs jų interneto svetainėje, skirtoje išvilioti aukos jautrią informaciją.



4 pav. Internetinės svetainės „www.google.com“ tiek domenas, tiek svetainės pavadinimas yra „google“

1.6. Duomenų viliojimo atakų pasekmės

Duomenų viliojimo atakos gali turėti neigiamų pasekmių tiek individualiems interneto naudotojams, tiek įmonėms bei organizacijoms. Pagrindinės duomenų viliojimo atakų pasekmės yra šios [JG22]:

1. Duomenų viliojimo atakos atskleidžia aukos jautrią informaciją ir sukelia finansinę žalą.
2. Atakos sukuria neigiamą požiūrį į interneto svetaines ir sukelia nepasitikėjimą internetu.
3. Dėl prarasto pasitikėjimo interneto naudotojai gali vengti internetinės bankininkystės paslaugų ar elektroninės prekybos.
4. Dėl duomenų viliojimo atakų įmonė gali prarasti klientų pasitikėjimą, reputaciją, įmonės prekės ženklo vertę, taip pat gali sumažėti įmonės akcijų kaina.

1.7. Įmonėms sukeliama duomenų viliojimo atakų žala

Duomenų viliojimo atakos daro didelę žalą įmonėms ir organizacijoms, pavogdamos vertingus duomenis, tokius kaip: darbuotojų vardus, gyvenamuosius adresus, banko sąskaitų informaciją, įmonės mokslinių tyrimų ir plėtros rezultatus, finansinę informaciją bei intelektinę nuosavybę. Be to, duomenų viliojimo atakų metu vagiami ir klientų prisijungimo duomenys, kurie vėliau parduodami juodojoje rinkoje už dideles kainas. Remiantis „Anti-Phising Working Group“ (APWG) 2019 m. ataskaita, per trečiąjį metų ketvirtį buvo aptikti 266 378 unikalūs duomenų viliojimo tinklapiai. Iš jų 80 % buvo nukreipti į finansinių paslaugų, internetinio pašto (angl. *webmail*), mokėjimo paslaugų ir el. komercijos sektorius. Dėl duomenų viliojimo atakos Austrijos aviacijos detalių gamintojas „FACC“ prarado 61 mln. dolerių. Šioje atakoje įsilaužėlis apsimetė įmonės generaliniu direktoriumi ir išsiuntė apgaulingą elektroninį laišką apskaitos darbuotojui, kuris pervedė lėšas į netikrą sąskaitą fiktyviam projektui. Be finansinių nuostolių, įmonės patiria ir operacinių trikdžių, nes duomenų viliojimo atakų metu pavogti duomenys gali būti panaudoti ir tolimesnėms atakoms. Be to, žala reputacijai gali būti ir negrįžtama, ypač jeigu įmonė nepajėgia laiku sureaguoti ir užtikrinti klientų bei partnerių duomenų saugumo. Tai rodo, kad šios atakos yra rimta grėsmė, į kurią įmonės ir organizacijos turi žiūrėti itin atsakingai ir skirti pakankamai lėšų tinkamoms prevencijos priemonėms [JG22].

1.8. Duomenų viliojimo atakų iššūkiai

Duomenų viliojimo atakos tampa vis didėjančia grėsme kiekvieno žmogaus interneto saugumui, nes surinkęs net ir nedidelį informacijos kiekį apie auką, užpuolikas gali sukurti individualizuotą ir patikimai atrodantį elektroninį laišką. Atakų kūrėjus taip pat nėra lengva ir sugauti, nes dauguma jų slepia savo serverių buvimo vietą, todėl dirba beveik visiškai anonimiškai. Tačiau yra daug būdų, kaip apsisaugoti nuo bandymų sukčiauti. Ataka gali būti aptikta dar nepasiekusi naudotojų, kai naudotojas pasiekia sukčiavimo svetainę, arba naudotojas tiesiog gali būti apmokytas žinoti apie atakas ir jų grėsmes. Naudojant šiuos metodus kartu, galima sukurti saugią ir patikimą aplinką [VK18].

Duomenų viliojimo atakų problema yra ta, kad užpuolikai nuolat ieško naujų ir išradingų būdų, kaip apgauti naudotojus, kad jie patikėtų, jog jų atliekami veiksmai atakos metu yra susiję su teisėta svetaine arba elektroniniu paštu. Atakų kūrėjai yra vis labiau įgudę klastoti svetaines, kad jos atrodytų identiškos. Naujieji sukčiavimo metodai naudoja asmens informaciją, kuri yra viešai prieinama internete, kad kurtų įtikinamas atakas, tiesiogiai nukreiptas prieš aukas. Tokie metodai, kaip socialinis sukčiavimas ir konteksto suvokimas, yra puikūs pavyzdžiai, kad atakos yra vykdomos pasinaudojant didžiuliu viešai prieinamu informacijos kiekiu. Ir nors šios atakos daro įtaką žmonėms visame pasaulyje ir jos vykdomos tarptautiniu mastu, sunku yra susekti ir patraukti baudžiamojon atsakomybėn už tai atsakingus nusikaltėlius [VK18].

Straipsnyje „Phishing – challenges and solutions“ [VK18] yra siūlomi tris būdai, kaip galima būtų aptikti sukčiavimo atakas: aptikti, kol jos dar nepasiekė naudotojo; aptikti, kai naudotojas jau pasiekė sukčiavimo svetainę; išmokyti naudotojus pačius aptikti ir užkirsti kelią duomenų viliojimo atakoms. Kiekvienas iš būdų turi savų privalumų ir trūkumų, tačiau straipsnio autoriai teigia, kad geriausias apsisaugojimo metodas yra visų trijų apsisaugojimo būdų derinys.

1. Pirmasis būdas – užkirsti kelią atakai dar nepasiekus naudotojo, įtraukiant į juodąjį sąrašą arba blokuojant sukčiavimo svetaines, arba filtruojant sukčiavimo el.laiškus.
2. Antrasis būdas – aptikti sukčiavimą. Kadangi užpuolikai naudoja sudėtingus metodus, kad užtikrintų, jog duomenų viliojimo atakų elektroniniai laiškai ir svetainės pasiektų pažeidžiamus naudotojus, yra ieškoma metodų, kaip nustatyti galimas sukčiavimo svetaines arba kaip nurodyti naudotojui vengti pateikti informaciją šiuose el. laiškuose ar svetainėse, net jei jis ir gavo (ir atidarė) kenkėjišką el.laišką. Daugelyje interneto naršyklių jau yra įdiegtos apsaugos nuo sukčiavimo svetainių priemonės, kurios turi pasyvųjį arba aktyvųjį indikatorių. Aktyvūs indikatoriai turi iššokančius langus su perspėjimu apie įtartiną svetainę, o pasyvūs indikatoriai netrukdo naudotojui atlikti užduoties. Kaip ir tikėtasi, daugelis naudotojų ignoruodavo arba tiesiog nepastebėdavo pasyvių indikatorių, nes kai kurie naudotojai pasitiki, kad svetainės, į kurias eina, yra būtent tokios, kokių ir tikisi. Kovojant su šiuo iššūkiu, gali būti naudinga taikyti patikimų ir saugių svetainių tikrinimo sistemą, kai naudotojai matys svetainės patikrinimą kiekvieną kartą lankydamiesi tikroje svetainėje, labiau tikėtina, kad pastebės, jog jo nėra netikroje svetainėje.
3. Trečiasis būdas – suinteresuotųjų šalių mokymas, kaip išvengti duomenų viliojimo atakų. Dauguma esamų bendrųjų mokymų apie sukčiavimą yra plataus masto ir nepadeda kovoti

su dabartinėmis pažangesnėmis sukčiavimo atakomis. Be to, mokymų rezultatai priklauso ir nuo to, ar naudotojai iš tiesų įsitraukia į mokomąją medžiagą ir ją skaito. Įspėjimų ar medžiagos siuntimas elektroniniu paštu paprastai neveikia, nes dauguma naudotojų yra įpratę nekreipti dėmesio į tokius laiškus ir mano, kad žino, kaip apsisaugoti. Straipsnio autoriai siūlo metodus, kurie naudoja žaidimus arba mokymo sistemų įterpimą į elektroninių laiškų serverius. Mokslininkai dirba ties tokiais žaidimais. Pavyzdžiui, vienas sėkmingiausių žaidimo formato pavyzdžių yra „Anti-Phising Phil“ žaidimas, padedantis išmokyti naudotojus atpažinti įtartinus URL adresus ir kitus sukčiavimo apgaulės komponentus. Toks mokymo metodas yra ir įtraukiantis naudotoją, ir informatyvus, tačiau naudotojai vis tiek turi patys pereiti prie šios programos. Kitas metodas – įterptinis mokymasis, kuris gali būti naudingas. Siunčiant imitacinius elektroninius laiškus, naudotojai, kurie dar nėra apmokyti vengti sukčiavimo apgaulės, bus apmokyti. Atidarę ir paspaudę laiške esančią nuorodą, naudotojai patektų į puslapį, kuriame būtų informuojami apie tai, kas su elektroniniu laišku buvo negerai ir į ką turėtų atkreipti dėmesį ateityje, kad išvengtų tikros atakos.

Aukščiau minėto straipsnio autorių rekomendacijos būsimiems darbams ir yra anksčiau aprašytą siūlomą kovos su sukčiavimu sprendimo sistemą įtraukti į elektroninio pašto paslaugų tiekėjų, pavyzdžiui „Gmail“, „Yahoo“ ir „Hotmail“ serverius. Tokiu būdu būtų užtikrinta, kad net ir tie, kurie neturi patirties su kompiuterine įranga ir sukčiavimo rizikomis, vis tiek būtų apsaugoti, kad ir pačiu paprasčiausiu lygmeniu. Dar būtų veiksmingiau, jeigu šie serveriai į savo elektroninio pašto paslaugas įtrauktų integruotas mokymo sistemas, nes tada naudotojai taptų labiau išprusę, žinotų, kaip ateityje apsisaugoti nuo duomenų viliojimo atakų, o tai leistų kurti sąmoningų naudotojų visuomenę ir labiau apsunkintų sėkmingas atakas.

1.9. Apibendrinimas

Išanalizavus duomenų viliojimo atakų procesą ir tipus, matyti, kad užpuolikai geba prisitaikyti prie besikeičiančių aplinkybių ir randa būdų, kaip išvilioti naudotojų jautrius duomenis. Išanalizavus literatūrą buvo rasti duomenų viliojimo atakų tipai, turintys naudotojo sąsają:

1. Personalizuotas duomenų viliojimas (angl. *spear phishing*).
2. Klaidingus įvedimus panaudojantis duomenų viliojimas (angl. *typo squating*).
3. Apgaulingas duomenų viliojimas (angl. *deceptive phishing*).
4. Reklamomis pagrįstas duomenų viliojimas (angl. *advertisement-based phishing*).
5. SMS duomenų viliojimas (angl. *smishing*).
6. Nuorodų manipuliavimu pagrįstas duomenų viliojimas (angl. *link manipulation*).
7. Klaidingą tarimą panaudojantis duomenų viliojimas (angl. *sound squating*).

Pastebėta, kad užpuolikai naudoja socialinės inžinerijos metodus, pavyzdžiui, svetainės ar el. laiško turinio pritaikymą pagal aukos asmeninę informaciją, randamą internete, socialiniuose tinkluose ar anksčiau nutekintuose duomenyse. Ši surinkta informacija naudojama siekiant padaryti

ataką kuo sunkiau atpažįstamą aukai. Užkirsti kelią duomenų viliojimo atakoms nėra paprasta, bet įmanoma, pasitelkiant:

1. **Ankstyvąjį blokavimą.** Ankstyvasis blokavimas – žinomų duomenų viliojimo svetainių blokavimas.
2. **Ankstyvąjį aptikimą.** Ankstyvasis aptikimas – naršyklės, el. pašto plėtiniai, gebantys atpažinti ir identifikuoti potencialias duomenų viliojimo atakas.
3. **Naudotojų mokymą.** Naudotojų mokymas – mokymas savarankiškai atpažinti potencialias duomenų viliojimo atakas.

Užpuolikai, rengdami duomenų viliojimo atakas, naudotoją laiko silpnąja grandimi ir bando išnaudoti naudotojų klaidas arba neatidumą. Gera žinia ta, kad duomenų atakų tipai turi panašumų, kuriais remiantis galima šviesti naudotoją ir mokyti atpažinti potencialias atakas arba panaudojant šiuos požymius (žr. 1 lentelę) kurti įrankius, gebančius atpažinti duomenų viliojimo atakas ir padėti apsaugoti potencialias duomenų viliojimo atakų aukas. Analizuojant literatūrą ir duomenų viliojimo atakų tipus pavyko rasti šiuos URL nuorodų ir internetinių svetainių požymius, kurie indikuoja apie potencialias duomenų viliojimo atakas.

1 lentelė. Duomenų viliojimo atakų požymiai

Požymiai URL nuorodoje	Požymiai internetinių svetainių naudotojo sąsajoje
UP.1 IP adresas UP.2 Ilgas URL adresas UP.3 URL nuoroda, turinti @ simbolį UP.4 URL nuorodoje priešdėlis ar priesaga atskirti simboliu „-“ UP.5 Subdomeno naudojimas URL adrese UP.6 Netikras ar nenaudojamas HTTPS protokolas UP.7 Domeno vardo amžius UP.8 Homoglifai domenų varduose UP.9 Nestandartiniai aukščiausio lygio domenai	SP.1 Prisijungimas iššokančiame lange SP.2 Raginimai ar įspėjimai kuo greičiau atlikti veiksmus SP.3 Neaktyvios nuorodos internetinėje svetainėje SP.4 Dešiniojo pelės mygtuko išjungimas SP.5 Puslapio pavadinimo ir domeno vardo nesutapimas SP.6 Nuorodų slėpimas naudojant hipertekstą

2. Duomenų viliojimo atakų įrankių apžvalga ir vertinimas pagal panaudojamumo, diegimo ir techninių sprendimų kriterijus

Šiame poskyryje yra identifikuojami kriterijai, kuriais remiantis bus vertinami įrankiai, skirti naudotojų apsaugai nuo duomenų viliojimo atakų. Panaudojamumo kriterijams formuluoti naudotos devynios iš dešimties Jakobo Nielseno euristikų. Nepanaudota euristika – „Padėti naudotojams atpažinti, diagnozuoti ir ištaisyti klaidas“. Šios euristikos nuspręsta netaikyti, nes sukurti įrankiai, skirti apsaugoti naudotojui nuo duomenų viliojimo atakų, klaidų nepraneša. Jų paskirtis – teikti įspėjimus ir informacinius pranešimus. Kadangi tokius apsaugos įrankius naudotojas įdiegia pats, galimų klaidų atveju pranešimus pateiktų naršyklė arba kompiuterio operacinė sistema, todėl ši euristika laikoma neaktualia. Panaudojamumo kriterijai surinkti remiantis [LH07] straipsniu, diegimo kriterijai rinkti remiantis [BHV+12] straipsnyje aprašytais diegimo kriterijais. Naudojami techninių sprendimų vertinimo kriterijai surinkti remiantis [AAO+24; AZ17]. Surinkti kriterijai papildyti. Kiekvienas kriterijus turi savo identifikatorių ir aprašymą, kuriame apibrėžiamas kriterijų taikymas apsaugos nuo viliojimo atakų priemonėms vertinti.

2.1. Panaudojamumo kriterijai

PK.1 **Sistemos būsenos matomumas.** Euristika tikrina vizualinius gebėjimus trijose stadijose: prieš patenkant į svetainę tikrinant svetainės autentiškumą, tikrinant svetainės autentiškumą bandant patekti į svetainę ir esant joje. Kiekvienoje stadijoje svetainė, kurioje lankosi naudotojas, turėtų informuoti naudotoją apie vykstantį procesą ir pateikti svetainės autentiškumo rezultatą. Rezultato pateikimas turėtų būti nuolat rodomas.

Vertinimas:

⊖– kriterijus neįgyvendinamas.

○– įrankio būsena yra matoma bent vienoje stadijoje.

◐– įrankio būsena yra matoma dviejose stadijose.

●– įrankio būsena yra matoma visose trijose stadijose.

PK.2 **Atitikimas tarp sistemos ir realaus pasaulio.** Didelė dalis pažeidžiamų naudotojų neturi pakankamai žinių apie kompiuterius ir internetą, todėl kiekviena operacija turi būti suprantama ir lengvai nuspėjama neįgudusiems naudotojams. Tai reiškia, kad žmonės, kurie neturi pakankamai žinių, gebėtų apsisaugoti remdamiesi nurodymais ar įspėjimais. Ši euristika apima žinomų žodžių, frazių, piktogramų ir vaizdų naudojimą, kurie būtų lengvai atpažįstami, išmokstami ir įsimenami.

Vertinimas:

⊖– įrankyje naudojami žodžiai, frazės, piktogramos, vaizdai nėra lengvai atpažįstami, išmokstami ir įsimenami, nėra jokių nurodymų ar įspėjimų.

○– įrankyje naudojami žodžiai, frazės, piktogramos, vaizdai yra atpažįstami, išmokstami, tačiau nėra jokių nurodymų ar įspėjimų.

◐– įrankyje naudojami žodžiai, frazės, piktogramos, vaizdai yra atpažįstami, išmokstami. Yra nurodymų ir įspėjimų, tačiau jie nėra lengvai atpažįstami.

●– įrankyje naudojami žodžiai, frazės, piktogramos, vaizdai yra lengvai atpažįstami, išmokstami ir įsimenami, remdamiesi nurodymais ar įspėjimais net ir neįgudę naudotojai gali greitai išmokti naudotis įrankiu.

PK.3 **Naudotojo kontrolė ir laisvė.** Kaip ir minėta ankstesnėje euristikoje, nereikėtų manyti, kad kiekvienas naudotojas gebės teisingai ir taip, kaip tikimasi, naudotis visomis svetainės ar įrankio funkcijomis. Naudotojai gali atlikti veiksmus per klaidą, todėl yra būtina suteikti galimybę naudotojams leisti atšaukti ar pakartoti savo atliktus veiksmus, jeigu jie pastebi, kad kažkas buvo atlikta neteisingai. Taip pat naudotojams turėtų būti suteikiama galimybė išeiti iš nepageidaujamos būsenos dar prieš užbaigiant visą operaciją.

Vertinimas:

⊖– naudotojams nėra galimybės anuliuoti ar pakartoti savo veiksmų, taip pat nėra suteikiama galimybė išeiti iš nepageidaujamos būsenos.

○– naudotojams yra suteikiama galimybė anuliuoti ar pakartoti atliktus veiksmus.

◐– naudotojams suteikiama galimybė išeiti iš nepageidaujamos būsenos prieš užbaigiant operaciją.

●– naudotojams yra leidžiama anuliuoti ar pakartoti savo atliktus veiksmus bei suteikiama galimybė išeiti iš nepageidaujamos būsenos prieš užbaigiant operaciją.

PK.4 **Nuoseklumas ir standartai.** Šis reikalavimas kyla iš sistemos reikalavimų. Pavyzdžiui, vienos operacinės sistemos naudotojui sunku pereiti prie kitų sistemų, nebent kitų sistemų naudotojo sąsaja bus panaši į „Microsoft Windows“. Tai galioja ir kuriamiems įrankiams. Įrankių kalba ir veiksmai turėtų atitikti platformos ar naršyklės standartus, kad naudotojas išvengtų painiavos. Tai reiškia, kad pateikiami įspėjimai, įvairūs patarimai turėtų būti nuoseklūs ir aiškūs. Tai svarbu, kad naudotojai galėtų suprasti rizikos grėsmes ir galėtų imtis tinkamų veiksmų.

Vertinimas:

⊖– įrankio kalba ir veiksmai atitinka tik konkrečios platformos ar naršyklės standartus (nėra pritaikyti kiekvienai platformai ar naršyklei).

●– įrankio kalba ar veiksmai yra pritaikyti skirtingoms platformoms ar naršyklėms.

PK.5 **Klaidų prevencija.** Kuriant įrankius, skirtus apsaugoti naudotoją nuo duomenų viliojimo atakų, svarbu yra užtikrinti, kad naudotojai galėtų lengvai atpažinti ir ištaisyti klaidas. Jeigu naudotojas atliko veiksmą, kuris gali kelti pavojų jo duomenų saugumui, pavyzdžiui, suvedė jautrią informaciją įtartinoje svetainėje, duomenų

viliojimo atakų apsaugos įrankis turėtų įspėti ir pateikti patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Šie patarimai turėtų būti pateikiami prieš naudotojo atliekamą veiksmą, veiksmo metu, arba po jo tam, kad naudotojas galėtų imtis tinkamų veiksmų ir apsaugotų savo duomenis.

Vertinimas:

⊖– įrankis neteikia įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą.

○– įrankis teikia įspėjimus, tačiau neteikia patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą.

◐– įrankis teikia įspėjimus ir patarimus, kaip ištaisyti klaidas arba atšaukti veiksmą, tačiau patarimai pateikiami ne visose naudotojo veiksmų stadijose.

●– įrankis teikia įspėjimus ir patarimus, kaip ištaisyti klaidas arba atšaukti veiksmą, patarimai pateikiami prieš naudotojo atliekamą veiksmą, veiksmo metu arba po jo.

PK.6 **Atpažinimas, o ne prisiminimas.** Kuriant įrankius, skirtus apsaugoti naudotoją nuo duomenų viliojimo atakų, svarbu yra užtikrinti, kad bet kuris naudotojas, nepriklausomai nuo jo įgūdžių, galėtų priimti tinkamą sprendimą norėdamas apsisaugoti nuo duomenų viliojimo atakų. Kiekvienas įrankio įspėjimas ar patarimas turėtų būti pakankamai aiškus ir lengvai suprantamas. Naudotojui neturėtų reikėti prisiminti nurodymų, kaip naudotis sąsaja, sistema arba įrankis turėtų pateikti reikiamą informaciją ir lengvai pasiekiamus aiškius nurodymus, kurie padėtų išvengti duomenų praradimo.

Vertinimas:

⊖– įrankyje nėra nei įspėjimų nei patarimų.

○– įrankyje yra įspėjimų, tačiau nėra patarimų.

◐– įrankyje yra įspėjimų ir patarimų, kaip apsisaugoti nuo duomenų viliojimo atakų, tačiau ne visi įspėjimai ar patarimai yra pakankamai aiškūs ir lengvai suprantami.

●– įrankyje yra įspėjimų ir patarimų, kaip apsisaugoti nuo duomenų viliojimo atakų, ir visi įspėjimai ar patarimai yra pakankamai aiškūs ir lengvai suprantami.

PK.7 **Lankstumas ir naudojimo efektyvumas.** Norėdami užkirsti kelią sukčiavimui paprastai naudotojai, kai aptinkamas bandymas sukčiauti, turi atlikti tam tikrą veiksmą. Kartais būna taip, kad patyrę naudotojai žino, kaip išvengti specifinių atakų, ir nenori skaityti pasikartojančių nurodymų. Tokiu atveju svarbu, kad sistemoje ar įrankyje būtų galimybė patyrusiems naudotojams praleisti pasikartojančius nurodymus ar atlikti iš anksto nustatytą veiksmą. Nenuostabu, kad lankstumas taip pat gali lemti ir klaidingą veikimą arba pažeidžiamumą, todėl taip pat būtina, kad naudotojai galėtų grįžti prie numatytųjų nustatymų, jeigu būtų padaryta klaida arba būtų noras atkurti pradinę būseną.

Vertinimas:

⊖– įrankyje nėra galimybės patyrusiems naudotojams praleisti pasikartojančius

veiksmus.

○– įrankyje yra galimybė patyrusiems naudotojams praleisti pasikartojančius veiksmus.

◐– įrankyje yra galimybė patyrusiems naudotojams praleisti pasikartojančius veiksmus, bet nėra galimybės grįžti prie numatytųjų nustatymų.

●– įrankyje yra galimybė patyrusiems naudotojams praleisti pasikartojančius veiksmus ir yra galimybės grįžti prie numatytųjų nustatymų.

PK.8 **Estetiškas ir minimalistinis dizainas.** Ši euristika teigia, kad įrankių tikslas – padėti naudotojams atpažinti ir sustabdyti atakas, o ne, pavyzdžiui, atkreipti dėmesį į komercines reklamas. Dėl šios priežasties įrankyje turi būti tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų. Glaustas ir tvarkingas dizainas padės naudotojui lengvai suprasti, į ką reikia atkreipti dėmesį ir kokių veiksmų imtis, kai pasirodo įspėjimas. Taip įrankis padės išvengti naudotojo suklaidinimo ir užtikrins greitą naudotojo atsaką į galimas grėsmes.

Vertinimas:

⊖– įrankyje yra daugiau informacijos, nesusijusios su duomenų viliojimo atakomis ir apsauga nuo jų, nei kad susijusios.

○– įrankyje yra informacija, susijusi su apsauga nuo duomenų viliojimo atakų, tačiau yra daugiau nei viena reklama ar informacija, kuri nesusijusi su apsauga nuo duomenų viliojimo atakų.

◐– įrankyje yra informacija, susijusi su apsauga nuo duomenų viliojimo atakų, tačiau yra ne daugiau nei viena reklama ar informacija, kuri nesusijusi su apsauga nuo duomenų viliojimo atakų

●– įrankyje yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

PK.9 **Pagalba ir dokumentacija.** Naudotojams gali reikėti mokytis, kaip savarankiškai naudotis įvairiais įrankiais ar sistemomis. Dėl šios priežasties yra svarbu, kad naudojami įrankiai turėtų prieinamus naudotojo vadovus, mokomąją medžiagą ir greitą bei lengvai surandamą pagalbą, kad kilus iššūkiams ar klausimams naudotojai galėtų greitai pasiekti reikiamą informaciją ir apsaugotų savo jautrius duomenis nuo duomenų viliojimo atakų.

Vertinimas:

⊖– nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.

○– įrankis turi naudotojo vadovą arba mokomąją medžiagą.

◐– įrankis turi greitai ir lengvai pasiekiamą pagalbą (virtualų asistentą).

●– įrankis turi prieinamus naudotojo vadovus, mokomąją medžiagą ir greitai bei lengvai pasiekiamą pagalbą (virtualų asistentą).

2.2. Diegimo kriterijai

DK.1 **Prieinamumas.** Naudotojai, kurie gali naudotis standartiniais įrankiais, nėra apriboti naudotis įrankiu dėl negalios ar kitų fizinių (ne kognityvinių) sąlygų.

Vertinimas:

⊖– įrankis nėra pritaikytas negalią turintiems naudotojams.

●– įrankis yra pritaikytas negalią turintiems naudotojams.

DK.2 **Minimalios išlaidos vienam naudotojui.** Bendros sukurto įrankio ar sistemos išlaidos vienam naudotojui, įskaitant bet kokius reikalingus įrenginius ar programinę įrangą, yra nedidelės. Tai reiškia, kad įrankis yra prieinamas naudotojams ar organizacijoms su ribotu biudžetu.

Vertinimas:

⊖– įrankio ar sistemos išlaidos vienam naudotojui yra didelės ir neprieinamos naudotojams bei organizacijoms su ribotu biudžetu (daugiau nei 100 eurų).

●– įrankio ar sistemos išlaidos vienam naudotojui yra nedidelės ir prieinamos naudotojams bei organizacijoms su ribotu biudžetu (mažiau nei 100 eurų).

DK.3 **Suderinamumas su naršyklėmis.** Naudotojams nereikia keisti savo turimų įrenginių ar diegti papildomos programinės įrangos, kad galėtų naudotis sukurtu įrankiu ar sistema. Tai reiškia, kad naudotojai gali tikėtis, jog įrankis veiks naudojant standartinius įrankius ir naršykles be papildomų diegimų.

Vertinimas:

⊖– įrankis nėra pritaikytas veikti skirtingose naršyklėse, todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

●– įrankis veikia naudojant standartinius įrankius ir naršykles be papildomų diegimų.

DK.4 **Brandumas.** Įrankis buvo įgyvendintas ir plačiai naudojamas realiomis sąlygomis, realiai apsaugai nuo duomenų viliojimo atakų, ne tik mokslinių tyrimų tikslais. Vertinant brandumą atsižvelgiama į tai, ar įrankis arba sistema buvo išbandyta naudotojų, ar priimta ir naudojama pramonėje, ar yra atvirojo kodo projektų ir, ar egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

Vertinimas:

⊖– įrankis nebuvo išbandytas naudotojų ir nėra literatūros, patvirtinančios įrankio efektyvumo, nenaudojamas pramonėje ir nėra atviro kodo projektų.

●– įrankis buvo išbandytas naudotojų, priimtas ir naudojamas pramonėje, yra atviro kodo projektų ir egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

DK.5 **Nepriklausomybė nuo nuosavybės teisių.** Kiekvienas naudotojas gali naudoti įrankį bet kokiam tikslui, nemokėdamas už tai autorinio atlyginimo. Atitinkamos technikos yra plačiai žinomos, viešai skelbiamos ir nėra apsaugotos patentais ar

komercinėmis paslaptimis.

Vertinimas:

⊖– įrankis yra apsaugotas patentais ar komercinėmis paslaptimis.

●– įrankiu galima naudotis nemokant už tai autorinio atlyginimo.

2.3. Techniniai sprendimai

TS.1 **Naudotojų mokymas**. Naudotojų mokymas ir švietimas – vienas iš būdų apsaugoti naudotojus nuo duomenų viliojimo atakų. Įrankiai, kuriais mokomi naudotojai, pateikia konkrečias rekomendacijas, kaip atpažinti duomenų viliojimo atakas, pavyzdžiui, moko naudotojus kaip išskaidyti URL nuorodą dalimis ir į kurias vietas reikėtų atkreipti dėmesį, kad pastebėtų potencialias duomenų viliojimo atakas, arba į kokias svetainės naudotojo sąsajos vietas reikėtų atkreipti dėmesį, kad įsitikintų, jog lankosi autentiškoje svetainėje. Taip pat dar vienas naudotojų mokymo būdas – imituoti tikras duomenų viliojimo atakas, o vėliau pateikti konstruktyvų grįžtamąjį ryšį su patarimais, kaip ateityje netapti duomenų viliojimo atakos auka. Nuolatinis ir į praktiką orientuotas švietimas labai padidina naudotojų atsparumą duomenų viliojimo atakoms.

Vertinimas:

⊖– įrankis nemoko naudotojų atpažinti duomenų viliojimo atakų.

●– įrankis moko naudotojus atpažinti duomenų viliojimo atakas.

TS.2 **Juodieji / baltieji sąrašai**. Juodieji sąrašai – duomenų bazės, kuriose saugomos žinomos URL nuorodos, naudojamos ar naudotos duomenų viliojimo atakų metu. Įrankiai, naudojantys juoduosius sąrašus, tikrina, ar nuoroda, kurią bando pasiekti naudotojas, egzistuoja juodajame sąraše. Radus nuorodą juodajame sąraše ji yra blokuojama ir naudotojui neleidžiama pasiekti šios svetainės. Baltieji sąrašai – visiška juodųjų sąrašų priešingybė. Baltųjų sąrašų duomenų bazėse yra saugomos patvirtintos ir pavojaus nekeliančios URL nuorodos, kuriose naudotojams leidžiama lankytis.

Vertinimas:

⊖– įrankis nenaudoja juodųjų arba baltųjų sąrašų.

●– įrankis naudoja juoduosius arba baltuosiu sąrašus.

TS.3 **Giliojo mokymosi metodai ir mašininis mokymasis**. Taikant mašininio mokymosi (angl. *machine learning*) metodus yra renkamos įvairios duomenų viliojimo atakų svetainių savybės, pavyzdžiui, URL nuorodos, svetainių struktūros bei „JavaScript“ ypatybės. Surinkti požymiai naudojami formuojant duomenų rinkinius. Šie duomenų rinkiniai naudojami treniruojant klasifikatorius, kurie mokomi atskirti atakoms naudojamas nuorodas nuo patikimų. Giliojo mokymosi (angl. *deep learning*) metodai yra laikomi pažangesne mašininio mokymosi kryptimi, kurioje naudojami gilieji

neuroniniai tinklai (angl. *deep neural networks*). Šis metodas, priešingai nei tradiciniai mašininio mokymosi algoritmai, gali automatiškai išgauti reikšmingus požymius tiesiai iš pirminių duomenų (URL nuorodų, tinklalapio turinio), todėl nereikalauja papildomo požymių atrinkimo. Tyrimai rodo, kad giliojo mokymosi algoritmai pasižymi geresniu tikslumu identifikuojant tiek žinomas, tiek naujai atsiradusias grėsmes, taip pat padeda sumažinti klaidingų pavojaus signalų skaičių (angl. *false positive rates*). Įrankiai, naudojantys šį techninį sprendimą, perduoda informaciją apie svetainę šiems dirbtinio intelekto modeliams ir, gavę atsakymą, kad svetainė potencialiai grėsminga, informuoja naudotoją.

Vertinimas:

⊖– įrankis nenaudoja giliojo mokymosi ar mašininio mokymosi metodų.

●– įrankis naudoja giliojo mokymosi ar mašininio mokymosi metodus.

TS.4 **Euristikomis grįstas atpažinimas**. Euristikomis grįstas atpažinimas remiasi įvairiomis savybėmis, kuriomis duomenų viliojimo atakoms skirtos svetainės skiriasi nuo autentiškų. Šio techninio sprendimo metu renkami įvairūs požymiai, kuriuos galima išgauti analizuojant svetainės šaltinio kodą (angl. *source code*), URL nuorodą, naudojamus saugumo sertifikatus bei domenų vardų sistemos įrašus (angl. *domain name system records*). Surinkus šiuos požymius jie lyginami su požymiais, kuriais pasižymi duomenų viliojimo atakoms kurtos svetainės ir radus neatitikimų naudotojas yra informuojamas apie potencialią ataką.

Vertinimas:

⊖– įrankis nenaudoja euristikomis grįsto atpažinimo.

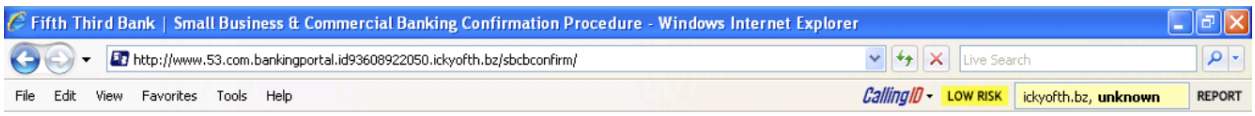
●– įrankis naudoja euristikomis grįstą atpažinimą.

2.4. Duomenų viliojimo atakų įrankių vertinimas

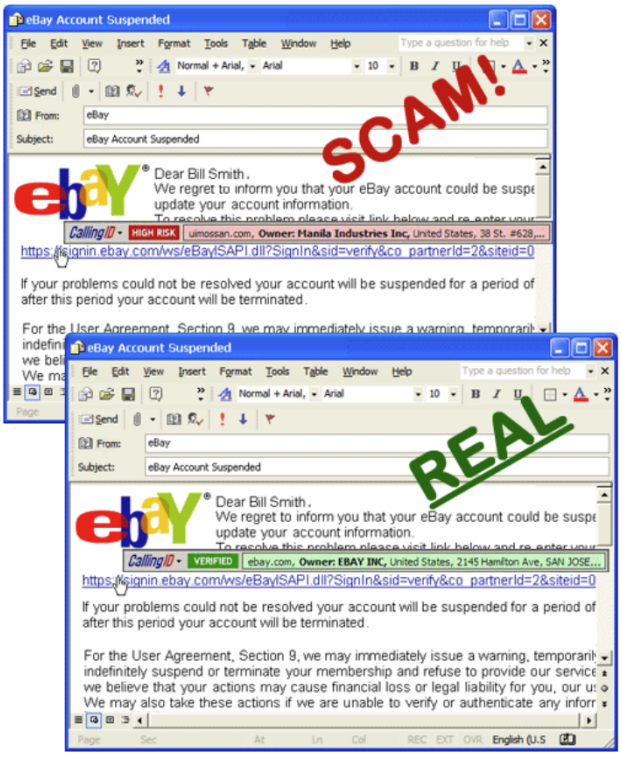
Šiame poskyryje, remiantis suformuluotais kriterijais, vertinami įrankiai, skirti apsaugoti naudotojus nuo duomenų viliojimo atakų. Įrankiai rasti [SS23; ZEC+07].

2.4.1. „CallingID“ įrankių juosta

Įrankis, kuris remdamasis 54 skirtingais patikrinimo testais, nustato svetainės teisėtumą. Šis įrankis remiasi pasyviais vizualiniais indikatoriais, kurie keičiasi priklausomai nuo svetainės rizikos. Indikatoriaus spalva keičiasi nuo žalios spalvos, kuri reiškia žinomą saugią svetainę, iki geltonos (žr. 5 paveikslą), kuri reiškia mažos rizikos svetainę, ir raudonos, kuri reiškia, kad tikėtina, jog tai sukčiavimo svetainė (žr. 6 paveikslą). Kai kurios naudojamos įrankio euristikos apima svetainės kilmės šalies analizę, registracijos trukmę, populiarumą, naudotojų ataskaitas bei juodųjų sąrašų duomenis. Įrankis veikia „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“.



5 pav. „CallingID“ įrankis praneša, apie mažos rizikos svetainę



6 pav. „CalingID“ įrankio pranešimo apie žinomą saugią svetainę ir apie sukčiavimo svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.

2. **PK.2** – ○

   Pagrindimas: įrankyje naudojamas indikatorius, kuris keičia spalvą priklausomai nuo svetainės saugumo. Naudojamos naudotojams žinomos ir lengvai atpažįstamos spalvos: žalia, geltona, raudona. Tačiau įrankyje nėra jokių nurodymų.

3. **PK.3** – N/A

   Pagrindimas: įrankis suteikia tik indikatorių, kuris informuoja apie svetainės saugumą, tačiau nesuteikia papildomo funkcionalumo, leidžiančio anuliuoti ar pakartoti savo veiksmus. Naudotojui suteikiama laisvė išeiti iš nesaugios svetainės arba pasilikti joje.

4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis yra pritaikytas ir veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti skirtingoms platformoms ar naršyklėms.

5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik indikatorių, kuris informuoja apie svetainės saugumą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.

6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi indikatorių, kuriame tiek spalva, tiek žodžiais nurodomas svetainės saugumas, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.

7. **PK.7** – N/A

   Pagrindimas: kadangi įrankis nesuteikia jokių veiksmų naudotojams (jokių veiksmų su įrankiu atlikti negalima) ir turi tik įrankių juostoje esantį indikatorių, todėl ir patyrusiems naudotojams nėra galimybės praleisti pasikartojančių veiksmų ir nėra galimybės grįžti prie numatytųjų nustatymų.

8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik indikatorius, esantis įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

9. **PK.9** – ⊖

   Pagrindimas: įrankis yra gana senas ir nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.

10. **DK.1** – ⊖

    Pagrindimas: įrankių juostoje esantis indikatorius nėra pritaikytas ir negalią turintiems naudotojams. (Negalima padidinti indikatoriaus šrifto, koreguoti spalvų, išgirsti garsu ir pan.)

11. **DK.2** – ●

    Pagrindimas: įrankis yra nemokamas ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu.

12. **DK.3** – ⊖

    Pagrindimas: kadangi įrankis yra pritaikytas ir veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, jis nėra pritaikytas veikti skirtingose naršyklėse, todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

13. **DK.4** – ●

    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, yra atviro kodo projektų ir egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

14. **DK.5** – ●

    Pagrindimas: įrankį galima įsidiegti nemokant už tai autorinio atlyginimo.

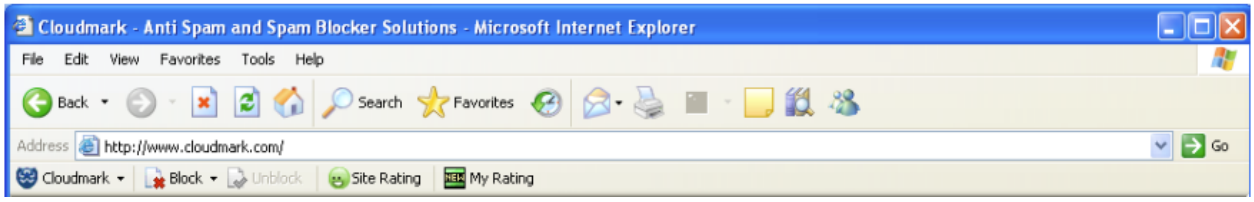
15. **TS.1** – ⊖

    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.

16. **TS.2** – ⊖
    Pagrindimas: įrankis nenaudoja juodųjų arba baltųjų sąrašų.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja 54 skirtingus euristinius testus patikrinti svetainės autentiškumą.

2.4.2. „Cloudmark Anti-Fraud“ įrankių juosta

Tai įrankis, kuris remiasi naudotojų vertinimais. Svetainėje apsilankęs naudotojas gali pranešti, ar svetainė yra patikima, ar ne. Atitinkamai, įrankių juostoje esančios piktogramos atvaizduojamos žaliai, jeigu svetainė įvertinta teisėtai, ir raudonai, jeigu nustatoma kaip apgaulinga (žr. 7 paveikslą). Jeigu nėra pakankamai informacijos svetainei vertinti, piktogramos atvaizduojamos geltona spalva. Kiekvienos svetainės įvertinimas apskaičiuojamos susumuojant visus pateiktus naudotojų vertinimus, kur kiekvieno žmogaus vertinimo svoris nustatomas pagal jo teisingai identifikuotų sukčiavimo svetainių istoriją. Svetainės, kurios nustatomos kaip apgaulingos, yra blokuojamos, naudotojai yra nukreipiami į informacinį puslapį ir jiems suteikiama galimybė panaikinti svetainės blokavimą. Kitų euristikų svetainei įvertinti nenaudojama. Šis įrankis veikia „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“.



7 pav. „Cloudmark Anti-Fraud“ įrankio pranešimo apie žinomą saugią svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○
   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ○
   Pagrindimas: įrankyje naudojamos piktogramos, kurios atvaizduojamos žaliai, jeigu svetainė yra įvertinta teisėtai, raudonai, jeigu nustatoma kaip apgaulinga, ir geltonai, jeigu nėra pakankamai informacijos svetainei vertinti. Tačiau įrankyje nėra jokių nurodymų ar įspėjimų.
3. **PK.3** – N/A
   Pagrindimas: įrankis atvaizduoja tik piktogramą, kuri informuoja apie svetainės saugumą, tačiau nesuteikia papildomo funkcionalumo, leidžiančio anuliuoti ar pakartoti savo veiksmus. Naudotojui suteikiama laisvė išeiti iš nesaugios svetainės arba pasilikti joje.

4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti skirtingoms platformoms ar naršyklėms.

5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik piktogramas, kurios informuoja apie svetainės saugumą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.

6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi piktogramą, kurios spalva nurodo svetainės saugumą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.

7. **PK.7** – N/A

   Pagrindimas: kadangi įrankis nesuteikia jokių veiksmų naudotojams (jokių veiksmų su įrankiu atlikti negalima) ir turi tik įrankių juostoje esančią piktogramą, todėl ir patyrusiems naudotojams nėra galimybės praleisti pasikartojančių veiksmų ir nėra galimybės grįžti prie numatytųjų nustatymų.

8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik piktograma, esanti įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

9. **PK.9** – ⊖

   Pagrindimas: įrankis yra gana senas ir nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.

10. **DK.1** – ⊖

    Pagrindimas: įrankių juostoje esanti piktograma nėra pritaikyta ir negalią turintiems naudotojams. (Negalima padidinti piktogramos, šalia piktogramos esančio šrifto, koreguoti spalvų, išgirsti instrukcijas garsu ir pan.)

11. **DK.2** – ●

    Pagrindimas: įrankis buvo nemokamas ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu. Šiuo metu įrankis nėra naudojamas, jo atsisiųsti nebegalima.

12. **DK.3** – ⊖

    Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, jis nėra pritaikytas veikti skirtingose naršyklėse, todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

13. **DK.4** – ●

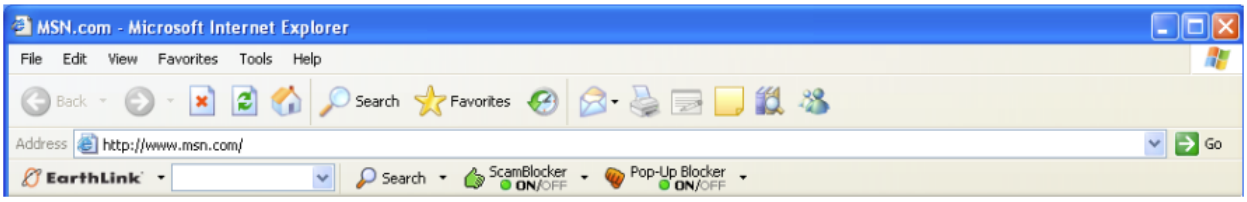
    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo

atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

14. **DK.5** – ●
    Pagrindimas: įrankį buvo galima įsidiegti nemokant už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą į kurį svetainės yra įtraukiamos remiantis naudotojų vertinimais.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ⊖
    Pagrindimas: įrankis nenaudoja euristikų atpažinti galimoms duomenų viliojimo atakoms.

2.4.3. „EarthLink“ įrankių juosta

Šis įrankis naudoja euristikų, naudotojų vertinimų ir rankinio patvirtinimo derinį. Įrankis leidžia naudotojams pranešti apie įtariamą sukčiavimo svetainę kompanijai „EarthLink“. Kai šios svetainės patikrinamos rankiniu būdu, jos įtraukiamos į juodąjį sąrašą. Įrankių juostoje vaizduojamas spalvotas nykštys, kuris keičia spalvą ir padėtį (žr. 8 paveikslą). Žalias nykštys, pakeltas aukštyn, rodo patvirtintą teisėtą svetainę, pilkas nykštys, pakeltas aukštyn, rodo, kad svetainė nėra įtartina, bet tai nėra patvirtinta. Raudonas nykštys, nuleistas žemyn, rodo, kad svetainė patvirtinta kaip apgaulinga, o geltonas nykštys, nuleistas žemyn, rodo, kad svetainė yra abejotina. Kartais apgaulingomis nustatytos svetainės yra blokuojamos ir naudotojai yra nukreipiami į informacinį puslapį, kuriame gali panaikinti svetainės blokavimą. Šis įrankis veikia su interneto naršyklėmis „Internet Explorer“ ir „Firefox“.



8 pav. „EarthLink“ įrankio pranešimo apie žinomą saugią svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○
    Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ⊖
    Pagrindimas: įrankyje naudojama nykščio piktograma, kuri atvaizduojama žaliai, jeigu svetainė yra įvertinta kaip saugi svetainė, pilkai, jeigu svetainė nėra įtartina, bet tai nėra patvirtinta, ir raudonai su nuleistu nykščiu, jeigu svetainė patvirtinta kaip apgaulinga.

Naudotojams gali būti neįprasta, kad įrankis naudoja pilką spalvą vietoje geltonos, nes dažniausiai naudotojai yra pratę matyti šviesoforo signalo spalvas, todėl šios spalvos piktograma nėra lengvai atpažįstama. Taip pat įrankyje nėra jokių nurodymų.

