Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų atpažinimas ir apsauga

Kibernetinių atakų atpažinimas

Sukčiavimo (angl. Phishing) atvejų ir technikų panaudojimo analizė

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Mokymosi tikslai

Paaiškinti įvairių sukčiavimo atakų poveikį ir kaip atpažinti bei valdyti šias sukčiavimo atakas.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Studento darbo krūvis

Paskaita	3 val.
Garso ir vaizdo medžiaga	3 val.
Panaudojimo atvejai	3 val.
Papildomi skaitiniai	6 val.
Pasiruošimas atsiskaitymui	3 val.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Turinys

- Kas yra sukčiavimo atakos ir rizikos?
- Sukčiavimo atakų atvejų analizė
  - Kokios yra sukčiavimo grėsmės ir rizikos kiekvienu atveju?
  - Kaip atpažinti ir įveikti šias sukčiavimo rizikas?

Funded by the
Erasmus+ Programme
of the European Union

Kas yra sukčiavimo ataka?

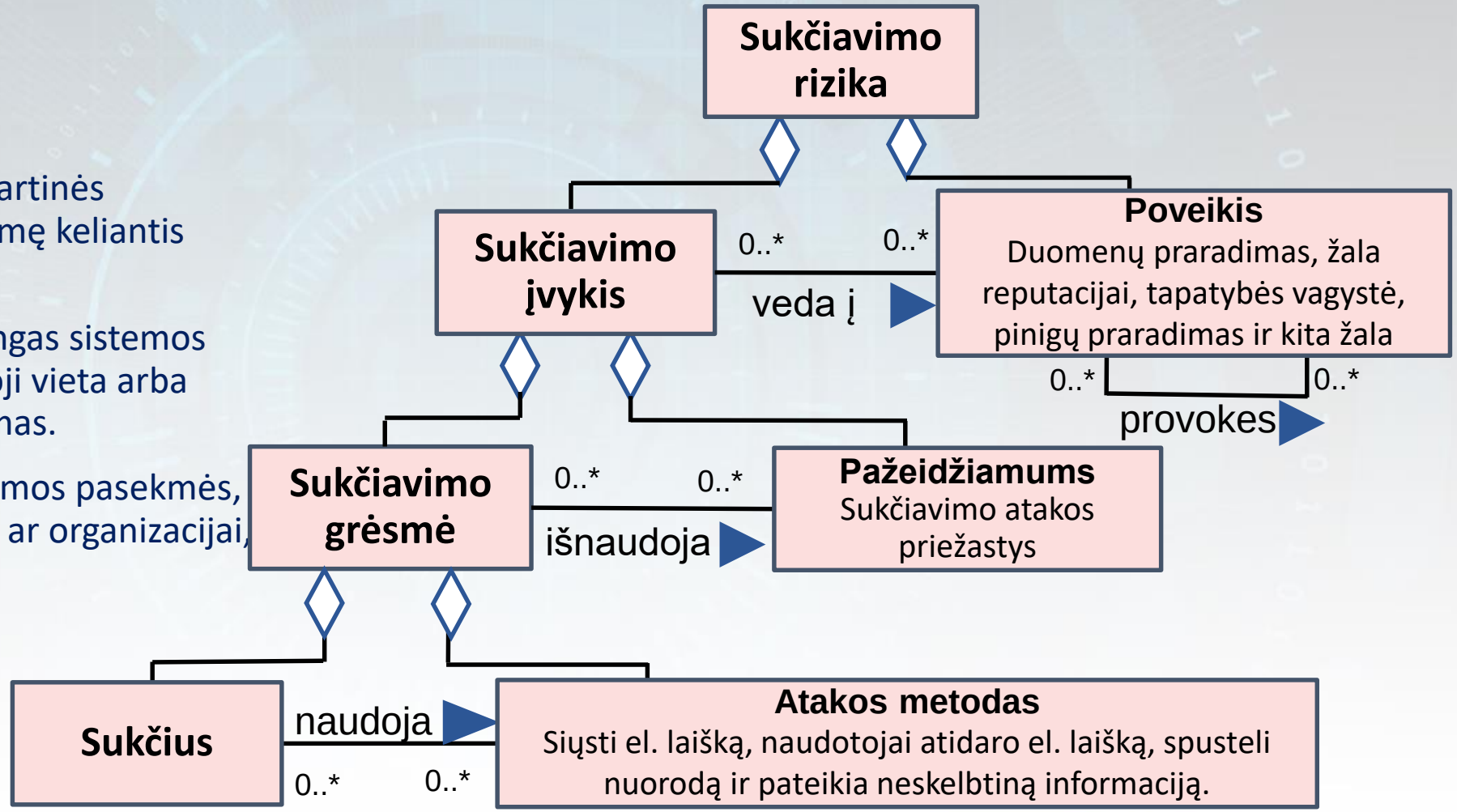
Sukčiavimas tai socialinės inžinerijos apgaulė, dėl kurios žmonės ir organizacijos gali prarasti duomenis, sugadinti savo reputaciją, patirti tapatybės vagystę, prarasti pinigus ir patirti daugybę kitų nuostolių. Sukčiavimas paprastai prasideda nuo elektroninio laiško, kuriuo bandoma įgyti potencialios aukos pasitikėjimą ir įtikinti ją atlikti užpuoliko pageidaujamus veiksmus.

