****

**Kauno technologijos universitetas**

Informatikos fakultetas

**Modulis „Tiriamasis projektas 1“  
Projektas: Mašininį mokymąsi naudojantis Google Chrome naršyklės įskiepis, vertinantis interneto svetainių saugumą pagal URL adresą**

Projekto paraiška

|  |  |
| --- | --- |
|  |  |
| **IFM 9/2 gr. Liudas Kazalupskis**  Studentas / Studentė | (parašas) (data) |
|  |  |
| **Prof. Robertas Damaševičius**  Projekto vadovas | (parašas) (data) |
|  |  |
| **Lekt. Virginija Limanauskienė**  Dėstytoja | (parašas) (data) |
|  |  |

**Kaunas, 2019**

Turinys

[1. Projekto paraiška 3](#_Toc27302653)

[1.1. Poreikis 3](#_Toc27302654)

[1.1.1. Projekto vartotojai ir klientai 3](#_Toc27302655)

[1.1.2. Vartotojo problemos 3](#_Toc27302656)

[1.1.3. Rinkos tyrimas 3](#_Toc27302657)

[1.1.4. Informacija apie klientus 4](#_Toc27302658)

[1.2. Pasiūlymas 4](#_Toc27302659)

[1.2.1. Produkto ar paslaugos apibūdinimas 4](#_Toc27302660)

[1.2.2. Sistemos kontekstas 4](#_Toc27302661)

[1.2.3. Bendri apribojimai 4](#_Toc27302662)

[1.2.4. Projekto įgyvendinimo planai ir kokybės vertinimas 5](#_Toc27302663)

[1.3. Nauda 5](#_Toc27302664)

[1.4. Konkurencija ir alternatyvos 6](#_Toc27302665)

[1.5. Santrauka 6](#_Toc27302666)

# Projekto paraiška

**Įvadas arba Santrauka**

Fišingas yra vienas kibernetinių nusikaltėlių vagiliavimo būdas. Dažniausiai per el. laiškus, žinutes siunčiami laiškais, kuriuose apsimetama teisėtais vartotojais, tokiais kaip draudėjai, paslaugų teikėjai ar su darbu susijusiais asmenimis ir prašoma prisijungti per jų svetainę ir tai padarius jūs prarandate savo duomenis ar pinigus.​ Tokios atakos dažnai būna nukreiptos į didelio kapitalo įmonėse dirbančius žmonės ir taip kėsinamasi į konfidencialią įmonės informaciją

Įskiepis, kuris gebėtų identifikuoti tokio tipo internetines svetaines pagal jų URL adresą padėtų žmonės apsaugoti asmeninius duomenis, o įmonėms įvairią konfidencialią informaciją nuo itin dažnai pasitaikančių kenkėjiškų interneto svetainių.

Atsižvelgiant į tai, kad vis daugiau sutarčių, sąskaitų ar kitokių dokumentų yra saugomi kompiuteriuose ar internetinėje erdvėje, fišingo tipo išpuolių skaičius tik augs ir jie tobulės, dėl to įrankis, kuris padėtų neįkliūti bus aktualus ir ateityje.

## Poreikis

### Projekto vartotojai ir klientai

Šios sistemos vartotojas yra kiekvienas asmuo, turintis prieigą prie interneto ir internete saugantis bet kokią informaciją. Paprastai žmonės skuba, per skubėjimą būna pasidaro neatidūs ir taip gali prarasti savo duomenis.

### Vartotojo problemos

Potencialus klientas yra kiekvienas interneto vartotojas, kurio privati informacija yra pasiekiama internete, tačiau reikalinga autentifikacija, kad ją pasiekti. Ypatingai tai yra svarbu žmonėms, kurie turi prieigą prie konfidencialios, dažniai įmonei priklausančios informacijos. Tokios informacijos nutekėjimas gali būti kritinis ir sužlugdyti įmonę.