3. **PK.3** – ○
   Pagrindimas: įrankis suteikia naudotojams funkcionalumą panaikinti svetainės blokavimą, jeigu naudotojas nori ir mano, kad svetainė yra teisėta.
4. **PK.4** – ⊖
   Pagrindimas: kadangi įrankis veikia tik su interneto naršyklėmis „Internet Explorer“ ir „Firefox“, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti kiekvienai platformai ar naršyklei.
5. **PK.5** – ⊖
   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik piktogramas, kurios informuoja apie svetainės saugumą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○
   Pagrindimas: kadangi įrankis turi piktogramas, kurių spalva nurodo svetainės saugumą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.
7. **PK.7** – ⊖
   Pagrindimas: įrankis suteikia galimybę pranešti apie įtariamą sukčiavimo svetainę arba panaikinti svetainių blokavimą, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančius veiksmus ir, pavyzdžiui, mygtukų kombinacija atlikti šiuos įrankio suteikiamus funkcionalumus.
8. **PK.8** – ●
   Pagrindimas: įrankį sudaro tik piktogramos, esančios įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.
9. **PK.9** – ⊖
   Pagrindimas: įrankis yra gana senas ir nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.
10. **DK.1** – ⊖
    Pagrindimas: įrankių juostoje esančios piktogramos nėra pritaikytos ir negalią turintiems naudotojams. (Negalima padidinti piktogramų ir šalia esančio teksto šrifto, koreguoti spalvų, išgirsti garsu ir pan.)
11. **DK.2** – ●
    Pagrindimas: įrankis buvo nemokamas ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu. Šiuo metu įrankių juosta nėra aktyviai palaikoma ar atnaujinama.
12. **DK.3** – ⊖
    Pagrindimas: kadangi įrankis veikia tik su interneto naršyklėmis „Internet Explorer“ ir

„Firefox“, jis nėra pritaikytas veikti su kitomis naršyklėmis, todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

13. **DK.4** – ●
    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu jis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.
14. **DK.5** – ●
    Pagrindimas: įrankį buvo galima įsidiegti nemokant už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą. Įrankio naudotojai gali pranešti apie potencialiai grėsmę keliančias svetaines. Kai šios svetainės patikrinamos rankiniu būdu, jos įtraukiamos į juodąjį sąrašą.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą. Jis tikrina tokias euristikas: svetainės amžius, šalis, kurioje registruotas domenas, svetainės savininkas.

2.4.4. „Ebay“ įrankių juosta

Šis įrankis naudoja euristikų ir juodųjų sąrašų derinį. Įrankių juostoje esantys indikatoriai informuoja naudotoją apie svetainės patikimumą. Indikatoriai turi tris spalvų rėžimus: žalią, raudoną ir pilką. Įrankių juostoje esanti piktograma vaizduojama žalia spalva, jeigu naudotojas lankosi svetainėje, kurioje yra integruotos „eBay“ ar „Paypal“ suteikiamos paslaugos (žr. 9 paveikslą). Raudona spalva vaizduojama, kai svetainė yra žinoma kaip sukčiavimo svetainė, o pilka spalva, kai svetainė nesinaudoja „eBay“ ar „Paypal“ paslaugomis ir nėra žinoma kaip sukčiavimo svetainė. Svetainės, kurios yra žinomos kaip apgaulingos, yra blokuojamos, o iššokantis langas suteikia galimybę naudotojams panaikinti svetainės blokavimą. Šis įrankis taip pat suteikia galimybę naudotojams patiems pranešti apie sukčiavimo svetaines, kurios patikrinamos ir įtraukiamos į juoduosius sąrašus. „eBay“ įrankių juosta veikia „Microsoft Windows 98/ME/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“.

9 pav. „Ebay“ įrankio pranešimo apie žinomą sukčiavimo svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ⊖

   Pagrindimas: įrankyje naudojami spalvų indikatoriai, kur žalia spalva nurodoma saugi svetainė, raudona spalva – kaip žinoma sukčiavimo svetainė ir pilka spalva, kai svetainė nėra žinoma kaip sukčiavimo svetainė, bet nesinaudoja „eBay“ ar „Paypal“ paslaugomis. Naudotojams gali būti neįprasta, kad įrankis naudoja pilką spalvą vietoje geltonos, nes dažniausiai naudotojai yra pratę matyti šviesoforo signalų spalvas, todėl šios spalvos piktograma nėra lengvai atpažįstama. Taip pat įrankyje nėra jokių nurodymų.
3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą panaikinti svetainės blokavimą, jeigu naudotojas nori ir mano, kad svetainė yra teisėta.
4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti skirtingoms platformoms ar naršyklėms.
5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik piktogramas, kurios informuoja apie svetainės saugumą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi piktogramas, kurių spalva nurodo svetainės saugumą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.
7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę pranešti apie įtariamą sukčiavimo svetainę arba panaikinti svetainių blokavimą, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančius veiksmus ir, pavyzdžiui, mygtukų kombinacija atlikti šiuos įrankio suteikiamus veiksmus.
8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik piktogramos, esančios įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.
9. **PK.9** – ⊖

   Pagrindimas: įrankis yra gana senas ir nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.
10. **DK.1** – ⊖

    Pagrindimas: įrankių juostoje esantis indikatorius su piktogramomis nėra pritaikytas ir

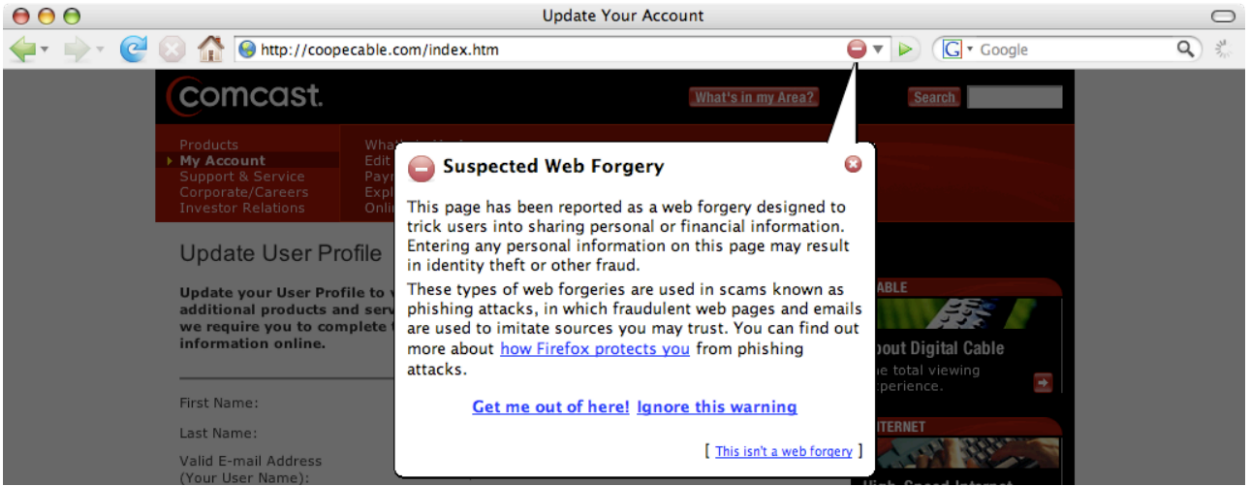
negalią turintiems naudotojams. (Negalima padidinti piktogramų ir šalia esančio teksto šrifto, koreguoti spalvų, išgirsti garsu ir pan.)

11. **DK.2** – ●
    Pagrindimas: įrankis buvo nemokamas „eBay“ klientams ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu. Šiuo metu įrankių juosta nėra aktyviai palaikoma ar atnaujinama.
12. **DK.3** – ⊖
    Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, jis nėra pritaikytas veikti skirtingose naršyklėse, todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.
13. **DK.4** – ●
    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.
14. **DK.5** – ●
    Pagrindimas: įrankį „eBay“ naudotojams / klientams buvo galima įsidiegti nemokant už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą. Įrankio naudotojai gali pranešti apie potencialiai grėsmę keliančias svetaines. Kai šios svetainės patikrinamos, jos įtraukiamos į juodąjį sąrašą.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą.

2.4.5. „Firefox 2“

Šis įrankis turi funkciją, skirtą atpažinti apgaulingoms svetainėms. Ją naudotojai gali naudoti kaip „Firefox“ plėtinį. Svetainių URL adresai tikrinami juodajame sąraše, kurį „Firefox“ periodiškai atnaujina. Jeigu yra įtariama, kad svetainė, kurioje lankosi naudotojas gali būti apgaulinga, parodomas iššokantis langas, kuris suteikia naudotojams galimybę palikti svetainę arba ignoruoti pranešimą (žr. 10 paveikslą). Taip pat įrankis suteikia galimybę siųsti kiekvieną URL adresą „Google“, kad būtų nustatoma, ar svetainėje gali pasitaikyti duomenų viliojimo atakų. Kaip rašoma „Google“, įrankių juosta tikrindama derina pažangius algoritmus su klaidinančių puslapių ataskaitomis iš įvairių šaltinių. Straipsnio autoriai mano, kad naudojami tiek juodieji sąrašai, tiek euristikos. Šis įrankis veikia „Microsoft Windows“, „Apple Mac OS X“ ir „Linux“ operacinėse

sistemose su interneto naršykle „Firefox“ arba su interneto naršykle „Internet Explorer“ kartu su „Windows XP/2000 SP3+“.



10 pav. „Firefox 2“ įrankio pranešimo apie įtariamą sukčiavimo svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ⊖

   Pagrindimas: naudotojui bandant atidaryti įtartiną ar žinomą sukčiavimo svetainę, įrankis atvaizduoja iššokantį įspėjamąjį langą su raudonos spalvos piktograma. Tačiau naudotojui bandant atidaryti saugią, žinomą svetainę, įrankis neatvaizduoja nieko, nes neturi jokio specialaus pranešimo, ar žymėjimo. Tai gali klaidinti naudotoją, nes jis nežinos, ar įrankis veikia, ar neveikia, iki kol nesusidurs su įtartina svetaine.
3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą ignoruoti pranešimą ir tęsti lankymąsi svetainėje, jeigu naudotojas nori ir mano, kad svetainė yra teisėta.
4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows“, „Apple Mac OS X“ ir „Linux“ operacinėse sistemose su interneto naršykle „Internet Explorer“ kartu su „Windows XP/2000 SP3+“ arba „Firefox“ naršyklėje daugumoje platformų, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti skirtingoms platformoms ar naršyklėms (pavyzdžiui, nėra pritaikyti: „Google Chrome“, „Safari“, „Opera“ naršyklėms).
5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik iššokantį įspėjamąjį langą, kuris informuoja naudotoją, kai jis lankosi nesaugioje svetainėje. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ◐

Pagrindimas: įrankyje yra ir įspėjimų (kai naudotojas apsilanko apgaulingoje svetainėje rodomas iššokantis įspėjamasis langas) ir patarimų, kaip apsisaugoti nuo duomenų viliojimo atakų (naudotojas gali perskaityti lange pateikiamą informaciją ir, paspaudęs ant nuorodos, plačiau pasiskaityti apie apsaugos būdus), tačiau ne visi įspėjimai ar patarimai yra gana aiškūs ir lengvai suprantami, nes naudotojas pats turi paspausti ir plačiau pasiskaityti, nėra iš karto pateikiamos svarbiausios informacijos.

7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę palikti svetainę arba ignoruoti pranešimą, taip pat suteikia galimybę siųsti kiekvieną URL adresą „Google“, kad būtų nustatoma, ar svetainėje gali pasitaikyti duomenų viliojimo atakų, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančius veiksmus ir, pavyzdžiui, mygtuku kombinacija atlikti šiuos įrankio suteikiamus veiksmus.

8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik piktograma, esanti įrankių juostoje, ir iššokantis pranešimų langas, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

9. **PK.9** – ⊖

   Pagrindimas: įrankis yra gana senas ir nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.

10. **DK.1** – ⊖

    Pagrindimas: kai naudotojas lankosi svetainėje, kuri gali būti apgaulinga, iššoka langas su pranešimu, kuris nėra pritaikytas negalią turintiems naudotojams. Tai reiškia, kad nėra galimybės pasididinti šrifto, pasikeisti spalvų, pasirinkti išgirsti rodomą informaciją garsu ir panašiai.

11. **DK.2** – ●

    Pagrindimas: įrankis buvo integruotas į naršyklę „Firefox“, todėl naudotojams, kurie naudojo šią naršyklę, įrankis buvo lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu.

12. **DK.3** – ⊖

    Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows“, „Apple Mac OS X“ ir „Linux“ operacinėse sistemose su interneto naršykle „Internet Explorer“ kartu su „Windows XP/2000 SP3+“ arba „Firefox“ naršyklėje daugumoje platformų, jis nėra pritaikytas veikti skirtingose naršyklėse (pavyzdžiui: „Google Chrome“, „Safari“, „Opera“), todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

13. **DK.4** – ●

    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

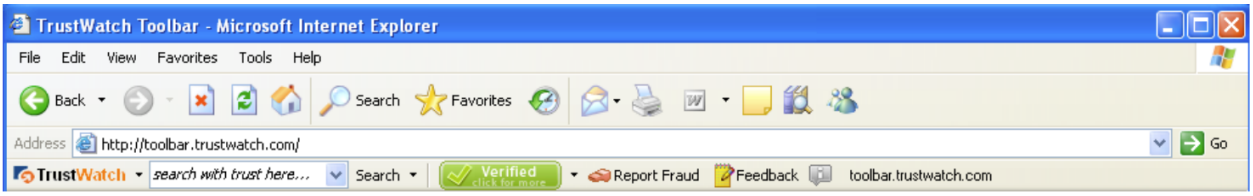
14. **DK.5** – ●

Pagrindimas: įrankis buvo visiškai nemokamas ir naudotojai galėjo nemokamai atsisiųsti ir įsidiegti „Firefox 2“ naršyklę su šiuo įrankiu.

15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą. URL nuorodos yra tikrinamos juodajame sąraše, kuris yra periodiškai atnaujinamas.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą.

2.4.6. „GeoTrust TrustWatch“

Šis įrankis taip pat naudoja trijų spalvų piktogramas įrankių juostoje. Žalios spalvos piktograma nurodo, kad svetainė yra patikima, geltona spalva, kad svetainė yra nepatikrinta, ir raudona, kad patikrinta ir apgaulinga svetainė (žr. 11 paveikslą). „GeoTrust“ bendradarbiauja su keliomis trečiųjų šalių reputacijos ir sertifikatų tarnybomis, kad patikrintų svetainės patikimumą. Interneto svetainėje „GeoTrust“ nėra pateikiama jokia informacija apie tai, kaip įrankis nustato, ar svetainė, kurioje lankosi naudotojas, yra patikima ar apgaulinga, tačiau įtariama, kad bendrovė sudaro juodąjį sąrašą, į kurį įtraukia tas svetaines, apie kurias naudotojai praneša, naudodami įrankyje esantį mygtuką. Įrankis naudotojams suteikia galimybę įrašyti pasirinktą vaizdą ar teksto fragmentą, kuris nuolat rodomas, kad naudotojas žinotų, jog įrankių juosta nėra suklastota. „TrustWatch“ įrankis veikia „Microsoft Windows 98/NT/2000/XP“ kartu su interneto naršykle „Internet Explorer“.



11 pav. „GeoTrust TrustWatch“ įrankio pranešimo apie žinomą saugią svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○
   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ○
   Pagrindimas: įrankyje naudojamas indikatorius, kuris keičia spalvą, priklausomai nuo svetainės saugumo. Naudojamos naudotojams žinomos ir lengvai atpažįstamos spalvos: žalia, geltona, raudona. Tačiau įrankyje nėra jokių nurodymų.
3. **PK.3** – N/A
   Pagrindimas: įrankis suteikia tik indikatorių, kuris informuoja apie svetainės saugu-

mą, tačiau nesuteikia papildomo funkcionalumo, leidžiančio anuliuoti ar pakartoti savo veiksmus. Naudotojui suteikiama laisvė išeiti iš nesaugios svetainės arba pasilikti joje.

4. **PK.4** – ⊖
   Pagrindimas: kadangi įrankis veikia „Microsoft Windows 98/NT/2000/XP“ kartu su interneto naršykle „Internet Explorer“, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti kiekvienai platformai ar naršyklei.
5. **PK.5** – ⊖
   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik piktogramas, kurios informuoja apie svetainės saugumą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○
   Pagrindimas: kadangi įrankis turi piktogramas, kurių spalva nurodo svetainės saugumą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.
7. **PK.7** – ⊖
   Pagrindimas: įrankis suteikia galimybę naudotojui pranešti apie įtariamą sukčiavimo svetainę, taip pat suteikia galimybę įrašyti pasirinktą vaizdą ar teksto fragmentą, kuris būtų nuolat rodomas, kad naudotojas žinotų, jog įrankių juosta nėra suklastota, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančius veiksmus ir, pavyzdžiui, mygtukų kombinacija atlikti šiuos įrankio suteikiamus funkcionalumus.
8. **PK.8** – ●
   Pagrindimas: įrankį sudaro tik piktogramos, esančios įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.
9. **PK.9** – ⊖
   Pagrindimas: įrankis yra gana senas ir nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.
10. **DK.1** – ⊖
    Pagrindimas: įrankių juostoje esančios piktogramos nėra pritaikytos ir negalią turintiems naudotojams. (Negalima padidinti piktogramų ir šalia esančio teksto šrifto, koreguoti spalvų, išgirsti instrukcijų garsu ir pan.)
11. **DK.2** – ●
    Pagrindimas: įrankis buvo nemokamas ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu. Šiuo metu įrankių juosta nėra aktyviai palaikoma ar atnaujinama.
12. **DK.3** – ⊖
    Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows 98/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“, jis nėra pritaikytas veikti skirtingose naršyklėse, todėl norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

13. **DK.4** – ●

    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

14. **DK.5** – ●

    Pagrindimas: įrankį buvo galima įsidiegti nemokant už tai autorinio atlyginimo.

15. **TS.1** – ⊖

    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.

16. **TS.2** – ●

    Pagrindimas: įrankis naudoja juodąjį sąrašą, į kurį svetainės gali būti įtrauktos remiantis naudotojų pranešimais.

17. **TS.3** – ⊖

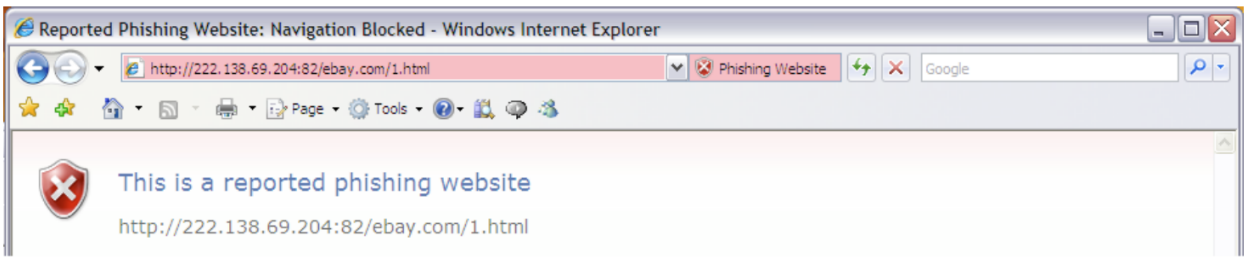
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.

18. **TS.4** – ⊖

    Pagrindimas: įrankis nenaudoja euristikų atpažinti galimoms duomenų viliojimo atakoms.

2.4.7. „Microsoft Internet Explorer 7“

„Microsoft“ sukčiavimo filtras – tai „Microsoft Internet Explorer 7“ interneto naršyklėje integruotas filtras, kuris remiasi „Microsoft“ esančiu juoduoju sąrašu. Šis įrankis taip pat naudoja tam tikrą euristiką, kai susiduria su svetaine, kuri dar nėra įtraukta į juodąjį sąrašą. Kai susiduriama su įtariama sukčiavimo svetaine, naudotojas yra nukreipiamas į integruotą įspėjamąjį pranešimą su klausimu, ar naudotojas tikrai nori lankytis svetainėje, ar nori uždaryti langą (žr. 12 paveikslą). Įrankis naudotojui taip pat suteikia galimybę pranešti apie įtariamas sukčiavimo svetaines arba pranešti, kad svetainė yra neteisingai įtraukta į juodąjį sąrašą.



12 pav. „Microsoft Internet Explorer 7“ įrankio pranešimo apie įtartiną sukčiavimo svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

    Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.

2. **PK.2** – ⊖

    Pagrindimas: naudotojui bandant atidaryti įtartiną ar žinomą sukčiavimo svetainę, įrankis nukreipia naudotoją į integruotą įspėjamąjį pranešimą su klausimu, ar naudotojas tikrai

nori lankytis svetainėje. Taip pat įrankių juostoje yra matoma raudonos spalvos įspėjanti skydo piktograma. Tačiau naudotojui bandant atidaryti saugią, žinomą svetainę, įrankis neatvaizduoja nieko, nes neturi jokio specialaus pranešimo ar žymėjimo. Tai gali klaidinti naudotoją, nes jis nežinos, ar įrankis veikia, ar neveikia, iki kol nesusidurs su įtartina svetaine.

3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą uždaryti integruotą įspėjamąjį pranešimą ir tęsti lankymąsi svetainėje, jeigu naudotojas nori ir mano, kad svetainė yra teisėta. Taip pat naudotojams įrankis suteikia galimybę pranešti apie įtariamas sukčiavimo svetaines, arba pranešti, kad svetainė neteisingai įtraukta į juodąjį sąrašą. Tačiau naudotojams nėra suteikiama galimybė pakartoti savo veiksmų. (Klaidingai pranešus apie neteisingai įtrauktą svetainę į juodąjį sąrašą nėra galimybės anuliuoti pranešimo.)

4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis yra integruotas konkrečioje naršyklėje, jis nėra pritaikytas skirtingoms platformoms ar naršyklėms.

5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik piktogramas, kurios informuoja apie svetainės saugumą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.

6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi raudono skydo piktogramą ir integruotą įspėjamąjį pranešimą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.

7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę naudotojui uždaryti įspėjamąjį langą, pranešti apie įtariamas sukčiavimo svetaines arba pranešti, kad svetainė neteisingai įtraukta į juodąjį sąrašą, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančius veiksmus ir, pavyzdžiui, mygtukų kombinacija atlikti šiuos įrankio suteikiamus funkcionalumus.

8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik skydo piktograma, esanti įrankių juostoje, ir integruotas įspėjamasis langas su klausimu, ar naudotojas tikrai nori tęsti lankymąsi svetainėje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

9. **PK.9** – ⊖

   Pagrindimas: įrankis yra nebenaudojamas, todėl nėra prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.

10. **DK.1** – ⊖

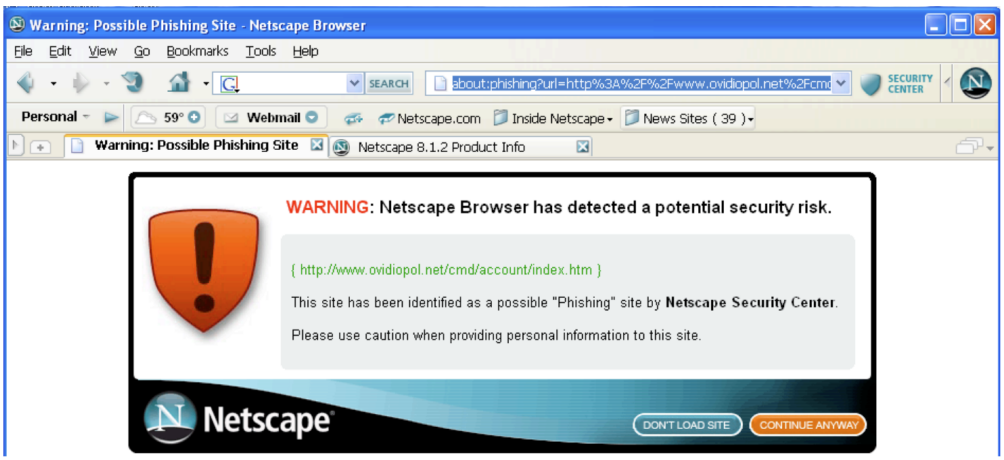
    Pagrindimas: įrankių juostoje esanti skydo piktograma ir įspėjamasis pranešimas nėra

pritaikytas negalią turintiems naudotojams. (Negalima padidinti piktogramos ir šalia esančio teksto šrifto, koreguoti spalvų, išgirsti instrukcijas garsu ir pan.)

11. **DK.2** – ●
    Pagrindimas: įrankis buvo nemokamas ir integruotas į „Microsoft Internet Explorer“ naršyklę, todėl jis buvo lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu. Šiuo metu įrankis nėra palaikomas ir jo atsisiųsti nebegalima.
12. **DK.3** – ⊖
    Pagrindimas: kadangi įrankis buvo integruotas tik į interneto naršyklę „Microsoft Internet Explorer“, jis nėra pritaikytas veikti skirtingose naršyklėse. Norint naudotis įrankiu, naudotojams reikia papildomų diegimų.
13. **DK.4** – ●
    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.
14. **DK.5** – ●
    Pagrindimas: įrankį buvo galima įsidiegti nemokant už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą. URL nuorodos yra tikrinamos juodajame sąraše. Įrankis taip pat suteikia naudotojams funkcionalumą pranešti apie potencialias duomenų viliojimo svetaines arba apie svetaines, kurios į juodąjį sąrašą buvo įtrauktos nepagrįstai.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą.

2.4.8. „Netscape Browser 8.1“

Įrankis „Netscape Navigator 8.1“ yra į interneto naršyklę integruotas apgaulės filtras. Šis įrankis remiasi tik juoduoju sąrašu, kuris yra dažnai tvarkomas ir atnaujinamas. Kai naudotojas susiduria su įtariama sukčiavimo svetaine, yra nukreipiamas į integruotą įspėjamąjį puslapį (žr. 13 paveikslą). Tuomet naudotojui yra parodomas pradinis URL adresas ir yra klausiama, ar norėtų tęsti savo veiksmus toliau. Naršyklė „Netscape Browser“ veikia „Microsoft Windows“, „Linux“ ir „Mac OS X“ operacinėse sistemose.



13 pav. „Netscape Browser 8.1“ įrankio pranešimo apie įtariamą sukčiavimo svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ⊖

   Pagrindimas: naudotojui bandant atidaryti įtartiną ar žinomą sukčiavimo svetainę, įrankis nukreipia naudotoją į integruotą įspėjamąjį pranešimą su klausimu, ar naudotojas tikrai nori lankytis svetainėje. Tačiau naudotojui bandant atidaryti saugią, žinomą svetainę, įrankis neatvaizduoja nieko, nes neturi jokio specialaus pranešimo ar žymėjimo. Tai gali klaidinti naudotoją, nes jis nežinos, ar įrankis veikia, ar neveikia, iki kol nesusidurs su įtartina svetaine.
3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą uždaryti integruotą įspėjamąjį pranešimą ir tęsti lankymąsi svetainėje, jeigu naudotojas nori ir mano, kad svetainė yra teisėta. Tačiau naudotojams nėra suteikiama galimybė pakartoti savo veiksmų. (Uždarius langą ir nespėjus perskaityti pranešimo, nėra iš naujo parodomas langas su įspėjamuoju pranešimu.)
4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis yra integruotas konkrečioje naršyklėje „Netscape Browser“, jis nėra pritaikytas skirtingoms platformoms ar naršyklėms.
5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Įrankis turi tik integruotą pranešimą, kuris informuoja naudotoją, kai šis lankosi sukčiavimo svetainėje. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi integruotą įspėjamąjį pranešimą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.

7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę naudotojui uždaryti įspėjamąjį langą, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančių veiksmų ir, pavyzdžiui, mygtukų kombinacija atlikti šį įrankio suteikiamą funkcionalumą.
8. **PK.8** – ◐

   Pagrindimas: naudotojui susidūrus su sukčiavimo svetaine įrankis nukreipia jį į integruotą įspėjamąjį puslapį, kur yra parodomas URL adresas ir klausiama, ar naudotojas norėtų tęsti savo veiksmus toliau. Įspėjamajame lange didelę dalį vietos užima raudonas skydas ir įrankio logotipas, todėl naudotojo dėmesys pirmiausiai nukreipiamas į šias detales. Galima teigti, kad įrankyje yra informacija, susijusi su apsauga nuo duomenų viliojimo atakų, tačiau yra ir informacijos (logotipų), kurie yra nesusiję su apsauga.
9. **PK.9** – ⊖

   Pagrindimas: įrankis nėra palaikomas, todėl nėra oficialiai prieinamų naudotojo vadovų, mokomosios medžiagos bei greitai ir lengvai surandamos pagalbos.
10. **DK.1** – ⊖

    Pagrindimas: įrankis, naudotojui patekus į sukčiavimo svetainę, nukreipia jį į įspėjamąjį puslapį, kuris nėra pritaikytas negalią turintiems naudotojams. (Negalima padidinti piktogramos ir šalia esančio teksto šrifto, koreguoti spalvų, išgirsti instrukcijas garsu ir pan.)
11. **DK.2** – ●

    Pagrindimas: įrankis nemokamas ir integruotas į „Netscape Browser“ naršyklę, todėl įrankis buvo lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu. Šiuo metu įrankis nėra palaikomas.
12. **DK.3** – ⊖

    Pagrindimas: kadangi įrankis integruotas tik į interneto naršyklę „Netscape Browser“, jis nėra pritaikytas veikti skirtingose naršyklėse. Norint naudotis įrankiu, naudotojams reikia papildomų diegimų.
13. **DK.4** – ●

    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.
14. **DK.5** – ●

    Pagrindimas: įrankį buvo galima įsidiegti nemokant už tai autorinio atlyginimo.
15. **TS.1** – ⊖

    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●

    Pagrindimas: įrankis naudoja juodąjį sąrašą, kuris yra dažnai tvarkomas ir atnaujinamas.
17. **TS.3** – ⊖

    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.

18. **TS.4** – ⊖

    Pagrindimas: įrankis nenaudoja euristikų atpažinti galimoms duomenų viliojimo atakoms.

2.4.9. „SpoofGuard“

„SpoofGuard“ yra įrankių juosta, kuri sukurta Stanfordo universitete. Skirtingai nei kiti įrankiai, „SpoofGuard“ nenaudoja juodųjų ar baltųjų sąrašų, o vietoje to naudoja šiuos euristinius metodus sukčiavimo puslapiams atpažinti:

1. Įrankių juosta patikrina svetainės, kurioje lankosi naudotojas, domeno pavadinimą ir palygina jį su neseniai naudotojo aplankytomis svetainėmis, kad būtų galima aptikti apgaulingas svetaines, turinčias panašiai atrodantį domeno pavadinimą.
2. Tuomet yra analizuojamas URL adresas, kad būtų aptinkami nestandartiniai požymiai.
3. Kai išanalizuojamas URL adresas, analizuojamas puslapio turinys atkreipiant dėmesį į slaptažodžių laukus ir įterptas nuorodas.
4. Galiausiai, įrankis nagrinėja paveikslėlius, atlikdamas jų kodavimą maišos funkcijomis (angl. *hashing*), kad nustatytų, ar kitose naudotojo aplankytose svetainėse buvo rasta identiškų paveikslėlių. Jeigu skirtingose svetainėse aptinkami du vienodi paveikslėliai, yra tikimybė, kad apgaulinga svetainė nukopijavo paveikslėlius iš teisėtos svetainės.

„SpoofGuard“ įrankis apskaičiuoja kiekvieno tinklapio įvertinimą kaip svertinę kiekvienos euristikos rezultatų sumą. Patys naudotojai gali keisti kiekvienos euristikos rinkinio rezultato svorį. Jeigu gautas rezultatas viršija tam tikrą ribą, įrankių juostoje yra rodoma raudonos spalvos piktograma, kuri įspėja naudotojus, kad svetainė yra teigiamai identifikuota kaip sukčiavimo svetainė. Jeigu kai kurie euristiniai požymiai suveikia, bet gautas rezultatas yra nepakankamas, kad viršytų ribą, piktograma tampa geltona ir nurodo, kad svetainės nustatyti negalima, o jeigu nesuveikia nė vienas iš euristinių požymių, piktograma nusispalvina žalia spalva ir rodo, kad svetainė yra saugi (žr. 14 paveikslą). Šis įrankis veikia „Microsoft Windows 98/NT/2000XP“ su interneto naršykle „Internet Explorer“.

14 pav. „SpoofGuard“ įrankio pranešimo apie žinomą saugią svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ○

   Pagrindimas: įrankyje naudojama piktograma, kuri nuspalvinama žaliai, jeigu svetainė, kurioje lankosi naudotojas, yra saugi, raudonai, jeigu svetainė identifikuota kaip suk-

čiavimo svetainė, ir geltonai, jeigu nepavyksta nustatyti svetainės teisėtumo. Įrankyje naudojamos naudotojams gerai pažįstamos ir lengvai išmokstamos spalvos, tačiau nėra jokių nurodymų ar įspėjimų, tik indikatorius.

3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą, kuris leidžia keisti kiekvienos euristikos rinkinio rezultatų svorį kiek nori kartų, tai reiškia, kad įrankis suteikia galimybę pakartoti savo veiksmus iš naujo ar juos pakeisti.

4. **PK.4** – ⊖

   Pagrindimas: kadangi įrankis veikia „Microsoft Windows 98/NT/2000/XP“ kartu su interneto naršykle „Internet Explorer“, negalime teigti, kad įrankio kalba ir veiksmai yra pritaikyti kiekvienai platformai ar naršyklei.

5. **PK.5** – ⊖

   Pagrindimas: įrankis neteikia jokių įspėjimų ir patarimų kaip ištaisyti klaidas arba atšaukti veiksmą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.

6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi integruotą įspėjamąjį pranešimą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.

7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę naudotojams keisti kiekvienos euristikos rinkinio rezultato svorį, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančių veiksmų ir, pavyzdžiui, mygtukų kombinacija atlikti šį įrankio suteikiamą funkcionalumą.

8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik piktogramos, esančios įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

9. **PK.9** – ○

   Pagrindimas: nors ir įrankis nėra naudojamas, oficialiame Stanfordo universiteto puslapyje vis dar galima rasti diegimo ir naudojimo instrukcijas bei informaciją apie įrankio funkcionalumą. (https://crypto.stanford.edu/SpoofGuard/). Tačiau įrankis neturi lengvai pasiekiamos pagalbos (virtualaus asistento.)

10. **DK.1** – ⊖

    Pagrindimas: įrankių juostoje esanti piktograma nėra pritaikyta ir negalią turintiems naudotojams. (Negalima padidinti piktogramos, koreguoti spalvų, išgirsti įspėjimų garsu ir panašiai.)

11. **DK.2** – ●

    Pagrindimas: įrankis nemokamas ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu.

12. **DK.3** – ⊖

    Pagrindimas: kadangi įrankis veikia tik „Microsoft Windows 98/NT/2000XP“ su interne-

to naršykle „Internet Explorer“, jis nėra pritaikytas veikti skirtingose naršyklėse. Norint naudotis įrankiu, naudotojams reikia papildomų diegimų.

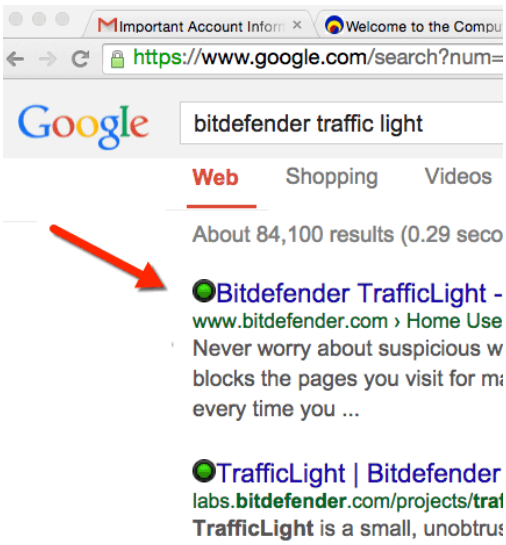
13. **DK.4** – ●
    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu įrankis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.
14. **DK.5** – ●
    Pagrindimas: įrankį buvo galima įsidiegti nemokant už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ⊖
    Pagrindimas: įrankis nenaudoja juodųjų ar baltųjų sąrašų.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą. Įrankis analizuoja, kokiose svetainėse anksčiau lankėsi naudotojas, analizuoja URL nuorodą, puslapio turinį bei paveikslėlius naudodamas euristikas.

2.4.10. „Bitdefender Traffic Light“

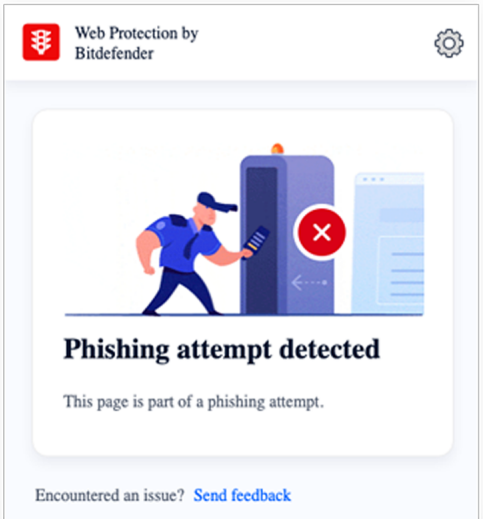
Šis įrankis yra nemokamas interneto naršyklės plėtinys, sukurtas dar 2001 metais kibernetinio saugumo bendrovės „Bitdefender“. Pirmą kartą plėtinys buvo išleistas 2012 metais ir nuo to laiko buvo nuolat naujinamas įtraukiant papildomas saugumo ir privatumo funkcijas. Įrankis nustato tinklapio saugumą, naudodamas svetainės turinio ir svetainės struktūros analizės metodų derinį. Turinio analizė apima tinklapio teksto ir paveikslų analizę, siekiant nustatyti galimas grėsmes. Kita vertus, kodo struktūra pagrįsta analizė apima pagrindinį tinklapio kodą ir struktūrą siekiant aptikti įtartina elgesį, pavyzdžiui: paslėptas nuorodas ar scenarijus, įtartinus peradresavimus ar užšifruotą kodą. Įrankio privalumai:

1. „Bitdefender“ analizuoja svetainės turinį ir nustato galimas grėsmes.
2. Įrankis analizuoja paieškos rezultatus ir raudonos spalvos piktograma pažymi svetaines, kuriose yra kenkėjiško turinio.
3. „Bitdefender“ įrankis saugo naudotojo privatumą, neleisdamas rinkti buvimo vietos duomenų ir naudotojo istorijos.
4. Įrankis veikia populiariausiose naršyklėse, tokiose kaip: „Chrome“, „Firefox“, „Microsoft Edge“ ir „Safari“.
5. Įrankis naudoja labai mažai kompiuterio atminties.
6. Norint naudoti šį įrankį, naudotojui tereikia naršyklėje įdiegti plėtinį.
7. Įrankis naudoja keturių spalvų indikatorius, norėdamas nustatyti svetainės saugumą (žr. 15 paveikslą). Žalia spalva žymimos patikimos svetainės, raudona spalva žymimos nesaugios svetainės, pilka spalva žymimos svetainės, kurios nėra įtrauktos į „Traffic Light“

duomenų bazę, arba nėra pakankamai informacijos saugumui nustatyti ir geltona spalva nurodo, kad svetainė gali turėti tam tikrų rizikų, tačiau nėra aiškiai identifikuota kaip pavojinga.



15 pav. „Bitdefender Traffic Light“ įrankio pranešimo apie žinomas saugias svetaines pavyzdys



16 pav. „Bitdefender Traffic Light“ įrankio pranešimo apie nesaugią svetainę pavyzdys

Vertinimas:

1. **PK.1** – ◐
   Pagrindimas: įrankis tikrina svetainės autentiškumą dviejose stadijose, pirmiausiai analizuoja paieškos rezultatus ir raudonos / žalios spalvos piktograma pažymi svetaines, kurios atitinkamai yra nesaugios / saugios. Taip pat įrankis tikrina svetainės autentiškumą, kai naudotojas jau yra užėjęs į svetainę.

2. **PK.2** – ●

   Pagrindimas: įrankyje naudojamos keturių spalvų piktogramos: žalia, raudona, geltona ir pilka. Naudotojams šios spalvos yra lengvai atpažįstamos ir išmokstamos. Nors ir pilka spalva nėra įprasta naudotojui, tačiau šiuo atveju ji tik nurodo, kad svetainė nėra įtraukta į duomenų bazę arba nėra pakankamai informacijos saugumui nustatyti, tačiau kitos spalvos, kaip jau įprasta, nurodo svetainių saugumą. Taip pat svetainėje naudojami ir įspėjimai (žr. 16 paveikslą). Jeigu naudotojas apsilanko nesaugioje svetainėje, ji yra užblokuojama ir naudotojui parodomas įspėjimo pranešimas.
3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą grįžti į puslapį ir tęsti naršymą, jeigu naudotojas nori ir mano, kad svetainė yra teisėta. Tačiau naudotojams nėra suteikiama galimybė pakartoti savo veiksmų. Uždarius langą ir nespėjus perskaityti pranešimo, nėra iš naujo parodomas langas su įspėjamuoju pranešimu, nebent naudotojas rankiniu būdu perkraus puslapį, tuomet pranešimas bus parodomas iš naujo, kadangi įrankis veikia realiu laiku.
4. **PK.4** – ●

   Pagrindimas: kadangi įrankis veikia populiariausiose naršyklėse, tokiose kaip „Chrome“, „Firefox“, „Microsoft Edge“ ir „Safari“, galima sakyti, kad jis yra pritaikytas skirtingoms platformoms ar naršyklėms.
5. **PK.5** – ○

   Pagrindimas: įrankis teikia įspėjimus, tačiau neteikia patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi spalvų indikatorius, taip pat blokuoja neteisėtas svetaines ir išmeta įspėjamąjį pranešimą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.
7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę naudotojams grįžti į puslapį ir tęsti naršymą po svetainės blokavimo, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančių veiksmų ir, pavyzdžiui, mygtukų kombinacija atlikti šį įrankio suteikiamą funkcionalumą.
8. **PK.8** – ●

   Pagrindimas: įrankį sudaro spalvotos piktogramos ir įspėjamieji pranešimai, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.
9. **PK.9** – ○

   Pagrindimas: įrankio oficialioje svetainėje (`https://www.bitdefender.com/consumer/support/user-guides/`) galima rasti įrankio vadovą ir mokomąją medžiagą, tačiau nėra virtualaus asistento.
10. **DK.1** – ⊖

Pagrindimas: įrankyje esančios piktogramos ir įspėjamieji pranešimai nėra pritaikyti negalią turintiems naudotojams. (Negalima padidinti piktogramos, koreguoti spalvų, išgirsti įspėjimų garsu ir panašiai.)

11. **DK.2** – ●
    Pagrindimas: įrankis yra nemokamas, tad įrankio išlaidos vienam naudotojui yra nedidelės ir prieinamos visiems naudotojams ar organizacijoms su ribotu biudžetu. Įrankyje taip pat yra ir papildomų funkcionalumų, už kuriuos jau reikia papildomai susimokėti (VPN paslaugos, 24/7 techninė pagalba, galimybė tėvams stebėti vaikų veiklą internete ir panašiai), tačiau bazinis funkcionalumas yra suteikiamas nemokamai.
12. **DK.3** – ●
    Pagrindimas: kadangi įrankis veikia populiariausiose naršyklėse, tokiose kaip „Chrome“, „Firefox“, „Microsoft Edge“ ir „Safari“, galima sakyti, kad jis veikia naudojant standartinius įrankius ar naršykles be papildomų diegimų.
13. **DK.4** – ●
    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu jis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.
14. **DK.5** – ●
    Pagrindimas: įrankis yra nemokamas interneto naršyklės plėtinys ir kiekvienas naudotojas gali šiuo įrankiu naudotis nemokėdamas už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ⊖
    Pagrindimas: įrankis nenaudoja juodųjų arba baltųjų sąrašų.
17. **TS.3** – ⊖
    Pagrindimas: įrankis nenaudoja dirbtinio intelekto modelių.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą. Įrankis analizuoja svetainės turinį ir struktūrą naudodamas euristikas, kad identifikuotų potencialias duomenų viliojimo atakas.

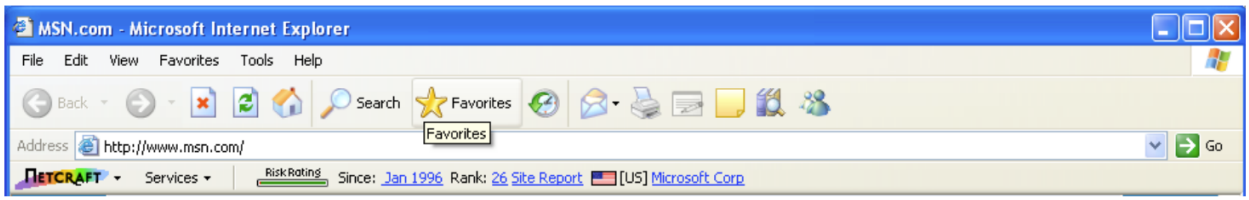
2.4.11. „Netcraft“

„Netcraft“ – tai naršyklės plėtinys, analizuojantis svetaines turinio analizės metodo pagrindu. „Netcraft“ nagrinėja tinklapių turinį ir analizuoja serverio atsakymų antraštės (angl. *response header*), kad nustatytų informaciją apie žiniatinklio serverį, operacinę sistemą ar kitas technines detales. Grėsmių atpažinimui įrankis taip pat naudoja mašininio mokymosi algoritmus, kurie padeda analizuoti URL adresų, domenų ir žiniatinklio turinio struktūrą. Įrankis taip pat informuoja, kiek laiko veikia serveriai, kokia jų veikimo trukmė bei kada jie paskutinį kartą buvo perkrauti ir panašiai. Įrankio privalumai:

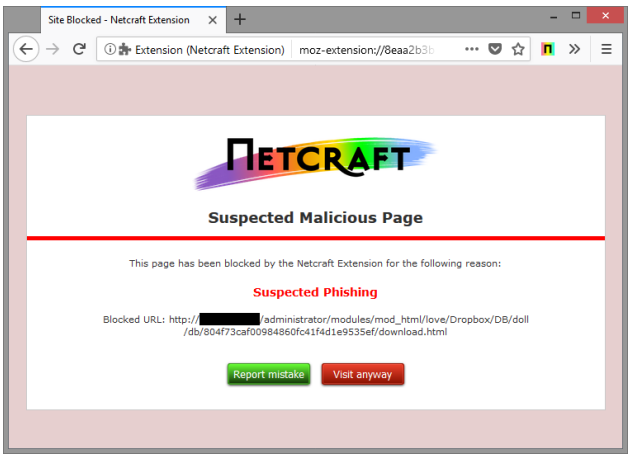
1. „Netcraft“ patikrina svetainę, kurią naudotojas nori aplankyti, sukčiavimo svetainių

duomenų bazėje ir užblokuoja, jei svetainė randama sukčiavimo svetainių duomenų bazėje.