[Abroshan, 2021]

Funded by the Erasmus+ Programme of the European Union

Kas yra sukčiavimo ataka?

- **Atakos metodas** – standartinės priemonės, kuriomis grėsmę keliantis agentas vykdo grėsmę
- **Pažeidžiamumas** – būdingas sistemos turtui, kuri gali būti silpnoji vieta arba sistemos saugumo trūkumas.
- **Poveikis** – galimos neigiamos pasekmės, kurios gali pakenkti turtui ar organizacijai, kai grėsmė įvykdoma



[*Dubois at al., 2010*]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukčiavimo atakų atpažinimas

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Atvejų analizė

Pasirinkti atvejai

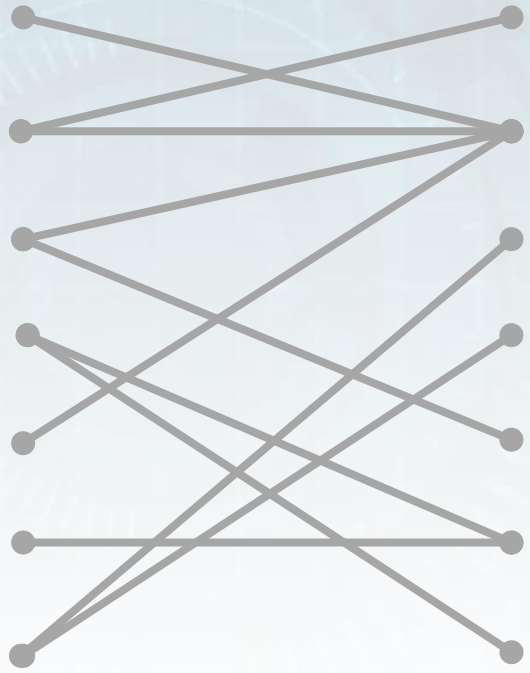
- Su COVID susijusios atakos
- Su BDAR susijusios atakos
- Techninės pagalbos atakos
- Kriptovaliutų sukčiavimai
- Išviliojimo sukčiavimai (angl. Extortion scam)
- Išankstinių mokesčių sukčiavimai (angl. Advance Fee Scams)
- Sukčiavimas socialiniuose tinkluose

Funded by the
Erasmus+ Programme
of the European Union

Atvejų analizė

Pasirinkti atvejai

- Su COVID susijusios atakos
- Su BDAR susijusios atakos
- Tech. pagalbos atakos
- Kriptovaliutų sukčiavimai
- Išviliojimo sukčiavimai
- Išankstinių mokesčių
- Sukčiavimas soc. tinkluose



- BDAR atakos
- El. laiškai
- Tiesioginiai pranešimai
- Socialiniai tinklai
- Svetainės
- Loterijos sukčiavimai
- SMS

Su COVID susijusios atakos

- COVID-19 metu pastebėjome, kad padaugėjo su pandemija susijusių sukčiavimo atvejų el. laiškais ir SMS žinutėmis, pvz., suklastotų Ligų kontrolės ir prevencijos centro (CDC) ar sveikatos organizacijų pranešimų apie vakcinacijos aprėptį, kur galima pasiskiepyti, vakcinų statistiką, darbuotojų skiepijimo būklę ir pan.
- Labiausiai paplitusios atakos – COVID sveikatos patarimų sukčiavimas el. paštu.

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė

COVID sukčiavimo rizika

ngimo duomenys, siekiant gauti
finansiniai duomenys, užkrėsti
istratoriai, išpirkos reikalaujanti
įranga ir kt.)