### Rinkos tyrimas

Rinkoje pavyko surasti tris įskiepius gebančius apsisaugoti nuo „Phishing“, tačiau visi jie yra skirtingi ir tarpusavyje, ir nuo kuriamo įskiepio.

Didžiausio pelno būtų galima pasiekti B2B sektoriuje įskiepį parduodant įmonės, turinčios vertingos informacijos saugomos elektroninėje erdvėje, kai prie jos prieiti gali daug darbuotojų iš savo asmeninių kompiuterių. Naudojant tokį įrankį būtų lengviau apsisaugoti nuo informacijos praradimo, kaip kibernetinių nusikaltėlių taikinyje atsiduria patiklieji darbuotojai. Tokį įrankį pardavus didelėms kompanijoms už mėnesinį prenumeratos mokestį gautume pastovias pajamas, kurios pirmiausiai padengtų gamybos ir palaikymo išlaidas, o vėliau neštų pelną.

### Informacija apie klientus

Klientai yra asmenys, kurie yra pilnamečiai, turintys bent vidutinį kompiuterinį raštingumą, dažniausiai pabaigę studijas aukštojoje mokykloje tiksliuosius mokslus, pavyzdžiui ekonomiką, informatiką, finansų valdymą.

## Pasiūlymas

### Produkto ar paslaugos apibūdinimas

Šio darbo tikslas yra pasitelkus mašininį mokymą apmokyti modelį naudojant viešai prieinamus duomenis su kenkėjiškais ir tinkamais URL adresais, kuris gebėtų didesniu nei 97% tikslumu atpažinti kenkėjiškas interneto svetaines.

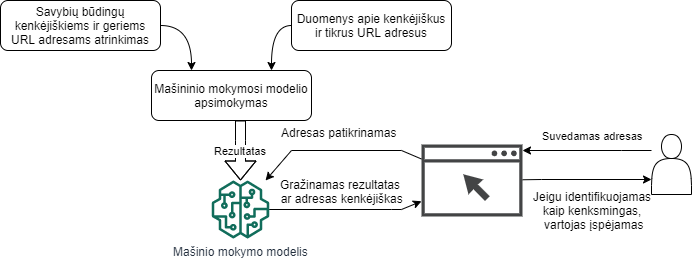
Realizuojant išorinę sąsają reikės sukurti naršyklės įskiepį, kuris identifikuotų kenkėjiškas internetines svetaines prieš vartotojui jas pasiekiant iš URL adreso naudodamas anksčiau minėtą modelį.

### Sistemos kontekstas

Pirmiausiai turi būti apmokytas modelis. Tam, kad tai padaryti reikia gauti duomenis apie kenkėjiškus ir korektiškus ULR adresus, juos išanalizuoti ir atrinkti savybės, pagal kurias galima identifikuoti ar kenkėjiškus adresus.

Apmokius mašininio mokymosi modelį, jį reikia integruoti į įskiepį, kuris vėliau bus įdiegtas į naršyklę.

Galiausiai, kai įskiepis jau įdiegtas, vartotojui įvedus URL adresą, jis yra patikrinamas ir jeigu identifikuojamas kaip kenkėjiškas – vartotojas būna įspėjamas apie galimą grėsmę.



### Bendri apribojimai

URL adreso identifikavimas turi būti atliekamas greičiau negu per 0.5 sekundės.

Kol vykdoma identifikacija naršyklė negali nustoti veikti, taip pat turi optimaliai naudoti kompiuterio resursus.

### Projekto įgyvendinimo planai ir kokybės vertinimas

Projekto veiklos ir rezultatai atitinka Magistrinio projekto įgyvendinimo akademinį grafiką.

Kokybės vertinimo kriterijų pasiūlymas, pateiktas 1 lentelėje.