2. Įrankis sukuria naudotojo lankomos svetainės ataskaitą, kurioje pateikiama SSL sertifikato, paslaugų tiekėjo ir domeno registracijos informacija.
3. „Netcraft“ tikrina tinklapio kodo struktūrą ir nustato sukčiavimo atvejus.
4. Įrankis analizuoja IP adresus ir DNS, kad nustatytų buvimo vietą.
5. Įrankis veikia populiariausiose naršyklėse, tokiose kaip: „Chrome“, „Firefox“, „Microsoft Edge“ ir „Opera“.



17 pav. „Netcraft“ įrankio pranešimo apie žinomą saugią svetainę pavyzdys



18 pav. „Netcraft“ įrankio pranešimo apie įtariamą sukčiavimo svetainę pavyzdys

Vertinimas:

1. **PK.1** – ○

   Pagrindimas: įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ●

   Pagrindimas: įrankyje yra naudojami dviejų spalvų indikatoriai: žalios spalvos indikatorius nurodo saugią svetainę (žr. 17 paveikslą), o jeigu naudotojas lankosi nesaugioje svetainėje, parodomas įspėjimo pranešimas su raudonos spalvos indikatoriumi ir naudotojui leidžiama arba pranešti apie klaidą, arba nepaisyti pranešimo ir užeiti į svetainę (žr. 18 paveikslą). Todėl galima teigti, kad svetainėje naudojami ir indikatoriai ir įspėjamieji pranešimai.
3. **PK.3** – ○

   Pagrindimas: įrankis suteikia naudotojams funkcionalumą grįžti į puslapį ir tęsti naršymą,

jeigu naudotojas nori ir mano, kad svetainė yra teisėta. Tačiau naudotojams nėra suteikiama galimybė pakartoti savo veiksmų. (Uždarius langą ir nespėjus perskaityti pranešimo, nėra iš naujo parodomas langas su įspėjamuoju pranešimu, nebent naudotojas rankiniu būdu perkraus puslapį, tuomet pranešimas bus parodomas iš naujo, kadangi įrankis veikia realiu laiku.)

4. **PK.4** – ●
   Pagrindimas: kadangi įrankis veikia populiariausiose naršyklėse, tokiose kaip „Chrome“, „Firefox“, „Microsoft Edge“ ir „Opera“, galima sakyti, kad jis yra pritaikytas skirtingoms platformoms ar naršyklėms.
5. **PK.5** – ○
   Pagrindimas: įrankis teikia įspėjimus, tačiau neteikia patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○
   Pagrindimas: kadangi įrankis turi integruotą įspėjamąjį pranešimą, galima teigti, kad įrankyje yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.
7. **PK.7** – ⊖
   Pagrindimas: įrankis suteikia galimybę naudotojams grįžti į puslapį ir tęsti naršymą po įspėjamojo pranešimo, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančių veiksmų ir, pavyzdžiui, mygtukų kombinacija atlikti šį įrankio suteikiamą funkcionalumą.
8. **PK.8** – ●
   Pagrindimas: įrankį sudaro tik piktogramos, esančios įrankių juostoje, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.
9. **PK.9** – ○
   Pagrindimas: įrankio oficialioje svetainėje (`https://www.netcraft.com/blog/netcraft-toolbar-tutorial`) galima rasti įrankio vadovą ir mokomąją medžiagą, tačiau nėra virtualaus asistento.
10. **DK.1** – ⊖
    Pagrindimas: įrankyje esantys spalvų indikatoriai ir įspėjamieji pranešimai nėra pritaikyti negalią turintiems naudotojams. (Negalima padidinti indikatorių, koreguoti spalvų, išgirsti įspėjimų garsu ir panašiai.)
11. **DK.2** – ●
    Pagrindimas: įrankis nemokamas ir lengvai prieinamas vienam naudotojui ar organizacijoms su ribotu biudžetu.
12. **DK.3** – ●
    Pagrindimas: kadangi įrankis veikia populiariausiose naršyklėse, tokiose kaip „Chrome“, „Firefox“, „Microsoft Edge“ ir „Opera“, galima sakyti, kad jis veikia naudojant standartinius įrankius ar naršykles be papildomų diegimų.
13. **DK.4** – ●

Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo atviro kodo projektų, tačiau šiuo metu jis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

14. **DK.5** – ●
    Pagrindimas: įrankis yra nemokamas interneto naršyklės plėtinys ir kiekvienas naudotojas gali šiuo įrankiu naudotis nemokėdamas už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakų.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą ir tikrina, ar svetainė, kurią bando pasiekti naudotojas, yra jame.
17. **TS.3** – ●
    Pagrindimas: įrankis naudoja dirbtinio intelekto modelius URL nuorodos ir svetainės turinio analizei, kad identifikuotų potencialiai grėsmę keliančias svetaines.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikomis grįstą atpažinimą. Jis analizuoja svetainės DNS įrašus, saugumo sertifikatus naudodamas euristikas.

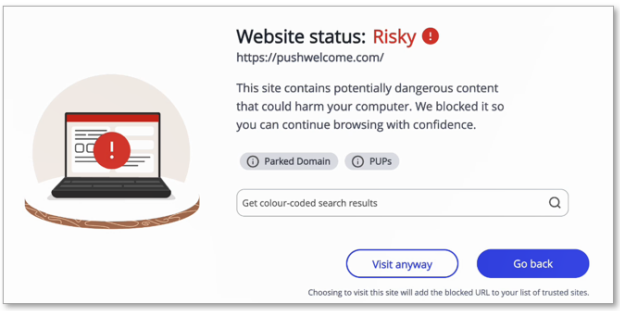
2.4.12. „McAfee Web Advisor“

Šis įrankis yra naršyklės plėtinys, kuris siūlo naudotojams apsaugą nuo internetinių grėsmių, tokių kaip: kenkėjiška programinė įranga, duomenų viliojimo atakos ir kitos kenkėjiškos svetainės. Šį plėtinį sukūrė kibernetinio saugumo bendrovė „McAfee“, jis buvo pradėtas naudoti 2016 metais. Šis įrankis yra nemokamas naršyklės plėtinys, kuris suteikia naudotojams apsaugą nuo interneto grėsmių realiuoju laiku. Šis plėtinys veikia su populiariausiomis interneto naršyklėmis, tokiomis kaip „Google Chrome“, „Mozilla Firefox“ ir „Microsoft Edge“. „McAfee Web Advisor“, ir naudoja svetainės turinio analize pagrįstą metodą, kad apsaugotų naudotojus nuo potencialiai žalingų svetainių ir interneto turinio. Įrankis, taikydamas įvairius metodus, pavyzdžiui, euristikas, parašų aptikimą ir mašininio mokymosi algoritmus, analizuoja tinklapių, failų ir atsisiunčiamų failų turinį, kad nustatytų, ar jie kelia pavojų duomenų saugumui.

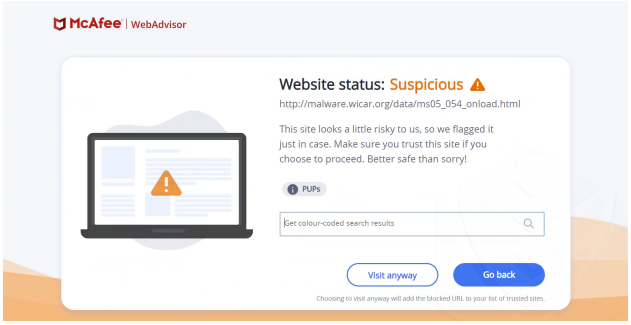
Įrankio privalumai:

1. „McAfee“ tvarko interneto svetainių ir URL adresų duomenų bazę ir, naudodamasis ja, kiekvienai svetainei priskiria reputacijos balą bei blokuoja svetaines, kurių reputacijos balas yra žemas.
2. Įrankis taip pat tvarko žinomų virusų ir kitų grėsmių duomenų bazę. Kai naudotojas atsiunčia kokį nors failą, „McAfee“ patikrina jį pagal duomenų bazę ir nustato, ar jis atitinka kokią nors grėsmę.
3. „McAfee“ siūlo saugius paieškos rezultatus, priskirdamas saugumo reitingą, ir tikrina, ar paieškos rezultatuose nėra kenkėjiškų nuorodų.
4. Įrankis turi skelbimų blokatorių, iššokančių langų blokatorių ir stebėjimo apsaugą, kad apsaugotų naudotoją nuo nepageidaujamų trukdžių (žr. 19 ir 20 paveikslus).

5. „McAfee“ naudoja slaptažodžių šifravimą ir dviejų veiksnių autentifikavimą, kad apsaugotų naudotojų slaptažodžius.



19 pav. „McAfee Web Advisor“ įrankio pranešimo apie įtariamą sukčiavimo svetainę pavyzdys



20 pav. „McAfee Web Advisor“ įrankio pranešimo apie įtartiną svetainę pavyzdys

Vertinimas:

1. **PK.1** – ◐
   Pagrindimas: įrankis tikrina svetainės autentiškumą dviejose stadijose, pirmiausiai jis tikrina svetainės autentiškumą vedant adresą paieškos laukelyje. Taip pat įrankis tikrina svetainės autentiškumą, kai naudotojas jau yra užėjęs į svetainę.
2. **PK.2** – ⊖
   Pagrindimas: naudotojui bandant atidaryti įtartiną ar žinomą sukčiavimo svetainę, įrankis nukreipia naudotoją į integruotus įspėjamuosius pranešimus su klausimu, ar naudotojas tikrai nori lankytis svetainėje. Tačiau naudotojui bandant atidaryti saugią, žinomą svetainę, įrankis neatvaizduoja nieko, nes neturi jokio specialaus pranešimo, ar žymėjimo. Tai gali klaidinti naudotoją, nes jis nežinos, ar įrankis veikia, ar neveikia, iki kol nesusidurs su įtartina svetaine.
3. **PK.3** – ○
   Pagrindimas: įrankis suteikia naudotojams funkcionalumą grįžti į puslapį ir tęsti naršymą, jeigu naudotojas nori ir mano, kad svetainė yra teisėta. Tačiau naudotojams nėra suteikiama galimybė pakartoti savo veiksmų. (Uždarius langą ir nespėjus perskaityti pranešimo, nėra iš naujo parodomas langas su įspėjamuoju pranešimu, nebent naudotojas rankiniu būdu perkraus puslapį, tuomet pranešimas bus parodomas iš naujo, kadangi įrankis veikia realiu laiku.)

4. **PK.4** – ●

   Pagrindimas: kadangi įrankis veikia populiariausiose naršyklėse, tokiose kaip „Google Chrome“, „Mozilla Firefox“ ir „Microsoft Edge“, galima sakyti, kad jis yra pritaikytas skirtingoms platformoms ar naršyklėms.
5. **PK.5** – ○

   Pagrindimas: įrankis teikia įspėjimus, tačiau neteikia patarimų, kaip ištaisyti klaidas arba atšaukti veiksmą. Jeigu naudotojas nesaugioje svetainėje suvedė jautrią informaciją, įrankis nepadeda naudotojui atšaukti šio veiksmo.
6. **PK.6** – ○

   Pagrindimas: kadangi įrankis turi integruotus įspėjamuosius pranešimus, galima teigti, kad jame yra įspėjimų, tačiau nėra patarimų, kurie padėtų išvengti duomenų praradimo.
7. **PK.7** – ⊖

   Pagrindimas: įrankis suteikia galimybę naudotojams grįžti į puslapį ir tęsti naršymą po įspėjamojo pranešimo, tačiau nėra žinomų būdų patyrusiems naudotojams praleisti pasikartojančių veiksmų ir, pavyzdžiui, mygtukų kombinacija atlikti šį įrankio suteikiamą funkcionalumą.
8. **PK.8** – ●

   Pagrindimas: įrankį sudaro tik įspėjamieji pranešimai, todėl galime teigti, kad yra tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.
9. **PK.9** – ○

   Pagrindimas: įrankio oficialioje svetainėje (`https://www.mcafee.com/support/s/article/000002207?language=en_US`) galima rasti įrankio vadovą ir mokomąją medžiagą, tačiau nėra virtualaus asistento.
10. **DK.1** – ⊖

    Pagrindimas: įrankyje esantys įspėjamieji pranešimai nėra pritaikyti negalią turintiems naudotojams. (Negalima padidinti piktogramos, koreguoti spalvų, išgirsti įspėjimų garsu ir panašiai.)
11. **DK.2** – ●

    Pagrindimas: kadangi įrankis yra nemokamas, jo išlaidos vienam naudotojui yra nedidelės ir prieinamos visiems naudotojams ar organizacijoms su ribotu biudžetu. Įrankyje taip pat yra ir papildomų funkcionalumų, už kuriuos jau reikia papildomai susimokėti, tačiau bazinis funkcionalumas yra suteikiamas nemokamai.
12. **DK.3** – ⊖

    Pagrindimas: šis plėtinys veikia su populiariausiomis interneto naršyklėmis, tokiomis kaip „Google Chrome“, „Mozilla Firefox“ ir „Microsoft Edge“, tačiau neveikia su „Safari“ ir „Opera“, todėl galima sakyti, kad įrankis reikalauja papildomų diegimų, jeigu naudotojas naudojasi naršyklėmis, kurios įrankio nepalaiko.
13. **DK.4** – ●

    Pagrindimas: įrankis buvo išbandytas naudotojų, priimtas ir naudojamas rinkoje, buvo

atviro kodo projektų, tačiau šiuo metu jis nėra prieinamas, egzistuoja literatūra, kuri patvirtina įrankio efektyvumą.

14. **DK.5** – ●
    Pagrindimas: įrankis yra nemokamas interneto naršyklės plėtinys ir kiekvienas naudotojas gali šiuo įrankiu naudotis nemokėdamas už tai autorinio atlyginimo.
15. **TS.1** – ⊖
    Pagrindimas: įrankis nemoko naudotojo atpažinti duomenų viliojimo atakos.
16. **TS.2** – ●
    Pagrindimas: įrankis naudoja juodąjį sąrašą, į kurį įtraukia svetaines, kurių reputacijos balas – žemas.
17. **TS.3** – ●
    Pagrindimas: įrankis naudoja dirbtinio intelekto modelius atpažinti potencialioms duomenų viliojimo atakoms.
18. **TS.4** – ●
    Pagrindimas: įrankis naudoja euristikas atpažinti potencialioms duomenų viliojimo atakoms.

2.5. Apibendrinimas

Anksčiau šiame darbe išanalizavus duomenų viliojimo atakų procesą ir tipus buvo identifikuoti duomenų viliojimo atakų požymiai naudotojo sąsajoje. Remiantis šiais požymiais galima šviesti ir mokyti naudotojus atpažinti duomenų viliojimo atakas bei kurti įrankius, naudotojų apsaugai nuo šių atakų. Šiame skyriuje buvo suformuluoti vertinimo kriterijai, kuriais remiantis buvo atliktas egzistuojančių įrankių, skirtų apsaugoti naudotoją nuo duomenų viliojimo atakų, vertinimas. Atlikus vertinimą pagal šiuos kriterijus gauti tokie rezultatai (žr. 2 lentelę).
Panaudojamumo kriterijai:

1. **PK.1 Sistemos būsenos matomumas.**
   Šį kriterijų dauguma analizuojamų įrankių (83,33 %) įgyvendina iš dalies – ○.
   Likę (16,67 %) įgyvendina pusiau – ◐.
2. **PK.2 Atitikimas tarp sistemos ir realaus pasaulio.**
   Šį kriterijų (50 %) analizuojamų įrankių neįgyvendina – ⊖,
   (33,33 %) įgyvendina iš dalies – ○,
   (16,67 %) visiškai įgyvendina – ●.
3. **PK.3 Naudotojo kontrolė ir laisvė.**
   Šį kriterijų dauguma analizuojamų įrankių (75 %) įgyvendina iš dalies – ○,
   likusiai daliai įrankių šis kriterijus nebuvo taikomas – N/A.
4. **PK.4 Nuoseklumas ir standartai.**
   Šio kriterijaus dauguma įrankių (75 %) neįgyvendina – ⊖,
   tačiau likusi dalis (25 %) įgyvendina visiškai – ●.
5. **PK.5 Klaidų prevencija.**

Šio kriterijaus dauguma įrankių (75 %) neįgyvendina – ⊖,
tačiau likusi dalis (25 %) įgyvendina iš dalies – ○.

6. **PK.6 Atpažinimas, o ne prisiminimas.**
   Šį kriterijų dauguma analizuojamų įrankių (91,67 %) įgyvendina iš dalies – ○,
   likusi dalis (8,33 %) įgyvendina pusiau – ◐.
7. **PK.7 Lankstumas ir naudojimo efektyvumas.**
   Šio kriterijaus dauguma analizuojamų įrankių (83,33 %) neįgyvendina – ⊖,
   likusiai daliai įrankių šis kriterijus nebuvo taikomas – N/A.
8. **PK.8 Estetiškas ir minimalistinis dizainas.**
   Šį kriterijų dauguma analizuojamų įrankių (91,67 %) įgyvendina visiškai – ●,
   likusi dalis (8,33 %) įgyvendina pusiau – ◐.
9. **PK.9 Pagalba ir dokumentacija.**
   Šio kriterijaus dauguma analizuojamų įrankių (66,67 %) neįgyvendina – ⊖,
   tačiau likusi dalis (33,33 %) įgyvendina iš dalies – ○.

Diegimo kriterijai:

1. **DK.1 Prieinamumas.**
   Šio kriterijaus neįgyvendina nė vienas įrankis (100 %) – ⊖.
2. **DK.2 Minimalios išlaidos vienam naudotojui.**
   Šį kriterijų visi įrankiai įgyvendina visiškai (100 %) – ●.
3. **DK.3 Suderinamumas su naršyklėmis.**
   Šio kriterijaus dauguma analizuojamų įrankių (83,33 %) neįgyvendina – ⊖,
   tačiau likusi dalis (16,67 %) įgyvendina visiškai – ●.
4. **DK.4 Brandumas.**
   Šį kriterijų visi įrankiai įgyvendina visiškai (100 %) – ●.
5. **DK.5 Nepriklausomybė nuo nuosavybės teisių.**
   Šį kriterijų visi įrankiai įgyvendina visiškai (100 %) – ●.

Techniniai sprendimai:

1. **TS.1 Naudotojų mokymas.**
   Šio techninio sprendimo nenaudoja nė vienas įrankis (100 %) – ⊖.
2. **TS.2 Juodieji / baltieji sąrašai.**
   Šį techninį sprendimą naudoja dauguma analizuojamų įrankių (75 %) – ●,
   likusi dalis (25 %) nenaudoja – ⊖.
3. **TS.3 Giliojo mokymosi metodai ir mašininis mokymasis.**
   Šio techninio sprendimo dauguma analizuojamų įrankių (83,33 %) nenaudoja – ⊖,
   tačiau likusi dalis (16,67 %) naudoja – ●.
4. **TS.4 Euristikomis grįstas atpažinimas.**
   Šį techninį sprendimą dauguma analizuojamų įrankių (75 %) naudoja – ●,
   likusi dalis (25 %) nenaudoja – ⊖.

2 lentelė. Įrankių analizės rezultatai

Įrankiai													
„CallingID“	„Cloudmark AntiFraud“	„EarthLink“	„Ebay“	„Firefox 2“	„GeoTrust TrustWatch“	„Microsoft Internet Explorer 7“	„Netscape Browser 8.1“	„SpoofGuard“	„Bitdefender Traffic Light“	„Netcraft“	„McAfee Web Advisor“		
○	○	○	○	○	○	○	○	○	◐	○	◐	PK.1 Sistemos būsenos matomumas.	**Panaudojamumo kriterijai**
○	○	⊖	⊖	⊖	○	⊖	⊖	○	●	●	⊖	PK.2 Atitikimas tarp sistemos ir realaus pasaulio.	
N/A	N/A	○	○	○	N/A	○	○	○	○	○	○	PK.3 Naudotojo kontrolė ir laisvė.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	●	●	●	PK.4 Nuoseklumas ir standartai.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○	PK.5 Klaidų prevencija.	
○	○	○	○	◐	○	○	○	○	○	○	○	PK.6 Atpažinimas, o ne prisiminimas.	
N/A	N/A	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	PK.7 Lankstumas ir naudojimo efektyvumas.	
●	●	●	●	●	●	●	◐	●	●	●	●	PK.8 Estetiškas ir minimalistinis dizainas.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	○	○	○	○	PK.9 Pagalba ir dokumentacija.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	DK.1 Prieinamumas.	**Diegimo kriterijai**
●	●	●	●	●	●	●	●	●	●	●	●	DK.2 Minimalios išlaidos vienam naudotojui.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	●	●	⊖	DK.3 Suderinamumas su naršyklėmis.	
●	●	●	●	●	●	●	●	●	●	●	●	DK.4 Brandumas.	
●	●	●	●	●	●	●	●	●	●	●	●	DK.5 Nepriklausomybė nuo nuosavybės teisių.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	TS.1 Naudotojų mokymas.	**Techniniai sprendimai**
⊖	●	●	●	●	●	●	●	⊖	⊖	●	●	TS.2 Juodieji / baltieji sąrašai.	
⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	●	●	TS.3 Giliojo mokymosi metodai ir mašininis mokymasis.	
●	⊖	●	●	●	⊖	●	⊖	●	●	●	●	TS.4 Euristikomis grįstas atpažinimas.	

⊖– neįgyvendinta, ○– iš dalies įgyvendinta, ◐– pusiau įgyvendinta, ●– visiškai įgyvendinta

3. Projektavimo gairės bakalauro darbe kuriamai priemonei

Atlikus vertinimą jau egzistuojančių įrankių, skirtų apsaugoti naudotoją nuo duomenų viliojimo atakų, galime suformuluoti projektavimo gaires bakalauro darbe kuriamai priemonei, remiantis gerosiomis praktikomis ir pastebėtais trūkumais vertintuose įrankiuose. Kiekviena projektavimo gairė turi unikalų identifikatorių, nurodantį, iš kurio kriterijaus ji kilo, ir pavadinimą, trumpai apibūdinantį gairės esmę.

1. **Kriterijus PK.1. Svetainės autentiškumo tikrinimas ir naudotojo edukacija.** Projektuojamas įrankis turėtų tikrinti svetainės autentiškumą naudotojui dar prieš užeinant į svetainę, taip pat naudotojui jau užėjus į svetainę ir mokyti naudotojus, kad šie patys atpažintų galimas duomenų viliojimo atakas ir nevestų savo jautrių duomenų sukčiavimo svetainėse.
2. **Kriterijus PK.2. Vizualinių įspėjimų aiškumas ir atpažįstamumas.** Projektuojamas įrankis turėtų naudoti naudotojams lengvai atpažįstamų spalvų piktogramas, naudoti standartinio šviesoforo įspėjamąsias spalvas, dar geriau, jeigu įrankis naudotų aktyviuosius indikatorius su lengvai išmokstamais ir atpažįstamais nurodymais ir įspėjimais.
3. **Kriterijus PK.3. Naudotojo veiksmų valdymas ir sprendimų patvirtinimas.** Projektuojamas įrankis turėtų leisti naudotojui anuliuoti ir pakartoti savo veiksmus. Tai reiškia, kad kai naudotojas užeina į nesaugią svetainę ir įrankis apie tai įspėja naudotoją, naudotojas turi turėti galimybę arba išeiti iš svetainės, arba pasilikti joje, tačiau jeigu naudotojas nusprendžia pasilikti svetainėje, įrankis turėtų perklausti, ar naudotojas tikrai nori ir yra įsitikinęs, kad nori lankytis nesaugioje svetainėje.
4. **Kriterijus PK.4. Pritaikomumas įvairioms naršyklėms.** Projektuojamas įrankis kiek įmanoma labiau turėtų būtų pritaikytas skirtingoms naršyklėms. Tai reiškia, kad kuriamo įrankio kalba, indikatoriai, veiksmai turėtų būti suprantami naudotojams, nepriklausomai nuo to, kokią naršyklę naudotojas yra įpratęs naudoti.
5. **Kriterijus PK.5. Įspėjimai ir pagalba prieš ir po apsilankymo svetainėje.** Projektuojamas įrankis turėtų teikti įspėjimus ir patarimus, kaip ištaisyti klaidas (kaip išeiti iš puslapio, į ką atkreipti dėmesį), ir tai turėtų daryti prieš naudotojui užeinant į svetainę ir naudotojui užėjus į svetainę.
6. **Kriterijus PK.6. Aiškūs ir tiesiogiai pateikiami įspėjimai.** Projektuojamas įrankis turi turėti įspėjimus ir patarimus, kaip apsisaugoti nuo duomenų viliojimo atakų ir tie patarimai turi būti aiškūs ir suprantami bei rodomi iš karto (o ne paspaudus ant dar vienos nuorodos, ar nuėjus į dar vieną svetainę).
7. **Kriterijus PK.7. Galimybė praleisti pasikartojančius veiksmus patyrusiems naudotojams.** Jeigu projektuojamame įrankyje būtų galimybė naudotojams atlikti veiksmus, kurie nekeltų pavojaus jų saugumui internete, būtų gerai, jeigu projektuojamas įrankis turėtų galimybę patyrusiems naudotojams praleisti pasikartojančius veiksmus.
8. **Kriterijus PK.8. Tikslinė informacija naudotojo sąsajoje.** Projektuojamame įrankyje turėtų būti tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų. Įrankio vizualinės dalies neturėtų užimti su saugumu nesusiję indikatoriai, logotipai ar reklamos.

9. **Kriterijus PK.9. Prieinama pagalba ir mokomoji medžiaga.** Projektuojamas įrankis turėtų turėti bent jau prieinamą dokumentaciją ar mokomąją medžiagą, kad naudotojai galėtų pasiskaityti apie funkcionalumus bei mokėtų patys savarankiškai įsidiegti įrankį savo kompiuteryje.
10. **Kriterijus DK.1. Pritaikymas regos negalią turintiems naudotojams.** Projektuojamas įrankis turėtų būti pritaikytas ir regos negalią turintiems naudotojams.
11. **Kriterijus DK.2. Prieinamumas.** Projektuojamas įrankis turėtų būti nemokamas ir lengvai prieinamas visiems naudotojams ar organizacijoms.
12. **Kriterijus DK.3. Suderinamumas su standartinėmis priemonėmis.** Projektuojamas įrankis turėtų veikti naudojant standartinius įrankius ar naršykles be papildomų diegimų.
13. **Kriterijus DK.4. Praktinis taikymas realiose situacijose.** Projektuojamas įrankis turėtų būti išbandytas naudotojų, naudojamas realiomis sąlygomis, realiai apsaugai nuo duomenų viliojimo atakų, ne tik mokslinių tyrimų tikslais.
14. **Kriterijus DK.5. Prieinamumas nemokant autorinio atlyginimo.** Projektuojamas įrankis turėtų būti prieinamas kiekvienam naudotojui ir juo turi būti galima naudotis nemokant už tai autorinio atlyginimo.
15. **Techninių sprendimų integracija ir naudotojo švietimas.** Projektuojamas įrankis turėtų naudoti bent tris iš keturių techninių sprendimų. Įrankis turėtų gebėti atpažinti jau žinomas duomenų viliojimo atakas (naudoti juoduosius / baltuosius sąrašus), turėtų gebėti atpažinti naujas duomenų viliojimo atakas (naudoti euristikomis grįstą atpažinimą) bei turėtų gebėti šviesti ir mokyti naudotoją savarankiškai atpažinti duomenų viliojimo atakas (mokyti naudotojus).

4. Alternatyvieji maketai

Alternatyvieji maketai kurti remiantis anksčiau aprašytomis projektavimo gairėmis. Nuoroda į maketus: **alternatyviųjų maketų nuoroda.**

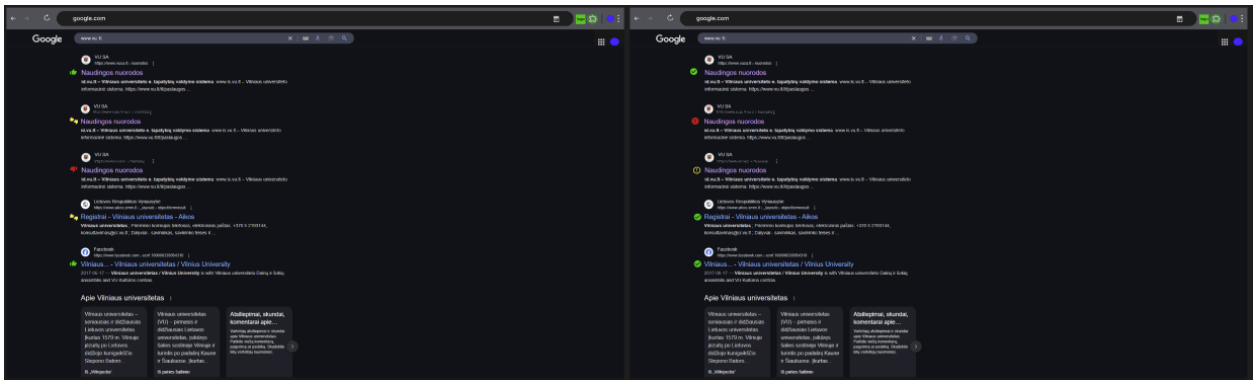
4.1. Įgyvendinama projektavimo gairė iš kriterijaus PK.1

Alternatyviuosiuose maketuose svetainės autentiškumas tikrinamas naudotojui dar prieš užeinant į svetainę. Šalia kiekvienos svetainės rodomos šviesoforo spalvų piktogramos, kurios nurodo svetainės saugumą (žr. 21 paveikslą). Pirmame makete:

- Saugią svetainę indikuoja žalios spalvos nykštys, pakeltas į viršų.
- Nesaugi svetainė pažymima raudonos spalvos nykščiu, nuleistu į apačią.
- Nežinoma svetainė pažymima geltonos spalvos piktograma su dviem nykščiais – vienu nuleistu į apačią, ir kitu, pakeltu į viršų.

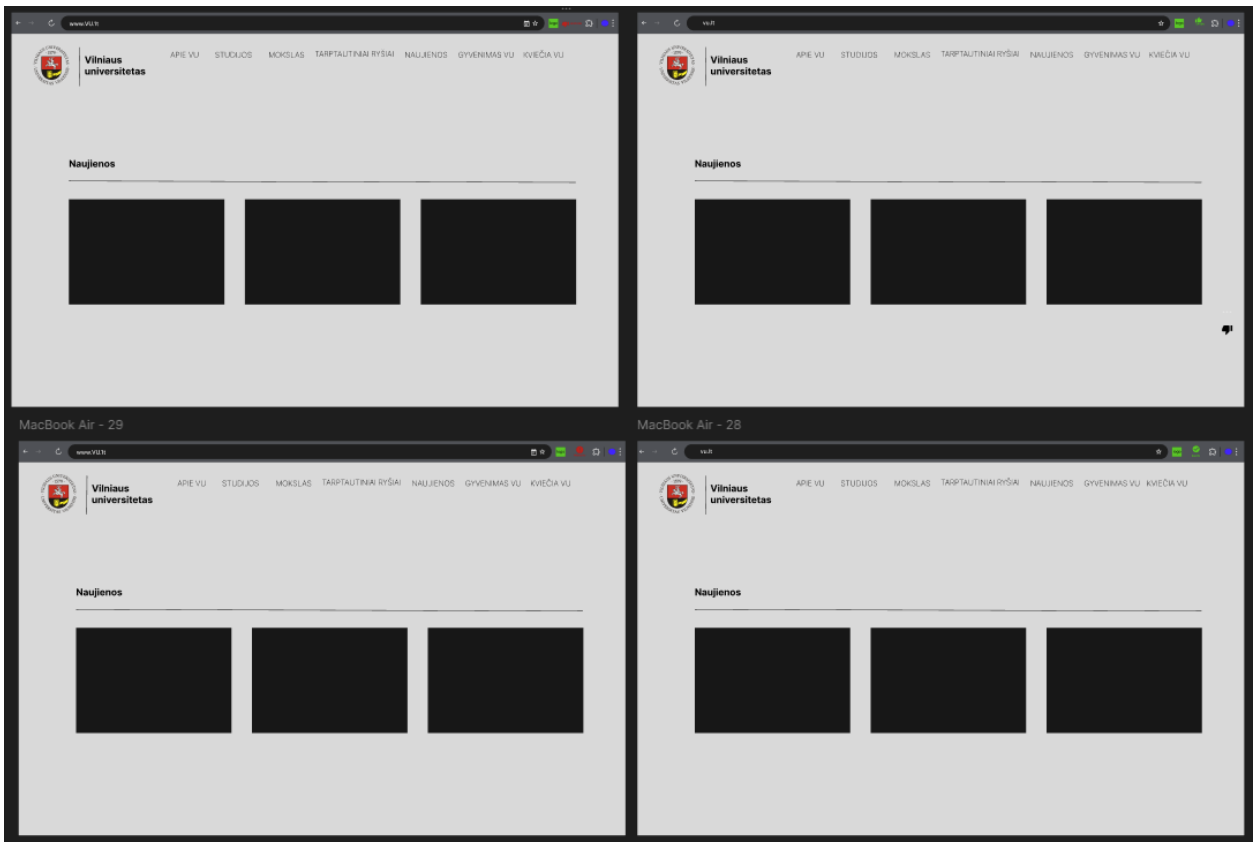
Antrame makete:

- Saugią žinomą svetainę indikuoja žalios spalvos apskritimo formos piktograma su varnele viduje.
- Nesaugią svetainę indikuoja raudonos spalvos apskritimo formos piktograma su šauktuku viduje.
- Nežinomą svetainę indikuoja geltonos spalvos apskritimo tuščiavidurė piktograma su šauktuku viduje.



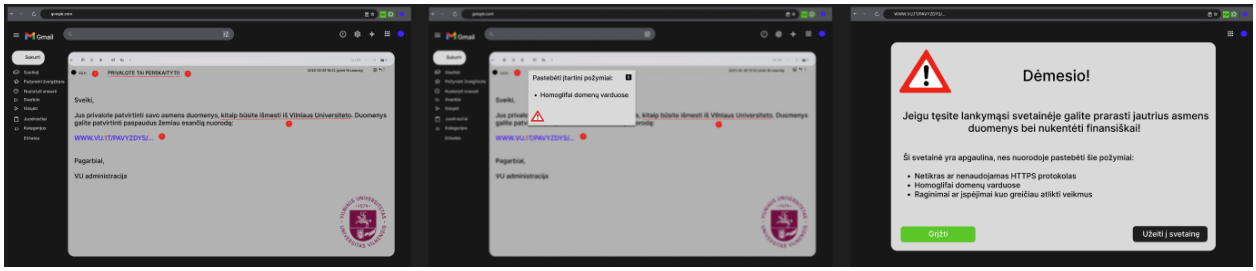
21 pav. Autentiškumo tikrinimas naudotojui prieš užeinant į svetainę

Maketuose taip pat tikrinamas svetainės autentiškumas naudotojui jau užėjus į svetainę (žr. 22 paveikslą). Pirmame makete apie svetainės autentiškumą naudotojas yra informuojamas nykščio formos piktogramomis ir žodžiu, nurodančiu, ar svetainė yra saugi, ar nesaugi. Antrame makete naudotojas apie svetainės autentiškumą yra informuojamas apskritimo formos piktograma ir žodžiu, kuris nurodo svetainės saugumą.



22 pav. Autentiškumo tikrinimas naudotojui užėjus į svetainę

Maketuose taip pat atvaizduojamas ir naudotojų mokymas (žr. 23 paveikslą). Naudotojui gavus suklastotą elektroninį laišką, viename iš maketų, šalia kiekvieno iš pastebėtų įtartinų požymių atsiranda raudonos spalvos apskritimo formos piktograma su šauktuku viduje, paspaudus ant šios piktogramos naudotojas gali peržiūrėti, koks rastas požymis indikuoja apie galimai potencialią duomenų vagystės ataką. Abiejuose maketuose, paspaudus ant įtartinos nuorodos, parodomi pranešimai, kuriuose taip pat naudotojas informuojamas, kokius požymius reikėtų pastebėti laiške bei įtartinoje nuorodoje.



23 pav. Naudotojų mokymas atpažinti duomenų viliojimo atakas

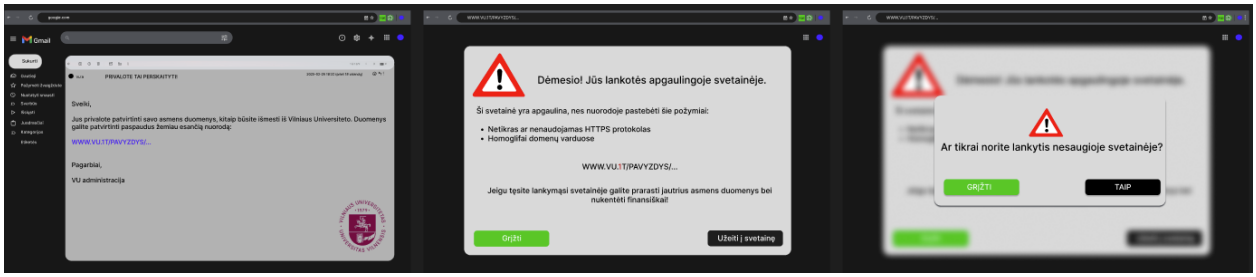
4.2. Įgyvendinama projektavimo gairė iš kriterijaus PK.2

Maketuose naudojamos lengvai atpažįstamos ir išmokstamos piktogramos, kurios nuspalvintos standartinio šviesoforo spalvomis. Taip pat naudojami aktyvūs įspėjimai, skirti informuoti naudotojus apie potencialią duomenų viliojimo ataką. Pranešimai turi būti lengvai atpažįstami. (žr. 24 paveikslą).

24 pav. Maketuose naudojamos piktogramos ir įspėjimai

4.3. Įgyvendinama projektavimo gairė iš kriterijaus PK.3

Maketuose leidžiama naudotojui anuliuoti savo veiksmus (žr. 25 paveikslą). Naudotojui paspaudus ant nesaugios svetainės nuorodos, projektuojamuose maketuose parodomas pranešimas, kuris įspėja naudotoją apie svetainės saugumą. Įspėjus naudotoją, šis turi galimybę pasirinkti, ar nori grįžti ir nesilankyti nesaugioje svetainėje ar, nepaisant pranešimo, likti joje. Naudotojui nusprendus pasilikti svetainėje, projektuojamas įrankis perklausia naudotojo, ar jis tikrai yra įsitikinęs, kad nori lankytis nesaugioje svetainėje.



25 pav. Funkcionalumas, leidžiantis naudotojui anuliuoti ir pakartoti savo veiksmus

4.4. Įgyvendinama projektavimo gairė iš kriterijaus PK.4

Maketuose naudojama kalba ir indikatoriai yra parinkti taip, kad būtų aiškūs, lengvai suprantami ir atpažįstami daugumai naudotojų. Šie elementai nesiskiria, nepriklausomai nuo to, kokia naršykle naudotojas įprastai naudojasi, todėl užtikrinamas nuoseklumas ir patogumas visiems naudotojams.

4.5. Įgyvendinama projektavimo gairė iš kriterijaus PK.5

Prieš naudotojui užeinant į svetainę pateikiamos šviesoforo spalvų piktogramos, nurodančios svetainės saugumą (žr. 21 paveikslą). Naudotojui užėjus į svetainę rodomas įspėjimas su nurodymais, į ką reikia atkreipti dėmesį, ir perklausiama naudotojo, ar jis tikrai nori lankytis nesaugioje svetainėje (žr. 25 paveikslą). Naudotojui jau užėjus į svetainę pateikiamos piktogramos, kurios taip pat nurodo svetainės saugumą (žr. 22 paveikslą).

4.6. Įgyvendinama projektavimo gairė iš kriterijaus PK.6

Maketuose matomi įspėjimai ir patarimai, į ką reikėtų atkreipti dėmesį ir kaip apsisaugoti nuo duomenų viliojimo atakų, ir šie patarimai yra rodomi iš karto (žr. 25 ir 23 paveikslus).

4.7. Įgyvendinama projektavimo gairė iš kriterijaus PK.7

Maketuose nėra tokių pasikartojančių veiksmų, kuriuos patyrusiems naudotojams būtų galimybė praleisti ir tai nekeltų pavojaus naudotojo duomenų saugumui.

4.8. Įgyvendinama projektavimo gairė iš kriterijaus PK.8

Be jau įkeltų maketų vizualų ir aprašyto funkcionalumo, maketuose atvaizduojamas funkcionalumas, leidžiantis naudotojui pačiam pranešti apie galimai nesaugią svetainę įklijuojant svetainės nuorodą (žr. 26 paveikslą). Visi įrankio suteikiami funkcionalumai yra susiję tik su apsauga nuo duomenų viliojimo atakų, nėra su saugumu nesusijusių indikatorių ar reklamų.

26 pav. Pranešimo apie galimai nesaugią svetainę pavyzdys

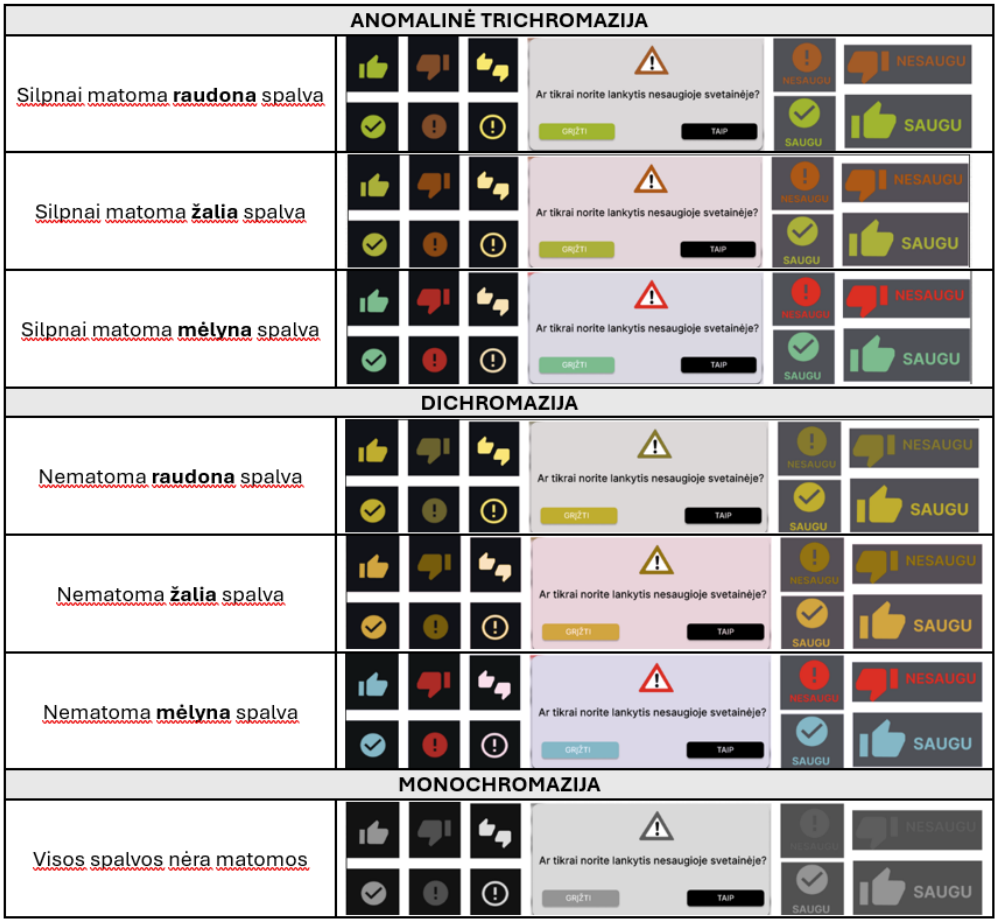
4.9. Įgyvendinama projektavimo gairė iš kriterijaus PK.9

Kadangi alternatyviuosiuose maketuose naudojamos vizualiai skirtingos piktogramos ir skiriasi funkcionalumo įgyvendinimo žingsniai (veiksmai, reikalingi tam tikrai funkcijai atlikti), mokomoji medžiaga bus kuriama vėliau – jau atlikus panaudojamumo testavimą, kuriant detalųjį prototipą. Tokiu būdu dokumentacijoje bus pateikta tiksli informacija apie pasirinktą funkcionalumą ir maketuose naudojamas piktogramas.

4.10. Įgyvendinama projektavimo gairė iš kriterijaus DK.1

Aklumas spalvoms ganėtinai dažnai pasitaikantis sveikatos sutrikimas tarp vyriškosios lyties atstovų. Yra atlikta nemažai apklausų, kurių tikslas nustatyti, koks procentas populiacijos susiduria su šia problema, o apibendrinus šias apklausas gauti rezultatai rodo, kad 8 % europiečių vyrų, 5 % azijiečių vyrų ir 4 % afrikiečių vyrų susiduria su aklumu spalvoms [Bir12]. Spalvų jutimas gali būti anomalinis (diagnozė: anomalinė trichromazija), kuomet žmogus vieną iš spalvų mato silpnai. Taip pat spalvų jutimas gali būti dischromazinis, kai žmogus gali nejusti vienos iš trijų spalvų, arba jutimas gali būti monochromazinis, kuomet žmogus visiškai neskiria spalvų, tačiau tokių atvejų pasitaiko ypač retai.

Alternatyviųjų maketų pagrindiniai indikatoriai pritaikyti ir regėjimo negalią turintiems naudotojams (filtrai taikyti naudojant internetinę svetainę „Colbis“ adresu: `https://www.color-blindness.com/coblis-color-blindness-simulator/`). Naudotojai, turintys anomalinį ar dischromazinį spalvų jutimo sutrikimą, taip pat gali nesunkiai atskirti skirtingų spalvų piktogramas, o pačios piktogramos gali padėti jiems įsiminti jų reikšmes. Tačiau žmonėms su monochromazija – kai regima tik viena spalva arba viskas atrodo pilka – gali kilti sunkumų atskiriant piktogramas, ypač jei jos yra dešiniajame įrankių juostos kampe pilkame fone. Dėl mažo kontrasto piktogramos susilieja su fonu ir tampa sunkiai pastebimos. Todėl kuriant įrankį svarbu numatyti funkcionalumą, leidžiantį naudotojui perjungti spalvų režimą, kuriame piktogramų ir fono kontrastas būtų ryškesnis ir labiau pastebimas.



27 pav. Regos negalią turinčių žmonių maketuose naudojamų spalvų matymas

4.11. Įgyvendinama projektavimo gairė iš kriterijų DK.2, DK.3, DK.4, DK.5

Maketams šie kriterijai nėra taikomi ir bus įgyvendinami kuriant įrankį, skirtą padėti apsaugoti naudotojus nuo duomenų viliojimo atakų.

5. Panaudojamumo testavimas

5.1. Dalyviai

Pirma grupė: Studentai, studijuojantys programų sistemas Vilniaus universitete bakalauro 4-ame kurse. Jų amžius svyruoja nuo 22 iki 23 metų. Dalyviai pasižymi aukštu kompiuteriniu raštingumo lygmeniu, kadangi jie naudojasi kompiuteriais ir mobiliaisiais įrenginiais kasdien, po mažiausiai 8 valandas per dieną. Be to, dalyviai yra įpratę naudotis įvairiais naršyklės įskiepiais ir geba palyginti bei įvertinti skirtingas naudotojo sąsajas bei funkcionalumą. Tai leidžia tikėtis nuoseklaus ir informatyvaus požiūrio į panaudojamumo testavimą.