0..*

as,
l
ų

ašant
maciją
usteli

Suk
gr

Sukčius

nau

0..*

Singapore Specialist : Corona Virus Safety Measures

DT

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

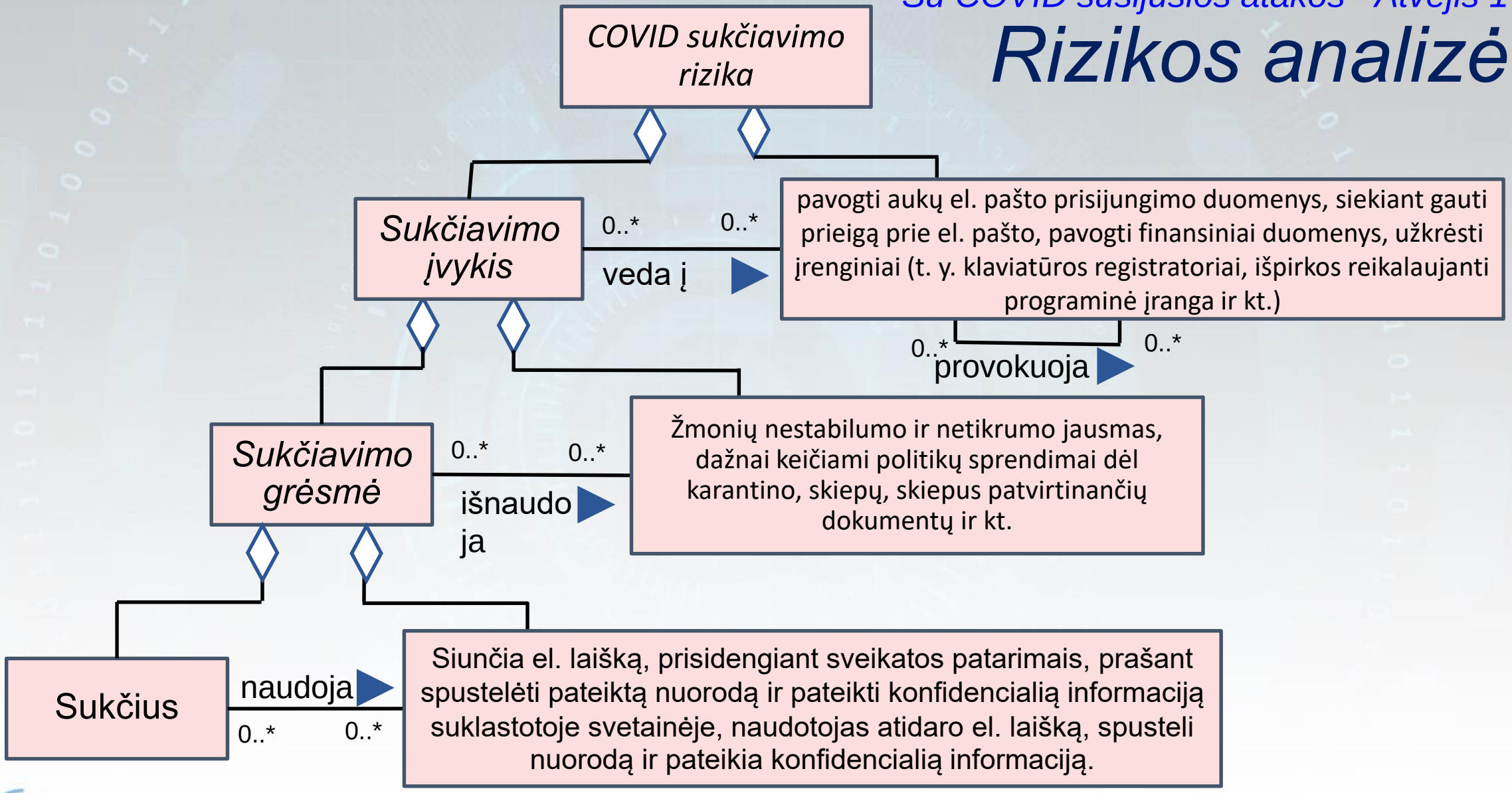
Regards
Dr
Specialist wuhan-virus-advisory

Koronaviruso sukčiavimo laiškasl (Šaltinis: Wired)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą, ir išanalizuokite, ar jis kenkėjiškas.
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: el. laiškas
Sukčiavimo žinutės anatomija:
a. Kas siunčia laišką?
b. Koks laiško turinys?
Koronaviruso saugos priemonės
c. Ar yra hipersaitų / priedų? *Taip*

