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

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.

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-

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“.

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.

		Įrankiai											
		„McAfee Web Advisor"	„Netcraft"	„Bitdefender Traffic Light"	„SpoofGuard"	„Netscape Browser 8.1"	„Microsoft Internet Explorer 7"	„GeoTrust TrustWatch"	„Firefox 2"	„Ebay"	„EarthLink"	„Cloudmark AntiFraud"	„CallingID"
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
	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.

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.

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

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.