Antra grupė: Dirbantys žmonės, neturintys išsilavinimo informacinių technologijų srityje. Amžius svyruoja nuo 18 iki 65. Dalyviai pasižymi mažu arba vidutinišku kompiuterio raštingumo lygmeniu, nes jie kompiuteriais ar mobiliaisiais įrenginiais naudojasi retai arba tiktai paprastoms užduotims atlikti. Dalyviai, ypač jaunesni, yra naudoję naršyklės įskiepius, tačiau kai kurie, tai daro nedažnai arba reikia pasitelkti geriau žinančio asmens pagalba. Ši grupė sudaro didžiausią dalį potencialių naršyklės įskiepio naudotojų, tad šių dalyvių rezultatai suteiks informacijos, kaip atrodys įprasto naršyklės plėtinio naudotojo patirtis.

Trečia grupė: Dirbančio amžiaus žmonės, turintys darbo patirtį arba išsilavinimą informacinių technologijų srityje. Amžius svyruoja nuo 18 iki 65. Dalyviai pasižymi vidutinišku arba aukštu kompiuterio raštingumo lygmeniu, nes jie kompiuteriais ar mobiliaisiais įrenginiais naudojasi kasdien paprastiems, su jų profesine sritimi susijusiems darbams atlikti. Šios grupės dalyviai dažnai yra susipažinę su naršyklės įskiepiais, tačiau kai kurie jais naudojasi tik darbo kompiuteriuose, kuriuos jiems suruošia infrastruktūrą prižiūrintys specialistai. Be to, tikėtina, kad dalyviai yra mokomi atpažinti duomenų viliojimo atakas darbdavio, todėl šių dalyvių rezultatai leis įsivertinti, ar kuriamas įskiepis palengvina duomenų atakų atpažinimą.

Ketvirta grupė: Mokyklinio amžiaus nepilnamečiai žmonės, tai yra iki 18 metų. Dalyviai pasižymi mažu arba vidutinišku kompiuterinio raštingumo lygmeniu, nes dauguma jau užaugo pasaulyje, kuriame egzistavo internetas ir stacionarūs bei nešiojamieji kompiuteriai, taigi jie turi pakankamai žinių, kaip naudotis programine įranga. Dalyviai yra naudoję naršyklės įskiepius, tačiau jie buvo naudojami ne apsisaugoti nuo interneto pavojų bei grėsmių. Šią dalyvių grupę ypač svarbu šviesti apie internete esančius pavojus, kad susiformuotų įgūdžiai, padėsiantys ateityje išvengti nemalonių pasekmių. Šios dalyvių grupės rezultatai suteiks įžvalgų, ar informacija pateikiama suprantamai, kad naudotojas, ateityje susidūręs su panašiomis grėsmėmis, jas gebėtų atpažinti savarankiškai.

Penkta grupė: Ekspertai, dirbantys informacinių technologijų įmonėse. Amžius svyruoja nuo 26 iki 35 metų. Dalyviai pasižymi aukštu kompiuterio raštingumo lygmeniu, nes jie kompiuteriais bei mobiliaisiais įrenginiais naudojasi kiekvieną dieną sudėtingoms užduotims atlikti bei, kas svarbiausia, patys kuria taikomąsias aplikacijas šiems įrenginiams. Šių dalyvių įžvalgos bei patarimai testavimo metu – labai svarbūs, nes iš savo sukauptos patirties jie gali pastebėti ir pakomentuoti maketuose padarytas klaidas.

Dalyvių pritraukimas: Norėdami pritraukti dalyvius mūsų naršyklės įskiepio alternatyvių-

jų maketų panaudojamumo testavimui, kreipėmės į savo artimuosius, pažįstamus ir bendrakursius. Visi dalyviai sutiko dalyvauti savanoriškai, be jokio atlygio. Siekiama pritraukti po du dalyvius iš kiekvienos iš penkių apibrėžtų naudotojų grupių. Toks paskirstymas leidžia į testavimą įtraukti skirtingo amžiaus ir kompiuterinio raštingumo lygio naudotojus. Tai padeda įvertinti maketų panaudojamumą bei surinkti skirtingų gebėjimų naudotojų patirtį ir pastebėjimus.

5.2. Testavimo tikslai

1. **Palyginti alternatyvius gairių projektinius sprendimus:** Stebint naudotojo veikimą identifikuoti defektus ir surinkti naudotojo atsiliepimus.
2. **Įvertinti naudotojo sąsają:** Įvertinti, ar naudotojo sąsaja yra intuityvi ir lengvai suprantama.
3. **Patikrinti naudotojo sąsajos funkcionalumą:** Užtikrinti, kad visi naudotojo sąsajos elementai (mygtukai, langai, pranešimai ir pan.) veiktų, kaip tikimasi.
4. **Rasti klaidas ir trūkumus:** Nustatyti įskiepio dizaino ir numatyto funkcionalumo defektus.
5. **Įvertinti įskiepio piktogramų atpažįstamumą ir pateikiamų įspėjimų funkcionalumą:** Užtikrinti, kad naudotojai galėtų lengvai suprasti pateikiamos informacijos svarbą ir pateikiamų įspėjimų bei piktogramų prasmę taip, kaip tikimasi.

5.3. Testavimo užduotys su sėkmės matais

5.3.1. Pranešimo apie nesaugią svetainę testavimas

Užduotis: Naršyklės įskiepyje išsiųsti pranešimą su nesaugios svetainės nuoroda.

- *Sėkmės matas: laikas*
  Naudotojui pavyks per ne ilgiau nei 1 minutę pirmą kartą naudojant naršyklės įskiepį pranešti apie galimai nesaugią svetainę. Naudotojas, kuris jau buvo susipažinęs su įskiepio veikimo anksčiau, šią užduotį gebės atlikti ne ilgiau nei per 30 sekundžių.
- *Sėkmės matas: klaidos*
  Naudotojas, pirmą kartą naudodamas naršyklės įskiepį, sugebės rasti, kaip išsiųsti pranešimą su nesaugios svetainės nuoroda, padaręs ne daugiau nei 1 klaidą. Susipažinę naudotojai šią užduotį atliks nepadarę klaidų.
- *Sėkmės matas: sėkmingų atlikimų skaičius*
  100 % naudotojų turėtų sugebėti šitą užduotį atlikti iš pirmo karto.
- *Sėkmės matas: pagalbos kreipimasis*
  Naudotojas, pirmą kartą naudodamas naršyklės įskiepį, sugebės pranešti apie galimai nesaugią svetainę be pagalbos.

5.3.2. Įspėjimų elektroniniame laiške apie potencialias duomenų viliojimo atakas testavimas

Užduotis: Naudojantis elektroniniu paštu atidaryti galimai nesaugų laišką su potencialia duomenų viliojimo ataka ir susipažinti su požymiais, atskleidžiančiais šią ataką.

- *Sėkmės matas: požymių prisiminimas*
  Naudotojui pavyks pirmą kartą naudojant naršyklės įskiepį prisiminti 3 požymius, indikuojančius potencialią duomenų viliojimo ataką.
- *Sėkmės matas: sėkmingų atlikimų skaičius*
  100 % naudotojų turėtų sugebėti prisiminti 3 indikuojančius požymius iš pirmo karto.

5.3.3. Naudotojo gebėjimo atpažinti saugią svetainę, remiantis spalvų piktogramomis, testavimas

Užduotis: Naudojantis naršyklės paieška, remiantis įspėjamosiomis spalvų piktogramomis, pasirinkti saugią svetainę.

- *Sėkmės matas: saugios svetainės atpažinimas*
  Naudotojui pavyks pirmą kartą naudojant naršyklės įskiepį, remiantis įspėjamosiomis spalvų piktogramomis, pasirinkti lankytis saugioje svetainėje.
- *Sėkmės matas: pagalbos kreipimasis*
  Naudotojas, pirmą kartą naudodamas naršyklės įskiepį, sugebės, remdamasis įspėjamosiomis piktogramomis, pasirinkti saugią svetainę be pagalbos.

5.3.4. Naudotojo gebėjimo identifikuoti svetainės saugumą pagal įrankių juostos piktogramą testavimas

Užduotis: Remiantis įrankių juostoje esančia piktograma įvardyti, ar svetainė, kurioje lankosi naudotojas, yra saugi ar nesaugi.

- *Sėkmės matas: svetainės saugumo atpažinimas*
  Naudotojui pavyks pirmą kartą naudojant naršyklės įskiepį, remiantis įspėjamosiomis spalvų piktogramomis, įvardyti, ar jis lankosi saugioje, ar nesaugioje svetainėje.
- *Sėkmės matas: pagalbos kreipimasis*
  Naudotojas, pirmą kartą naudodamas naršyklės įskiepį, sugebės atpažinti įrankių juostoje esančias įspėjamąsias piktogramas ir remiantis jomis įvardyti svetainės saugumą be pagalbos.

5.3.5. Naršyklės įskiepio piktogramos, nurodančios praneštų svetainių sąrašą, funkcionalumo testavimas

Užduotis: Naršyklės įskiepyje surasti sąrašą, kuriame būtų naudotojo praneštų nesaugių svetainių sąrašas.

- *Sėkmės matas: laikas*

Naudotojui pavyks per ne ilgiau nei 1 minutę pirmą kartą naudojant naršyklės įskiepį surasti sąrašo piktogramą ir peržiūrėti sąrašą, kuriame būtų svetainių nuorodos, apie kurias naudotojas jau buvo pranešęs naudodamas įskiepį. Naudotojas, kuris jau buvo susipažinęs su įskiepio veikimu anksčiau, šią užduotį gebės atlikti ne ilgiau nei per 30 sekundžių.

- *Sėkmės matas: klaidos*
  Naudotojas, pirmą kartą naudodamas naršyklės įskiepį, sugebės rasti sąrašo piktogramą ir peržiūrės sąrašą padaręs ne daugiau nei 1 klaidą. Susipažinę naudotojai šią užduotį atliks nepadarę klaidų.
- *Sėkmės matas: sėkmingų atlikimų skaičius*
  100 % naudotojų turėtų sugebėti šitą užduotį atlikti iš pirmo karto.
- *Sėkmės matas: pagalbos kreipimasis*
  Naudotojas, pirmą kartą naudodamas naršyklės įskiepį, sugebės šią užduotį atlikti be pagalbos.

5.4. Testavimo aplinka

Testavimo aplinka rami, netriukšminga, kad dalyviai galėtų susikaupti. Naudojamas nešiojamasis arba stacionarusis kompiuteris, kuriame bus testuojamos naršyklės įskiepio versijos bei laikmatis užduočių atlikimo laikui stebėti. Testavimo aplinkoje dalyvis bus ne vienas – bent su vienu iš maketų kūrėjų, kuris pirmiausiai paleis kiekvieną iš maketų, kad testavimo dalyviui to nereiktų daryti pačiam, taip pat žymėsis visas pastabas apie dalyvio potyrius testavimo metu ir laiką, kiek užtruko atlikti užduotims.

5.5. Testavimo sesija

Testavimo sesijos pradžioje kiekvienam iš testavimo dalyvių bus pasiūlytos 2 minutės susipažinti su naršyklės įskiepių maketais ir jose esančiais langais bei funkcijomis.

5.6. Klausimynų pateikimas

Testavimo sesijos pradžioje kiekvienam testavimo dalyviui duodama pasirašyti sutikimo forma dalyvauti maketų testavime. Sutikimo formą pateikiama prieduose (žr. 2 priedą). Kai testavimo dalyvis sutinka dalyvauti testavime, jis pasirašo duotą formą. Tuomet dalyvio paprašoma užpildyti mūsų sukurtą anketą (**panaudojamumo dalyvio klausimyną prieš testavimą**). Ji skirta susipažinti su testavimo dalyviu ir įvertinti jo kompiuterinio raštingumo lygį, kad analizuojant būtų galima paskirti jį į vieną iš penkių apibrėžtų testavimo dalyvių grupių. Atlikus maketų testavimą, dalyvio paprašoma užpildyti dar vieną formą (**panaudojamumo dalyvio klausimyną po testavimo**), skirtą sužinoti, kaip sekėsi dalyviui naudotis sukurtais maketais: ar turėjo pakankamai laiko išmokti jais naudotis bei kuriais iš maketų naudotis buvo lengviau.

Apklausos duomenų rinkimas apima tiek kiekybinius, tiek kokybinius aspektus:

- Kiekybiniai duomenys: Vienas iš maketų kūrėjų testavimo metu fiksuoja naudotojų užduočių atlikimo laikus ir padarytų klaidų skaičių, viską dokumentuodamas savo užrašuose.

- Kokybiniai duomenys: Testavimo dalyviai patys užpildo apklausas prieš ir po testavimo, kurios apima įvairius su maketais susijusius aspektus. Kita dalis kokybinių duomenų yra surenkama stebint ir fiksuojant testavimo metu dalyvių pasakytus komentarus, o šį procesą vykdo vienas iš naršyklės įskiepio maketų kūrėjų.

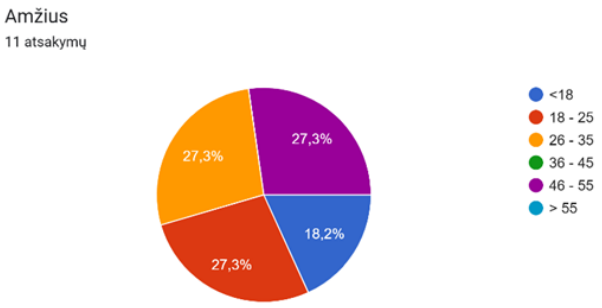
5.7. Panaudojamumo testavimo rezultatai

5.7.1. Testavimo dalyviai

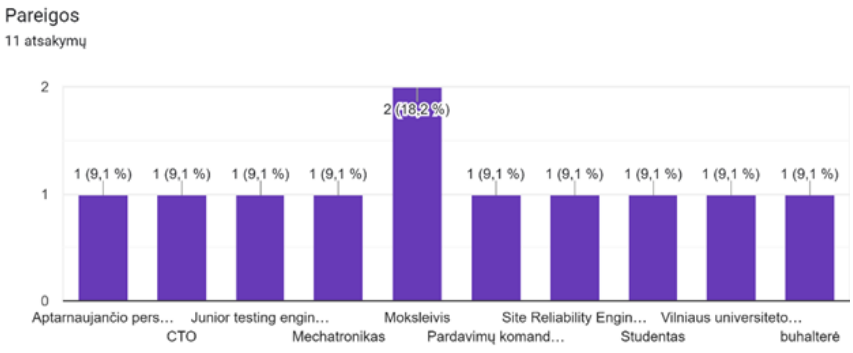
Testavimo sesijoje iš viso maketus testavo vienuolika testavimo dalyvių, iš kurių:

Trys pirmos grupės	Dalyvių ID: 1, 4, 11
Du antros grupės	Dalyvių ID: 6, 7
Du trečios grupės	Dalyvių ID: 2, 10
Du ketvirtos grupės	Dalyvių ID: 8, 9
Du penktos grupės	Dalyvių ID: 3, 5

Testavimo dalyviai į šias grupes paskirstyti remiantis jų amžiumi (žr. 28 paveikslą) bei pareigomis (žr. 29 paveikslą). Šią informaciją dalyviai pateikė pildydami panaudojamumo dalyvio klausimyną prieš testavimą.



28 pav. Testavimo dalyvių amžiaus pasiskirstymas



29 pav. Testavimo dalyvių pareigos

5.7.2. Pranešimo apie nesaugią svetainę testavimo rezultatai

Šios testavimo išvados suformuluotos remiantis sudaryta testavimo rezultatų lentele (žr. 30 paveikslą) bei dalyvio klausimynais po panaudojamumo testavimo (žr. 31 paveikslą):

1. Visi testavimo dalyviai sėkmingai atliko užduotį savarankiškai, nesikreipdami pagalbos.
2. Aštuoni dalyviai atliko užduotį be klaidų.
3. Trys dalyviai užduoties atlikimo metu padarė po vieną klaidą.
4. Pirmą kartą naudodamiesi naršyklės įskiepiu, visi dalyviai užduotį atliko greičiau nei per vieną minutę. Naudojant antrąjį maketą, užduotis buvo įvykdyta dar greičiau – per mažiau nei 30 sekundžių.
5. 100 % dalyvių sugebėjo atlikti užduotį iš pirmo karto.
6. Daugumai dalyvių (8 iš 11, t. y. 72,7 %) antrasis maketas pasirodė intuityvesnis. Likusiai daliai (27,3 %) lengviau buvo naudotis pirmuoju maketu.

PIRMAS MAKETAS 5.3.1. Pranešimo apie nesaugią svetainę testavimas				ANTRAS MAKETAS 5.3.1. Pranešimo apie nesaugią svetainę testavimas			
ID	Laikas	Klaidos	Pagalbos kreipimasis	ID	Laikas	Klaidos	Pagalbos kreipimasis
1	13, 12 s	0	-	1	11, 09 s	0	-
2	20, 43 s	1	-	2	10, 23 s	0	-
3	9, 08 s	0	-	3	7, 02 s	0	-
4	7, 49 s	0	-	4	6, 27 s	0	-
5	6, 45 s	0	-	5	9, 18 s	0	-
6	35, 02s	1	-	6	26, 12 s	1	-
7	11, 18 s	0	-	7	27,20 s	0	-
8	12, 14 s	0	-	8	11, 34 s	0	-
9	38, 36 s	0	-	9	19, 33 s	0	-
10	21, 6 s	1	-	10	17, 76 s	0	-
11	9, 0 s	0	-	11	7, 23 s	0	-

30 pav. Pranešimo apie nesaugią svetainę testavimo rezultatai

31 pav. Maketų intuityvumo rezultatai pirmai užduočiai atlikti

Remiantis testavimo išvadomis bei rezultatais galime teigti, kad antrasis maketas šiai užduočiai atlikti naudotojams buvo intuityvesnis ir turėtų būti naudojamas projektuojant detalųjį prototipą.

5.7.3. Įspėjimų elektroniniame laiške apie potencialias duomenų viliojimo atakas testavimo išvados

Išvados suformuluotos remiantis sudaryta testavimo rezultatų lentele (žr. 32 paveikslą) bei dalyvio klausimynais po panaudojamumo testavimo (žr. 33 paveikslą):

1. Visi testavimo dalyviai, naudodamiesi antruoju maketu, įsiminė daugiau duomenų viliojimo atakų požymių nei kad pirmuoju.
2. Visi testavimo dalyviai sėkmingai atliko užduotį savarankiškai, nesikreipdami pagalbos.
3. Testavimo dalyviai įvardijo antrojo maketo trūkumą, teigdami, kad paspaudus elektroniniame laiške ant nesaugios nuorodos norėtųsi matyti ne tik išvardytus įtartinus požymius, bet ir pačią nuorodą.
4. Visiems testavimo dalyviams (11 iš 11, t. y. 100 %) antrasis maketas pasirodė intuityvesnis, nes šiame makete įskiepio naudotojas gali peržiūrėti įtartinus požymius dar nepaspaudęs ant nuorodos.

PIRMAS MAKETAS 5.3.2. Įspėjimų elektroniniame laiške apie potencialias duomenų viliojimo atakas testavimas		ANTRAS MAKETAS 5.3.2. Įspėjimų elektroniniame laiške apie potencialias duomenų viliojimo atakas testavimas	
ID	Prisimintų požymių skaičius	ID	Prisimintų požymių skaičius
1	2	1	3
2	4	2	5
3	3	3	5
4	4	4	5
5	4	5	5
6	0	6	2
7	1	7	3
8	3	8	3
9	1	9	3
10	3	10	3
11	4	11	5

32 pav. Įspėjimų elektroniniame laiške apie potencialias duomenų viliojimo atakas testavimo rezultatai

33 pav. Maketų intuityvumo rezultatai antrai užduočiai atlikti

Remiantis testavimo išvadomis bei rezultatais galima teigti, kad antrasis maketas šiai užduočiai atlikti naudotojams buvo intuityvesnis ir turėtų būti naudojamas projektuojant detalųjį prototipą, atsižvelgiant ir į testavimo dalyvių išsakytus trūkumus.

5.7.4. Naudotojo gebėjimo atpažinti saugią svetainę, remiantis spalvų piktogramomis, testavimo išvados

Šios testavimo išvados suformuluotos remiantis sudaryta testavimo rezultatų lentele (žr. 34 paveikslą) bei dalyvio klausimynais po panaudojamumo testavimo (žr. 35 paveikslą):

1. Penki testavimo dalyviai suklydo rinkdamiesi, jų manymu, saugią svetainę, prie kurios nebuvo piktogramų, indikuojančių svetainės saugumą, tačiau testuojant maketą, kuriame buvo rodomi indikatoriai, visi testavimo dalyviai gebėjo pasirinkti teisingai.
2. Visi testavimo dalyviai sėkmingai atliko užduotį savarankiškai, nesikreipdami pagalbos.
3. Dalyviai, pasižymintys mažu kompiuterinio raštingumo lygmeniu, testavimo metu pamatę panašiai atrodančias svetainių nuorodas, rinkosi pačią pirmąją, nors tai buvo nuoroda, vedanti į nesaugią svetainę.
4. Visiems testavimo dalyviams (11 iš 11, t. y. 100 %) antrasis maketas pasirodė intuityvesnis, nes naudojami svetainių saugumo indikatoriai buvo lengviau atpažįstami.
5. Ekspertų grupės dalyviai įvardijo, kad būtų gerai, jog paspaudus ant indikatoriaus būtų parodoma įskiepio naudotojui, kodėl yra pasirinktas konkretus indikatorius, kokie požymiai indikuoja apie galimai nesaugią svetainę.

PIRMAS MAKETAS 5.3.3. Naudotojo gebėjimo atpažinti saugią svetainę, remiantis spalvų piktogramomis, testavimas			ANTRAS MAKETAS 5.3.3. Naudotojo gebėjimo atpažinti saugią svetainę, remiantis spalvų piktogramomis, testavimas		
ID	Svetainės pasirinkimas	Saugios svetainės atpažinimas	ID	Svetainės pasirinkimas	Saugios svetainės atpažinimas
1	+	+	1	+	+
2	+	+	2	+	+
3	+	+	3	+	+
4	+	+	4	+	+
5	+	+	5	+	+
6	-	+	6	-	+
7	-	+	7	-	+
8	-	+	8	-	+
9	-	+	9	-	+
10	-	+	10	-	+
11	+	+	11	+	+

34 pav. Naudotojo gebėjimo atpažinti saugią svetainę, remiantis spalvų piktogramomis, testavimo rezultatai

35 pav. Maketų intuityvumo rezultatai trečiai užduočiai atlikti

Apibendrinant, antrasis maketas šiai užduočiai atlikti naudotojams buvo intuityvesnis ir turėtų

būti naudojamas projektuojant detalųjį prototipą, atsižvelgiant ir į testavimo dalyvių (ekspertų) išsakytus tobulintinus funkcionalumus.

5.7.5. Naudotojo gebėjimo identifikuoti svetainės saugumą pagal įrankių juostos piktogramą testavimo išvados

Šios testavimo išvados suformuluotos remiantis sudaryta testavimo rezultatų lentele (žr. 36 paveikslą) bei dalyvio klausimynais po panaudojamumo testavimo (žr. 37 paveikslą):

1. Visi testavimo dalyviai (11 iš 11, t. y. 100 %), remdamiesi įrankių juostoje esančia piktograma, gebėjo įvardyti, ar lankosi saugioje, ar nesaugioje svetainėje.
2. Visi testavimo dalyviai sėkmingai atliko užduotį savarankiškai, nesikreipdami pagalbos.
3. Daugumai dalyvių (10 iš 11, t. y. 90,9 %) antrasis maketas pasirodė intuityvesnis. Likusiai daliai (9,1 %) lengviau buvo naudotis pirmuoju maketu.
4. Keletas testavimo dalyvių įvardijo, kad naudojant pirmą kartą naršyklės įskiepį sunku yra pastebėti įrankių juostoje esančias piktogramas, ir mano, kad prieš naudojantis norėtų būti informuojami, kad naršyklės saugumo indikatorius galima rasti įrankių juostoje dešiniame kampe.

PIRMAS MAKETAS 5.3.4. Naudotojo gebėjimo identifikuoti svetainės saugumą pagal įrankių juostos piktogramą testavimas			ANTRASIS MAKETAS 5.3.4. Naudotojo gebėjimo identifikuoti svetainės saugumą pagal įrankių juostos piktogramą testavimas		
ID	Svetainės saugumo atpažinimas	Svetainės saugumo atpažinimas	ID	Svetainės saugumo atpažinimas	Svetainės saugumo atpažinimas
1	+	+	1	+	+
2	+	+	2	+	+
3	+	+	3	+	+
4	+	+	4	+	+
5	+	+	5	+	+
6	+	+	6	+	+
7	+	+	7	+	+
8	+	+	8	+	+
9	+	+	9	+	+
10	+	+	10	+	+
11	+	+	11	+	+

36 pav. Naudotojo gebėjimo identifikuoti svetainės saugumą pagal įrankių juostos piktogramą testavimo rezultatai

37 pav. Maketų intuityvumo rezultatai ketvirtai užduočiai atlikti

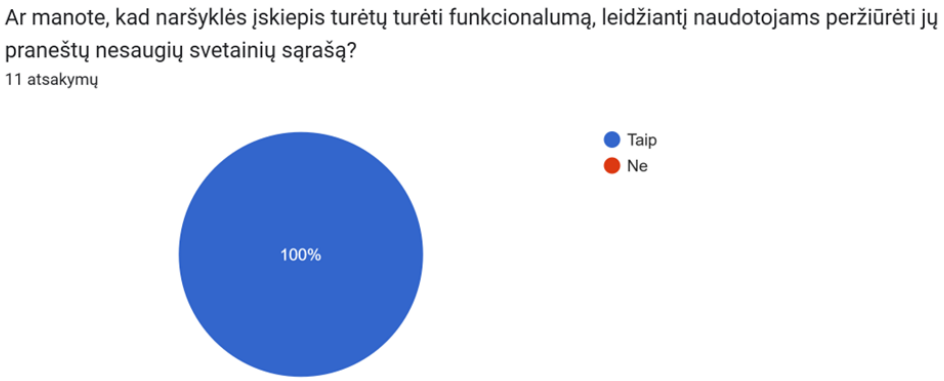
Analizuojant gautus rezultatus paaiškėjo, kad antrasis maketas šiai užduočiai atlikti naudotojams buvo intuityvesnis ir turėtų būti naudojamas projektuojant detalųjį prototipą.

5.7.6. Naršyklės įskiepio piktogramos, nurodančios praneštų svetainių sąrašą, funkcionalumo testavimo išvados

1. Visi testavimo dalyviai, naudodamiesi naršyklės funkcionalumu peržiūrėti praneštų svetainių sąrašą, užduotį gebėjo atlikti per ne ilgiau nei 1 minutę.
2. Visi testavimo dalyviai (11 iš 11, t. y. 100 %) teigė, kad naršyklės įskiepis turėtų turėti funkcionalumą, leidžiantį naudotojams peržiūrėti jų praneštų nesaugių svetainių sąrašą.
3. 100 % naudotojų sugebėjo užduotį atlikti iš pirmo karto.
4. Visi testavimo dalyviai sėkmingai atliko užduotį savarankiškai, nesikreipdami pagalbos.
5. Testavimo dalyviai įvardijo maketo trūkumą, teigdami, kad praneštų svetainių sąrašo peržiūros mygtukas galėtų būti be „X“ tiesiog sąrašo logotipas, nes dalyviams makete esantis sąrašo mygtukas labiau asocijavosi su išjungimo mygtuku.

ANTRASIS MAKETAS 5.3.5. Naršyklės įskiepio piktogramos, nurodančios praneštų svetainių sąrašą, funkcionalumo testavimas			
ID	**Laikas**	**Klaidos**	**Pagalbos kreipimasis**
1	12,27 s	0	0
2	15,18 s	0	0
3	9,03 s	0	0
4	9,34 s	0	0
5	6,09 s	0	0
6	27,28 s	0	0
7	25,32 s	0	0
8	12,0s	0	0
9	17,30 s	0	0
10	40,38 s	0	0
11	6,02 s	0	0

38 pav. Naršyklės įskiepio piktogramos, nurodančios praneštų svetainių sąrašą, funkcionalumo testavimo rezultatai



39 pav. Maketų intuityvumo rezultatai penktai užduočiai atlikti

Išanalizavus testavimo rezultatus, matyti, kad naršyklės įskiepis turėtų turėti funkcionalumą, leidžiantį naudotojams peržiūrėti jų praneštų nesaugių svetainių sąrašą, todėl šis funkcionalumas turėtų būti naudojamas projektuojant detalųjį prototipą, tačiau reikėtų atsižvelgti į testavimo dalyvių rekomendacijas pakeisti svetainių sąrašo peržiūros mygtuko piktogramą.

5.7.7. Panaudojamumo testavimo išvados

1. Iš panaudojamumo testavimo metu gautų rezultatų galima matyti, kad naudotojai, turintys žemą kompiuterinio raštingumo lygį, dažnai neatsižvelgia į URL svetainės nuorodas ir intuityviai renkasi pirmąjį naršyklės paieškoje pateiktą rezultatą. Dėl šios priežasties reikia, kad naršyklės įskiepis šalia kiekvienos svetainės nuorodos turėtų piktogramą, nurodančią svetainės saugumo lygį. Tačiau norint užtikrinti, kad naudotojai tinkamai supras šias piktogramas, svarbu, kad jie būtų supažindinti su jų reikšmėmis, todėl įrankis turėtų turėti mokomąją medžiagą arba naudotojo vadovą.
2. Testavimo rezultatai taip pat parodė, kad naudotojams kur kas lengviau įsiminti duomenų viliojimo atakas indikuojančius požymius, kai šie požymiai yra pateikiami kartu su pavyzdžiais. Pavyzdžiui, elektroniniame laiške šalia kiekvieno požymio, rodančio galimą ataką, esanti įspėjamoji piktograma ne tik atkreipia naudotojų dėmesį į šį požymį, bet ir padeda jį lengviau įsiminti. Tai rodo, kad vizualiniai elementai, derinami su paaiškinimais, gali žymiai pagerinti naudotojų gebėjimą atpažinti grėsmes.
3. Testavimo dalyviai minėjo, kad jiems nepatinka, kai jie yra perklausiami, ar tikrai nori atlikti konkretų veiksmą, ypač situacijose, kurios nekelia grėsmės jų duomenų saugumui. Todėl įskiepio funkcionalumas, leidžiantis naudotojui pranešti apie galimai nesaugią svetainę, turėtų būti suprojektuotas taip, kad naudotojas galėtų atlikti šį veiksmą be papildomų patvirtinimų. Tai padidintų naudotojo patogumą ir pagerintų jo naudojimosi patirtį.
4. Iš ekspertų išsakytų pasiūlymų maketams tobulinti paaiškėjo, kad daugiau patirties turintys naudotojai, t.y. ekspertai, supranta, jog naudotojui svarbu ne tik matyti įspėjančiąją piktogramą, bet ir žinoti, kodėl ji buvo pasirinkta būtent tokia. Todėl kuriamas įrankis turėtų suteikti galimybę naudotojui, paspaudus ant piktogramos, peržiūrėti žodinį paaiškinimą, kuris pateiktų informaciją apie pasirinktos piktogramos priežastį. Tai ne tik padidintų naudotojo pasitikėjimą naršyklės įskiepiu, bet ir suteiktų jam daugiau aiškumo bei mokytų patį naudotoją atpažinti galimas rizikas naršant internete.
5. Testavimo rezultatai parodė, kad naudotojai yra linkę geriau atpažinti ir suprasti piktogramas, kurios jiems jau yra pažįstamos ir savaime suprantamos. Pavyzdžiui, testuojant sąrašo funkcionalumą, naudotojams, turintiems žemą kompiuterinio raštingumo lygį, kilo sunkumų suprantant makete naudotą sąrašo piktogramą. Tai lėmė tai, kad jie buvo įpratę matyti sąrašą žyminčią piktogramą, vaizduojančią tris horizontalius brūkšnelius. Todėl svarbu, kad įrankis naudotų naudotojui lengvai atpažįstamas piktogramas.

6. Tyrimas

Po panaudojamumo testavimo buvo atliktas papildomas kiekybinis tyrimas, kurio **tikslas** – išsiaiškinti, ar žmonės naudoja naršyklės įskiepius siekdami apsisaugoti nuo duomenų viliojimo (angl. *phishing*) atakų, kokios yra jų naudojimo ar nenaudojimo priežastys bei kaip būtų galima paskatinti tokių įrankių naudojimą siekiant didesnio kibernetinio saugumo.

Tyrimas buvo vykdomas nuotoliniu būdu – internetinėje erdvėje dalyviams buvo pateikta apklausos anketa. Apklausos klausimai buvo parengti taip, kad padėtų išsamiai įvertinti respondentų patirtis, įpročius bei požiūrį į naršyklės įskiepių naudojimą saugumo tikslais.

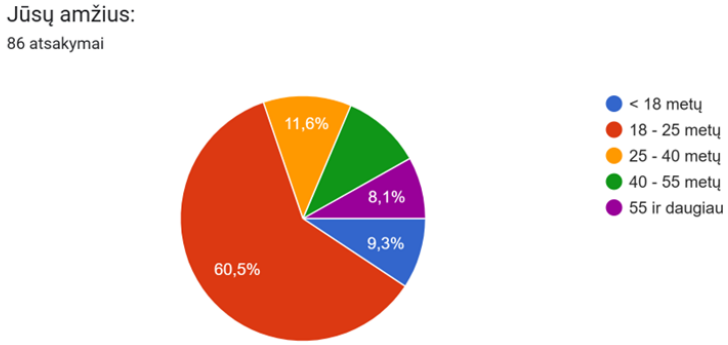
Tyrimas vyko **2025 m. kovo 19-31 d.** Per šį laikotarpį apklausą užpildė **86** respondentai. Surinkti duomenys padėjo geriau suprasti naudotojų elgseną ir iššūkius, susijusius su saugumo įrankių taikymu kasdienėje interneto naršymo praktikoje.

Nuoroda į **klausimyną: Naršyklės įskiepių naudojimas apsaugai nuo duomenų viliojimo atakų.**

6.1. Tyrimo dalyviai

6.1.1. Dalyvių amžius

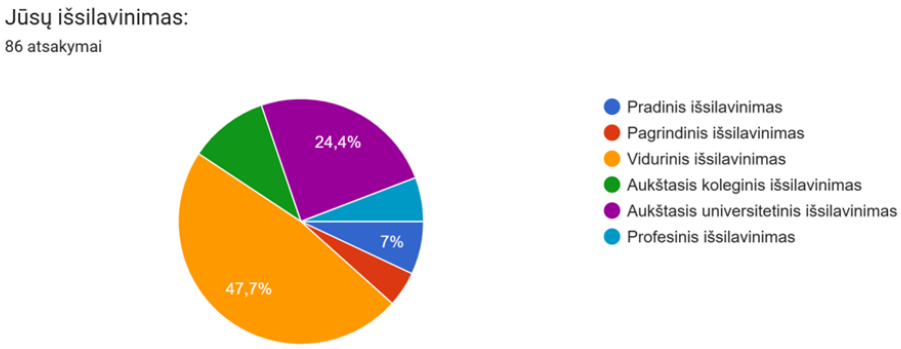
Didžioji dalis tyrimo dalyvių (52 iš 86, t. y. 60,5 %) buvo 18–25 metų amžiaus. Kitos amžiaus grupės pasiskirstė taip: 11,6 % sudarė 25–40 metų amžiaus asmenys, 10,5 % – 40–55 metų, 9,4 % – jaunesni nei 18 metų, o 8,1 % respondentų buvo 55 metų ir vyresni (žr. 40 paveikslą).



40 pav. Tyrimo dalyvių amžiaus pasiskirstymo skritulinė diagrama

6.1.2. Dalyvių išsilavinimas

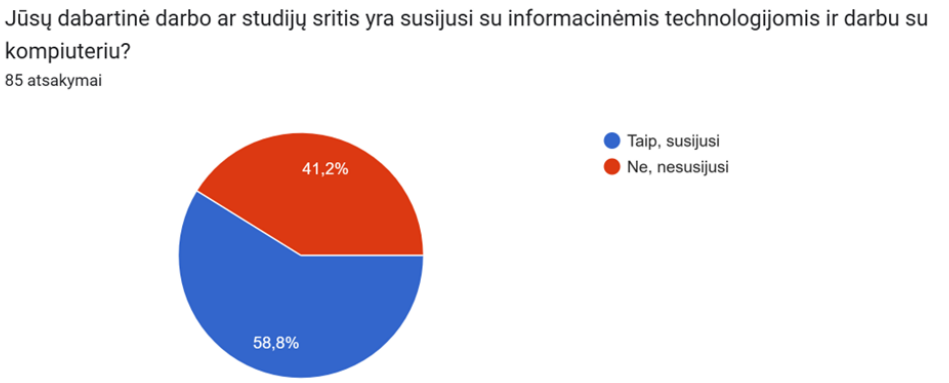
Tyrimo dalyvių išsilavinimas pasiskirstė taip: dauguma respondentų (41 iš 86, t. y. 47,7 %) buvo įgiję vidurinį išsilavinimą. Aukštąjį universitetinį išsilavinimą turėjo 24,4 % dalyvių, aukštąjį neuniversitetinį – 10,5 %. Pradinį išsilavinimą nurodė 7% respondentų, profesinį – 5,8%, o pagrindinį – 4,7 % (žr. 41 paveikslą).



41 pav. Tyrimo dalyvių išsilavinimo skritulinė diagrama

6.1.3. Dalyvių informacinių technologijų naudojimo gebėjimo lygmuo

Tyrimo duomenimis, 50 iš 86 respondentų (t. y. 58,8 %) nurodė, kad jų dabartinė darbo ar studijų sritis yra susijusi su informacinėmis technologijomis ir darbu su kompiuteriu. Likusieji 36 dalyviai (41,2 %) teigė, kad jų veikla nėra tiesiogiai susijusi su informacinių technologijų sritimi (žr. 42 paveikslą).



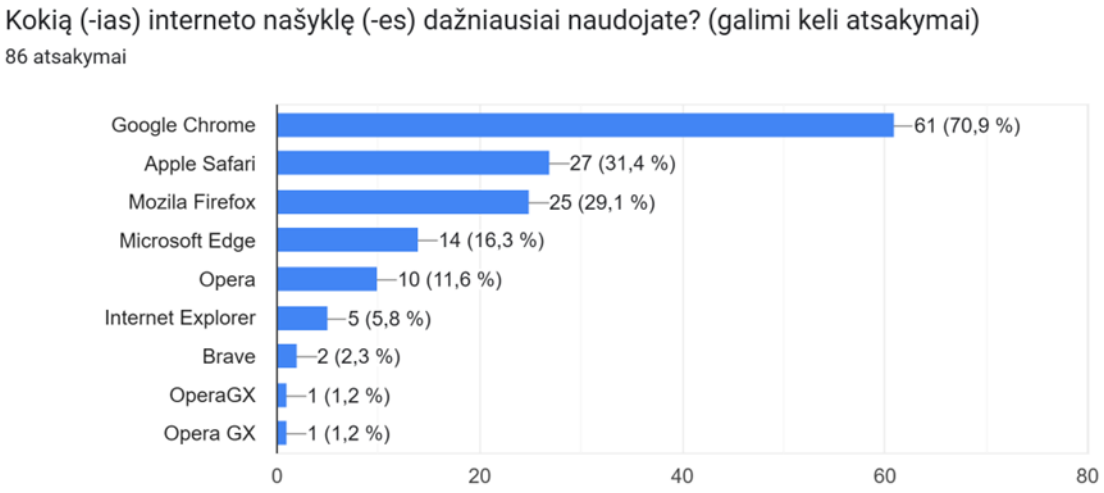
42 pav. Tyrimo dalyvių ryšio su technologijos skritulinė diagrama

6.1.4. Dalyvių dažniausiai naudojamos interneto naršyklės

Dauguma respondentų (61 iš 86, t. y. 70,9 %) dažniausiai naudoja interneto naršyklę „Google Chrome“. Antroje vietoje – „Apple Safari“, kurią naudoja 27 respondentai (31,4 %), o trečioje – „Mozilla Firefox“, kurią naudoja 25 dalyviai (29,1 %).

„Microsoft Edge“ naršyklę kaip pagrindinę nurodė 14 respondentų (16,3 %), o „Opera“ – 10 dalyvių (11,6 %). „Internet Explorer“ vis dar naudojasi 5 dalyviai (5,8 %), o retesnės naršyklės, tokios kaip „Brave“ ir „Opera GX“, buvo pasirinktos dviejų respondentų (po 2,3 %).

Pažymėtina, kad dalyviai galėjo pasirinkti daugiau nei vieną naršyklę, todėl procentų suma viršija 100 % (žr. 43 paveikslą).

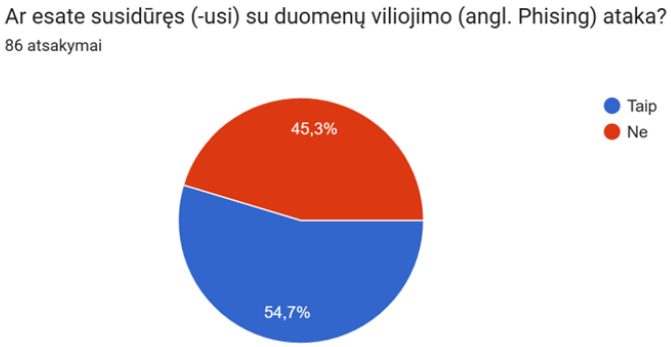


43 pav. Tyrimo dalyvių dažniausiai naudojamos interneto naršyklės pavaizduotos stulpeline diagrama

6.2. Dalyvių patirtis su duomenų viliojimo atakomis

6.2.1. Patirtis su duomenų viliojimo atakomis

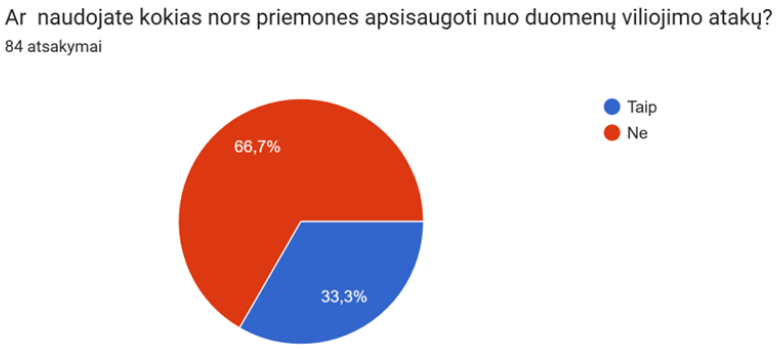
Paklausus respondentų, ar jie yra susidūrę su duomenų viliojimo atakomis, šiek tiek daugiau nei pusė (47 iš 86, t. y. 54,7 %) nurodė, kad yra susidūrę su tokiomis atakomis. Likusieji 45,3 % dalyvių teigė, kad nėra patyrę šių atakų (žr. 44 paveikslą).



44 pav. Tyrimo dalyvių susidūrimo su duomenų viliojimo atakomis pasiskirstymas pavaizduotas skrituline diagrama

6.2.2. Naudojamos apsaugos priemonės nuo duomenų viliojimo atakų

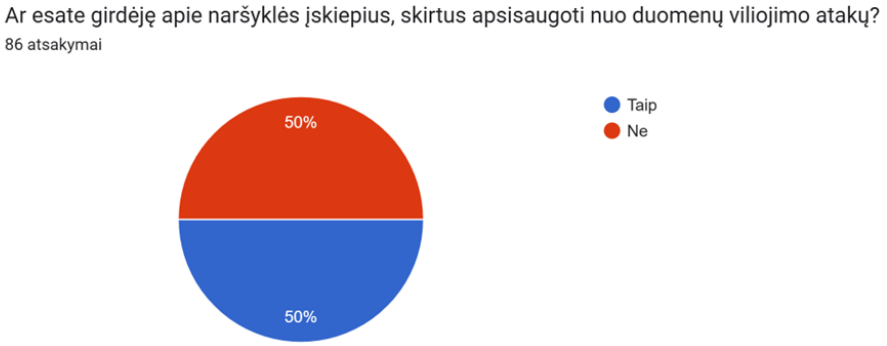
Dauguma apklaustųjų (56 iš 86, t. y. 66,7 %) nenaudoja jokių priemonių, skirtų apsisaugoti nuo duomenų viliojimo atakų. Visgi, likusieji 33 % respondentų naudoja apsaugos priemones (žr. 45 paveikslą).



45 pav. Tyrimo dalyvių, naudojančių ir nenaudojančių priemones apsaugai nuo duomenų viliojimo atakų, pasiskirstymas

6.2.3. Susipažinimas su naršyklės įskiepiais apsaugai nuo duomenų viliojimo atakų

Paklausus, ar tyrimo dalyviai yra girdėję apie naršyklės įskiepius, skirtus apsisaugoti nuo duomenų viliojimo atakų, respondentų atsakymai pasiskirstė tolygiai. 50 % dalyvių teigė, kad yra girdėję apie tokius įskiepius, o likusieji 50 % atsakė, kad nėra (žr. 46 paveikslą).



46 pav. Tyrimo dalyvių, susipažinimo su naršyklės įskiepiais, apsaugai nuo duomenų viliojimo atakų, pasiskirstymas

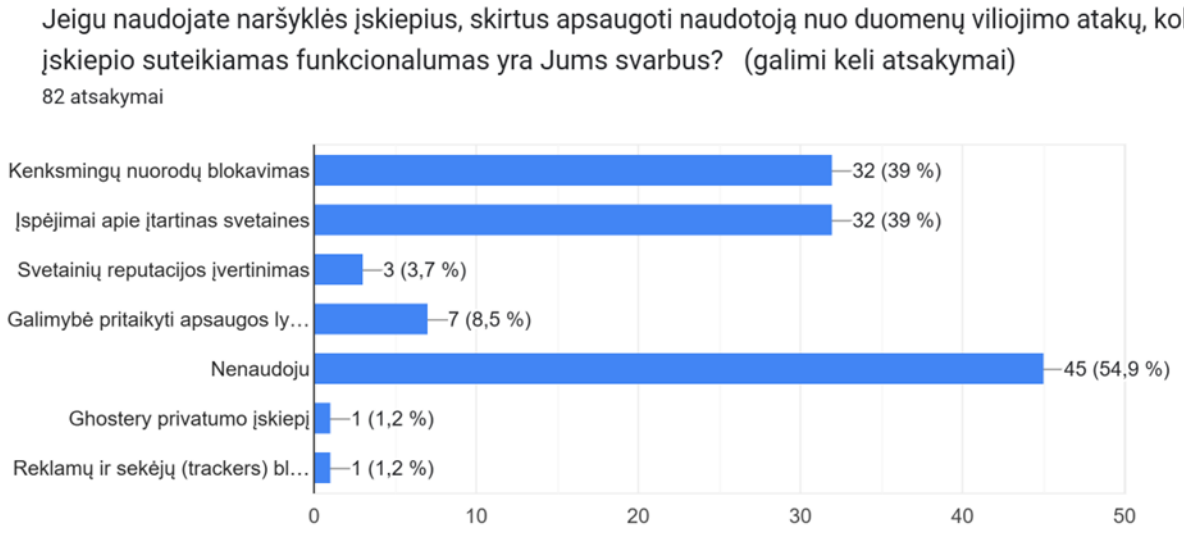
6.2.4. Tyrimo dalyviams svarbiausios naršyklės įskiepio suteikiamos funkcijos, skirtos apsaugai nuo duomenų viliojimo atakų

Dauguma respondentų (45 iš 86, t. y. 54,9 %) nurodė, kad nesinaudoja naršyklės įskiepiais, skirtais apsaugai nuo duomenų viliojimo atakų. 32 dalyviai (30 %) teigė, kad jiems svarbiausi funkcionalumai yra:

- kenksmingų nuorodų blokavimas,
- įspėjimai apie įtartinas svetaines.