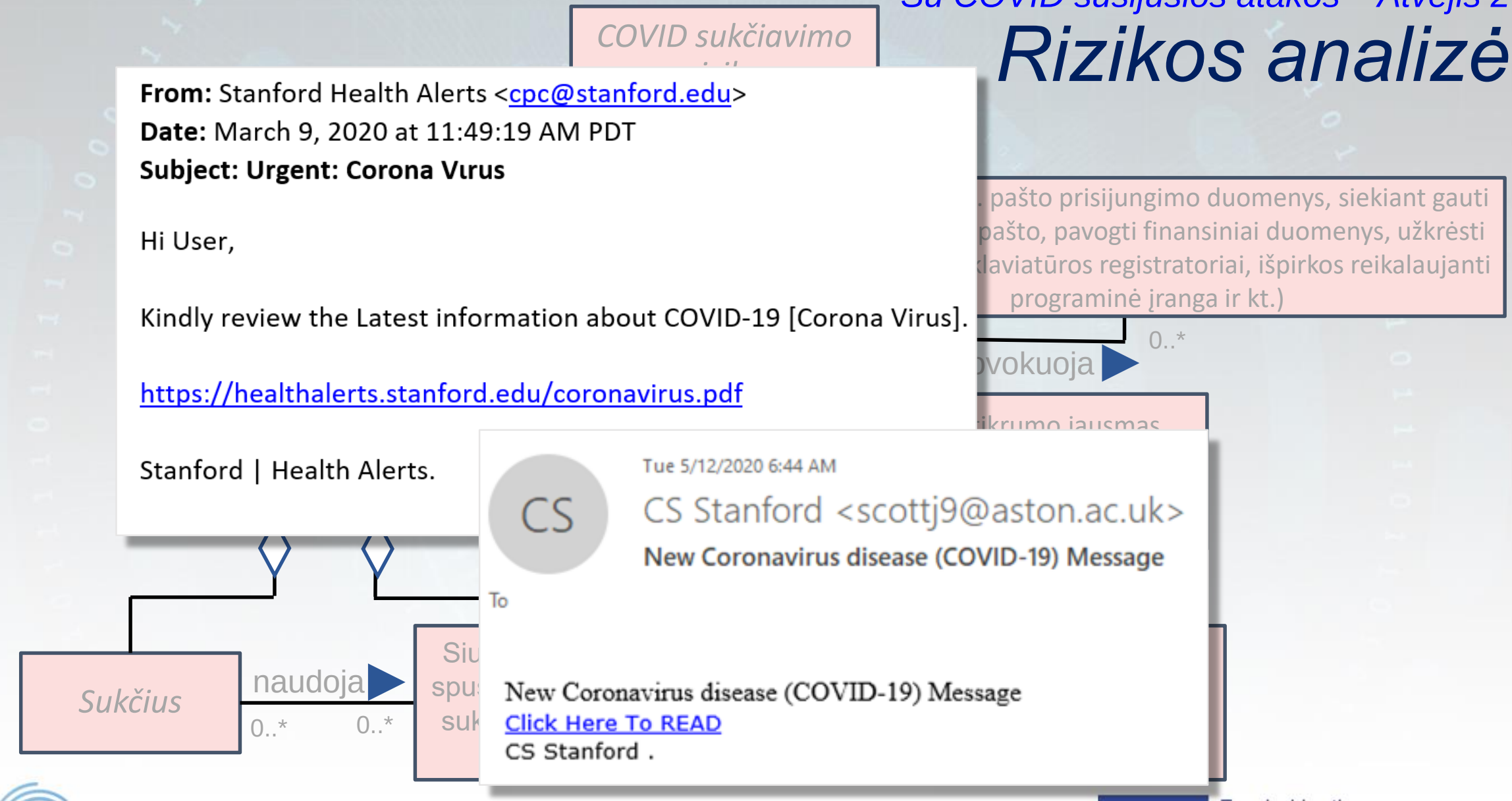
Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius (angl. red flags)
3.1 Patikimi COVID informacijos šaltiniai nesiunčia nepageidaujamų el. laiškų
3.2 Teisėtuose el. laiškuose paprastai kreipiamasi vardu
3.3 Teisėti el. laiškai neturi rašybos ir gramatikos klaidų.

4. Kritinis mąstymas
4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio
4.2 Atsargiai elkitės su hipersaitais ir (arba) priedais; juose gali būti nuorodų į kenkėjiškus išteklius.
4.3 Būkite atsargūs, kai el. laiškuose prašoma imtis skubių veiksmų.
4.4 Prieš pasitikėdami el. laišku, naudokitės paieškos sistema, kad sužinotumėte daugiau informacijos apie el. laiško turinį.
4.5 Peržiūrėkite galimai apgaulingus URL adresus naudodami nemokamus sukčiavimo aptikimo įrankius
4.6 Ištrinkite gautą el. laišką, jei pagrįstai įsitikinote, kad tai sukčiavimas.