**1 lentelė.** Sistemos vertinimo kriterijai

|  |  |  |
| --- | --- | --- |
| Nr. | Kriterijus | Pagrindimas |
| 1 | Tikslumas | Kokiu tikslumu įskiepis geba identifikuoti kenkėjiškus ir nekenkėjiškus URL adresus. |
| 2 | Panaudojamumas | Įskiepio įdiegimo sudėtingumas |
| 3 | Greitaveika | Kaip greitai yra identifikuojami URL adresai |

Projektą įgyvendins Liudas Kazalupskis, jam vadovaus Prof. Robertas Damaševičius.

Projekto biudžeto skaičiavimas pateiktas 2 lentelėje.

**2lentelė.** Projekto biudžetas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Išlaidos | Vienetas | Vienetų skaičius | Vieneto kaina, Eur | Viso, Eur |
| 1. Žmonių ištekliai |  |  |  |  |
| Analitikas | Darbo diena | 50 | 100 | 5000 |
| Architektas | Darbo diena | 30 | 120 | 3600 |
| Programuotojas | Darbo diena | 200 | 70 | 1400 |
| Pardavimų vadybininkas | Darbo diena | 100 | 40 | 4000 |
| *Iš viso žmonių išteklių* |  | 380 |  | 27600 |
| 3. Įranga ir prekės |  |  |  |  |
| Kompiuteris | Vienetas | 4 | 1500 | 6000 |
| Monitorius | Vienetas | 4 | 500 | 2000 |
| Priedai (pagal poreikį) | Vienetas | 10 | 50 | 500 |
| *Iš viso Įranga ir prekės* |  |  |  | 8500 |
| 4. Biuro išlaikymas | Mėnesis | 12 | 400 | 4800 |
| 4.1.Biuro prekės | Vienetas | 10 | 20 | 200 |
| 4.2.Elektros,šildymo,telefono,nuomos išlaidos | Vienetas | 0 | 0 | 0 |
| *Iš viso biuro išlaikymas* |  |  |  | 5000 |
| 6. Viso tiesioginiai projekto kaštai |  |  |  | 41100 |

## Nauda

Įmonėje atliekant tyrimus, kurie tikrina darbuotojų atidumą, dėl fišingo išpuolių, kiekis nuėjusių į imituotą fišingo puslapį turėtų sumažėti bent 80% per pirmąjį tyrimą, po įskiepio įdiegimo.

## Konkurencija ir alternatyvos

Konkurentai, kurie šiuo metu yra rinkoje atlieka identifikavimą skirtingais būdais, tačiau dažniausiai pagal turinį, būta pritaikyti specifiniams atvejams, arba identifikuoja priemonėmis, kurios gali neužkirsti kelio išpuoliams. Pavyzdžiui „Netcraft Extension“ turi daug įvairių funkcijų atpažinti kenkėjiškas svetaines, tačiau pagal URL identifikuoja juodojo sąrašo principu, ką reiškia, kad vartotojas turi įrašyti kenkėjišką adresą ir tik tada jis bus identifikuojamas kaip kenkėjiškas. Kiti konkurentai analizuoja pagal turinį, vieni pagal el. laiško turinį (Cloudphish), kitas pritaikytas bankų svetainėms (PhishDetector).

## Santrauka

**Vertėmis grįstas pasiūlymas**

Įmonės, kuriose darbuotojai dirba su konfidencialia informacija, nepatenkinti dabartinėmis alternatyvomis, nes jos nepakankamai sumažina rizika. Mūsų kuriamas produktas, mašininio mokymosi pagalba, naudodamas kenkėjiškiems URL adresams būdingas savybes, galės identifikuoti svetaines, kurios potencialiai priklauso kibernetiniams nusikaltėliams tik pagal URL adresą. Skirtingai nei naudojant kitas alternatyvas, visos svetainės į kurias eina vartotojas yra patikrinamos, o ne tik specifinės arba patenkant į svetaines per el. paštą ir taip padidinama apsauga.

Projekto planuojami kaštai neviršys 45000 Eur. Programų sistema bus įdiegta užsakovo aplinkoje iki 2021-05-31