Toliau septyni respondentai (8,5 %) išskyrė kaip svarbų funkcionalumą galimybę pritaikyti apsaugos lygį pagal poreikius. Trims respondentams (3,7 %) svarbus buvo svetainių reputacijos vertinimas,

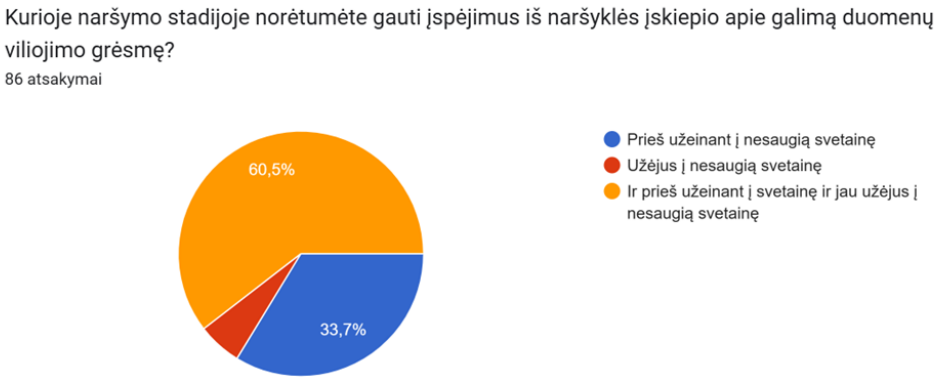
o vienas dalyvis nurodė, kad jam svarbus funkcionalumas yra reklamų ir sekėjų blokavimas (žr. 47 paveikslą).



47 pav. Tyrimo dalyvių pasirinktos svarbiausios funkcijos, suteikiamos naršyklės įskiepių, skirtos apsaugai nuo duomenų viliojimo atakų

6.2.5. Įspėjimų apie duomenų viliojimo grėsmes gavimo stadijos

Dauguma tyrimo dalyvių (52 iš 86, t. y. 60,5 %) nurodė, kad įspėjimus apie galimą duomenų viliojimo grėsmę norėtų gauti tiek prieš įeinant į svetainę, tiek jau užėjus į nesaugią svetainę. 33,7 % dalyvių pageidautų gauti įspėjimus tik prieš užeinant į nesaugią svetainę, o 5,8 % – tik užėjus į nesaugią svetainę (žr. 48 paveikslą).

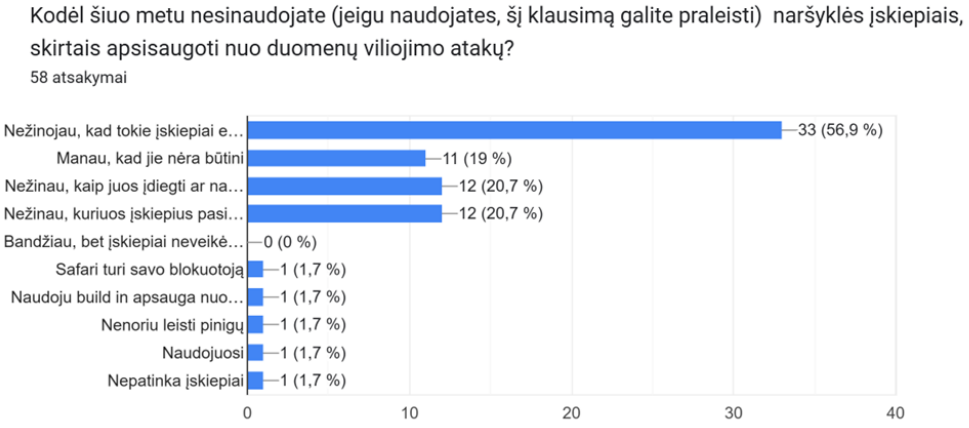


48 pav. Tyrimo dalyvių naršymo stadijos pasirinkimas gauti įspėjimus apie galimą duomenų viliojimo ataką

6.2.6. Priežastys, kodėl nesinaudojama naršyklės įskiepiais apsaugai nuo duomenų viliojimo atakų

Dauguma respondentų (56,9 %) nurodė, kad nesinaudoja naršyklės įskiepiais, nes nežinojo apie tokių įskiepių egzistavimą. 20,7 % dalyvių teigė, kad nesinaudoja dėl nežinojimo, kaip įsidiegti ar naudoti tokius įskiepius, arba nežino, kuriuos įskiepius reikėtų pasirinkti. 19 % apklaustųjų mano, kad tokie įskiepiai nėra būtini.

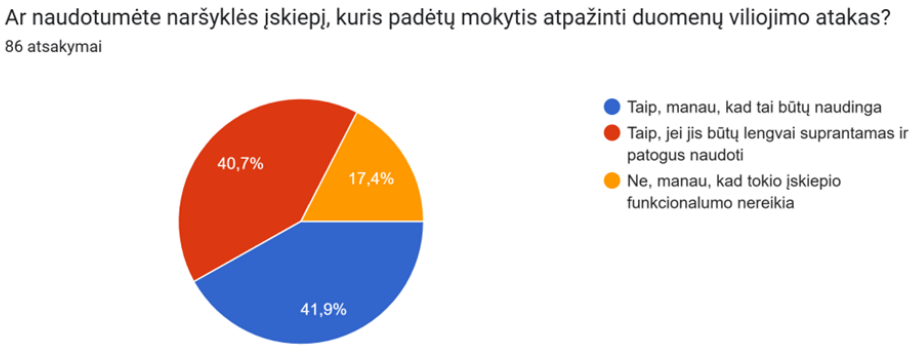
Vienas respondentų nurodė, kad nesinaudoja, nes naršyklė „Safari“ turi savo blokuotoją. Kitas dalyvis teigė, kad jau naudoja įdiegtą apsaugą nuo atakų, o dar vienas atsakė, kad nesinaudoja, nes nenori išleisti pinigų arba tiesiog nepatinka naršyklės įskiepiai (žr. 49 paveikslą).



49 pav. Tyrimo dalyvių priežastys, nurodančios, kodėl jie nesinaudoja naršyklės įskiepiais apsaugai nuo duomenų viliojimo atakų

6.2.7. Motyvacija naudoti naršyklės įskiepius, skirtus mokytis atpažinti duomenų viliojimo atakas

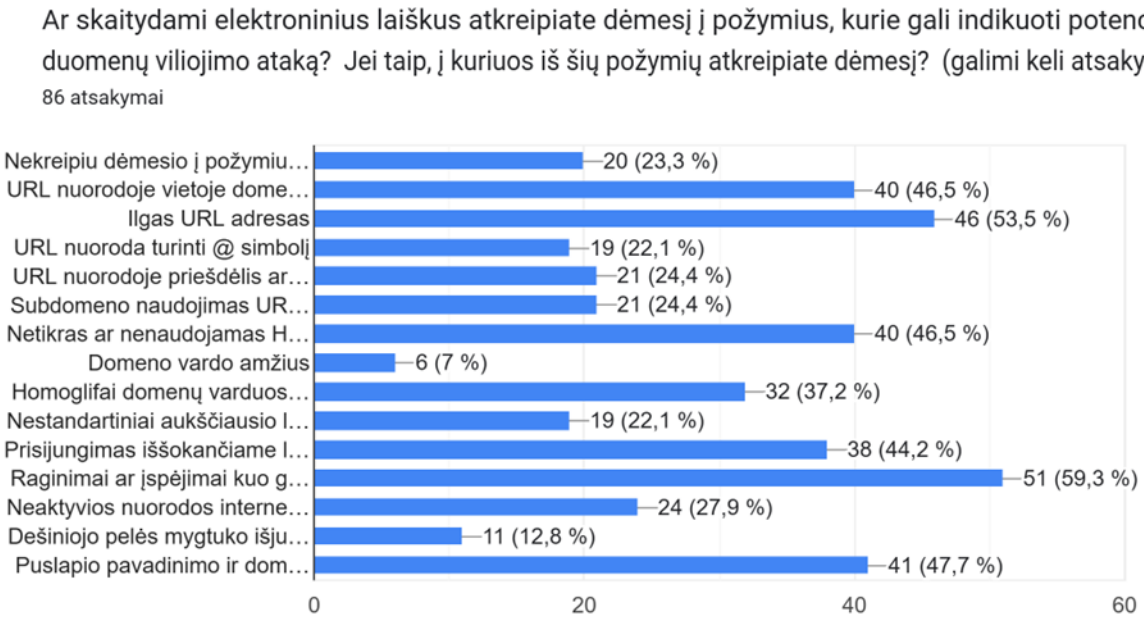
41,9 % visų apklaustųjų teigė, kad naršyklės įskiepis, padedantis mokytis atpažinti duomenų viliojimo atakas, būtų naudingas ir jie naudotųsi šiuo funkcionalumu. Šiek tiek mažesnė dalis, 40,7 %, nurodė, kad naudotųsi šiuo įskiepiu, jei jis būtų lengvai suprantamas ir patogus naudoti. Likę 17,4 % respondentų mano, kad nesinaudotų tokiu įskiepiu, nes laikosi nuomonės, kad toks funkcionalumas nėra reikalingas (žr. 50 paveikslą).



50 pav. Tyrimo dalyvių požiūris į naršyklės įskiepio naudojimą, padedantį mokytis atpažinti duomenų viliojimo atakas

6.3. Požymiai, į kuriuos dalyviai atkreipia dėmesį skaitydami elektroninius laiškus, galinčius indikuoti duomenų viliojimo atakas

- Dauguma tyrimo dalyvių (51 iš 86, t. y. 59,3 %) nurodė, kad atkreipia dėmesį į raginimus ar įspėjimus, skatinančius kuo greičiau atlikti veiksmus.
- 46 dalyviai (53,5 %) pažymėjo, kad atkreipia dėmesį į ilgą URL adresą.
- 41 dalyvis (47,7 %) teigė, kad atkreipia dėmesį į puslapio pavadinimo ir domeno vardo nesutapimą.
- 40 respondentų (46,5 %) nurodė, kad atkreipia dėmesį į IP adresų naudojimą vietoj domeno vardo ir į netikrą arba nenaudojamą HTTPS protokolą.
- 38 dalyviai (44,2 %) nurodė, kad atkreipia dėmesį į prisijungimo prašymus iššokančiame lange.
- 32 respondentai (37,2 %) teigė, kad atkreipia dėmesį į homoglifus domenų varduose.
- 24 dalyviai nurodė, kad atkreipia dėmesį į neaktyvias nuorodas internetinėse svetainėse.
- 21 dalyvis (24,4 %) pažymėjo, kad atkreipia dėmesį į URL nuorodose esantį „-“ simbolį priešdėliuose ir priesagose bei subdomenų naudojimą URL adresuose.
- 23,3 % apklaustųjų nurodė, kad iš viso nekreipia dėmesio į galimus požymius.
- 19 dalyvių (22,1 %) teigė, kad atkreipia dėmesį į URL nuorodą, turinčią @ simbolį, ir į nestandartinius aukščiausio lygio domenus.
- Tik 11 respondentų (12,8 %) nurodė, kad atkreipia dėmesį į dešiniojo pelės mygtuko išjungimą.
- Mažiausiai respondentų (tik 6, t.y. 7 %) atkreipia dėmesį į domeno vardo amžių (žr. 51 paveikslą).

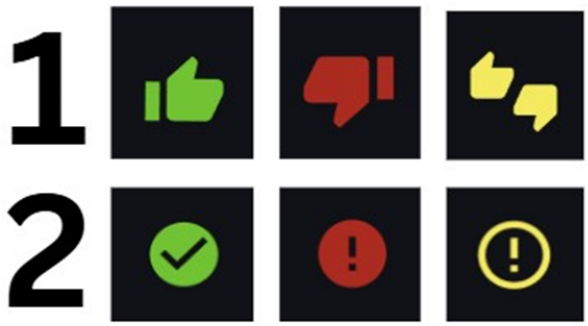


51 pav. Tyrimo dalyvių atkreipiamas dėmesys į potencialius duomenų viliojimo atakų požymius elektroniniuose laiškuose

6.4. Alternatyvieji maketai

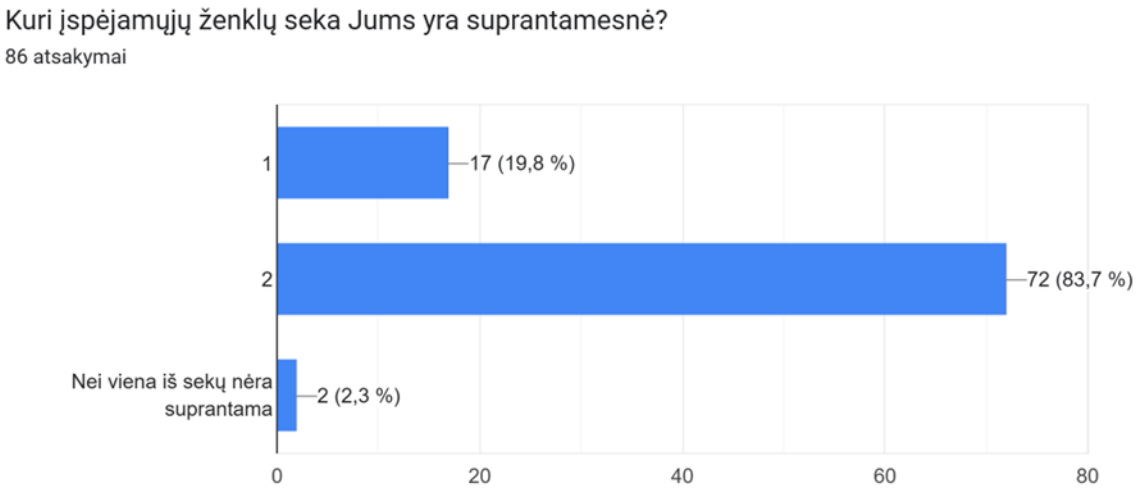
6.4.1. Maketuose naudojamų įspėjamųjų ženklų suprantamumas

Tyrimo dalyviai buvo paklausti, kuri įspėjamųjų ženklų seka, naudojama alternatyviuose maketuose, jiems yra suprantamesnė. Pirmoji įspėjamųjų ženklų seka buvo naudojama pirmame alternatyviame makete, o antroji – antrajame makete (žr. 52 paveikslą).



52 pav. Įspėjamųjų ženklų seka

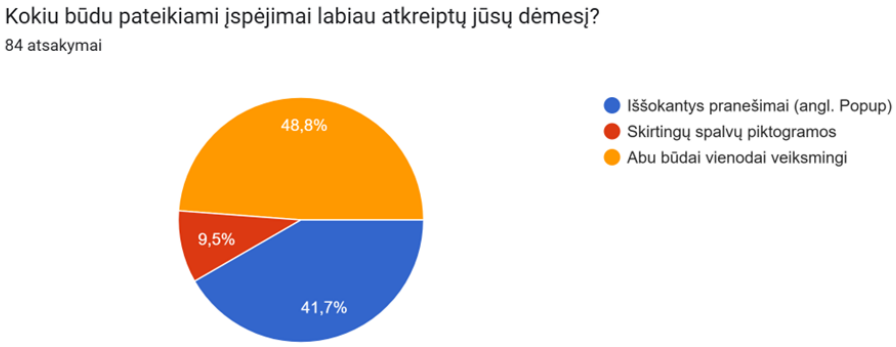
Didžioji dalis respondentų (72 iš 86, t. y. 83,7 %) nurodė, kad antroji įspėjamųjų ženklų seka buvo suprantamesnė. 17 dalyvių (19,8 %) pažymėjo, kad pirmoji seka buvo jiems aiškesnė. Tik du respondentai teigė, kad nė viena iš sekų jiems nėra suprantama (žr. 53 paveikslą).



53 pav. Tyrimo dalyvių pasirinkimų pasiskirstymas, atvaizduojantis suprantamesnės įspėjamųjų ženklų sekos rezultatus

6.4.2. Įspėjimų pateikimo būdai

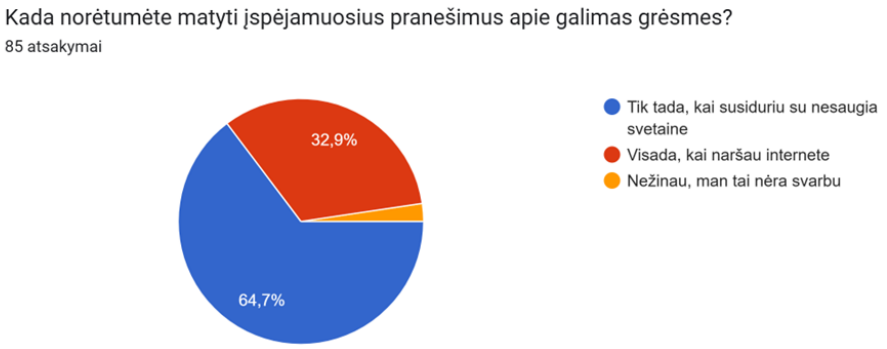
Tyrimo dalyvių paklausus, kokiu būdu pateikiami įspėjimai labiau atkreiptų jų dėmesį, daugiau nei pusė respondentų (41 iš 86, t. y. 48,8 %) nurodė, kad tiek iššokantys pranešimai, tiek skirtingų spalvų piktogramos yra vienodai veiksmingi būdai. Šiek tiek mažesnė dalis apklaustųjų (41,7 %) teigė, kad jų dėmesį labiau patrauktų iššokantys pranešimai, o 9,5 % respondentų mano, kad jų dėmesį labiau atkreiptų skirtingų spalvų piktogramos (žr. 54 paveikslą).



54 pav. Tyrimo dalyvių pasirinkimai apie įspėjimų pateikimo būdus, kurie labiausiai atkreiptų dėmesį

6.4.3. Pageidaujamas įspėjimų apie grėsmes rodymo momentas

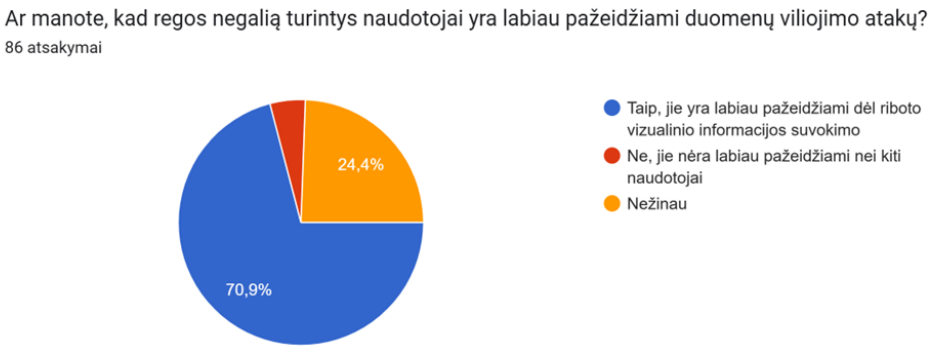
Didžioji dalis tyrimo dalyvių (55 iš 86, t. y. 64,7 %) nurodė, kad įspėjamuosius pranešimus apie galimas grėsmes norėtų matyti tik tada, kai susiduria su nesaugia svetaine. 32,9 % apklaustųjų pageidautų matyti įspėjimus visada, kai naršo internete, o likusi dalis dalyvių nežino, nes jiems tai nėra svarbu (žr. 55 paveikslą).



55 pav. Tyrimo dalyvių pasirinkimai dėl įspėjimų apie galimas grėsmes rodymo momento

6.4.4. Regos negalią turinčių naudotojų pažeidžiamumas dėl duomenų viliojimo atakų

Didžioji dalis tyrimo dalyvių (61 iš 86, t. y. 70,9 %) mano, kad regos negalią turintys naudotojai yra labiau pažeidžiami dėl riboto vizualinio informacijos suvokimo. Mažesnė dalis (21 iš 86, t. y. 24,4 %) nurodė, kad nežino, o likusi dalis respondentų teigė, kad regos negalią turintys naudotojai nėra labiau pažeidžiami nei kiti naudotojai.



56 pav. Tyrimo dalyvių nuomonių pasiskirstymas apie regos negalią turinčių naudotojų pažeidžiamumą dėl duomenų viliojimo atakų

6.5. Tyrimo apibendrinimas

1. Nors dauguma respondentų (54,7 %) yra patyrę duomenų viliojimo atakas, tik nedidelė dalis (33,3 %) imasi veiksmų apsisaugoti nuo jų. Tai rodo, kad, nors naudotojai yra susidūrę su duomenų viliojimo atakomis, jie galbūt nėra pakankamai informuoti apie galimus apsaugos įrankius arba nesuvokia šių grėsmių rimtumo. Apklausos rezultatai atskleidžia, kad dauguma dalyvių nesinaudoja naršyklės įskiepiais, nes nežino apie jų egzistavimą (56,9 %). Be to, dalis respondentų (po 20,7 %) nurodė, kad nežino, kaip įsidiegti ar naudoti tokius įskiepius, arba nesugeba pasirinkti tinkamų įrankių. Dar 19 % dalyvių teigia, kad nemato poreikio naudoti šių įskiepių, kas rodo, kad jie nesuvokia galimų grėsmių pasekmių.

2. Dauguma tyrimo dalyvių teigė, kad atkreipia dėmesį skaitydami elektroninius laiškus į požymius, galinčius indikuoti duomenų viliojimo atakas, tačiau nėra nė vieno požymio, kurį pastebėtų visi apklaustieji. Pavyzdžiui, kai kurie dalyviai neatkreipia dėmesio į tokius požymius kaip: dešiniojo pelės mygtuko išjungimas ar domeno vardo amžius, o 23,3 % visų apklaustųjų nurodė, kad iš viso nekreipia dėmesio į galimus požymius. Tai rodo, kad siekiant užtikrinti naudotojų saugumą, reikėtų įrankio, kuris automatiškai atpažintų visus paminėtus požymius ir įspėtų naudotoją apie galimas grėsmes, arba mokytų naudotoją patį šių požymių atpažinimo, kadangi dauguma naudotojų (41,7 %) nurodė, kad toks funkcionalumas būtų naudingas ir dar 41,7 % tyrimo dalyvių naudotų tokį įskiepį, jei jis būtų lengvai suprantamas ir patogus naudoti.
3. Iš apklausos rezultatų matyti, kad naudotojai yra labiau įpratę reaguoti į šviesoforo spalvų įspėjamuosius ženklus, kurie jiems yra pažįstami ir kuriuos jie jau yra matę anksčiau. Pavyzdžiui, raudonos spalvos apskritimas su šauktuku aiškiai signalizuoja įspėjimą apie galimas rizikas, o varnelė žaliame apskritime dažniausiai asocijuojasi su saugia svetaine. Nykščio formos piktogramos dažnai sukelia asociacijas su socialinių tinklų patiktukais, o ne su saugumo įspėjimais. Tai rodo, kad pažįstamų ir plačiai naudojamų simbolių taikymas gali būti kur kas efektyvesnis, nes naudotojai greičiau juos atpažįsta ir teisingiau juos interpretuoja.
4. Apklausos rezultatai taip pat atskleidžia, kad dauguma naudotojų mano, jog regos negalią turintys naudotojai yra labiau pažeidžiami dėl riboto vizualinio informacijos suvokimo. Tačiau iššūkių dėl duomenų viliojimo atakų kyla ir gerą regą turintiems naudotojams, kurie neretai nepastebi požymių, galinčių indikuoti atakas. Todėl svarbu, kad įrankis būtų pritaikytas visiems naudotojams ir turėtų specialų režimą, kuriame būtų naudojamos spalvos, pritaikytos regos negalią turintiems asmenims. Tai leistų šiems naudotojams lygiavertiškai naudotis naršyklės įskiepiu ir efektyviai apsisaugoti nuo grėsmių, kaip ir kitiems vartotojams.

7. Patikslintos projektavimo gairės

Remiantis panaudojamumo testavimo ir tyrimo rezultatais, patikslintos projektavimo gairės. Patikslinimai yra pridėti **mėlynos spalvos** šriftu.

1. **Kriterijus PK.1. Svetainės autentiškumo tikrinimas ir naudotojo edukacija.** Įrankis turėtų tikrinti svetainės autentiškumą naudotojui dar prieš užeinant į svetainę, **naudotojui užeinant į svetainę** taip pat, naudotojui jau užėjus į svetainę ir mokyti naudotojus, kad šie patys atpažintų galimas duomenų viliojimo atakas ir nevestų savo jautrių duomenų sukčiavimo svetainėse. **Naudotojų mokymui duomenų viliojimo atakų atpažinimo požymiai turėtų būti pateikiami kartu su pavyzdžiais.**
2. **Kriterijus PK.2. Vizualinių įspėjimų aiškumas ir atpažįstamumas.** Įrankyje naudojamos piktogramos spalvos turėtų būti lengvai atpažįstamos, tinka naudoti standartinio šviesoforo įspėjamąsias spalvas, dar geriau, jeigu įrankis naudotų aktyviuosius indikatoriais su lengvai išmokstamais ir atpažįstamais nurodymais ir įspėjimais. **Įrankis turėtų suteikti galimybę naudotojui paspausti ant įspėjamųjų piktogramų ir peržiūrėti žodinį paaiškinimą, kodėl pasirinkta būtent tokios spalvos įspėjamoji piktograma.**
3. **Kriterijus PK.3. Naudotojo veiksmų valdymas ir sprendimų patvirtinimas.** Projektuojamas įrankis turėtų leisti naudotojui anuliuoti ir pakartoti savo veiksmus. Tai reiškia, kad kai naudotojas užeina į nesaugią svetainę ir įrankis apie tai įspėja naudotoją, naudotojas turi turėti galimybę arba išeiti iš svetainės, arba pasilikti joje, tačiau jeigu naudotojas nusprendžia pasilikti svetainėje, įrankis turėtų perklausti, ar naudotojas tikrai nori ir yra įsitikinęs, kad nori lankytis nesaugioje svetainėje. **Tais atvejais, kai nekeliama grėsmė naudotojo saugumui, įrankis neturėtų perklausti naudotojo, ar jis tikrai nori / yra įsitikinęs savo pasirinkimu. Pavyzdžiui, pranešant apie nesaugią svetainę.**
4. **Kriterijus PK.4. Pritaikomumas įvairioms naršyklėms.** Projektuojamas įrankis kiek įmanoma labiau turėtų būtų pritaikytas skirtingoms naršyklėms. Tai reiškia, kad kuriamo įrankio kalba, indikatoriai, veiksmai turėtų būti suprantami naudotojams, nepriklausomai nuo to, kokią naršyklę naudotojas yra įpratęs naudoti. **Įrankis, kiek tai įmanoma, turėtų naudoti naudotojams lengvai atpažįstamas ir suprantamas piktogramas, kurios yra plačiai naudojamos ir kitose sistemose ar programėlėse.**
5. **Kriterijus PK.5. Įspėjimai ir pagalba prieš ir po apsilankymo svetainėje.** Projektuojamas įrankis turėtų teikti įspėjimus ir patarimus, kaip ištaisyti klaidas (kaip išeiti iš puslapio, į ką atkreipti dėmesį), ir tai turėtų daryti prieš naudotojui užeinant į svetainę, **naudotojui bandant užeiti į svetainę** ir naudotojui užėjus į svetainę.
6. **Kriterijus PK.6. Aiškūs ir tiesiogiai pasiekiami įspėjimai.** Projektuojamas įrankis turi turėti įspėjimus ir patarimus, kaip apsisaugoti nuo duomenų viliojimo atakų ir tie patarimai turi būti aiškūs ir suprantami bei rodomi iš karto (o ne paspaudus ant dar vienos nuorodos, ar nuėjus į dar vieną svetainę).
7. **Kriterijus PK.7. Galimybė praleisti pasikartojančius veiksmus patyrusiems naudotojams.** Jeigu projektuojamame įrankyje būtų galimybė naudotojams atlikti

veiksmus, kurie nekeltų pavojaus jų saugumui internete, būtų gerai, jeigu projektuojamas įrankis turėtų galimybę patyrusiems naudotojams praleisti pasikartojančius veiksmus.

8. **Kriterijus PK.8. Tikslinė informacija naudotojo sąsajoje.** Projektuojamame įrankyje turėtų būti tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų. Įrankio vizualinės dalies neturėtų užimti su saugumu nesusiję indikatoriai, logotipai ar reklamos.
9. **Kriterijus PK.9. Prieinama pagalba ir mokomoji medžiaga.** Projektuojamas įrankis turėtų turėti bent jau prieinamą dokumentaciją ar mokomąją medžiagą, kad naudotojai galėtų pasiskaityti apie funkcionalumus **ir naudojamas piktogramas** bei mokėtų patys savarankiškai įsidiegti įrankį savo kompiuteryje.
10. **Kriterijus DK.1. Pritaikymas regos negalią turintiems naudotojams. Regos negalią turintys naudotojai turėtų galėti persijungti spalvų režimą, pritaikytą jų poreikiams, ir režimo pakeitimo mygtukas turėtų būti naudojamas standartinis, visuotinai pripažintas.**
11. **Kriterijus DK.2. Prieinamumas** Projektuojamas įrankis turėtų būti nemokamas ir lengvai prieinamas visiems naudotojams ar organizacijoms.
12. **Kriterijus DK.3. Suderinanumas su standartinėmis priemonėmis.** Projektuojamas įrankis turėtų veikti naudojant standartinius įrankius ar naršykles be papildomų diegimų.
13. **Kriterijus DK.4. Praktinis taikymas realiose situacijose.** Projektuojamas įrankis turėtų būti išbandytas naudotojų, naudojamas realiomis sąlygomis, realiai apsaugai nuo duomenų viliojimo atakų, ne tik mokslinių tyrimų tikslais.
14. **Kriterijus DK.5. Prieinamumas nemokant autorinio atlyginimo.** Projektuojamas įrankis turėtų būti prieinamas kiekvienam naudotojui ir juo turi būti galima naudotis nemokant už tai autorinio atlyginimo.
15. **Techninių sprendimų integracija ir naudotojo švietimas.** Projektuojamas įrankis turėtų naudoti bent tris iš keturių techninių sprendimų. Įrankis turėtų gebėti atpažinti jau žinomas duomenų viliojimo atakas (naudoti juoduosius / baltuosius sąrašus), turėtų gebėti atpažinti naujas duomenų viliojimo atakas (naudoti euristikomis grįstą atpažinimą, **gebėtų automatiškai atpažinti požymius, indikuojančius duomenų viliojimo ataką**) bei turėtų gebėti šviesti ir mokyti naudotoją savarankiškai atpažinti duomenų viliojimo atakas (mokyti naudotojus).

8. Detalusis prototipas

Remiantis panaudojamumo testavimo ir tyrimo rezultatais bei suformuluotomis patikslintomis projektavimo gairėmis suprojektuotas detalusis maketo prototipas. Nuoroda į detalųjį prototipą: **detaliojo maketo nuoroda.**

Detalusis prototipas yra sudarytas iš dviejų režimų:

- Standartinio režimo, kuris skirtas daugumai naudotojų, turinčių įprastus regos gebėjimus. Jame naudojamos šviesoforo spalvų piktogramos.
- Prieinamumo režimo, kuris specialiai pritaikytas regos negalią turintiems naudotojams. Šiuo režimu užtikrinamas didesnis kontrastas tarp piktogramų ir fono. Šis maketo suteikiamas funkcionalumas skirtas žmonėms turintiems monochromazijos sutrikimus tam, kad galėtų lengviau pastebėti, suprasti ir naudotis įrankiu.

Režimui perjungti naudojama visuotinai pripažinta universalios prieigos piktograma, t.y. žmogaus figūra, pavaizduota apskritime. Naudotos piktogramos pavaizduotos 57 paveiksle (žr. 57 paveikslą). Pirmoje eilutėje matomos spalvos naudotojui, turinčiam įprastus regėjimo gebėjimus, o antroje eilutėje matomos spalvos monochromazijos sutrikimus turinčiam naudotojui. (Filtrai taikyti naudojant internetinę svetainę „Colbis“ adresu: `https://www.color-blindness.com/coblis-color-blindness-simulator/`).

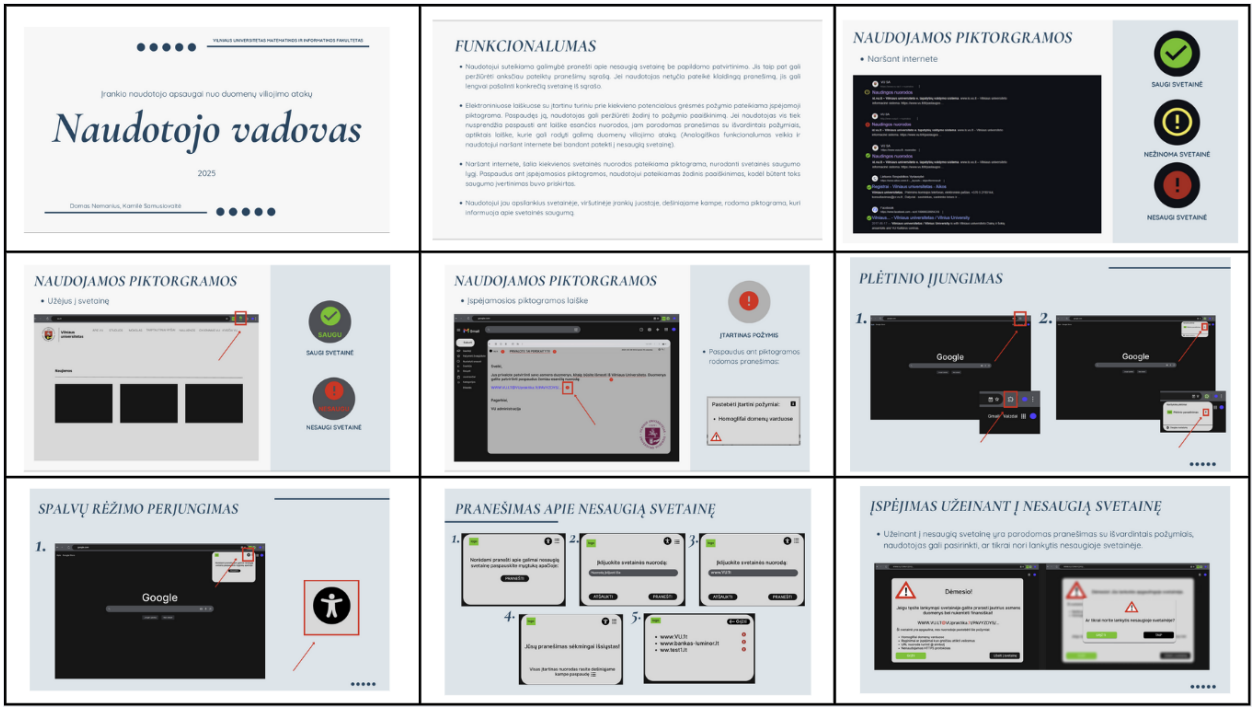
57 pav. Detaliajame prototipe naudotos piktogramos

Detaliojo prototipo funkcionalumas sudarytas iš:

1. Naudotojui suteikiama galimybė pranešti apie nesaugią svetainę be papildomo patvirtinimo. Jis taip pat gali peržiūrėti anksčiau pateiktų pranešimų sąrašą. Jei naudotojas netyčia pateikė klaidingą pranešimą, jis gali lengvai pašalinti konkrečią svetainę iš sąrašo.
2. Elektroniniuose laiškuose su įtartinu turiniu prie kiekvieno potencialaus grėsmės požymio pateikiama įspėjamoji piktograma. Paspaudęs ją, naudotojas gali peržiūrėti žodinį to požymio paaiškinimą. Jei naudotojas vis tiek nusprendžia paspausti ant laiške esančios nuorodos, jam parodomas pranešimas su išvardintais požymiais, aptiktais laiške, kurie gali rodyti galimą duomenų viliojimo ataką. Analogiškas funkcionalumas veikia ir naudotojui naršant internete bei bandant patekti į nesaugią svetainę.

3. Naršant internete, šalia kiekvienos svetainės nuorodos pateikiama piktograma, nurodanti svetainės saugumo lygį. Paspaudus ant įspėjamosios piktogramos, naudotojui pateikiamas žodinis paaiškinimas, kodėl būtent toks saugumo įvertinimas buvo priskirtas.
4. Naudotojui jau apsilankius svetainėje, viršutinėje įrankių juostoje, dešiniajame kampe, rodoma piktograma, kuri informuoja apie svetainės saugumą.

Po detaliojo prototipo sukūrimo buvo parengtas ir naudotojo vadovas (įgyvendinama projektavimo gairė iš kriterijaus PK.9), kuriame aprašytas įrankio funkcionalumas bei paaiškintos naudojamos piktogramos (žr. 58 paveikslą). Nuoroda į **naudotojo vadovą**.



58 pav. Naudotojo vadovas

9. Naršyklės įskiepis

9.1. Naudotos technologijos

Naršyklės įskiepiui sukurti buvo naudotos šios technologijos:

- Aplinka **„Visual Studio“** – tai „Microsoft“ sukurta integruota kūrimo aplinka (IDE), skirta įvairaus tipo programinės įrangos kūrimui, įskaitant naršyklės įskiepius. Ši aplinka taip pat palaiko versijų kontrolės sistemas, tokias kaip „Git“, leidžiančias efektyviai bendradarbiauti komandoje ir valdyti kodo pokyčius.
- **„JavaScript“** – tai dinaminė, interpretuojamoji programavimo kalba, plačiai naudojama kuriant interaktyvias žiniatinklio aplikacijas. Naršyklės įskiepiuose ši kalba yra pagrindinė logikos įgyvendinimo priemonė – ji leidžia valdyti DOM (angl. *Document Object Model*). DOM – tai vidinė internetinio puslapio struktūra, vaizduojama kaip medžio pavidalo modelis, kuriame kiekvienas elementas, pavyzdžiui, antraštė, pastraipa ar mygtukas, yra tarsi medžio mazgas. Naudodamiesi šia struktūra, programuotojai gali keisti puslapio tekstą, stilių, pridėti naujų elementų bei reaguoti į naudotojo veiksmus. Be to, DOM gali sąveikauti su naršyklės API (angl. *Application Programming Interface*) ir padeda užtikrinti įskiepio funkcionalumą. API – tai programavimo sąsaja, leidžianti skirtingoms programoms ar sistemoms bendrauti tarpusavyje, siunčiant užklausas ir gaunant atsakymus pagal iš anksto nustatytas taisykles.
- **„HTML“** (angl. *HyperText Markup Language*) – tai žymėjimo kalba, naudojama internetinio turinio struktūrai apibrėžti. Kuriant naršyklės įskiepį, HTML formuoja naudotojo sąsajos pagrindą, įskaitant mygtukus, laukus, informacijos blokelius ir kitus naudotojo sąsajos komponentus.
- **„CSS“** (angl. *Cascading Style Sheets*) – tai stiliaus aprašymo kalba, naudojama vizualinei HTML turinio išvaizdai formuoti. Ji leidžia apibrėžti spalvas, šriftus, išdėstymą, animacijas ir kitus stiliaus aspektus, padedančius sukurti patogią ir estetišką naudotojo patirtį naršyklės įskiepyje.
- **„WHOIS API“** – tai programinė sąsaja, leidžianti automatiškai gauti informaciją apie tai, kam priklauso konkretus domenas ar IP adresas, kada jis buvo registruotas, kada baigsis jo galiojimas, taip pat kokie yra registratoriaus ar savininko kontaktai (jeigu jie yra viešai prieinami). „WHOIS API“ veikia per HTTPS užklausas ir grąžina duomenis JSON formatu.
- **„Google Safe Browsing API“** – tai „Google“ sukurta programinė sąsaja, leidžianti patikrinti, ar pateikta svetainė, URL ar IP adresas nėra įtraukti į žinomų nesaugių svetainių juodąjį sąrašą.

9.2. Naršyklės įskiepio reikalavimai

9.2.1. Funkciniai reikalavimai

FR.1 Naršyklės įskiepis turi rodyti raudonas perspėjimo piktogramas šalia kiekvieno nustatyto duomenų viliojimo atpažinimo požymio elektroniniame laiške.

FR.2 Paspaudus ant perspėjimo piktogramos, naršyklės įskiepis turi leisti naudotojui peržiūrėti įspėjantį pranešimą, kuriame nurodomas konkretus pastebėtas požymis, galintis indikuoti potencialią duomenų viliojimo ataką.

FR.3 Naršyklės įskiepis turi tikrinti, ar URL adrese naudojamas IP adresas.

FR.4 Naršyklės įskiepis turi patikrinti, ar URL adresas nėra per ilgas.

FR.5 Naršyklės įskiepis turi tikrinti, ar URL nuorodoje yra „@“ simbolis, kuris gali nukreipti naudotoją į adresą, esantį po „@“ simbolio.

FR.6 Naršyklės įskiepis turi patikrinti, ar URL nuorodoje priešdėlis arba priesaga yra atskirti brūkšneliu „-“.

FR.7 Naršyklės įskiepis turi nustatyti, ar URL adrese naudojamas subdomenas.

FR.8 Naršyklės įskiepis turi patikrinti, ar URL naudoja saugų HTTPS protokolą.

FR.9 Naršyklės įskiepis turi tikrinti domeno vardo amžių.

FR.10 Naršyklės įskiepis turi patikrinti, ar domeno varde nėra homoglifų.

FR.11 Naršyklės įskiepis turi nustatyti, ar URL adrese naudojami nestandartiniai aukščiausio lygio domenai.

FR.12 Naršyklės įskiepis turi parodyti įspėjamą pranešimą naudotojui, kai jis paspaudžia ant nuorodos, jei pastebėti įtartini požymiai, ir išvardyti visus šiuos požymius pranešime. Parodžius įspėjamą pranešimą naudotojas gali nuspręsti, ar nori toliau lankytis svetainėje, ar išeiti iš svetainės.

FR.13 Naudotojui ieškant puslapio paieškos varikliuose, tokiuose kaip „Google“, šalia kiekvienos nuorodos turi būti rodoma įspėjamoji piktograma. Paspaudus ant šios piktogramos, turi būti pateikiamas pranešimas su išvardytais įtartinais požymiais.

FR.14 Naudotojui pateikiami įspėjimai turėtų būti rodomi iš karto. Tai reiškia, kad naudotojui neturi reikėti paspausti dar vieną nuorodą ar mygtuką, kad pamatytų įspėjimą ir jo priežastį.

FR.15 Naršyklės įskiepis turėtų leisti naudotojui pranešti apie nesaugią svetainę įterpiant svetainės nuorodą ir atliekant šį veiksmą naudotojo neturi būti perklausiama, ar jis tikrai yra įsitikinęs, kad svetainė yra nesaugi.

FR.16 Naršyklės įskiepis turi tikrinti, ar sutampa puslapio pavadinimas ir domeno vardas.

FR.17 Naršyklės įskiepis turi turėti universalaus prieinamumo piktogramą, kurią paspaudus būtų pakeičiama įrankio piktogramų spalvų paletė.

FR.18 Naršyklės įskiepis turi tikrinti, ar nėra slepiamų nuorodų naudojant hipertekstą.

9.2.2. Nefunkciniai reikalavimai

NR.1 Naršyklės įskiepis turi veikti „Google Chrome“ naršyklėje, užtikrinant sklandų integravimą ir funkcionalumą.

NR.2 Naršyklės įskiepis turi veikti tik tada, kai aptinkamas bent vienas duomenų viliojimo atpažinimo požymis, kad būtų išvengta nereikalingų pranešimų.

NR.3 Vienu metu gali būti atidarytas tik vienas įspėjamasis langas iš naršyklės plėtinio, kad naudotojas galėtų efektyviai atkreipti dėmesį į įspėjimą ir jo turinį.

NR.4 Įskiepis turi greitai reaguoti į pokyčius, t.y. turėtų būti mažas atidėjimo laikas tarp požymių aptikimo ir įspėjimo rodymo.

NR.5 Įskiepio dizainas turi būti paprastas ir intuityvus.

NR.6 Įrankis turi būti nemokamas ir lengvai prieinamas visiems naudotojams ir organizacijoms.

NR.7 Projektuojamas įrankis turėtų veikti naudojant standartinius įrankius ar naršykles be papildomų diegimų.

NR.8 Projektuojamas įrankis turi būti prieinamas naudotojui nemokant už tai autorinio atlyginimo.

NR.9 Naršyklės įskiepis turi būti pritaikytas naudotojams, turintiems regos negalią.

NR.10 Naršyklės įskiepis turi naudoti standartinio šviesoforo įspėjamąsias piktogramas, kurios naudotojams būtų lengvai atpažįstamos.

NR.11 Naršyklės įskiepyje turi būti tik informacija, susijusi su apsauga nuo duomenų viliojimo atakų.

NR.12 Naršyklės įskiepis turi turėti prieinamą dokumentaciją ar / ir mokomąją medžiagą.

9.3. Reikalavimų ir projektavimo gairių atsekamumo matrica

Šiame poskyryje pateikiama atsekamumo matrica, kurioje vaizduojami ryšiai tarp suformuluotų funkcinių ir nefunkcinių reikalavimų ir projektavimo gairių. Matricoje pateikiami tik tie funkciniai ir nefunkciniai reikalavimai, kurie įgyvendina projektavimo gaires. Tie reikalavimai, kurie nepadengia nė vienos projektavimo gairės, atsekamumo matricoje nepavaizduoti. Remiantis matrica, nustatyta, kad du projektavimo kriterijai:

1. PK.4 – Pritaikomumas įvairioms naršyklėms
2. DK.4 – Praktinis taikymas realiose situacijose

liko nepadengti esamais reikalavimais (žr. 59 paveikslą). Dėl šios priežasties daroma išvada, kad naršyklės įskiepis šiuo metu neatitinka visų iškeltų projektavimo gairių ir yra tobulintinas.