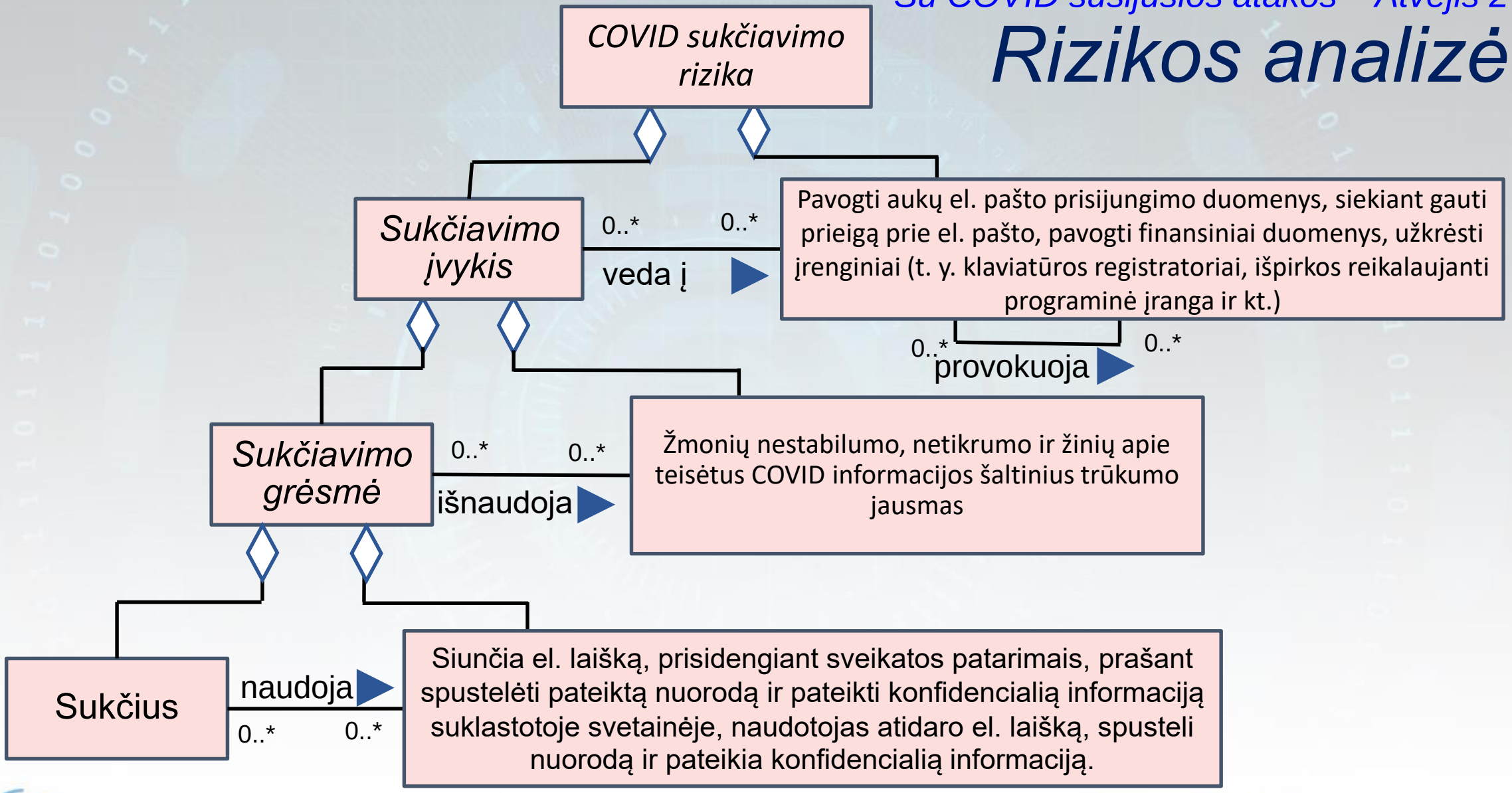
Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Koronoviruso sukčiavimo laiškas (Šaltinis Wired)

Rizikos analizė



CyberPhish
Safeguarding your digital future

Coronavirus Phishing Email (Source: Wired)

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą ir išanalizuotumėte, ar jis kenkėjiškas.

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: el. laiškas
Sukčiavimo žinutės anatomija:
a. Kas siunčia laišką?
cpc@stanford.edu, scottj9@aston.ac.uk
b. Koks laiško turinys? *Koronavirusas*
c. Ar yra hipersaitų / priedų? *Taip*

Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius
3.1 Patikimi COVID informacijos šaltiniai nesiunčia nepageidaujamų el. laiškų
3.2 Teisėtuose el. laiškuose paprastai kreipiamasi vardu
3.3 Teisėti el. laiškai yra profesionalūs ir turi vienodą šablono formatą.

4. Kritinis mąstymas
4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio
4.2 Būkite atsargūs su hipersaitais / priedais; juose gali būti nuoroda į kenkėjišką šaltinį
4.3 Prieš pasitikėdami pranešimu, naudokitės paieškos sistema, kad sužinotumėte daugiau informacijos apie el. laiško turinį
4.4 Patikrinkite galimai apgaulingus URL adresus naudodamiesi nemokamomis apgaulės aptikimo priemonėmis
4.5 Ištrinkite gautą el. laišką, jei esate pagrįstai įsitikinę, kad tai sukčiavimas

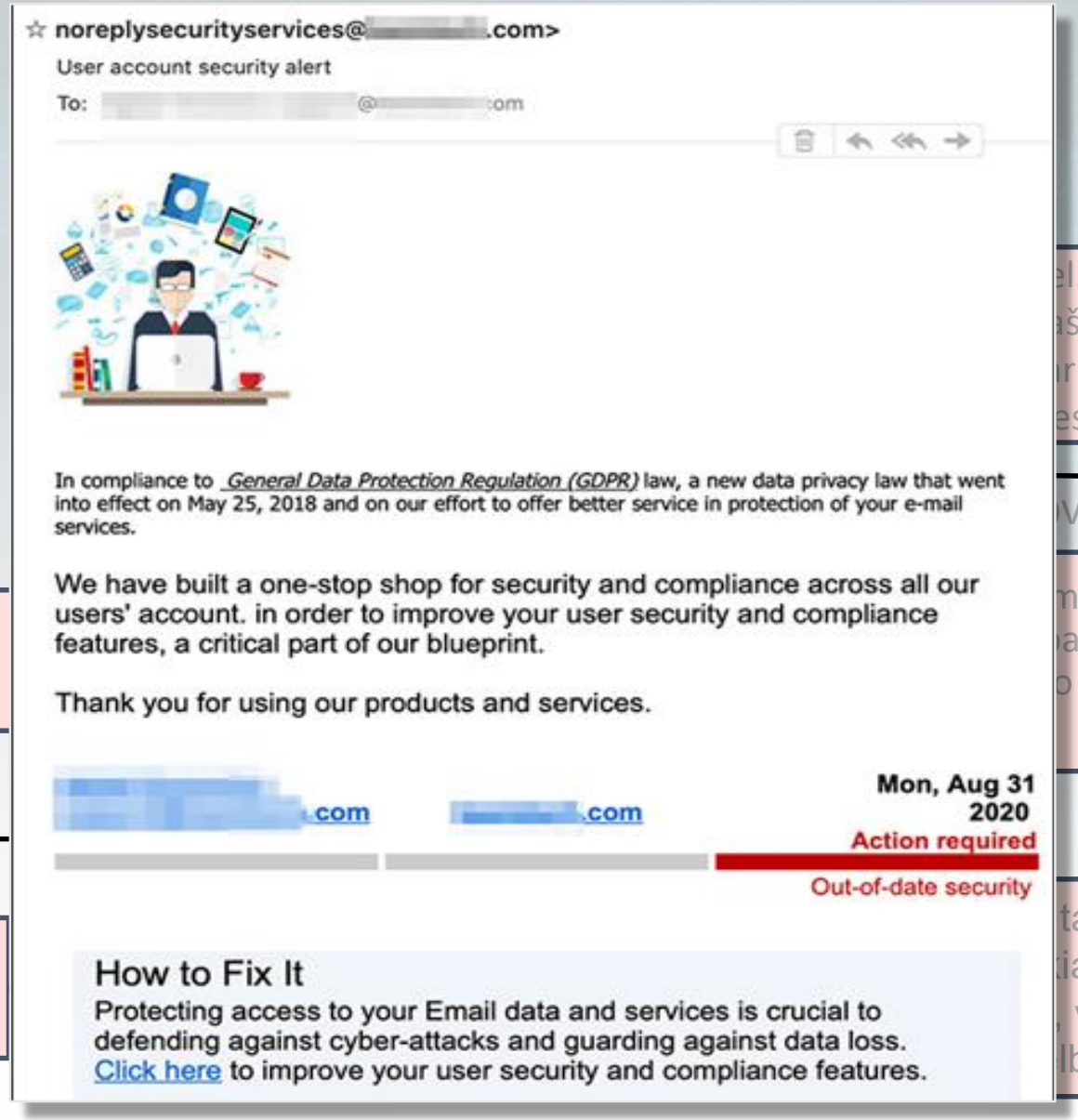
Funded by the Erasmus+ Programme of the European Union

Su BDAR susijusios atakos

- Daugelis su *BDAR* susijusių sukčiavimo atakų pasirodė 2018 m., nes visos įmonės ir organizacijos buvo įpareigotos įgyvendinti BDAR savo organizacijose
- Užpuoliko taktika gali apimti siuntimą
  - *netikrus elektroninius laiškus, apsimetus, kad įmonė padeda vykdyti BDAR veiklą, pavogti informaciją*
  - *netikrus elektroniniai laiškus, apsimetus, kad įmonė klientui teikia informaciją apie duomenų politikos pakeitimus*

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



el. pašto prisijungimo duomenys, kad gautų
ašto. Iš aukos el. pašto gali būti pavogti jautrūs
rba pavogti kontaktai gali būti panaudoti
esnėms kibernetinėms atakoms.