PROJEKTAVIMO GAIRĖS	FUNKCINIAI REIKALAVIMAI (FR.) IR NEFUNKCINIAI REIKALAVIMAI (NR.)																									
	FR.1	FR.2	FR.3	FR.4	FR.5	FR.6	FR.7	FR.8	FR.9	FR.10	FR.11	FR.12	FR.13	FR.14	FR.15	FR.16	FR.17	FR.18	NR.6	NR.7	NR.8	NR.9	NR.10	NR.11	NR.12	N/A
Kriterijus PK.1. Svetainės autentiškumo tikrinimas ir naudotojo edukacija.	+											+	+													
Kriterijus PK.2. Vizualinių įspėjimų aiškumas ir atpažįstamumas.		+																					+			
Kriterijus PK.3. Naudotojo veiksmų valdymas ir sprendimų patvirtinimas.												+			+											
Kriterijus PK.4. Pritaikomumas įvairioms naršyklėms.																										
Kriterijus PK.5. Įspėjimai ir pagalba prieš ir po apsilankymo svetainėje.	+											+	+													
Kriterijus PK.6. Aiškus ir tiesiogiai pasiekiami įspėjimai.														+												
Kriterijus PK.7. Galimybė praleisti pasikartojančius veiksmus patyrusiems naudotojams.																										+
Kriterijus PK.8. Tikslinė informacija naudotojo sąsajoje.																								+		
Kriterijus PK.9. Prieinama pagalba ir mokomoji medžiaga.																									+	
Kriterijus DK.1. Pritaikymas regos negalią turintiems naudotojams.																	+					+				
Kriterijus DK.2. Prieinamumas.																			+							
Kriterijus DK.3. Suderinamumas su standartinėmis priemonėmis.																				+						
Kriterijus DK.4. Praktinis taikymas realiose situacijose.																										
Kriterijus DK.5. Prieinamumas nemokant autorinio atlyginimo.																					+					
Techninių sprendimų integracija ir naudotojo švietimas.			+	+	+	+	+	+	+	+	+					+		+								

59 pav. Atsekamumo matrica tarp reikalavimų ir projektavimo gairių

9.4. Naršyklės įskiepio funkcionalumas

Šiame skyriuje aprašytas sukurto „Google Chrome“ naršyklės įskiepio funkcionalumas.

9.4.1. Naršyklės įskiepio aptinkami požymiai

Siekiant įgyvendinti naršyklės įskiepio funkcionalumus, sukurtas naršyklės įskiepis aptinka šiuos požymius (Numeraciją **ĮP** nurodo, kad tai **į**gyvendintas **p**ožymis):

ĮP.1 **URL adrese naudojamą IP adresą.**
Naršyklė įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai nėra IP adresai. Naršyklės įskiepis tai tikrina naudodamas *regular expresion*.

ĮP.2 **Ilgą URL adresą.**
Naršyklės įskiepis tikrina, ar elektroniniame laiške pateiktuose URL adresuose svetainės vardo dalis nėra ilgesnė nei 54 simboliai.

ĮP.3 **URL nuorodoje esantį „@“ simbolį.**
Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai neturi „@“ simbolio.

ĮP.4 **URL nuorodoje esantį simbolį „-“, kuris atskiria priešdėlį ar priesagą.**
Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai neturi simbolio „-“, kuris atskirtų priesagą ar priešdėlį URL nuorodos domeno vardo dalyje.

ĮP.5 **URL adrese esantį subdomeną.**
Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai nenaudoja keleto subdomenų kombinacijos. Naršyklės įskiepis tai tikrina analizuodamas taškų kiekį esantį svetainės varde. Jei taškų kiekis – daugiau už 3, nuoroda naudoja kelių subdomenų kombinaciją ir yra pažymima kaip įtartina.

ĮP.6 **Nenaudojamą HTTPS protokolą.**

Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai naudoja HTTPS protokolą. Jei elektroniniame laiške pateikta nuoroda neprasideda „https://“ – ji pažymima kaip įtartina.

ĮP.7 **Homoglifus domenų varduose.**

Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai neturi simbolių ar simbolių junginių, kurie vizualiai gali atrodyti kaip kiti simboliai. Kadangi „Gmail“ URL nuorodose, kurias galima įterpti į laišką, leidžia naudoti tik ASCII simbolius, naršyklės įskiepis turi iš anksto apibrėžtą ASCII simbolių ir ASCII simbolių junginių sąrašą, kurie gali klaidinti naudotoją, tad jų ieško elektroniniame laiške esančiose URL nuorodose.

ĮP.8 **Nestandartinius aukščiausio lygio domenus.**

Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai naudoja standartinius aukščiausio lygio domenus, kurių sąrašas įskiepyje yra iš anksto nurodytas. Standartiniai aukščiausio lygio domenai surinki remiantis „Understanding evolution and adoption of Top-level Domain names“ straipsniu [JDB+15]. Jei nuorodoje naudojamo aukščiausio lygio domeno nėra tarp standartinių – jis pažymimas kaip įtartinas.

ĮP.9 **Įtartiną domeno vardo amžių.**

Naršyklės įskiepis tikrina elektroniniame laiške pateiktų URL adresų domeno vardų amžių. Domenai, užregistruoti anksčiau nei prieš 6 mėnesius – klasifikuojami kaip įtartini. Naršyklės įskiepis šią informaciją tikrina siųsdamas užklausas į „whoisxmlapi“.

ĮP.10 **Raginimus ar įspėjimus kuo greičiau atlikti veiksmus.**

Naršyklės įskiepis, siekdamas aptikti raginimus ar įspėjimus kuo greičiau atlikti veiksmus, naudoja sudarytą žodžių ir frazių banką (žr. 60 paveikslą). Frazės ir žodžiai surinkti remiantis apgaulingų laiškų pavyzdžiais, esančiais internete. Šis bankas suskirstytas į tris kategorijas pagal raginimo intensyvumą:

- Netiesioginis raginimas – frazės, naudojamos kaip mandagūs priminimai ar paskatinimai, nenurodantys aiškios grėsmės ar pasekmių.
- Tiesioginis spaudimas – frazės, kurios akcentuoja konkrečius terminus ar būtinybę veikti.
- Stiprus spaudimas – grėsmingos ar stresą keliančios frazės, naudojamos siekiant išgąsdinti naudotoją ir paskatinti impulsyvius veiksmus.

Tokiu būdu naršyklės įskiepis geba identifikuoti socialinės inžinerijos pagrindu rengiamų atakų veiksmus, būdingus duomenų viliojimo atakoms.

ĮP.11 **Nuorodą, įtrauktą į juodąjį sąrašą.**

Naršyklės įskiepis tikrina, ar elektroniniame laiške pateikti URL adresai nėra įtraukti į juodąjį sąrašą. Naršyklės įskiepis šią informaciją tikrina siųsdamas užklausas į „Google safe browsing api“.

ĮP.12 **Nuorodos slėpimą, naudojant hipertekstą.**

Naršyklės įskiepis tikrina, ar elektroniniame laiške nėra URL nuorodų, kurios būtų

slepiamos naudojant hipertekstą. Įskiepis tai tikrina lygindamas vizualiai matomą tekstą ir po juo paslėptą URL nuorodą.

ĮP.13 **Puslapio pavadinimo ir domeno vardo sutapimą.**

Naršyklės įskiepis tikrina, ar „Google“ paieškos variklio rezultatuose pateiktų URL nuorodų domenų vardai sutampa su paieškos rezultatuose pateiktais svetainių pavadinimais.

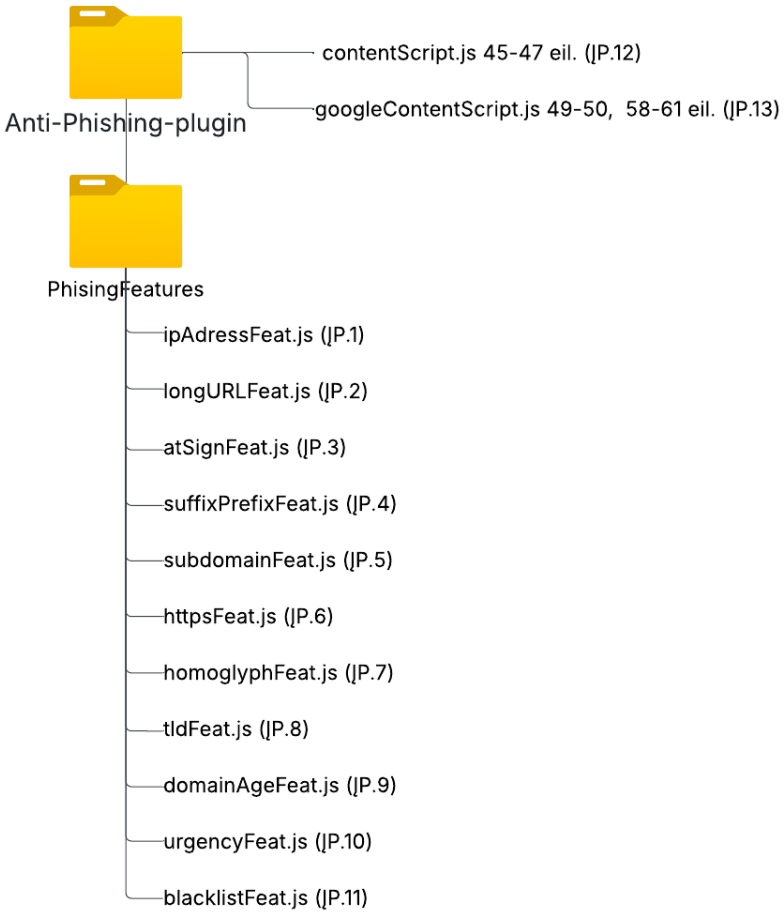
Netiesioginis raginimas, naudojamas kaip mandagus priminimas	
Rekomenduojama patikrinti savo paskyrą	Nelaukite paskutinės minutės
Laiku neprisijungus gali kilti nepatogumų	Prisijunkite dar šią savaitę
Geriausia tai padaryti kuo greičiau	Patvirtinkite kai tik galėsite
Veikite laiku	Tai svarbu jūsų paskyros saugumui
Įsitikinkite, kad jūsų paskyra yra aktyvi	Verta prisijungti
Jeigu neprisijungsite, galite susidurti su nesklandumais	Galite išvengti trikdžių
Rekomenduojama pasitikrinti/prisijungti	Informuojame apie galimus pakeitimus
Profilaktiškai atnaujinkite paskyros duomenys	Kuo greičiau tuo geriau
Tiesioginis spaudimas, akcentuojant konkretų laiko terminą ar būtinybę	
Greitai, greičiau	Turite tik kelias valandas
Skubiai, Skubiau, Skubu	Patvirtinkite šiandien
Nedelsiant, neatidėliotinai, neatidėliotinas veiksmas	Paskyra gali būti apribota/užblokuota
Privalote prisijungti	Baigiasi paskyros galiojimas
Jūsų paskyroje aptiktas įtartinas prisijungimas	Prisijunkite iki dienos pabaigos
Paskutinė valanda patvirtinti duomenis	Nepamirškite prisijungti šiandien
Iki vidurnakčio privalote prisijungti	Terminas baigiasi šiandien
Turite ribotą laiką	Peržiūrėkite šią informaciją dabar
Atnaujinkite paskyrą iki šios datos	Paskutinė galimybė aktyvinti
Pavėlavus gali kilti pasėkmių	Reaguokite iki nustatyto termino
Stiprus spaudimas, naudojamas stresui sukelti	
Jūsų paskyra yra užblokuota	Nepatvirtinus neteksite prieigos
Paskutinė galimybė išsaugoti prieigą	Tai paskutinis įspėjimas
Veikite dabar	Nutekinti duomenys
Nepatvirtinus paskyros ji bus ištrinta	Potencialus įsilaužimas – veikite iš karto
Likusios tik kelios valandos	Prisijunkite tuoj pat, kad atkurtumėte saugumą
Nedelsiant prisijunkite, nes gresia pavojus paskyrai	Duomenys gali būti prarasti
Skubus saugumo atnaujinimas	Jūsų paskyra laikinai išjungta
Paskyrai gresia pavojus	Prisijunkite tuoj pat
Skubus saugumo pranešimas	Pastebėtas įtartinas aktyvumas
Pavojus jūsų tapatybei	Privalote užtikrinti saugumą dabar
Paskyra buvo pažeista privalote ją atkurti	Nepaisant įspėjimo būsite užblokuota/s
Neteksite visų duomenų	Sistemoje įvyko klaida – būtina prisiregistruoti iš naujo

60 pav. Raginimų ir įspėjimų kuo greičiau atlikti veiksmus žodžių ir frazių bankas

9.4.1.1. Įgyvendintų požymių realizacijos atsekamumas programinio kodo lygmeniu

Šiame poskyryje pateikiamas paveikslėlis (žr. 61 paveikslą), kuriame vaizdžiai atvaizduojama, kaip konkretūs įskiepyje įgyvendinti duomenų viliojimo atakų atpažinimo požymiai susiejami su atitinkamomis programinio kodo vietomis. Šis atvaizdavimas leidžia aiškiai identifikuoti, kuriame konkrečiame .js faile yra realizuota tam tikro požymio atpažinimo logika. Kiekvienas failo

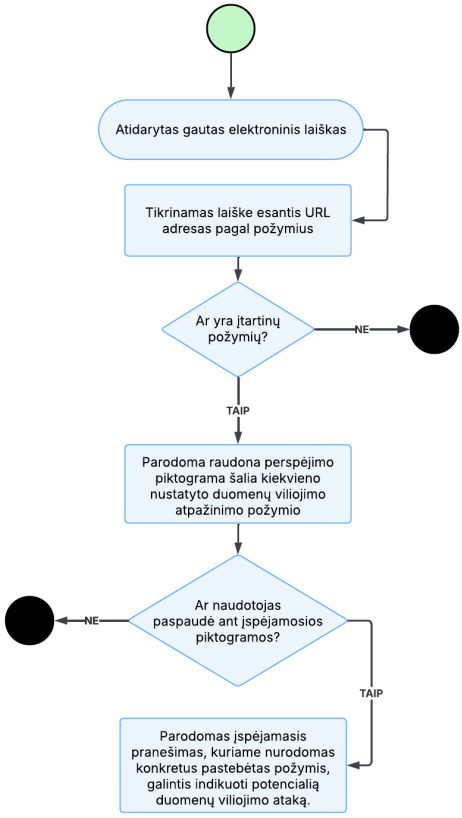
pavadinimas diagramoje papildytas skliausteliuose pateiktu požymio identifikatoriumi, atitinkančiu reikalavimų sąraše aprašytą funkcionalumą. Pavyzdžiui, ĮP.1 požymis, atsakingas už IP adreso naudojimo URL adrese atpažinimą, yra realizuotas faile *ipAdressFeat.js*, esančiame projekto *Anti-Phishing-plugin* aplanke *PhishingFeatures*.



61 pav. Įgyvendintų požymių susiejimas su kodu

9.4.2. Duomenų viliojimo atakos požymių atpažinimas elektroniniame laiške

Vienas iš sukurto naršyklės įskiepio funkcionalumų – duomenų viliojimo atakos požymių atpažinimas elektroniniuose laiškuose. Šis procesas iliustruojamas diagramoje (žr. 62 paveikslą). Įskiepis šalia kiekvieno aptikto požymio laiško turinyje pateikia įspėjamąją piktogramą – raudonos spalvos burbuliuką. Paspaudus piktogramą, naudotojui pateikiamas pranešimas, kuriame nurodomas konkretus identifikuotas požymis, galintis signalizuoti apie galimą duomenų viliojimo ataką. Įskiepis elektroniniame laiške atpažįsta anksčiau aprašytus požymius **ĮP.1**-**ĮP.12**. Požymių atpažinimas realizuotas tik „Gmail“ elektroninio pašto dėžutėje.



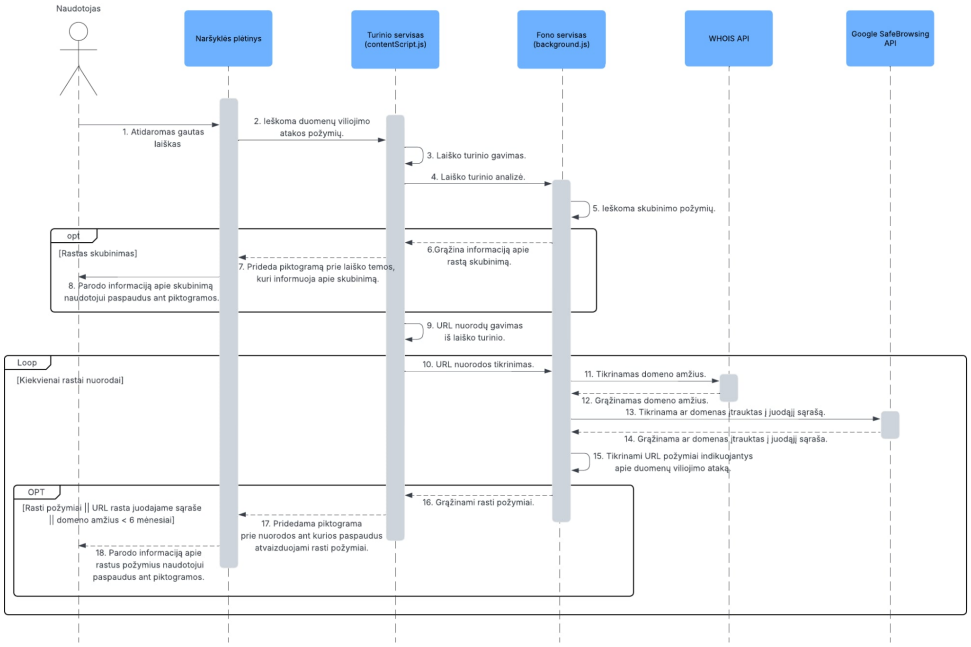
62 pav. Duomenų viliojimo atakos požymių identifikavimas elektroniniame laiške

9.4.2.1. Proceso eiga

Žemiau pateikiama sekų diagrama (žr. 63 paveikslą), vaizduojanti procesą nuo elektroninio laiško atidarymo iki požymių pateikimo iššokančiame lange naudotojui paspaudus įspėjamąją piktogramą.

Diagramoje naudojami komponentai:

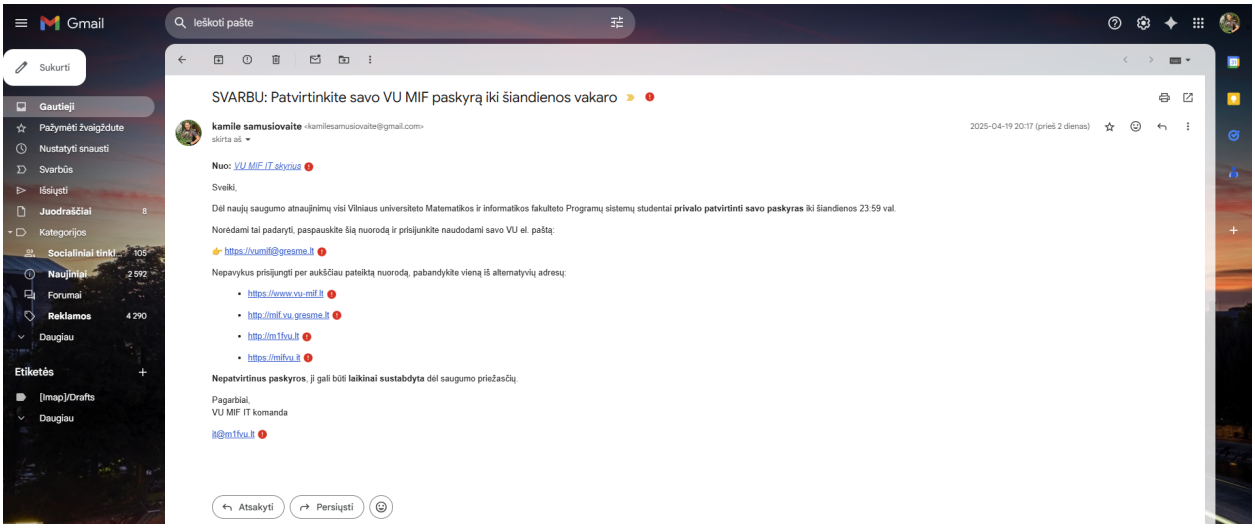
- Turinio servisas (angl. *content script)* – tai naršyklės įskiepio komponentas, kuris vykdomas tiesiogiai tinklalapyje ir turi prieigą prie jo DOM struktūros (vidinė tinklapio struktūra, kurioje kiekvienas HTML elementas vaizduojamas kaip objektas hierarchiniame medyje). Šis servisas atsakingas už el. laiško turinio nuskaitymą, analizę, įspėjamųjų piktogramų įterpimą ir sąveiką su naudotojo matomu turiniu.
- Fono servisas (angl. *background script)* – tai atskirai nuo tinklalapio veikiantis įskiepio komponentas, kuris veikia fone, nepriklausomai nuo aktyvaus naršyklės lango. Jis atsakingas už sąsajas su išorinėmis paslaugomis (pvz., „Google Safe Browsing API“, „WHOIS API“), URL nuorodų tikrinimą ir ryšio palaikymą tarp kitų įskiepio dalių.
- „WHOIS API“ ir „Google Safe Browsing API“ detaliau aprašyti 9.1 skyriuje.



63 pav. Duomenų viliojimo atakų požymių elektroniniame laiške atpažinimo procesas pavaizduotas sekų diagrama (angl. *sequence diagram)*

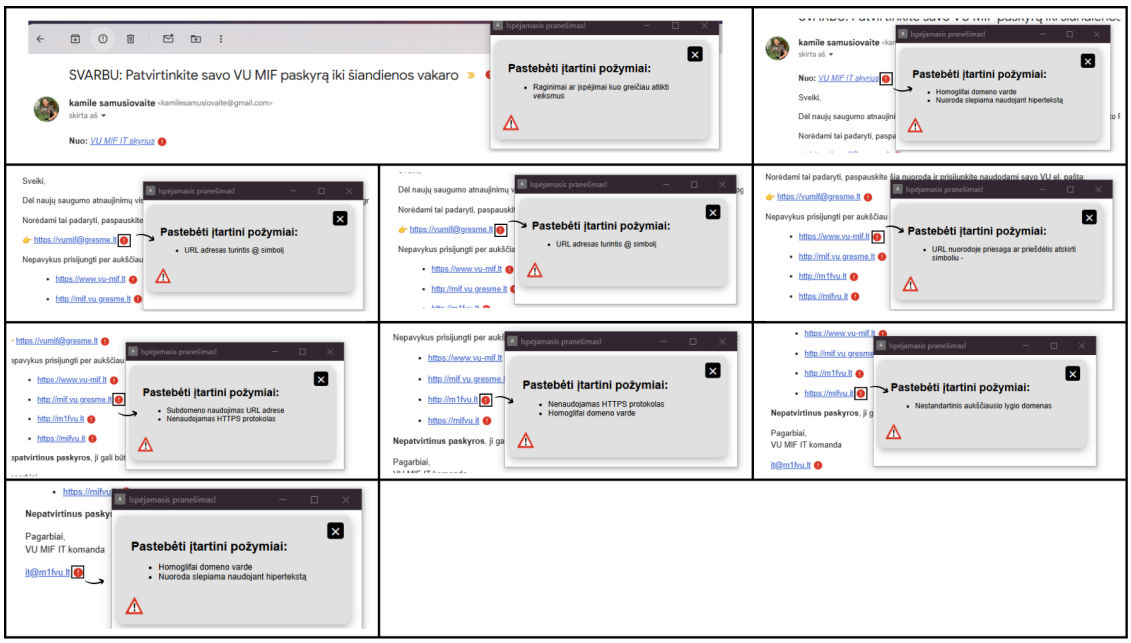
9.4.2.2. Funkcionalumo demonstracija

Norėdami pavaizduoti naršyklės įskiepio veikimą sukūrėme pavyzdinį elektroninį laišką, kuriame pateiktos įvairios nuorodos su duomenų viliojimo atakoms būdingais URL požymiais (žr. 64 paveikslą).



64 pav. Duomenų viliojimo atakų požymių atpažinimas elektroniniame laiške

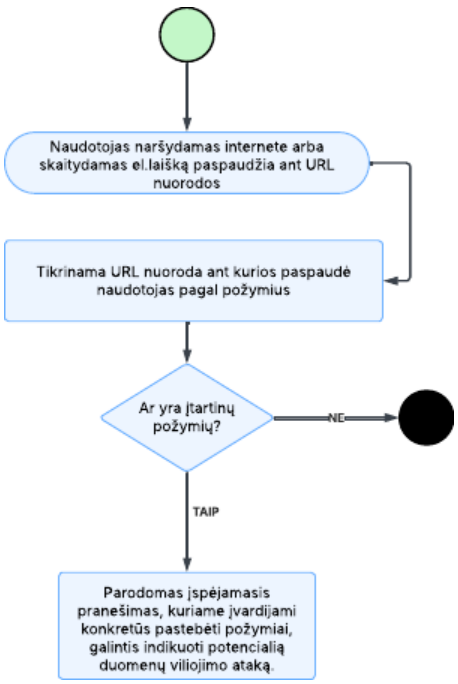
Naudotojui paspaudus ant kiekvienos įspėjamosios piktogramos, naršyklės įskiepis pateikia iššokantį langą, kuriame sąrašo forma išvardijami identifikuoti duomenų viliojimo požymiai (žr. 65 paveikslą).



65 pav. Įspėjamųjų pranešimų atvaizdavimas naudotojui paspaudus įspėjamąją piktogramą

9.4.3. Duomenų viliojimo atakos atpažinimas paspaudus ant įtartinos nuorodos (bandant patekti į svetainę)

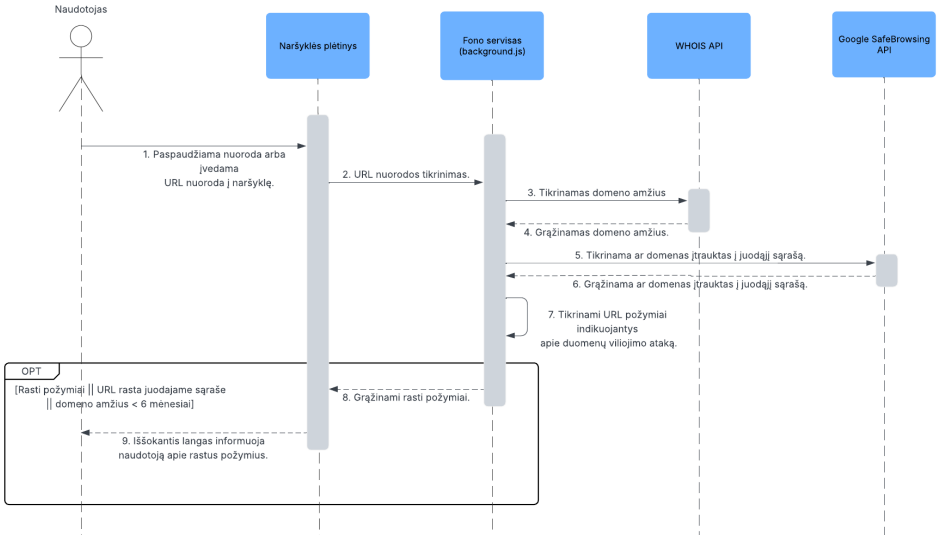
Kitas naršyklės įskiepio funkcionalumas – naudotojo įspėjimas apie galimą duomenų viliojimo ataką jam bandant apsilankyti įtartinoje svetainėje. Šis procesas pavaizduotas 66 paveiksle. Bandant atidaryti nesaugią svetainę (paspaudus ant URL nuorodos), naudotojui pateikiamas įspėjamasis pranešimas, kuriame nurodomi konkretūs identifikuoti požymiai pastebėti URL nuorodoje. Įskiepis, paspaudus ant įtartinos nuorodos, atpažįsta anksčiau aprašytus požymius **ĮP.1-ĮP.11**.



66 pav. Duomenų viliojimo atakos požymių atpažinimas naudotojui bandant užeiti į apgaulingą svetainę

9.4.3.1. Proceso eiga

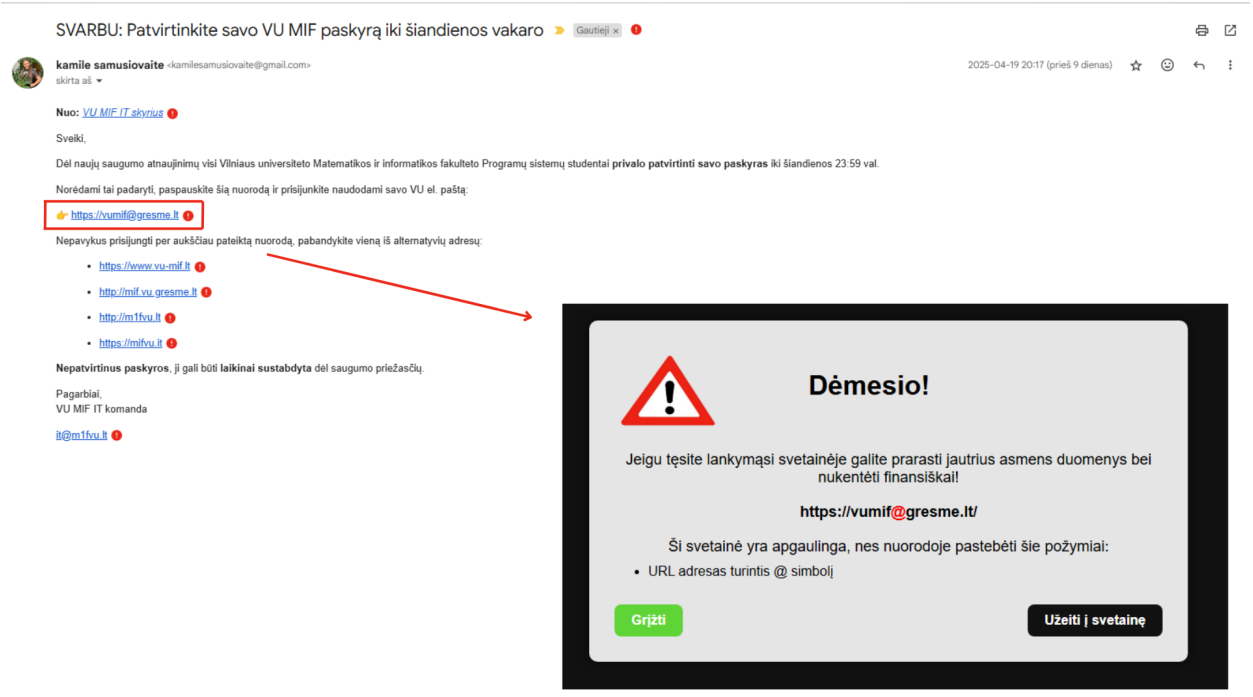
Žemiau pateikiama sekų diagrama (žr. 67 paveikslą), vaizduojanti procesą, paspaudus ant įtartinos nuorodos.



67 pav. Duomenų viliojimo atakų požymių atpažinimo procesas paspaudus ant URL nuorodos pavaizduotas sekų diagrama (angl. *sequence diagram)*

9.4.3.2. Funkcionalumo demonstracija

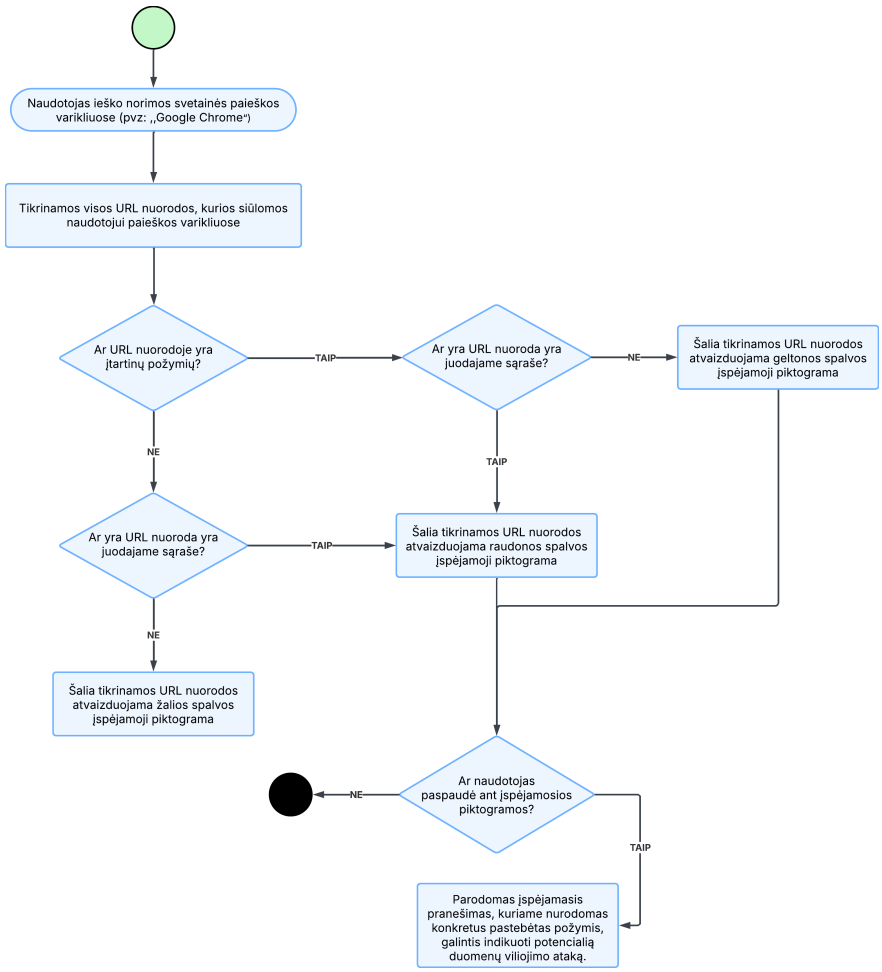
Naudotojui paspaudus bet kurią iš gautame elektroniniame laiške esančių nuorodų, pateikiamas įspėjamasis langas, kuriame išvardijami nustatyti įtartini požymiai (žr. 68 paveikslą). Lange taip pat pateikiama ir URL nuoroda, ant kurios paspaudė naudotojas, o joje aptiktos įtartinos vietos vizualiai išskiriamos raudona spalva.



68 pav. Įspėjamojo pranešimo atvaizdavimas naudotojui paspaudus įtartiną URL nuorodą

9.4.4. Duomenų viliojimo atakos atpažinimas naršant internete

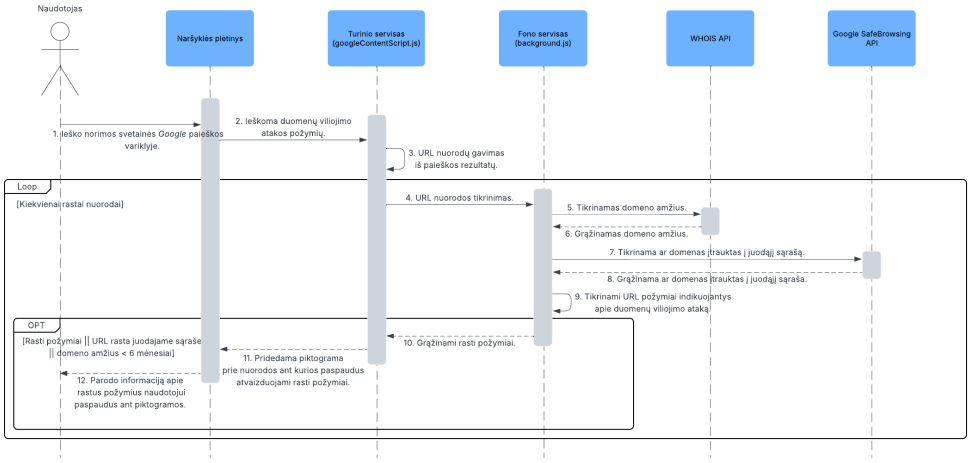
Naršyklės įskiepis taip pat atlieka URL nuorodų tikrinimą paieškos varikliuose, tokiuose kaip „Google“. Įskiepis šį patikrinimą atlieka remdamasis anksčiau aprašytais požymiais **ĮP.1**-**ĮP.11**, **ĮP.13**. Naršant internete, šalia kiekvienos siūlomos nuorodos rodoma įspėjamoji piktograma: žalia spalva žymima, kai URL neturi įtartinų požymių, geltona – kai aptinkami tam tikri rizikos požymiai, tačiau nuoroda nėra įtraukta į juoduosius sąrašus, ir raudona – kai nustatomi įtartini požymiai, o nuoroda randama juoduosiuose sąrašuose. Paspaudus geltoną arba raudoną įspėjamąją piktogramą, naudotojui pateikiamas įspėjamasis pranešimas su išvardytais pastebėtais įtartinais požymiais aptiktais URL nuorodoje. Šis procesas pavaizduotas 69 paveiksle.



69 pav. URL nuorodų tikrinimo proceso diagrama paieškos varikliuose

9.4.4.1. Proceso eiga

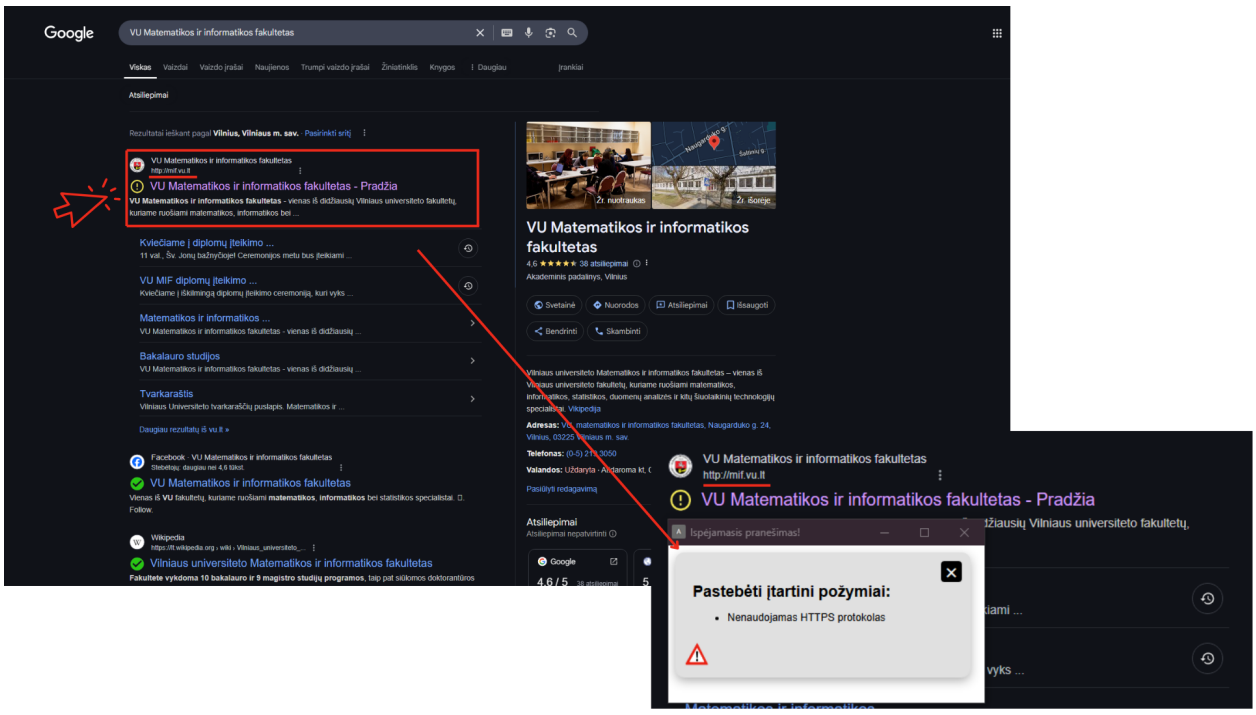
Žemiau pateikiama sekų diagrama (žr. 70 paveikslą), vaizduojanti procesą nuo užklausos įvedimo į paieškos variklį iki požymių pateikimo naudotojui iššokančiame lange paspaudus įspėjamąją piktogramą.



70 pav. Duomenų viliojimo atakų požymių „Google“ paieškos variklio rezultatuose atpažinimo procesas pavaizduotas sekų diagrama (angl. *sequence diagram)*

9.4.4.2. Funkcionalumo demonstracija

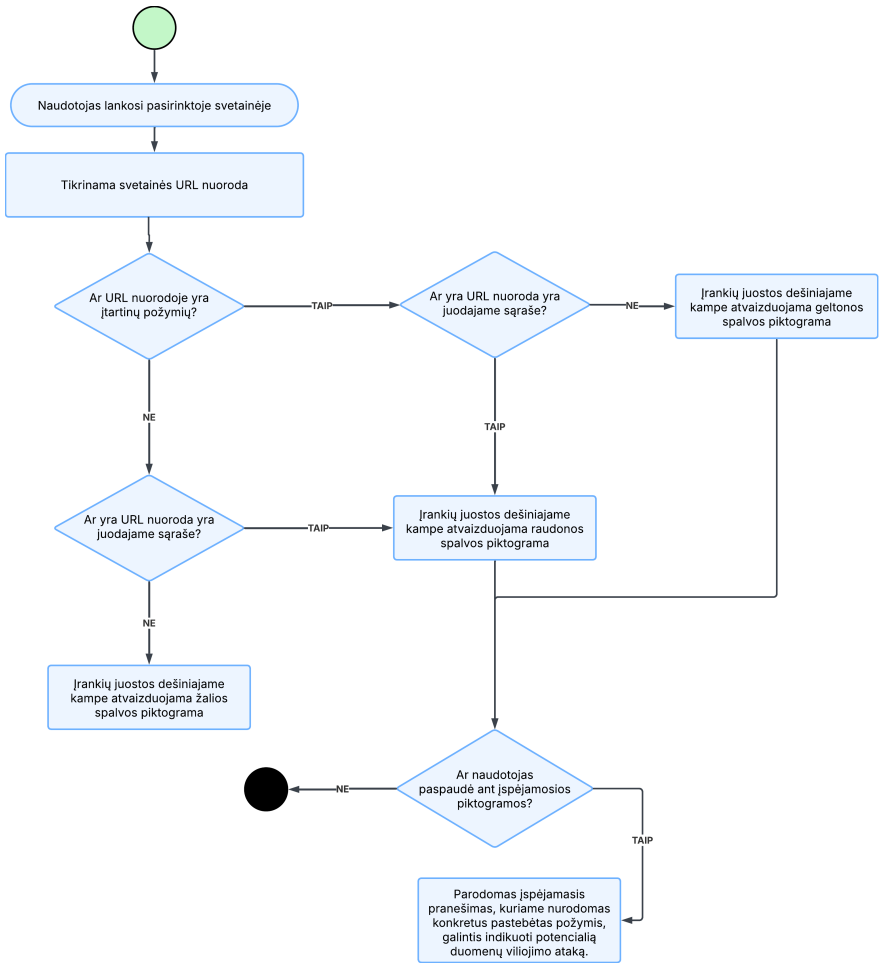
Naudotojui ieškant informacijos apie Vilniaus universiteto Matematikos ir informatikos fakultetą naudojant paieškos variklį „Google Chrome“, šalia kiekvieno pateikto rezultato rodoma įspėjamoji piktograma. Pavyzdžiui, prie pirmosios nuorodos pateikiama geltonos spalvos piktograma, nes naršyklės įskiepis, tikrindamas URL, aptiko vieną rizikos požymį – naudojamas neapsaugotas HTTP protokolas. Paspaudęs įspėjamąją piktogramą, naudotojas gali peržiūrėti konkrečius nustatytus įtartinus požymius. Šis funkcionalumo veikimo scenarijus pavaizduotas 71 paveiksle.



71 pav. Įspėjamųjų piktogramų pateikimas paieškos rezultatuose

9.4.5. Duomenų viliojimo atakos atpažinimas užėjus į svetainę

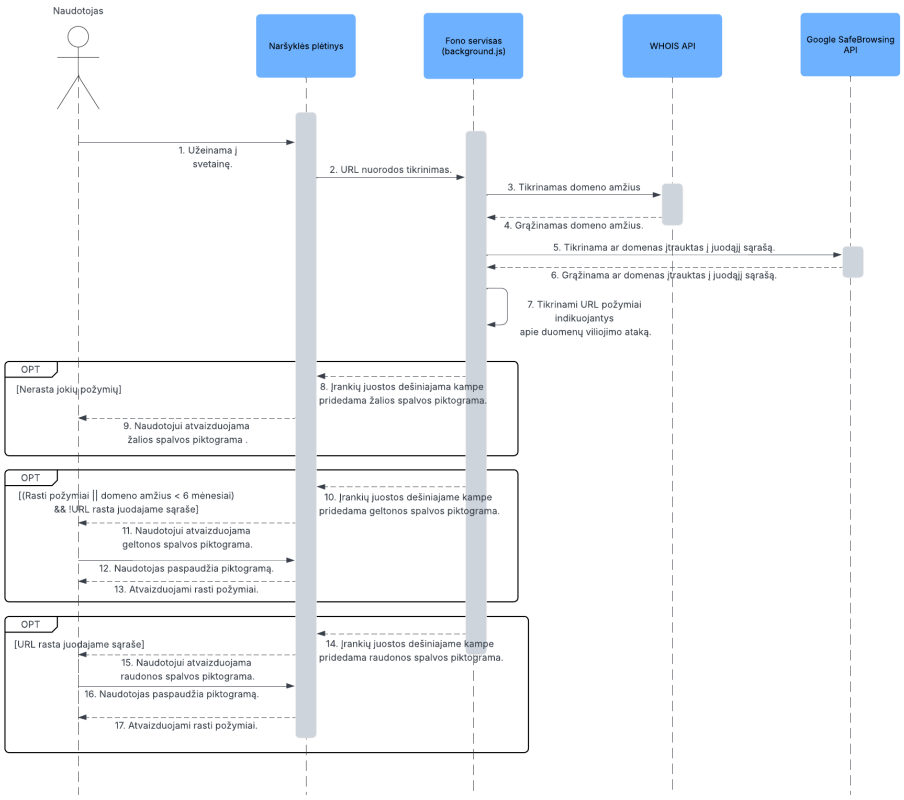
Naudotojui apsilankius svetainėje, naršyklės įskiepis automatiškai patikrina jos URL adresą. Įskiepis URL nuorodos tikrinimą atlieka remdamasis anksčiau aprašytais požymiais **ĮP.1-ĮP.11**. Jei URL neturi įtartinų požymių, įrankių juostoje dešiniajame kampe rodoma žalios spalvos piktograma. Naršyklės įskiepiui aptikus tam tikrus požymius, bet neradus nuorodos juodajame sąraše, rodoma geltonos spalvos piktograma. Jei nuoroda randama juoduosiuose sąrašuose, pateikiama raudonos spalvos piktograma. Paspaudus ant geltonos arba raudonos spalvos piktogramos, naudotojui parodomas įspėjamasis pranešimas su išvardintais pastebėtais požymiais. Šį procesą iliustruoja 72 diagrama.



72 pav. URL nuorodos tikrinimo procesas naudotojui lankantis svetainėje

9.4.5.1. Proceso eiga

Žemiau pateikiama sekų diagrama (žr. 73 paveikslą), vaizduojanti URL nuorodos tikrinimo ir įspėjamųjų piktogramų pateikimo procesą naudotojui užėjus į svetainę.

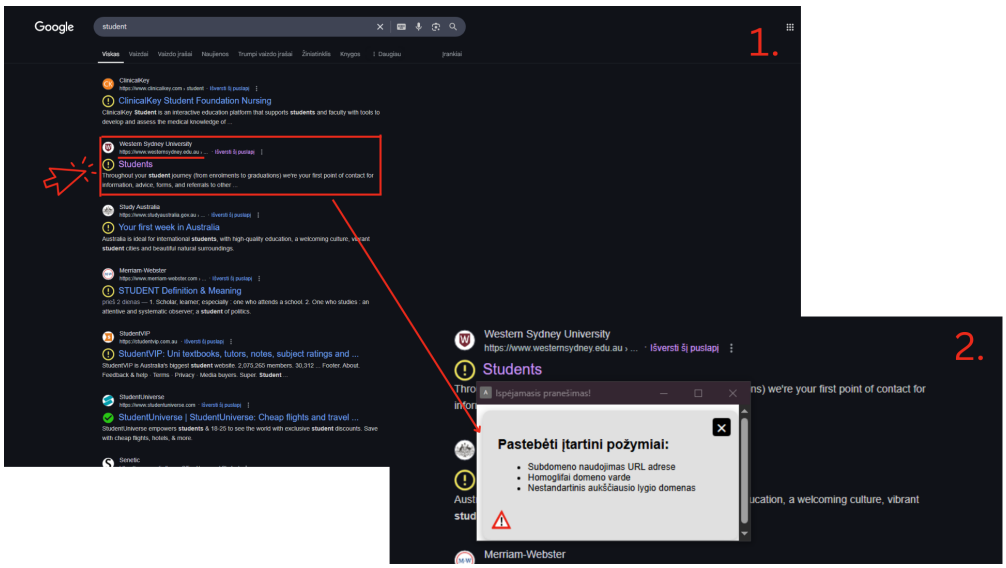


73 pav. URL nuorodos tikrinimas naudotojui lankantis svetainėje pavaizduotas sekų diagrama (angl. *sequence diagram*)

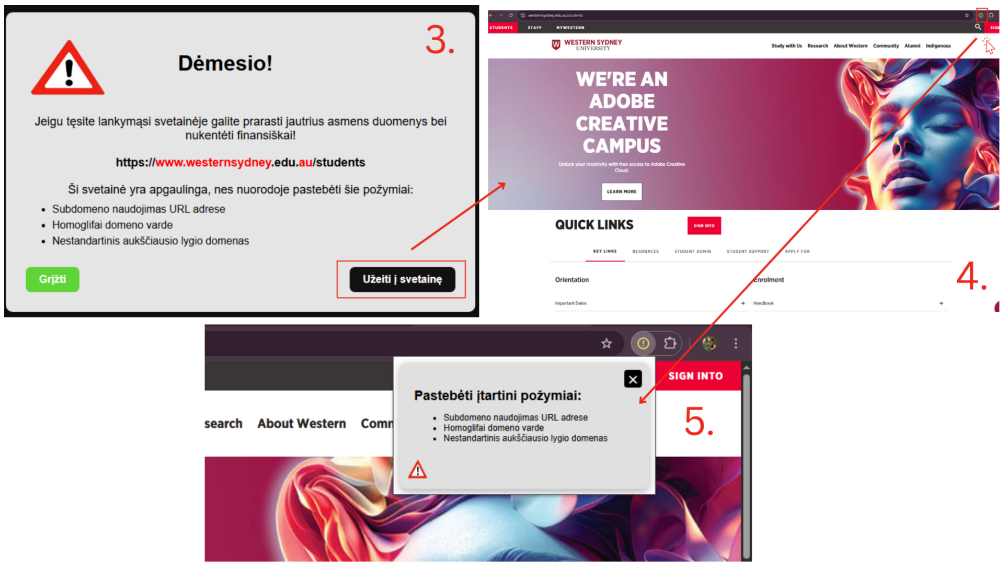
9.4.5.2. Funkcionalumo demonstracija

Naudotojui ieškant svetainės paieškos varikliuose, šalia kiekvienos URL nuorodos pateikiama įspėjamoji piktograma. Paspaudus šią piktogramą, galima peržiūrėti identifikuotus įtartinus požymius, susijusius su atitinkama nuoroda (funkcionalumas: duomenų viliojimo atakos atpažinimas naršant internete) (žr. 74 paveikslą).

Jei naudotojas vis tiek nusprendžia apsilankyti tokioje svetainėje, naršyklės įskiepis parodo papildomą pranešimą su svetainės adresu bei išsamiai išvardytais rizikos veiksniais, kurie gali įspėti apie galimą duomenų viliojimo ataką (funkcionalumas: duomenų viliojimo atakos atpažinimas paspaudus ant įtartinos nuorodos (bandant patekti į svetainę)). Naudotojui pasirinkus tęsti naršymą nesaugioje svetainėje, įskiepio piktograma naršyklės įrankių juostoje pasikeičia į įspėjamąją. Jei ši piktograma yra geltonos arba raudonos spalvos, paspaudus ją, naudotojui dar kartą pateikiami aptikti įtartini požymiai, identifikuoti svetainės URL nuorodoje (žr. 75 paveikslą).



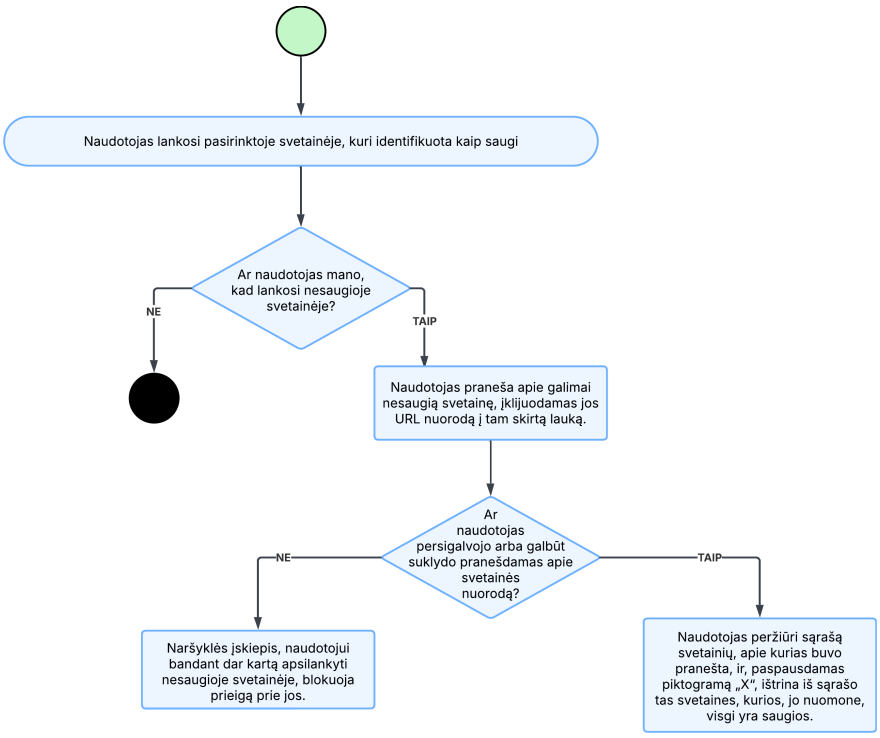
74 pav. Įspėjamosios piktogramos pateikimas ir pastebėtų požymių pranešimas naršant internete



75 pav. Įspėjamasis pranešimas bandant užeiti į svetainę ir lankantis svetainėje

9.4.6. Pranešimas apie nesaugią svetainę

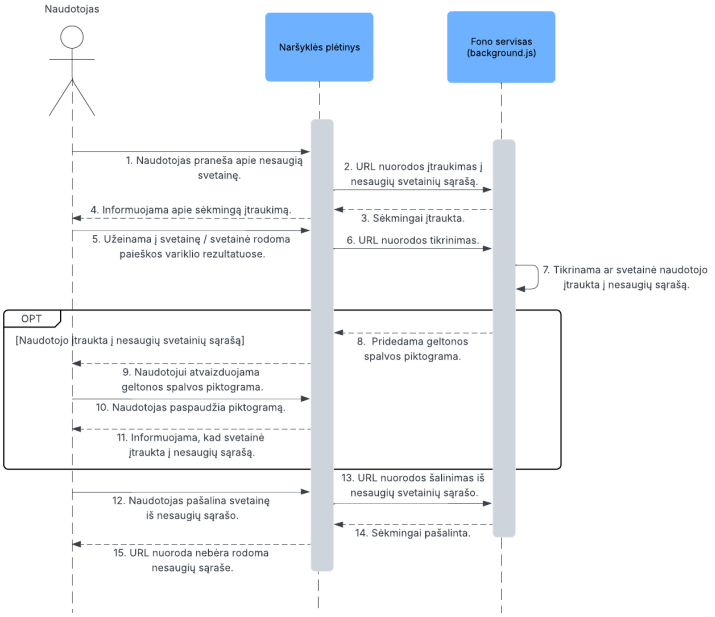
Naudotojui apsilankius svetainėje, kuri naršyklės įskiepio yra identifikuota kaip saugi, įskiepis naršyklės įrankių juostoje rodo žalios spalvos įspėjamąją piktogramą. Paspaudęs šią piktogramą, naudotojas gali įklijuoti lankomos svetainės URL adresą į tam skirtą lauką ir pateikti pranešimą, jei mano, kad svetainė iš tikrųjų gali būti nesaugi. Pateikus tokį pranešimą, įskiepis įtraukia svetainę į nesaugių svetainių sąrašą ir kitą kartą bandant ją pasiekti – automatiškai blokuoja prieigą prie jos. Jei vėliau naudotojas nusprendžia, kad pranešimas buvo klaidingas, jis gali paspausti sąrašo piktogramą, peržiūrėti visų anksčiau pažymėtų svetainių sąrašą ir pašalinti bet kurią jų paspausdamas „X“ piktogramą. Tokiu būdu prieiga prie pasirinktos svetainės vėl tampa galima. Šis procesas pavaizduotas 76 paveiksle.



76 pav. Pranešimo apie nesaugią svetainę proceso vaizdavimo diagrama

9.4.6.1. Proceso eiga

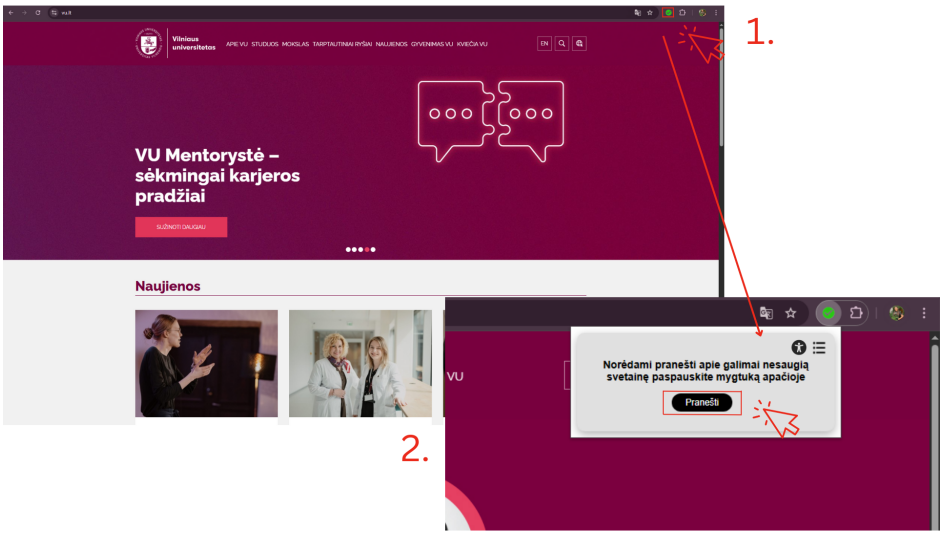
Žemiau pateikiama sekų diagrama (žr. 77 paveikslą), vaizduojanti svetainės įtraukimą į nesaugių svetainių sąrašą ir naudotojo informavimą lankantis joje bei svetainės pašalinimą iš nesaugių svetainių sąrašo.



77 pav. URL nuorodos įtraukimas į nesaugių sąrašą pavaizduotas sekų diagrama (angl. *sequence diagram*)

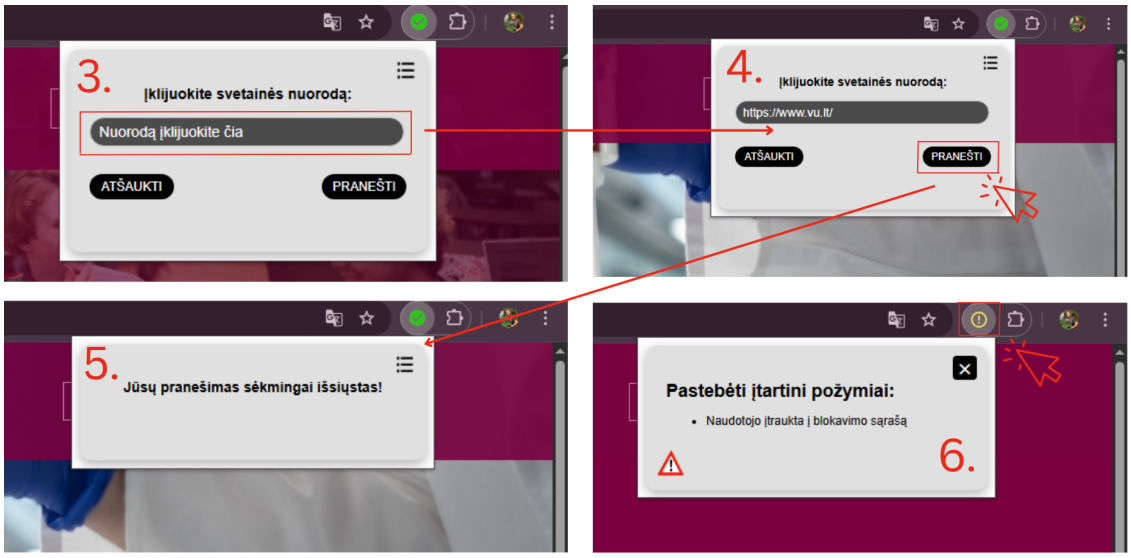
9.4.6.2. Funkcionalumo demonstracija

Pirmiausiai, naudotojui apsilankius svetainėje, kuri naršyklės įskiepio yra identifikuota kaip saugi, tačiau naudotojui manant, jog ji yra nesaugi, naršyklės įskiepis turi funkcionalumą, kuris suteikia galimybę apie tai pranešti. Tam reikia paspausti įrankių juostoje esančią saugios svetainės piktogramą – žalią apskritimą su varnele viduryje. Paspaudus šią piktogramą, naršyklės įskiepis parodo iššokantį langą, kuriame matomas juodos spalvos mygtukas su užrašu „Pranešti“. Šis žingsnis pavaizduotas 78 paveiksle.



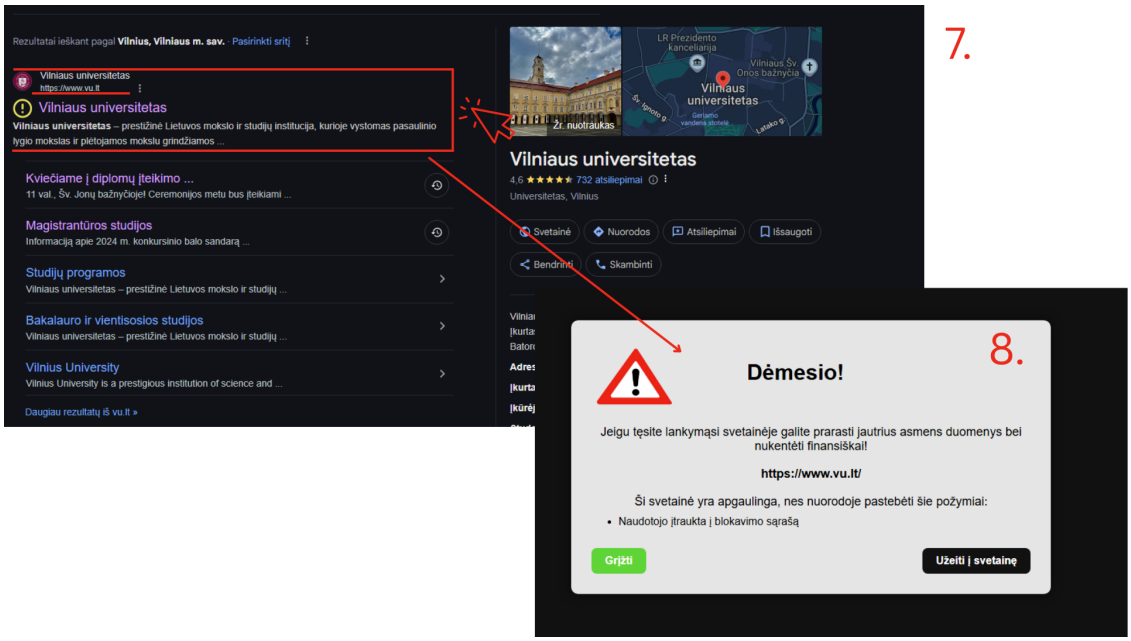
78 pav. Pranešimo apie nesaugią svetainę pirmasis žingsnis

Paspaudus mygtuką „Pranešti“, naudotojui pateikiamas laukelis, kuriame galima įvesti svetainės, kuri, jo nuomone, yra nesaugi, URL adresą. Įvedus nuorodą, belieka dar kartą paspausti mygtuką „Pranešti“ ir palaukti, kol naršyklės įskiepis patvirtins, kad pranešimas buvo sėkmingai išsiųstas. Po patvirtinimo, įrankių juostos dešiniajame kampe esanti žalia piktograma pasikeičia į geltoną. Paspaudus šią piktogramą, naudotojui pateikiama informacija, kad lankomasi svetainėje, kuri yra jo paties įtraukta į blokuojamų svetainių sąrašą. Šis procesas pavaizduotas 79 paveiksle.



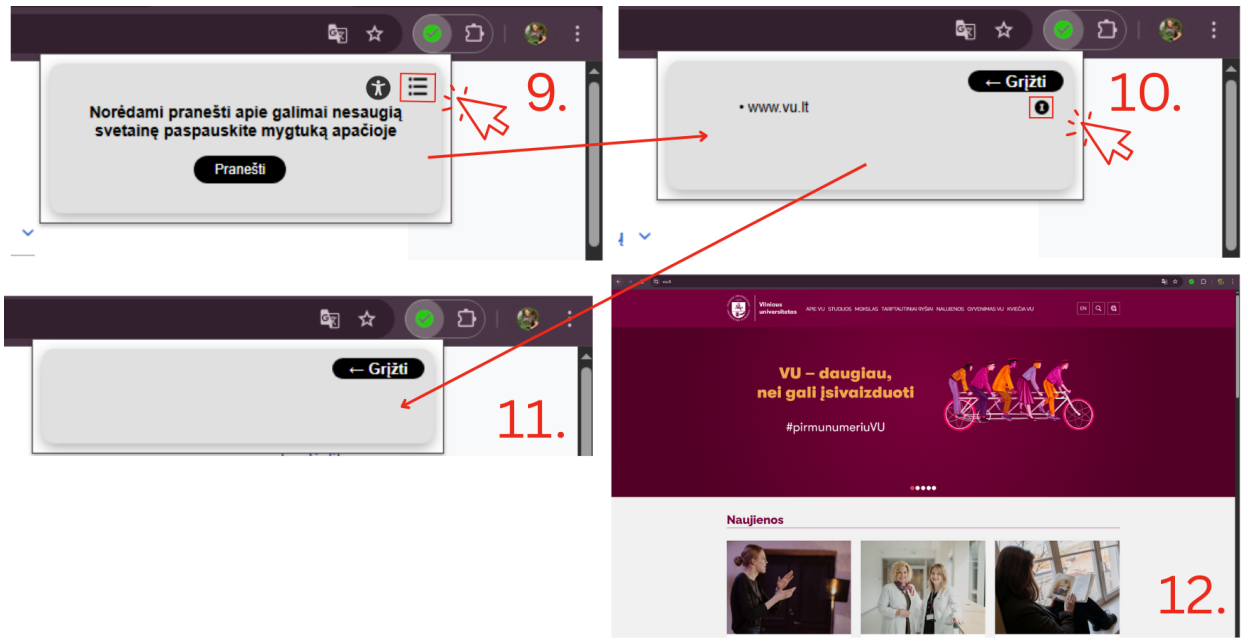
79 pav. Pranešimo apie nesaugią svetainę antrasis žingsnis

Kai naudotojas pateikia pranešimą apie nesaugią svetainę, kitą kartą lankantis joje naršyklės įskiepis automatiškai blokuoja prieigą ir pateikia įspėjamąjį pranešimą. Šis veiksmas pavaizduotas 80 paveiksle.



80 pav. Svetainės blokavimas naudotojui bandant užeiti į svetainę, apie kurią pranešė pateikdamas svetainės URL

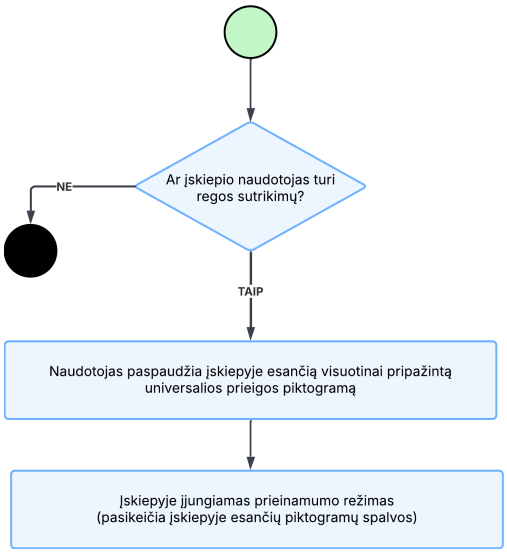
Jeigu naudotojas persigalvoja ir mano, kad neteisingai pranešė apie svetainę kaip nesaugią, naršyklės įskiepis leidžia pašalinti ją iš blokuojamų svetainių sąrašo. Tam reikia paspausti piktogramą įrankių juostoje, pasirinkti sąrašo piktogramą ir ištrinti atitinkamą svetainę. Šis procesas pavaizduotas 81 paveiksle.



81 pav. Svetainės URL panaikinimas iš blokuojamų svetainių sąrašo

9.4.7. Prieinamumo režimo įjungimas regos negalią turintiems naudotojams

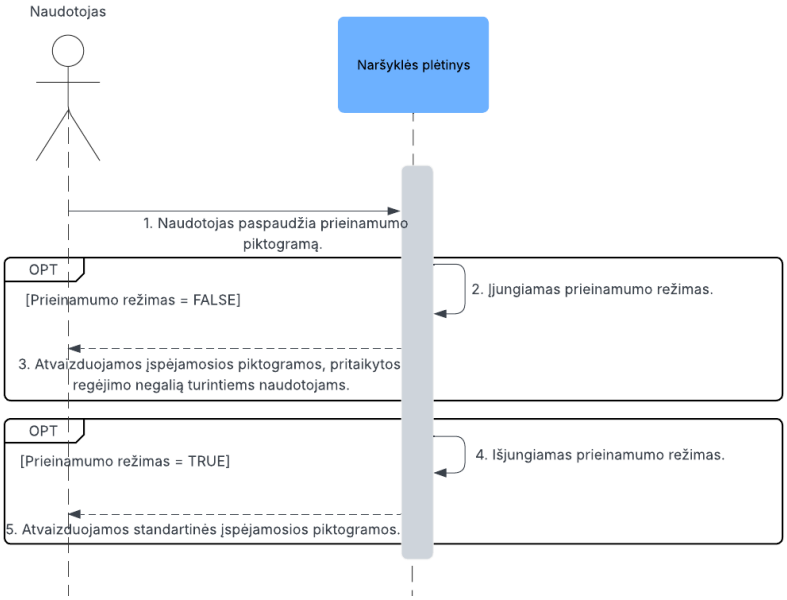
Regos negalią turintys naudotojai taip pat gali naudotis naršyklės įskiepiu. Jiems tereikia paspausti universalios prieigos piktogramą, ir įskiepis pakeičia piktogramų spalvų paletę į regos sutrikimų turintiems naudotojams pritaikytas spalvas. Šį procesą iliustruoja 82 diagrama.



82 pav. Prieinamumo režimo įjungimo procesas

9.4.7.1. Proceso eiga

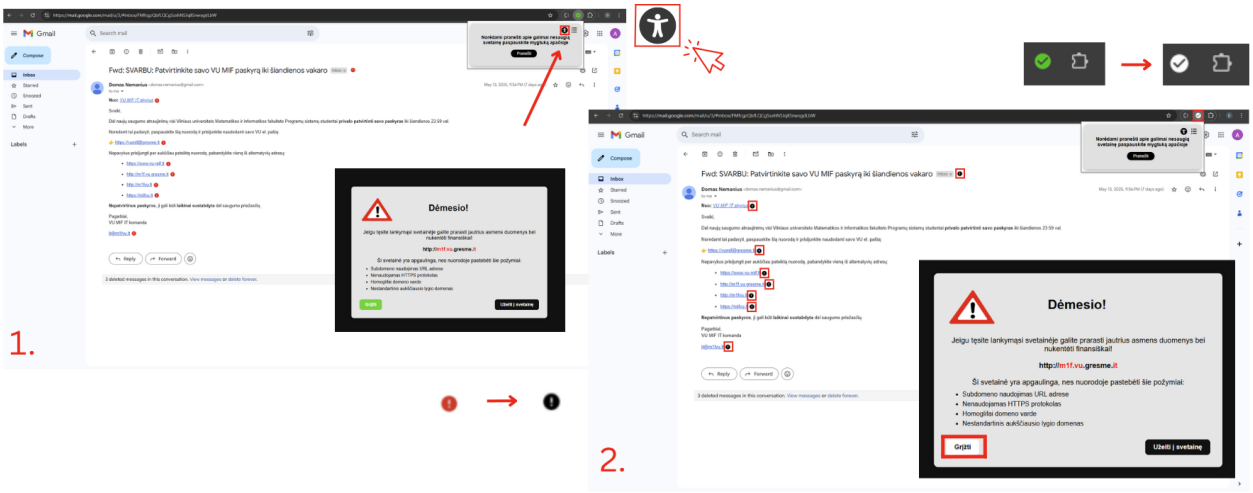
Toliau pateikta sekų diagrama (žr. 83 paveikslą) iliustruoja spalvų paletės pasikeitimo procesą, inicijuojamą naudotojui paspaudus universalios prieigos piktogramą.



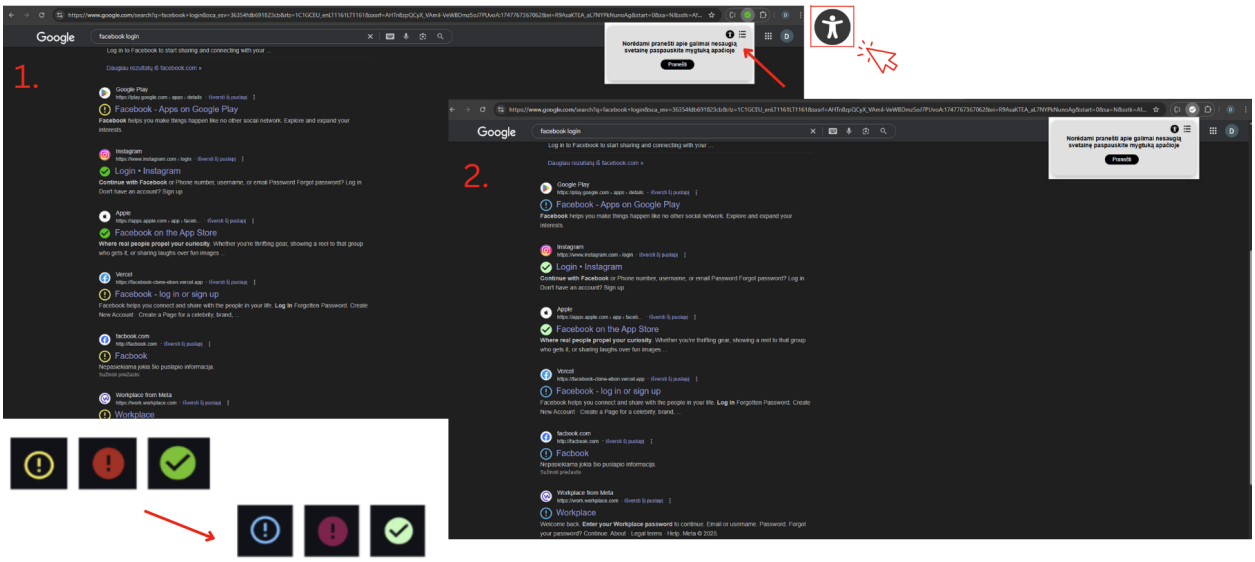
83 pav. Prieinamumo režimo įjungimo procesas, pavaizduotas sekų diagrama (angl. *sequence diagram*)

9.4.7.2. Funkcionalumo demonstracija

Paspaudus universalios prieigos piktogramą, naršyklės įskiepis automatiškai pakeičia spalvų paletę: įprastos šviesoforo spalvos piktogramos pakeičiamos į regos sutrikimų turintiems naudotojams pritaikytas spalvas, kurios pateiktos 57 paveiksle. Spalvų paletės pasikeitimo procesai pavaizduoti 84 ir 85 paveiksluose.



84 pav. Prieinamumo režimo įjungimas naudotojui skaitant elektroninį laišką

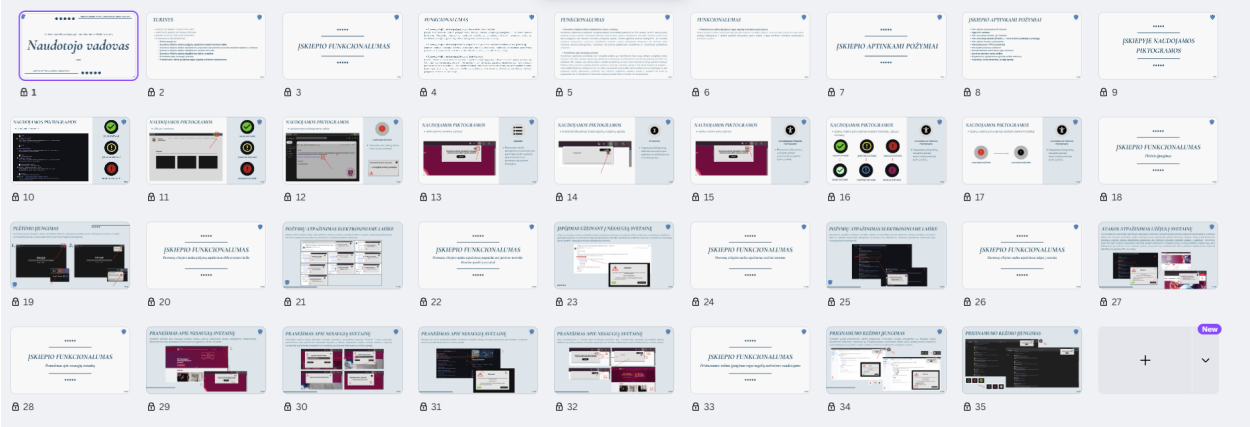


85 pav. Prieinamumo režimo įjungimas naudotojui naršant internete

9.5. Naršyklės įskiepio naudotojo vadovas

Sukūrus naršyklės įskiepį, buvo sukurtas ir naudotojo vadovas, kuriame pristatytas naršyklės funkcionalumas kartu su kiekvieno funkcionalumo aprašymu, aprašomi naršyklės įskiepio aptinkami požymiai, naudojamų piktogramų reikšmės. Sukurtas naudotojo vadovas, skirtas padėti naudotojui lengvai suprasti naršyklės plėtinio veikimą, išmokti atpažinti įspėjamuosius ženklus ir sužinoti, kaip naudotis visais įskiepio suteikiamais funkcionalumais. Naudotojo vadovą sudaro 35

skaidrės (žr. į 86 paveikslą), kuriose nuosekliai ir aiškiai pateikiama visa svarbiausia informacija apie įskiepio naudojimą. Nuoroda į **sukurto naršyklės įskiepio naudotojo vadovą.**



86 pav. Sukurto naršyklės įskiepio naudotojo vadovas

9.5.1. Naršyklės įskiepio logotipas

Sukūrus naudotojo vadovą, taip pat buvo sukurtas ir naršyklės plėtinio logotipas, kurio pagrindą sudaro skydo formos herbas (žr. į 87 paveikslą). Skydo viduje pavaizduoti trys pagrindiniai simboliai: spyna, kabliukas ir įspėjamasis ženklas, kurių kiekvienas turi aiškią reikšmę:

1. Spyna – simbolizuoja naudotojo duomenų saugumą ir parodo, kad pagrindinis plėtinio tikslas yra užtikrinti, jog naudotojo informacija nebūtų pasiekiama kenkėjiškais tikslais.
2. Kabliukas – vaizduoja sukčiavimo techniką, kai naudotojai tarsi „užkabinami“ apgaulės būdu.
3. Įspėjamasis ženklas – atspindi plėtinio funkciją: informuoti naudotoją apie galimą pavojų ir pateikti aiškius įspėjimus, kai svetainė atrodo įtartina.

Šie simboliai viename herbe perteikia pagrindinį sukurto naršyklės plėtinio tikslą – apsaugoti naudotoją nuo duomenų viliojimo atakų.

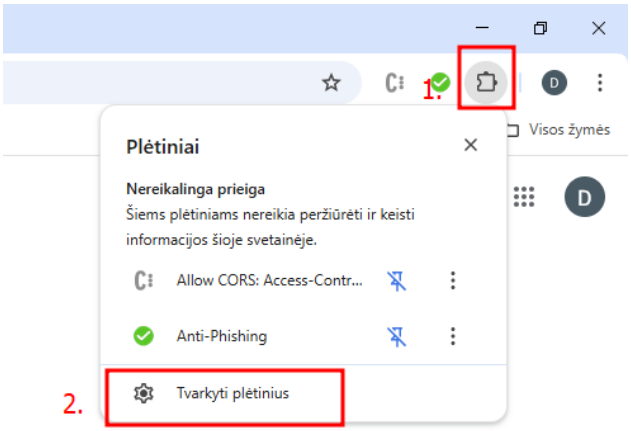
87 pav. Sukurto naršyklės įskiepio logotipas

9.6. Naršyklės įskiepio diegimas ir paleidimas

Šiame poskyryje pateikiamos sukurto „Google Chrome“ naršyklės plėtinio diegimo ir paleidimo instrukcijos. Sukurto „Google Chrome“ naršyklės plėtinio kodą galima rasti: „**GitHub**“. Taip pat sukurtas naršyklės plėtinys anglų kalba, jo programinį kodą galima rasti pasirinkus *main-eng* kodo versijavimo sistemos „GitHub“ šaką (angl. *branch*).

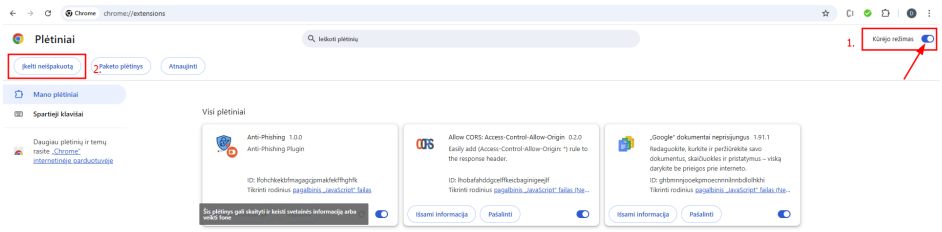
Naršyklės plėtinio įdiegimas ir paleidimas:

1. Atidaryti nuorodą: **naršyklės plėtinio nuoroda**.
2. Atsisiųsti *Anti-Phishing-plugin-lt.zip* (versija anglų kalba *Anti-Phishing-plugin-eng.zip*) failą.
3. Išarchyvuoti *Anti-Phishing-plugin-lt.zip* (versija anglų kalba *Anti-Phishing-plugin-eng.zip*) failą.
4. Įsijungti „Google Chrome“ naršyklę.
5. Spausti „Plėtiniai“ ir toliau spausti „Tvarkyti plėtinius“ (žr. 88 paveikslą). Nematant plėtinio ženkliuko, spausti „Nustatymai“ ir toliau „Plėtiniai“.



88 pav. Patekimas į naršyklės plėtinių tvarkymo langą

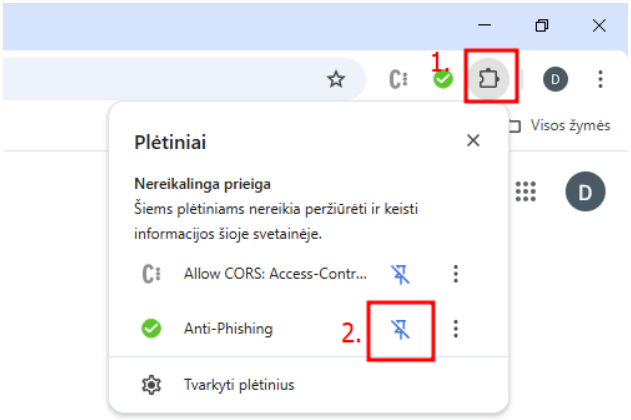
6. Įgalinti „Kūrėjo režimas“ ir toliau spausti „Įkelti neišpakuotą“ (žr. 89 paveikslą). Failų naršyklėje suraskite *Anti-Phishing-plugin-lt* (versija anglų kalba *Anti-Phishing-plugin-eng*) aplanką ir įkelkite. Įkėlus sėkmingai turėtumėte matyti naršyklės plėtinį tarp kitų plėtinių.



89 pav. Naršyklės plėtinio įkėlimas

7. Jei turite įdiegtą reklamų blokavimo plėtinį – išjunkite. Jis gali blokuoti naršyklės plėtinio iššokančius langus.

8. Uždaryti visus naršyklės langus ir iš naujo įjungti „Google Chrome“ naršyklę.
9. Spausti „Plėtiniai“ ir toliau spausti „Smeigtuko“ piktogramą, kad naršyklės įskiepis atsirastų naršyklės viršutinėje įrankių juostoje (žr. 90 paveikslą).



90 pav. Naršyklės plėtinio pridėjimas naršyklės įrankių juostoje

9.7. Sukurto naršyklės įskiepio demonstracinis video

Sukurto naršyklės įskiepio veikimas pristatomas video formatu. Vaizdo įrašas patalpintas „Google Drive“ platformoje ir pasiekiamas per viešai prieinamą **demonstracinio video** nuorodą.

10. Ateities darbai

Sukurtame naršyklės įskiepyje įgyvendintas pagrindinis funkcionalumas, skirtas naudotojų apsaugai nuo duomenų viliojimo atakų. Ateityje numatomi patobulinimai esamoms funkcijoms, papildomų požymių atpažinimo galimybių integravimas naudotojo sąsajoje bei likusių projektavimo gairių realizavimas.

10.1. Esamo naršyklės įskiepio funkcionalumo tobulinimai

1. Šiuo metu raginimai ir skubinantys įspėjimai atlikti konkrečius veiksmus elektroniniuose laiškuose yra atpažįstami remiantis iš anksto sudarytu žodžių ir frazių banku. Nors šis metodas leidžia identifikuoti daugelį standartinių atvejų, jis nėra nuolat atsinaujinantis ir pajėgus atpažinti raginimų, išreikštų kita formuluote, kurios nėra žodžių ir frazių banke. Ateityje būtų tikslinga integruoti dirbtinio intelekto sprendimus, gebančius automatiškai analizuoti elektroninių laiškų kontekstą ir identifikuoti įvairius raginimus ir skubinimus, būdingus duomenų viliojimo atakoms. Toks įskiepio funkcionalumas galėtų kur kas labiau padidinti atakų aptikimo tikslumą.
2. Šiuo metu aukščiausio lygio domenų baltasis sąrašas yra statinis ir realiu laiku neatsinaujinantis, todėl gali praleisti naujai atsiradusius teisėtus domenus arba neteisingai pažymėti juos kaip įtartinus. Siekiant užtikrinti tikslesnį URL adresų vertinimą ir sumažinti klaidingų atvejų skaičių, ateityje reikėtų integruoti automatiškai atsinaujinantį aukščiausio lygio domenų baltąjį sąrašą, sinchronizuojamą su oficialiais šaltiniais.
3. Šiuo metu naršyklės įskiepis naudoja juodąjį sąrašą, paremtą „Google Safe Browsing API“ protokolu, kuris leidžia identifikuoti iš anksčiau žinomas grėsmingas svetaines. Vis dėlto toks URL nuorodų tikrinimo sprendimas priklauso nuo anksčiau užfiksuotų nuorodų, kurios saugomos duomenų bazėje, todėl gali neaptikti naujai atsiradusių, dar neįtrauktų į ją svetainių. Ateityje rekomenduojama integruoti dirbtinio intelekto modelį, apmokytą su duomenų viliojimo atakų URL pavyzdžiais, kuris gebėtų identifikuoti potencialiai grėsmingus URL adresus remiantis jų struktūra, turiniu ar kontekstu, net ir tais atvejais, kai nuorodos nėra įtrauktos į oficialius pavojų keliančius svetainių sąrašus.
4. Šiuo metu naršyklės įskiepis diegiamas rankiniu būdu, tačiau ateityje plėtinys turėtų būti lengvai pasiekiamas populiariausių interneto naršyklių įskiepių parduotuvėse, siekiant užtikrinti lengvą prieigą, patogų diegimą ir platesnį naudotojų pasiekiamumą.
5. Šiuo metu naršyklės įskiepis pritaikytas regos negalią, aklumą spalvoms, turintiems naudotojams. Ateityje būtų tikslinga, kad įrankis atitiktų žiniatinklio turinio prieinamumo gaires (angl. *Web Content Accessibility Guidelines* (WCAG)) [Wor24]. WCAG nurodo, kokius prieinamumo reikalavimus turi atitikti programų sistema, kad būtų pritaikyta regos (angl. *visual*), klausos (angl. *auditory*), pažinimo (angl. *cognitive*), neurologinėms (angl. *neurological*), fizinėms (angl. *physical*) bei kalbos (angl. *speech*) negalioms.

10.2. Neįgyvendintos projektavimo gairės

1. **Projektavimo gairės „Suderinamumas su standartinėmis priemonėmis“ įgyvendinimas.** Šiuo metu naršyklės plėtinys yra sukurtas ir veikia tik „Google Chrome“ naršyklėje bei „Gmail“ elektroninio pašto dėžutėje. Siekiant užtikrinti projektavimo gairės DK.3 – Suderinamumas su standartinėmis priemonėmis įgyvendinimą, ateityje būtina išplėsti plėtinio funkcionalumą ir suderinamumą su kitomis plačiai naudojamomis naršyklėmis, tokiomis kaip „Mozila Firefox“, „Apple Safari“, „Microsoft Edge“, „Internet Explorer“, „Opera“ bei elektroninio pašto dėžutėmis, tokiomis kaip „Outlook“, „Yahoo“, „Thunderbird“. Toks išplėtimas padidintų įrankio prieinamumą ir panaudojamumo galimybes skirtingų naudotojų aplinkose.
2. **Projektavimo gairės „Praktinis taikymas realiose situacijose“ įgyvendinimas.** Kol kas sukurtą naršyklės plėtinį išbandė tik šio bakalauro darbo autoriai, jis nebuvo išbandytas kitų realių naudotojų. Ateityje būtų tikslinga įgyvendinti projektavimo gairę, kylančią iš kriterijaus DK. 4 – Praktinis taikymas realiose situacijose. Įrankis turėtų būti išbandytas naudotojų, naudojamas realiomis sąlygomis, realiai apsaugai nuo duomenų viliojimo atakų, ne tik mokslinių tyrimų tikslais. Tai suteiktų vertingą grįžtamąjį ryšį, praktines įžvalgas ir padėtų tobulinti plėtinio funkcionalumą bei gerinti naudotojo patirtį.

10.3. Neįgyvendintų duomenų viliojimo požymių atpažinimo galimybės naudotojo sąsajoje

1. **Prisijungimai iššokančiame lange.** Šis požymis – dažna duomenų viliojimo metodų praktika, iššokantys langai dažnai imituoja teisėtų paslaugų prisijungimo formas. Plečiant naršyklės įskiepio funkcionalumą ateityje reikėtų įdiegti mechanizmą, kuris identifikuotų prisijungimo formas, atvaizduojamas iššokančiuose languose ir įspėtų naudotoją apie galimą grėsmę, ypač, jeigu tokie langai naudoja URL nuorodas, kurios turi įtartinų požymių.
2. **Neaktyvios nuorodos internetinėje svetainėje.** Svetainės, skirtos duomenų viliojimo atakoms, dažnai naudoja tik kelias aktyvias nuorodas, pavyzdžiui, skirtas prisijungti ar patvirtinti informaciją, o kitos nuorodos dažnai būna neaktyvios. Siekiant užtikrinti šio požymio atpažinimą ateityje būtina išplėsti įskiepio funkcionalumą mechanizmu, kuris automatiškai patikrintų, kiek nuorodų svetainėje yra funkcionalios ir pateiktų naudotojui įspėjimą, kai pastebimas didelis kiekis neaktyvių nuorodų svetainėje, kurioje lankosi naudotojas.
3. **Dešiniojo pelės mygtuko išjungimas.** Duomenų viliojimo svetainėse neretai yra išjungiama dešiniojo pelės mygtuko funkcija siekiant užkirsti kelią naudotojams kopijuoti tekstą arba peržiūrėti puslapio šaltinio kodą. Tobulinant naršyklės įskiepį ateityje reikėtų išplėsti funkcionalumą pridedant automatinį fiksavimo mechanizmą, kuris informuotų naudotoją, pateikdamas paaiškinimą, kad toks elgesys kaip dešiniojo pelės mygtuko išjungimas dažnai pasitaiko nesaugiose, sukčiavimo tikslais sukurtose svetainėse.

Rezultatai

Darbe nagrinėtas duomenų viliojimo atakos gyvavimo ciklas, atakų tipai, požymiai, vertinti prevencijai skirti įrankiai remiantis suformuluotais vertinimo kriterijais. Taip pat kurti alternatyvieji maketai, atliktas maketų panaudojamumo testavimas, kiekybinis tyrimas, suprojektuotos projektavimo gairės, sukurtas detalusis prototipas bei naršyklės įskiepis. Darbo tikslas – identifikuoti duomenų viliojimo atakų požymius naudotojo sąsajoje, siekiant palengvinti naudotojo mokymąsi, atakų atpažinimą, sukurti projektavimo gaires bakalauro darbe kuriamai priemonei bei sukurti naršyklės įskiepį – priemonę, kuri padėtų apsaugoti naudotoją nuo duomenų viliojimo atakų. Darbo metu pasiekti šie rezultatai:

1. Literatūros analizės metu apžvelgtas duomenų viliojimo atakos gyvavimo ciklas, išskirti ir aprašyti duomenų viliojimo atakų tipai, kuriuos galima identifikuoti naudotojo sąsajoje.
2. Analizuojant duomenų viliojimo atakų tipus išskirti naudotojo sąsajos požymiai, identifikuojantys potencialias atakas. Šie požymiai sugrupuoti į URL nuorodoje aptinkamus požymius ir internetinių svetainių naudotojo sąsajoje aptinkamus požymius.
3. Jakobo Nielseno euristikos pritaikytos formuluojant panaudojamumo kriterijus, taip pat suformuluoti diegimo ir techninių sprendimų kriterijai.
4. Surinkti įrankiai, skirti apsaugoti naudotojus nuo duomenų viliojimo atakų. Atliktas įrankių vertinimas, remiantis suformuluotais panaudojamumo, diegimo ir techninių sprendimų kriterijais.
5. Suformuluotos projektavimo gairės kuriamai priemonei, skirtai apsaugoti naudotoją nuo duomenų viliojimo atakų, remiantis jomis parengti alternatyvieji maketai bei atliktas jų panaudojamumo testavimas.
6. Remiantis panaudojamumo testavimo rezultatais patikslintos projektavimo gairės.
7. Remiantis patikslintomis projektavimo gairėmis sukurtas detalusis prototipas.
8. Sukurtas „Google Chrome" naršyklės plėtinys, padedantis naudotojui atpažinti duomenų viliojimo atakas.
9. Bakalauro darbo tarpiniai rezultatai pristatyti 13-ojoje jaunųjų mokslininkų konferencijoje „Fizinių ir technologijos mokslų tarpdalykiniai tyrimai" š. m balandžio 11 dieną. Konferencijos programa pateikiama prieduose (žr. 3 priedą).
10. Iš bakalauro metu atlikto naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimo gautų rezultatų parašytas straipsnis publikuoti [SNL25]. Straipsnis pateikiamas prieduose (žr. 6 priedą). Taip pat pristatytas žodinis pranešimas 6-ojoje konferencijoje „Lietuvos magistrantų informatikos ir IT tyrimai" š.m. gegužės 13 dieną. Pažymėjimas, patvirtinantis dalyvavimą ir straipsnio publikavimą, pateikiamas prieduose (žr. 4 priedą). Pažymėjimai, patvirtinantys pristatytą pranešimą, pateikiami prieduose (žr. 5 priedą).