0..*

vokuoja

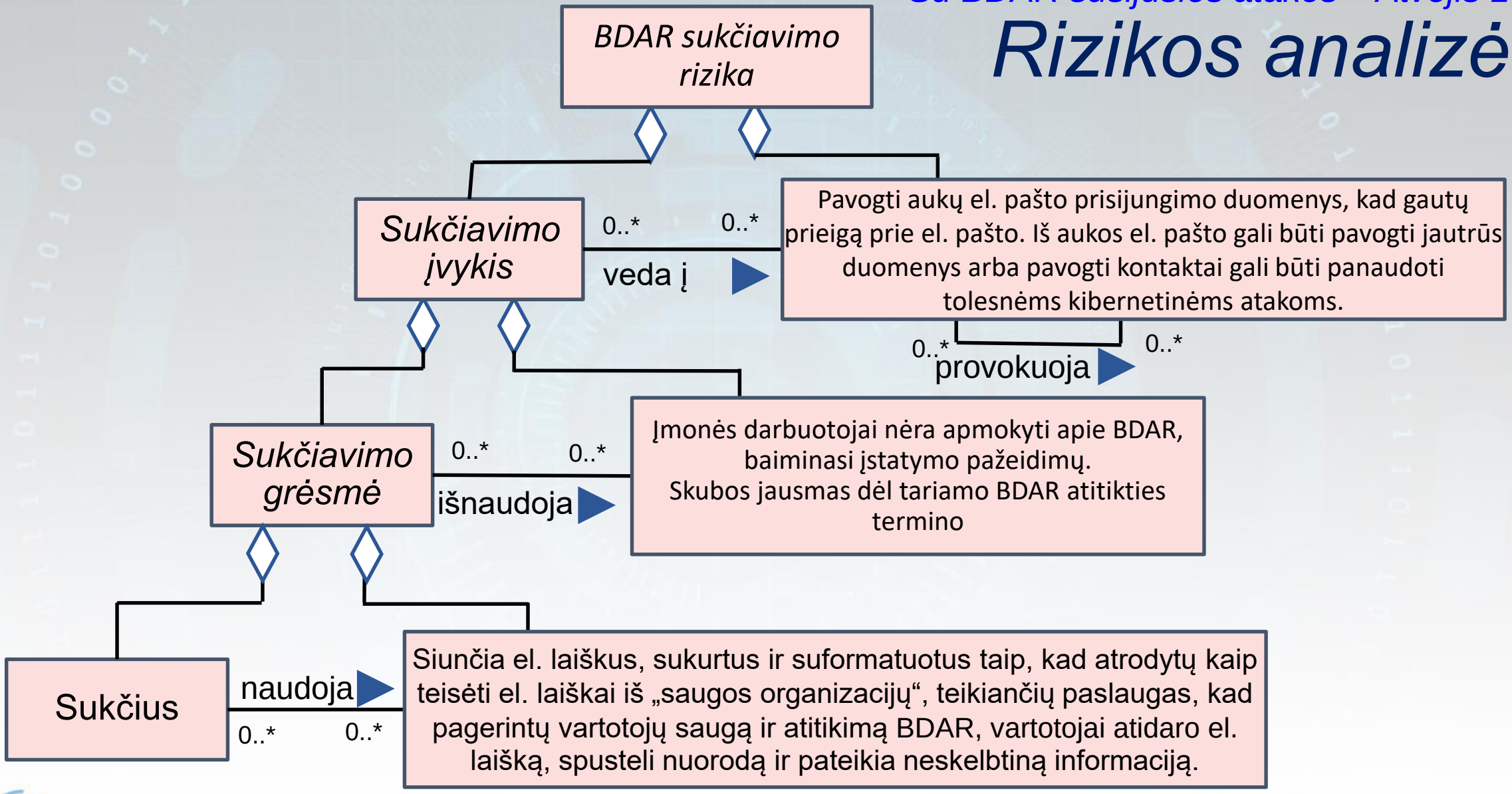
mokyti apie BDAR,
ažeidimų.
o BDAR atitikties

taip, kad atrodytų kaip
iančių paslaugas, kad
, vartotojai atidaro el.
lbtiną informaciją.