Išvados

Iš darbo metu gautų rezultatų galima daryti tokias išvadas:

1. Atlikus duomenų viliojimo atakų analizę, pastebėta, kad jos turi bendrų požymių, kuriuos galima išskirti naudotojo sąsajoje, o remiantis šiais požymiais galima mokyti naudotojus atpažinti duomenų viliojimo atakas ir kurti įrankius, skirtus apsaugoti naudotoją nuo duomenų viliojimo atakų.
2. Įvertinus įrankių panaudojamumą pastebėta, kad:
   a) įrankiai identifikuoja potencialias duomenų viliojimo atakas, tačiau nepaaiškina naudotojui, kodėl svetainė yra identifikuota kaip nesaugi, todėl galima teigti, kad nėra įrankio, kuris ne tik gebėtų atpažinti ir informuoti naudotoją apie potencialią duomenų viliojimo ataką, bet ir patį naudotoją mokytų atpažinti šias atakas;
   b) nėra įrankio, pritaikyto regėjimo negalią turinčiam naudotojui;
   c) įrankiai, naudojantys standartinio šviesoforo spalvas kaip pasyvų indikatorių informuoti apie potencialią grėsmę, yra suprantamesni pradedančiajam naudotojui, kuris nėra įpratęs ir nežino, ką reiškia kiti žymėjimai. Regėjimo negalią (aklumą spalvoms) turinčiam naudotojui, šalia spalvų indikatoriaus reikėtų ir piktogramos, informuojančios apie svetainės saugumą. Taigi, norėdamas patenkinti tiek pradedančiųjų, tiek regėjimo negalią turinčių naudotojų poreikius, kuriamas įrankis turėtų naudoti spalvų indikatoriaus ir piktogramos kombinaciją.
3. Atlikus įrankių vertinimą, matome, kad nėra įrankio, kuris visiškai padengtų visus vertinimo kriterijus. Daugiausiai kriterijų įgyvendina įrankiai: „McAfee Web Advisor“, „Netcraft“ ir „Bitdefender Traffic Light“. Vis dėlto, įrankiai neįgyvendina kriterijų: lankstumas ir naudotojo efektyvumas, prieinamumas, naudotojų mokymas. Iš dalies įgyvendina kriterijus: naudotojo kontrolė ir laisvė, klaidų prevencija, atpažinimas, o ne prisiminimas, pagalba ir dokumentacija. Šie kriterijai yra tobulintini.
4. Alternatyviųjų maketų panaudojamumo testavimo metu nustatyta, kad žemą kompiuterinio raštingumo lygį turintys naudotojai, neįvertina svetainių nuorodų patikimumo ir dažnai intuityviai renkasi pirmąjį paieškos rezultatą. Todėl naršyklės įskiepis, skirtas apsaugoti nuo duomenų viliojimo atakų, turėtų šalia kiekvieno paieškos rezultato rodyti svetainės saugumo lygį nurodančią piktogramą. Siekiant ne tik informuoti naudotoją, bet ir ugdyti jo gebėjimą atpažinti atakas, paspaudus piktogramą turėtų būti pateikiamas paaiškinimas, kodėl svetainė įvertinta kaip nesaugi. Tai leistų mokytis iš konkretaus pavyzdžio, susiejant matomą nuorodą su įvardytais rizikos požymiais.
5. Kiekybinio tyrimo rezultatai parodė, kad tyrimo metu nebuvo naudotojo, kuris, peržiūrėdamas el. laiškus ir juose pateikiamas nuorodas arba lankydamasis svetainėse, atkreiptų dėmesį į visus duomenų viliojimo atakas indikuojančius požymius. Dažniausiai ignoruojami tokie požymiai kaip dešiniojo pelės mygtuko išjungimas ar domeno vardo amžius. Todėl kuriami naršyklės įskiepiai turėtų automatiškai identifikuoti šiame darbe apibrėžtus požymius, galinčius indikuoti potencialią duomenų viliojimo ataką ir aktyviai įspėtų naudotoją apie galimas grėsmes, taip užtikrinant efektyvesnę apsaugą nuo sukčiavimo.

Šaltiniai

[AAO+24] R. K. Ayeni, A. A. Adebiyi, J. O. Okesola, E. Igbekele. Phishing Attacks and Detection Techniques: A Systematic Review. Iš: *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*. 2024, p. 1–17. Prieiga per internetą: https://doi.org/10.1109/SEB4SDG60871.2024.10630203.

[AAT14] N. Abdelhamid, A. Ayesh, F. Thabtah. Phishing detection based Associative Classification data mining. *Expert Systems with Applications*. 2014, tomas 41, numeris 13, p. 5948–5959. ISSN 0957-4174. Prieiga per internetą: https://doi.org/https://doi.org/10.1016/j.eswa.2014.03.019.

[AHN+21] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*. 2021, tomas 3, p. 563060. Prieiga per internetą: https://tinyurl.com/3rjt8kte.

[ARV19] K. Althobaiti, G. Rummani, K. Vaniea. A Review of Human- and Computer-Facing URL Phishing Features. Iš: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*. 2019, p. 182–191. Prieiga per internetą: https://doi.org/10.1109/EuroSPW.2019.00027.

[AZ17] A. Aleroud, L. Zhou. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*. 2017, tomas 68, p. 160–196. ISSN 0167-4048. Prieiga per internetą: https://doi.org/https://doi.org/10.1016/j.cose.2017.04.006.

[BHV+12] J. Bonneau, C. Herley, P. C. Van Oorschot, F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Iš: *2012 IEEE symposium on security and privacy*. IEEE, 2012, p. 553–567. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/6234436.

[Bir12] J. Birch. Worldwide prevalence of red-green color deficiency. *J. Opt. Soc. Am. A*. 2012, tomas 29, numeris 3, p. 313–320. Prieiga per internetą: https://doi.org/10.1364/JOSAA.29.000313.

[BZL+21] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, K. Kifayat. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*. 2021, tomas 76, p. 139–154. Prieiga per internetą: https://link.springer.com/article/10.1007/s11235-020-00733-2.

[DTH06] R. Dhamija, J. D. Tygar, M. Hearst. Why phishing works. Iš: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Montréal, Québec, Canada: Association for Computing Machinery, 2006, p. 581–590. CHI '06. ISBN 1595933727. Prieiga per internetą: https://doi.org/10.1145/1124772.1124861.

[GAP18] B. B. Gupta, N. A. Arachchilage, K. E. Psannis. Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*. 2018, tomas 67, p. 247–267. Prieiga per internetą: https://link.springer.com/article/10.1007/s11235-017-0334-z.

[GTJ+17] B. B. Gupta, A. Tewari, A. K. Jain, D. P. Agrawal. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*. 2017, tomas 28, p. 3629–3654. Prieiga per internetą: https://link.springer.com/article/10.1007/s00521-016-2275-y.

[Int23] L. Interisle Consulting Group. *Phishing Landscape 2023 A Study of the Scope and Distribution of Phishing*. 2023. [žiūrėta 2024-09-17]. Prieiga per internetą: https://static1.squarespace.com/static/63dbf2b9075aa2535887e365/t/65b966b32f82d97c583eccfc/1706649269929/PhishingLandscape2023.pdf.

[IWG+08] D. Irani, S. Webb, J. Giffin, C. Pu. Evolutionary study of phishing. Iš: *2008 eCrime Researchers Summit*. IEEE, 2008, p. 1–10. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/4696967.

[JDB+15] T. Jarassriwilai, T. Dauber, N. Brownlee, A. Mahanti. Understanding evolution and adoption of top-level domain names. Iš: *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*. IEEE, 2015, p. 687–694. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/7365915.

[JG22] A. K. Jain, B. Gupta. A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*. 2022, tomas 16, numeris 4, p. 527–565. Prieiga per internetą: https://www.tandfonline.com/doi/full/10.1080/17517575.2021.1896786.

[KLD+20] Y. Kwak, S. Lee, A. Damiano, A. Vishwanath. Why do users not report spear phishing emails? *Telematics and Informatics*. 2020, tomas 48, p. 101343. ISSN 0736-5853. Prieiga per internetą: https://doi.org/https://doi.org/10.1016/j.tele.2020.101343.

[LH07] L. Li, M. Helenius. Usability evaluation of anti-phishing toolbars. *Journal in Computer Virology*. 2007, tomas 3, p. 163–184. Prieiga per internetą: https://link.springer.com/article/10.1007/s11416-007-0050-4.

[LYC+19] Y. Li, Z. Yang, X. Chen, H. Yuan, W. Liu. A stacking model using URL and HTML features for phishing webpage detection. *Future Generation Computer Systems*. 2019, tomas 94, p. 27–39. ISSN 0167-739X. Prieiga per internetą: https://doi.org/https://doi.org/10.1016/j.future.2018.11.004.

[MTM12] R. M. Mohammad, F. Thabtah, L. McCluskey. An assessment of features related to phishing websites using an automated technique. Iš: *2012 International Conference for Internet Technology and Secured Transactions*. 2012, p. 492–497. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/6470857.

[PKK+10] P. Prakash, M. Kumar, R. R. Kompella, M. Gupta. Phishnet: predictive blacklisting to detect phishing attacks. Iš: *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, p. 1–5. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/5462216.

[SAE+24] A. H. Salem, S. M. Azzam, O. Emam, A. A. Abohany. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*. 2024, tomas 11, numeris 1, p. 105. Prieiga per internetą: https://link.springer.com/article/10.1186/s40537-024-00957-y.

[SC22] C. Surya prakasam, T. Chithralekha. A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*. 2022, tomas 9, p. 446–476. Prieiga per internetą: https://doi.org/10.19101/IJATEE.2021.875031.

[SNL25] K. Samusiovaitė, D. Nemanius, K. Lapin. Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas. *Vilnius University Open Series*. 2025, p. 209–217. Prieiga per internetą: https://doi.org/10.15388/LMITT.2025.24.

[SS23] I. Sharma, A. K. Sharma. Anti-phishing tools: A thorough comparison of features and performance. *International Journal for Research in Applied Science and Engineering Technology*. 2023, tomas 11, p. 478–482. Prieiga per internetą: https://www.researchgate.net/profile/Ishant-Sharma-8/publication/370634267_Anti-Phishing_Tools_A_Thorough_Comparison_of_Features_and_Performance/links/645b130c6090c43d0f5e6c7a/Anti-Phishing-Tools-A-Thorough-Comparison-of-Features-and-Performance.pdf.

[VK18] I. Vayansky, S. Kumar. Phishing–challenges and solutions. *Computer Fraud & Security*. 2018, tomas 2018, numeris 1, p. 15–20. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S1361372318300071.

[Wor24] World Wide Web Consortium. *Web Content Accessibility Guidelines (WCAG) 2.2*. 2024-12. W3C Recommendation, REC-WCAG22-20241212. W3C. Prieiga per internetą: https://www.w3.org/TR/WCAG22/.

[ZEC+07] Y. Zhang, S. Egelman, L. Cranor, J. Hong. Phinding phish: Evaluating anti-phishing tools. 2007. Prieiga per internetą: https://kilthub.cmu.edu/articles/journal_contribution/Phinding_Phish_Evaluating_Anti-Phishing_Tools/6470321/files/11898878.pdf.

Priedai

1 priedas

Peržiūrėtų šaltinių sąrašas

3 lentelė. Peržiūrėtų šaltinių sąrašas

Paieškos raktažodžiai	Rezultatų skaičius	Peržiūrėti šaltiniai	Mokslinė duomenų bazė	Šaltinio citavimų skaičius
Phishing	Apie 215 000 rezult.	https://dl.acm.org/doi/abs/10.1145/1124772.1124861	acm.org	2182
		https://ieeexplore.ieee.org/abstract/document/10049452	iee.org	79
		https://www.sciencedirect.com/science/article/pii/S0957417416000385	sciencedirect.com	291
		https://link.springer.com/chapter/10.1007/978-3-540-77465-5_19	researchgate.net	323
		https://ieeexplore.ieee.org/abstract/document/5254068	ieee.org	82
		https://www.sciencedirect.com/science/article/pii/S0167404817300810	sciencedirect.org	406
		https://ieeexplore.ieee.org/abstract/document/4696967	ieee.org	72
		https://arxiv.org/abs/1106.4692	arxiv.org	61
Phishing attack	Apie 108 000 rezult.	https://link.springer.com/article/10.1007/s00521-016-2275-y	spinger.com	387
		https://www.tandfonline.com/doi/full/10.1080/17517575.2021.1896786	tandfonline.com	186
		https://dl.acm.org/doi/abs/10.1145/2063176.2063197	acm.org	807
		https://dl.acm.org/doi/abs/10.1145/1314389.1314391	acm.org	738
		https://www.mdpi.com/1999-5903/12/10/168	mdpi.com	257
		https://ieeexplore.ieee.org/abstract/document/4149954	researchgate.net	213
		https://ieeexplore.ieee.org/abstract/document/1510078	ieee.org	248
		https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060	frontiersin.org	188
		https://www.accentsjournals.org/paperInfo.php?journalPaperId=1414	accentsjournals.org	13
Phishing attack challenges	Apie 71 500 rezult.	https://www.sciencedirect.com/science/article/pii/S1361372318300071	sciencedirect.com	155
		https://www.sciencedirect.com/science/article/pii/S0736585320300022?via%3Dihub	sciencedirect.com	96
Phishing attack prevention tools	Apie 48 800 rezult.	https://ieeexplore.ieee.org/abstract/document/9055943	ieee.org	46
		https://ieeexplore.ieee.org/abstract/document/6282648	ieee.org	45
		https://www.sciencedirect.com/science/article/pii/S0167404823002973	sciencedirect.com	69
		https://dl.acm.org/doi/abs/10.1145/1357010.1352620	acm.org	69
		https://link.springer.com/article/10.1007/s11416-007-0050-4	springer.com	62
Antipishing tools	Apie 1930 rezult.	https://ieeexplore.ieee.org/abstract/document/8256835	researchgate.net	1
		https://kilthub.cmu.edu/articles/journal_contribution /Phinding_Phish_Evaluating_Anti-Phishing_Tools/6470321/files/11898878.pdf	cmu.edu	437
Phising detection	Apie 90 000 rezult.	https://ieeexplore.ieee.org/abstract/document/6497928	ieee.org	776
		https://onlinelibrary.wiley.com/doi/full/10.1155/2017/5421046	wiley.com	256
		https://ieeexplore.ieee.org/abstract/document/8970564	ieee.org	138
		https://ieeexplore.ieee.org/document/10630203	ieee.org	3
		https://www.sciencedirect.com/science/article/pii/S0957417414001481	sciencedirect.com	445
		https://link.springer.com/article/10.1007/s11235-020-00733-2	springer.com	409
		https://ieeexplore.ieee.org/abstract/document/5462216	ieee.org	550
		https://link.springer.com/article/10.1186/s40537-024-00957-y	springer.com	24
Phishing attack prevention	Apie 60 800 rezult.	https://www.sciencedirect.com/science/article/pii/S1877050915007395	sciencedirect.com	40
		https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/meta	ioscience.iop.org	12
		https://link.springer.com/article/10.1007/s11235-017-0334-z	springer.com	400
URL features phishing	Apie 35 500 rezult.	https://www.nature.com/articles/s41598-022-10841-5	nature.com	49
		https://www.mdpi.com/2079-9292/9/9/1514	mdpi.com	110
		https://ieeexplore.ieee.org/document/8802422	ieee.org	44
Websites phishing features	Apie 101 000 rezult.	https://ieeexplore.ieee.org/abstract/document/6470857	ieee.org	308
		https://www.sciencedirect.com/science/article/pii/S0167739X1830503X	sciencedirect.com	246

2 priedas

Sutikimas dalyvauti panaudojamumo testavimo tyrime

SUTIKIMAS
DALYVAUTI PANAUDOJAMUMO TESTAVIME

Vilniaus universiteto Informatikos instituto programų sistemų 4 kurso studentų komanda atlieka naršyklės įskiepio panaudojamumo testavimą.

Jei sutinkate dalyvauti tyrime, būsite prašoma(s) naudoti naršyklės įskiepio prototipą, atlikti užduotis ir atsakyti į keletą klausimų. Klausimai bus pateikiami prieš tyrimą ir po jo. Jūsų sąveika su prototipu bus fiksuojama užrašuose ir stebima.

Negalime pasiūlyti jokio atlygio už dalyvavimą, nebent naudą, kurią gausite susipažindama(s) su būsimomis technologijomis. Tikime, kad šis tyrimas bus naudingas, tobulinant naršyklės įskiepį. Šis tyrimas Jums nekelia jokių pavojų, išskyrus kasdieninio gyvenimo rizikas.

Visa vertinimo sesijos informacija yra konfidenciali ir žymima ID numeriu. Jūsų vardo ir ID numerio atitikimo lentelė bus konfidenciali. Įsipareigojame neminėti vardų diskutuodami tarpusavyje ir publikuodami tyrimų rezultatus. Po tyrimo įrašai bus saugojami vidiniam tyrėjų naudojimui. Visiems saugomiems duomenims bus taikomi konfedencialumo reikalavimai.

Jūsų dalyvavimas yra laisvanoriškas. Jus galite atsisakyti ir nutraukti tyrimą bet kuriuo momentu. Jeigu turite klausimų dėl tyrimo, prašome kreiptis į Kamilę Samusiovaitę kamile.samusiovaite@stud.mif.vu.lt arba Domą Nemanių domas.nemanius@stud.mif.vu.lt. Galite kopijuoti šį sutikimą.

Sutinku _____
(vardas pavardė, data)

91 pav. Sutikimas dalyvauti tyrime

3 priedas

13-osios jaunųjų mokslininkų konferencijos „Fizinių ir tehcnologijos mokslų tarpdalykiniai tyrimai“ programa

13-toji jaunųjų mokslininkų konferencija
„Fizinių ir technologijos mokslų tarpdalykiniai tyrimai“

KONFERENCIJOS PROGRAMA

2025 balandžio 11

Vieta: Lietuvos mokslų akademija, Gedimino pr. 3, Vilnius

9:00 – 10:00	Registracija					
10:00 – 10:15	Konferencijos atidarymas Sveikinimo žodžiai					
10:15 – 10:20	Pasiskirstymas į sekcijas					
	Fizinių mokslų sekcija, LMA Mažoji salė			Technologijos mokslų sekcija, LMA 210 salė		
	Pranešėjas	Institucija	Pranešimo pavadinimas	Pranešėjas	Institucija	Pranešimo pavadinimas
	Moderatorius: dr. Vytautas Klimavičius			Moderatorius dr. Tadas Kallatka		
10:20 – 10:35	Marija Kalnaitytė	VU	Natūralaus pigmento magnio chlorofilino spektroskopinių savybių pokyčiai vandeninėse terpėse	Kamilė Samusiovaitė; Domas Nemanius	VU	Naudotojo apsauga nuo duomenų viliojimo atakų
10:35 – 10:50	Gerarda Jocytė	FTMC	Stibio selenido heterosandūrų tyrimas rentgeno ir ultravioletinių fotoelektronų spektroskopijos metodais	Teymur Aghayev	Vilnius TECH	Neuroscience combined with Artificial Intelligence
10:50 – 11:05	Simona Armalytė	VU	Didelio pasikartojimo dažnio femtosekundinio kontinuumo, sugeneruoto kristalinėse terpėse ir plinai normalios dispersijos fotoninių kristalų šviesolaidyje lyginamasis tyrimas	Anton Zagzin	VU	Skaidymo metodų vertinimas skirtingiems duomenų bazių tipams
11:05 – 11:20	Simona Bendžiūtė	VU	Stroncio chloropatito legiruoto europiu sintezė bei liuminescencinės savybės	Virgilijus Krinickij	VU	An Infrastructure for Asynchronous Network Data

92 pav. Konferencijos „Fizinių ir technologijos mokslų tarpdalykiniai tyrimai“ programa

4 priedas

Pažymėjimas, patvirtinantis straipsnio publikavimą ir dalyvavimą konferencijoje „Lietuvos magistrantų informatikos ir IT tyrimai“

PAŽYMĖJIMAS

2025-04-14
Vilnius

Kamilei Samusiovaitei, Domui Nemaniui

Mokslinės konferencijos „Lietuvos magistrantų informatikos ir IT tyrimai“ programinio komiteto vardu patvirtiname, kad Jūsų pateiktas straipsnis *„Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“* priimtas publikavimui ir žodiniam pranešimui šioje konferencijoje, kuri vyks 2025 m. gegužės 13 d. Lietuvos mokslų akademijoje. Straipsnis bus publikuotas konferencijos medžiagoje, išleistoje Vilniaus universiteto leidykloje.

Programinio komiteto pirmininkė

prof. dr. Olga Kurasova

93 pav. Pažymėjimas, patvirtinantis dalyvavimą konferencijoje ir straipsnio publikavimą

5 priedas

Pažymėjimai, patvirtinantys pristatytą pranešimą tema „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ konferencijoje „Lietuvos magistrantų informatikos ir IT tyrimai“

Pažymėjimas

Domas Nemanius

Vilniaus universitetas

dalyvavo VI-oje konferencijoje

Lietuvos magistrantų informatikos ir IT tyrimai

vykusioje 2025 m. gegužės 13 dieną
ir skaitė pranešimą

Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas

Programinis komitetas:

Prof. Gintautas Dzemyda

Prof. Olga Kurasova

Prof. Julius Žilinskas

Vilnius, 2025-05-13

94 pav. Pažymėjimas, skirtas Domui Nemaniui

Pažymėjimas

Kamilė Samusiovaitė

Vilniaus universitetas

dalyvavo VI-oje konferencijoje

Lietuvos magistrantų informatikos ir IT tyrimai

vykusioje 2025 m. gegužės 13 dieną
ir skaitė pranešimą

Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas

Programinis komitetas:

Prof. Gintautas Dzemyda

Prof. Olga Kurasova

Prof. Julius Žilinskas

Vilnius, 2025-05-13

95 pav. Pažymėjimas, skirtas Kamilei Samusiovaitei

6 priedas

Publikuotas straipsnis tema „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“

Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas

Kamilė Samusiovaitė, Domas Nemanius, Kristina Lapin

Vilniaus universitetas, Matematikos ir informatikos fakultetas,
Informatikos institutas,
Didlaukio g. 47, LT-08303 Vilnius
kamile.samusiovaite@mif.stud.vu.lt
domas.nemanius@mif.stud.vu.lt
kristina.lapin@mif.vu.lt

Santrauka. Straipsnyje siekiama atlikti apsaugos nuo duomenų viliojimo atakų įrankių panaudojamumo analizę ir remiantis gautais rezultatais sukurti projektavimo gaires priemonei, skirtai duomenų išviliojimo prevencijai. Straipsnyje surinkti ir aprašyti įrankiai, skirti apsaugoti naudotoją nuo duomenų viliojimo atakų. Jakobo Nielseno euristikos pritaikytos formuluojant panaudojamumo kriterijus, taip pat suformuluoti diegimo ir techninių sprendimų kriterijai. Remiantis šiais kriterijais atliktas įrankių vertinimas. Identifikuoti esamų įrankių privalumai ir neišnaudotos galimybės. Gautų rezultatų pagrindu, suformuluotos projektavimo gairės priemonei, skirtai apsaugoti naudotoją nuo duomenų viliojimo atakų.

Raktiniai žodžiai: duomenų viliojimas, įrankių vertinimas, panaudojamumas, diegimas.

1 Įvadas

Terminą duomenų viliojimo ataka (angl. *phishing*) pirmą kartą internete 1996 m. pavartojo įsilaužėlių grupė, kuri pavogė „America Online“ paskyras, apgaule privertusi naudotojus atskleisti savo slaptažodžius [1]. Nuo to laiko atakų skaičius vis augo, 2016 metais siekė 1,2 milijonus ir tai yra 65 % daugiau nei 2015 metais [2]. Remiantis naujausiu „Intersile Consulting Group, LLC“ atliktu tyrimu „Phishing Lanscape 2023: A Study of the Scope and Distribution of Phishing“, kuris buvo paskelbtas 2023 m. rugpjūčio 9 d., duomenų vagystės atakų skaičius per laikotarpį nuo 2022 m. gegužės iki 2023 m. balandžio išaugo 65 % lyginant su ankstesniu tyrimo laikotarpiu ir siekė 1,8 milijonus unikalių atakų [3]. Ir nors kasmet atakų skaičius vis didėja, vyksta nuolatinės varžybos tarp naujų sukčiavimo atakų ir joms atpažinti naudojamų apsaugos priemonių, juk nenuostabu, kad duomenų vagystės atakų

DOI: https://doi.org/10.15388/LMITT.2025.24

96 pav. Pirmasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis

atakų rengėjai keičia sukčiavimo strategiją atsižvelgdami į tas pačias rekomendacijas ir gaires, kuriomis naudojasi apsaugos priemonių kūrėjai [4] [5].

Duomenų vagystės atakos pasikeitė nuo jų atsiradimo 1990–aisiais. Ankstyvosiose atakose kibernetiniai nusikaltėliai naudojo paprastas taktikas – suklastotus elektroninius laiškus, kuriuose naudotojai buvo raginami prisijungti prie savo paskyrų. Pastaruoju metu duomenų vagystės atakos iš apgaulingų laiškų siuntinėjimo išsivystė į sudėtingas technikas, kurios remiasi psichologiniu manipuliavimu, išgaunant asmeninę informaciją [6]. Siekiant užtikrinti interneto naudotojų saugumą yra ieškoma įvairių kovos su duomenų viliojimo atakomis metodų.

Darbo tikslas – palyginti esamus prevencijos įrankius ir sukurti projektavimo gaires priemonei, kuri padėtų apsaugoti naudotoją nuo duomenų viliojimo atakų.

2 Duomenų viliojimo atakų prevencijos įrankių palyginimas

Šiame skyriuje yra identifikuojami kriterijai, kuriais remiantis straipsnyje vertinti įrankiai, skirti naudotojų apsaugai nuo duomenų viliojimo atakų. Panaudojamumo kriterijams formuluoti naudotos Jakobo Nielseno euristikos [7]. Taip pat suformuluoti diegimo kriterijai [8] bei naudojamų techninių sprendimų vertinimo kriterijai [9] [10]. Visi straipsnyje suformuluoti kriterijai pateikti žemiau esančioje lentelėje (žr. 1 lentelę).

1 lentelė. Įrankių vertinimo kriterijai.

Panaudojamumo kriterijai	PK. 1 Sistemos būsenos matomumas. PK. 2 Atitikimas tarp sistemos ir realaus pasaulio. PK. 3 Naudotojo kontrolė ir laisvė. PK. 4 Nuoseklumas ir standartai. PK. 5 Klaidų prevencija. PK. 6 Atpažinimas, o ne prisiminimas. PK. 7 Lankstumas ir naudojimo efektyvumas. PK. 8 Estetiškas ir minimalistinis dizainas. PK. 9 Pagalba ir dokumentacija.
Diegimo kriterijai	DK. 1 Prieinamumas. DK. 2 Minimalios išlaidos vienam naudotojui. DK. 3 Suderinamumas su naršyklėmis. DK. 4 Brandumas. DK. 5 Nepriklausomybė nuo nuosavybės teisių.
Techniniai sprendimai	TS. 1 Naudotojų mokymas. TS. 2 Juodieji/baltieji sąrašai. TS. 3 Giliojo mokymosi metodai ir mašininis mokymasis.

97 pav. Antrasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis

Kiekvienas kriterijus papildytas identifikatoriumi ir kriterijaus taikymo aprašymu. Kriterijų identifikatoriai yra nustatomi pagal pirmąsias žodžių raides, pavyzdžiui, „Panaudojumo kriterijai“ – PK. Toliau straipsnyje pateikiami keli vertinimo kriterijų pavyzdžiai PK.8 ir PK.1. Tarkime, Nielseno euristika „Estetiškas ir minimalistinis dizainas“ teigia, kad „Naudotojo sąsajoje neturėtų būti informacijos, kuri yra nesvarbi arba retai reikalinga. Kiekvienas papildomas informacinis elementas naudotojo sąsajoje varžosi su svarbiais informaciniais elementais ir mažina jų santykinį matomumą.“ Ši euristika straipsnyje performuluota štai taip:

PK.8 Estetiškas ir minimalistinis dizainas. Ši euristika teigia, kad įrankių tikslas – padėti naudotojams atpažinti ir sustabdyti atakas, o ne, pavyzdžiui, atkreipti dėmesį į komercines reklamas. Dėl šios priežasties įrankyje turi būti tik informacija susijusi su apsauga nuo duomenų viliojimo atakų. Glaustas ir tvarkingas dizainas padės naudotojui lengvai suprasti, į ką reikia atkreipti dėmesį ir kokių veiksmų imtis, kai pasirodo įspėjimas. Taip įrankis padės išvengti naudotojo suklaidinimo ir užtikrins greitą naudotojo atsaką į galimas grėsmes.

Kiekvienam kriterijui yra apibrėžiamas taikymas naudojant keturias piktogramas, kiekvienai nurodyta, kuo įrankis turi pasižymėti, kad gautų atitinkamą įvertį.

Pavyzdžiui, kriterijui PK.8, straipsnyje apibrėžiamas toks jo taikymas (žr. 2 lentelę):

2 lentelė. PK.8 kriterijaus taikymas.

⊖	– įrankyje yra daugiau informacijos nesusijusios su duomenų viliojimo atakomis ir apsauga nuo jų, nei kad susijusios.
○	– įrankyje yra informacija susijusi su apsauga nuo duomenų viliojimo atakų, tačiau yra daugiau nei viena reklama ar informacija, kuri nesusijusi su apsauga nuo duomenų viliojimo atakų.
◐	– įrankyje yra informacija susijusi su apsauga nuo duomenų viliojimo atakų, tačiau yra ne daugiau nei viena reklama ar informacija, kuri nesusijusi su apsauga nuo duomenų viliojimo atakų
●	– įrankyje yra tik informacija susijusi su apsauga nuo duomenų viliojimo atakų.

Remiantis Nielseno euristika „Sistemos būsenos matomumas“ „Dizainas visada turėtų informuoti naudotojus apie tai, kas vyksta, ir per atitinka-

98 pav. Trečiasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis

mą laiką suteikti tinkamą grįžtamąjį ryšį.“ Šiam kriterijui euristika perfomuluota taip:

PK.1 būsenos matomumas. Euristika tikrina vizualinius gebėjimus trijose stadijose: prieš patenkant į svetainę tikrinant svetainės autentiškumą, tikrinant svetainės autentiškumą bandant patekti į svetainę ir esant joje. Kiekvienoje stadijoje svetainė, kurioje lankosi naudotojas, turėtų informuoti naudotoją apie vykstantį procesą ir pateikti svetainės autentiškumo rezultatą. Rezultato pateikimas turėtų būti nuolat rodomas. Šio kriterijaus taikymas pavaizduotas (žr. 3 lentelę).

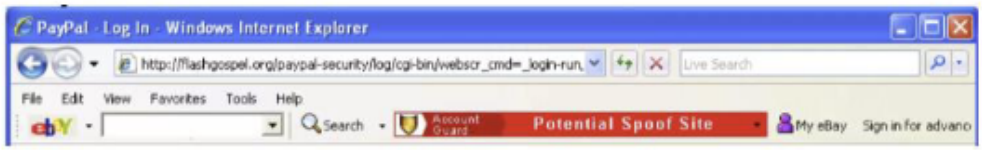
3 lentelė. PK.1 kriterijaus taikymas.

⊖	– kriterijus neįgyvendinamas.
○	– įrankio būsena yra matoma bent vienoje stadijoje.
◐	– įrankio būsena yra matoma dvejose stadijose.
●	– įrankio būsena yra matoma visose trijose stadijose.

Visi straipsnyje rasti ir aprašyti įrankiai įvertinti pagal visus apibrėžtus panaudojamumo, diegimo bei techninių sprendimų kriterijus. Žemiau pateikiamas vieno iš įrankių vertinimo pavyzdys pagal keletą apibrėžtų vertinimo kriterijų.

„eBay“ įrankių juostos aprašymas: Šis įrankis naudoja euristikų ir juodųjų sąrašų derinį. Įrankių juostoje esantys indikatoriai informuoja naudotoją apie svetainės patikimumą. Indikatoriai turi tris spalvas: žalią, raudoną ir pilką. Įrankių juostoje esanti piktograma vaizduojama žalia spalva, jeigu naudotojas lankosi svetainėje, kurioje yra integruotos „eBay“ ar „Paypal“ suteikiamos paslaugos (žr. 1 paveikslą). Raudona spalva vaizduojama, kai svetainė yra žinoma kaip sukčiavimo svetainė, o pilka spalva, kai svetainė nesinaudoja „eBay“ ar „Paypal“ paslaugomis ir nėra žinoma kaip sukčiavimo svetainė. Svetainės, kurios yra žinomos kaip apgaulingos yra blokuojamos, o iššokantis langas suteikia galimybę naudotojams panaikinti svetainės blokavimą. Įrankis taip pat suteikia galimybę naudotojams patiems pranešti apie sukčiavimo svetainės, kurios patikrinamos ir įtraukiamos į juoduosius sąrašus. „eBay“ įrankių juosta veikė „Microsoft Windows 98/ME/NT/2000/XP“ operacinėse sistemose su interneto naršykle „Internet Explorer“.

99 pav. Ketvirtasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis



1 pav. „Ebay" įrankis praneša apie sukčiavimo svetainę. Ekrano nuotrauka paimta iš straipsnio *[11]*.

Vertinimo pavyzdys:

- ◯ **PK.1 – Pagrindimas:** įrankis tikrina svetainės autentiškumą tik vienoje stadijoje, kai naudotojas jau yra užėjęs į svetainę.
- ⊖ **PK.8 –Pagrindimas:** įrankį sudaro tik piktogramos esančios įrankių juostoje, todėl galime teigti, kad yra tik informacija susijusi su apsauga nuo duomenų viliojimo atakų

Įrankių vertinimas atskleidė, kad nėra įrankio, kuris pilnai padengtų visus vertinimo kriterijus. Daugiausiai kriterijų įgyvendina naujausi įrankiai: „McAfee Web Advisor", „Netcraft" ir „Bitdefender Traffic Ligh". Vis dėlto, šie įrankiai neįgyvendina kriterijų: lankstumas ir naudotojo efektyvumas, prieinamumas, naudotojų mokymas. Išvardinti įrankiai dalinai įgyvendina kriterijus: naudotojo kontrolė ir laisvė, klaidų prevencija, atpažinimas, o ne prisiminimas, pagalba ir dokumentacija. Šie kriterijai yra tobulintini (žr. 2 paveikslą).

3 Projektavimo gairės

Atlikus jau egzistuojančių įrankių, skirtų apsaugoti naudotoją nuo duomenų viliojimo atakų, vertinimą, suformuluotos projektavimo gaires, remiantis pastebėtais įrankių privalumais ir trūkumais vertintuose įrankiuose.

1. **Projektavimo gairė iš kriterijaus PK.1** Projektuojamas įrankis turėtų tikrinti svetainės autentiškumą naudotojui dar prieš užeinant į svetainę, taip pat, naudotojui bandant užeiti į svetainę ir jau užėjus į svetainę bei mokyti naudotojus, kad šie patys atpažintų galimas duomenų viliojimo atakas ir nevestų savo jautrių duomenų sukčiavimo svetainėse.
2. **Projektavimo gairė iš kriterijaus PK.2** Projektuojamas įrankis turėtų naudoti naudotojams lengvai atpažįstamų spalvų piktogramas, naudoti standartinio šviesoforo įspėjamąsias spalvas, dar geriau, jeigu įrankis naudotų aktyviuosius indikatoriais su lengvai išmokstamais ir atpažįstamais nurodymais ir įspėjimais.

100 pav. Penktasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas" puslapis

	Įrankiai											
	„CallingID“	„Cloudmark AntiFraud“	„EarthLink“	„Ebay“	„Firefox 2“	„GeoTrust TrustWatch“	„Microsoft Internet Explorer 7“	„Netscape Browser 8.1“	„SpoofGuard“	„Bitdefender Traffic Light“	„Netcraft“	„McAfee Web Advisor“
Panaudojamumo kriterijai												
PK.1 Sistemos būsenos matomumas.	○	○	○	○	○	○	○	○	○	◐	○	◐
PK.2 Atitikimas tarp sistemos ir realaus pasaulio.	○	○	○	⊘	⊘	○	⊘	⊘	○	●	●	⊘
PK.3 Naudotojo kontrolė ir laisvė.	N/A	N/A	○	○	○	N/A	○	○	○	○	○	○
PK.4 Nuoseklumas ir standartai.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	●	●	●
PK.5 Klaidų prevencija.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	○	○	○
PK.6 Atpažinimas, o ne prisiminimas.	○	○	○	○	◐	○	○	○	○	○	○	○
PK.7 Lankstumas ir naudojimo efektyvumas.	N/A	N/A	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
PK.8 Estetiškas ir minimalistinis dizainas.	●	●	●	●	●	●	●	◐	●	●	●	●
PK.9 Pagalba ir dokumentacija.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	○	○	○	○
Diegimo kriterijai												
DK.1 Prieinamumas.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
DK.2 Minimalios išlaidos vienam naudotojui.	●	●	●	●	●	●	●	●	●	●	●	●
DK.3 Suderinamumas su naršyklėmis.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	●	●	⊘
DK.4 Brandumas.	●	●	●	●	●	●	●	●	●	●	●	●
DK.5 Nepriklausomybė nuo nuosavybės teisių.	●	●	●	●	●	●	●	●	●	●	●	●
Techniniai sprendimai												
TS.1 Naudotojų mokymas.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
TS.2 Juodieji/baltieji sąrašai.	⊘	●	●	●	●	●	●	●	⊘	⊘	●	●
TS.3 Giliojo mokymosi metodai ir mašininis mokymasis.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	●	●
TS.4 Euristikomis grįstas atpažinimas.	●	⊘	●	●	●	⊘	●	⊘	●	●	●	●

⊘ – neįgyvendinta, ○ – dalinai įgyvendinta, ◐ – pusiau įgyvendinta, ● – pilnai įgyvendinta

2 pav. Įrankių vertinimo rezultatai.

101 pav. Šeštasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis

3. **Projektavimo gairė iš kriterijaus PK.3** Projektuojamas įrankis turėtų leisti naudotojui anuliuoti ir pakartoti savo veiksmus. Tai reiškia, kad kai naudotojas užeina į nesaugią svetainė ir įrankis apie tai įspėja naudotoją, naudotojas turi turėti galimybę arba išeiti iš svetainės, arba pasilikti joje, tačiau jeigu naudotojas nusprendžia pasilikti svetainėje tai įrankis turėtų perklausti, ar naudotojas tikrai nori ir yra įsitikinęs, kad nori lankytis nesaugioje svetainėje.
4. **Projektavimo gairė iš kriterijaus PK.4** Projektuojamas įrankis kiek įmanoma labiau turėtų būtų pritaikytas skirtingoms naršyklėms. Tai reiškia, kad kuriamo įrankio kalba, indikatoriai, veiksmai turėtų būti suprantami naudotojams nepriklausomai nuo to, kokią naršyklę naudotojas yra pratęs naudotis.
5. **Projektavimo gairė iš kriterijaus PK.5** Projektuojamas įrankis turėtų teikti įspėjimus ir patarimus kaip ištaisyti klaidas (kaip išeiti iš puslapio, į ką atkreipti dėmesį) ir tai turėtų daryti prieš naudotojui užeinant į svetainę ir naudotojui užėjus į svetainę.
6. **Projektavimo gairė iš kriterijaus PK.6** Projektuojamas įrankis turi turėti įspėjimus ir patarimus, kaip apsisaugoti nuo duomenų viliojimo atakų ir tie patarimai turi būti aiškus ir suprantami bei rodomi iš karto (o ne paspaudus ant dar vienos nuorodos, ar nuėjus į dar vieną svetainė).
7. **Projektavimo gairė iš kriterijaus PK.7** Jeigu projektuojamame įrankyje būtų galimybė naudotojams atlikti veiksmus, kurie nekeltų pavojaus jų saugumui internete, tai būtų gerai, jeigu projektuojamas įrankis turėtų galimybę patyrusiems naudotojams praleisti pasikartojančius veiksmus.
8. **Projektavimo gairė iš kriterijaus PK.8** Projektuojamame įrankyje turėtų būti tik informacija susijusi su apsauga nuo duomenų viliojimo atakų. Įrankio vizualinę dalį neturėtų užimti su saugumu nesusiję indikatoriai, logotipai ar reklamos.
9. **Projektavimo gairė iš kriterijaus PK.9** Projektuojamas įrankis turėtų turėti bent jau prieinamą dokumentaciją ar mokomąją medžiagą, kad naudotojai galėtų pasiskaityti apie funkcionalumus bei mokėtų patys savarankiškai įsidiegti įrankį savo kompiuteryje.
10. **Projektavimo gairė iš kriterijaus DK.1** Projektuojamas įrankis turėtų būti pritaikytas ir regos negalią turintiems naudotojams.
11. **Projektavimo gairė iš kriterijaus DK.2** Projektuojamas įrankis turėtų būti nemokamas ir lengvai prieinamas visiems naudotojams ar organizacijoms.

102 pav. Septintasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis

12. **Projektavimo gairė iš kriterijaus DK.3** Projektuojamas įrankis turėtų veikti naudojant standartinius įrankius ar naršykles be papildomų diegimų.
13. **Projektavimo gairė iš kriterijaus DK.4** Projektuojamas įrankis turėtų būti išbandytas naudotojų, naudojamas realiomis sąlygomis, realiai apsaugai nuo duomenų viliojimo atakų ne tik mokslinių tyrimų tikslais.
14. **Projektavimo gairė iš kriterijaus DK.5** Projektuojamas įrankis turėtų būti prieinamas kiekvienam naudotojui ir juo turi būti galima naudotis nemokant už tai autorinio atlyginimo.
15. **Projektavimo gairė iš techninių sprendimų kriterijų**. Projektuojamas įrankis turėtų naudoti bent tris iš keturių techniniu sprendimų. Įrankis turėtų gebėti atpažinti jau žinomas duomenų viliojimo atakas (naudoti juoduosius/baltuosius sąrašus), turėtų gebėti atpažinti naujas duomenų viliojimo atakas (naudoti euristikomis grįstą atpažinimą) bei turėtų šviesti ir mokyti naudotoją savarankiškai atpažinti duomenų viliojimo atakas (mokyti naudotojus).

4 Išvados

Straipsnyje įvertinus ir palyginus duomenų viliojimo atakų prevencijai skirtus įrankius, techninių sprendimų vertinimas atskleidė, kad vertinti įrankiai identifikuoja potencialias duomenų viliojimo atakas, tačiau nepaaiškina naudotojui, kodėl svetainė yra identifikuota kaip nesaugi, todėl galima teigti, kad nėra įrankio, kuris ne tik gebėtų atpažinti ir informuoti naudotoją apie potencialią duomenų viliojimo ataką, bet ir patį naudotoją mokytų atpažinti potencialias atakas.

Panaudojamumo vertinimo metu pastebėta, kad įrankiai naudojantys standartinio šviesoforo spalvas kaip pasyvų indikatorių informuoti apie potencialią grėsmę yra suprantamesni pradedančiajam naudotojui, kuris nėra pratęs ir nežino ką reiškia kitokie žymėjimai. Informavimas apie grėsmes yra svarbus naudotojo saugumui užtikrinti, todėl ateityje kuriami įrankiai turėtų tikrinti svetainės autentiškumą trijose naršymo stadijose: prieš užeinant į nesaugią svetainę (gavus svetainės nuorodą), užeinant (paspaudus ant nuorodos) ir esant joje. Taip pat nėra nei vieno įrankio, kuris turėtų lengvai suprantamą ir prieinamą pagalba ar dokumentaciją, tai svarbu pradedantiesiems naudotojams norint greitai išmokti naudotis įrankiu.

Vertinimas pagal diegimo kriterijus atskleidė, kad nėra įrankio pritaikyto regėjimo negalią turinčiam naudotojui. Be to, regėjimo negalią (aklumą

103 pav. Aštuntasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas“ puslapis

spalvoms) turinčiam naudotojui, šalia spalvų indikatoriaus reikėtų ir piktogramos informuojančios apie svetainės saugumą. Taigi, norėdamas patenkinti tiek pradedančiųjų tiek regėjimo negalią turinčių naudotojų poreikius, kuriamas įrankis turėtų naudoti spalvų indikatoriaus ir piktogramos kombinaciją.

Literatūra

[1] Gupta, Brij B , Tewari, Aakanksha, Jain ir Anki, „Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications,* pp. 3629--3654, 2017.

[2] Basit, Abdul, Zafar, Maham, Liu, Xuan, Javed, A. Rehman, Jalil, Z. a. Kifayat ir Kashif, „A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems,* pp. 139--154, 2021.

[3] Consulting, Group L. Interisle, „Phishing Landscape 2023 A Study of the Scope," 2024.

[4] Dhamija, R. a. Tygar, J. D. a. Hearst ir Marti, „Why phishing works," įtraukta *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Montréal, Québec, Canada, 2006.

[5] Irani, D. a. Webb, S. a. Giffin, J. a. Pu ir Calton, „Evolutionary study of phishing," įtraukta *2008 eCrime Researchers Summit*, 2008.

[6] Alkhalil, Z. Hewage, C. Nawaf, L. Khan ir Imtiaz, „Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science,* 2021.

[7] Li, L. a. Helenius ir Marko, „Usability evaluation of anti-phishing toolbars," *Journal in Computer Virology,* pp. 163-184, 2007.

[8] Bonneau, J. a. Herley, C. a. V. Oorschot, P. C. a. Stajano ir Frank, „The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *2012 IEEE symposium on security and privacy,* pp. 553-567, 2012.

[9] Ayeni, R. Korede, Adebiyi, A. Ariyo, Okesola, J. Olatunji, Igbekele ir Ennmanuel, „Phishing Attacks and Detection Techniques: A Systematic Review," *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG),* pp. 1-17, 2024.

[10] Zhou ir A. A. a. Lina, „Phishing environments, techniques, and countermeasures: A survey," *Computers & Security,* pp. 160-196, 2017.

[11] ZHANG, Yue ir e. al., „Phinding phish: Evaluating anti-phishing tools," 2007.

104 pav. Devintasis publikuoto straipsnio „Naudotojo apsaugos nuo duomenų viliojimo atakų įrankių palyginimas" puslapis