Sukčius

BDAR sukčiavimo el. laiškas (Šaltinis: Databreachtoday)

Rizikos analizė



Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą ir išanalizuotumėte, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: El. laiškas
Sukčiavimo žinutės anatomija
a. Kas siunčia laišką? *noreplysecurityservices*
b. Koks laiško turinys? *Paskyros saugos įspėjimas*
c. Ar yra hipersaitų / priedų? *Taip*

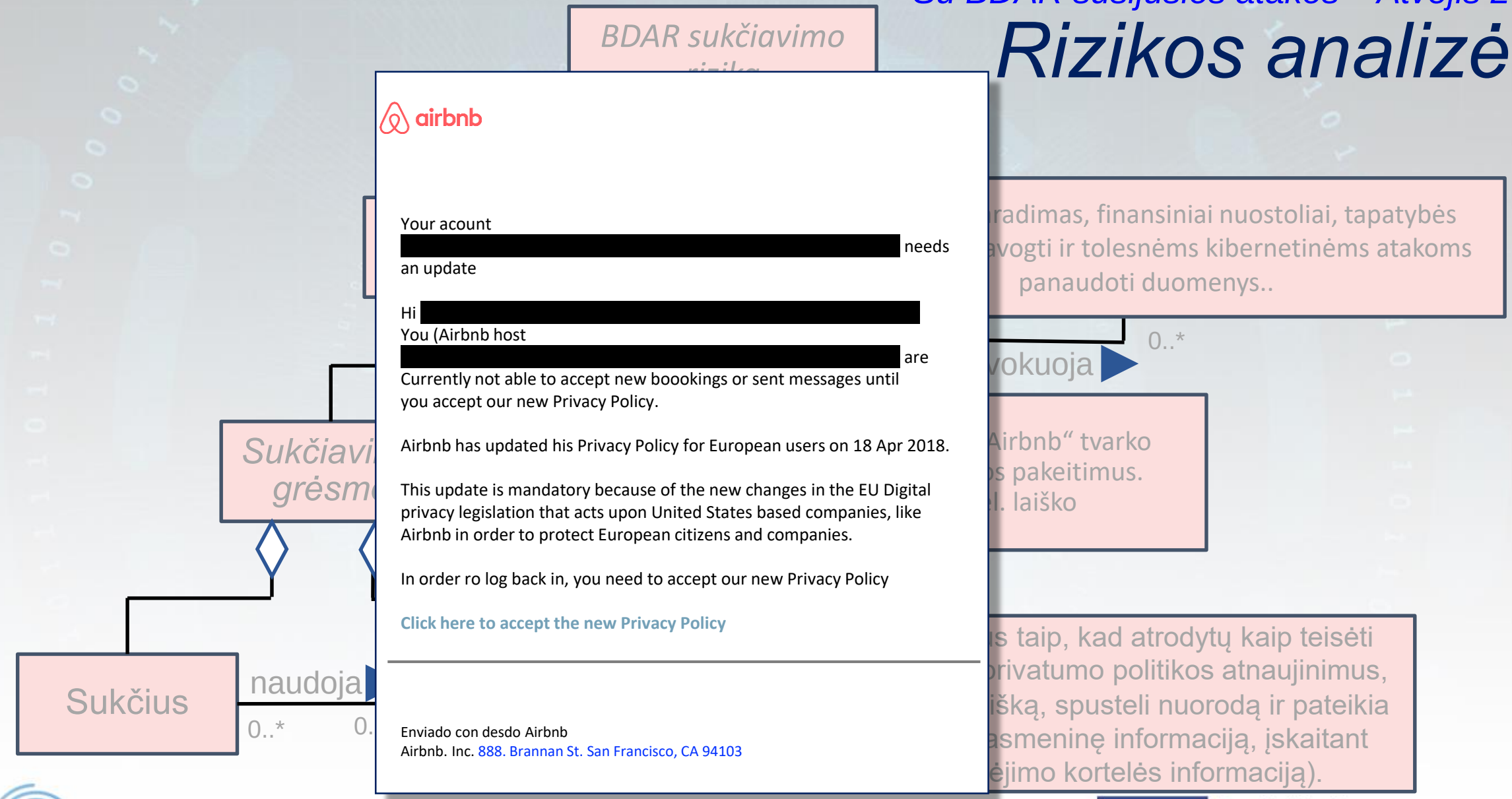
Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius
3.1 Teisėtų el. laiškų turinys nėra prieštaringas, pvz., „BDAR“ ir „Pasenusi apsauga“.
3.2 Teisėtų paslaugų el. laiškai yra profesionalūs ir vieningo formato.

4. Critical Thinking
4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio
4.2 Būkite atsargūs su hipersaitais / priedais; juose gali būti nuoroda į kenkėjišką šaltinį
4.3 Prieš pasitikėdami pranešimu, naudokitės paieškos sistema, kad sužinotumėte daugiau informacijos apie el. laiško turinį
4.4 Patikrinkite galimai apgaulingus URL adresus naudodamiesi nemokamomis apgaulės aptikimo priemonėmis
4.5 Ištrinkite gautą el. laišką, jei esate pagrįstai įsitikinę, kad tai sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



airbnb

Your acount [redacted] needs an update

Hi [redacted]
You (Airbnb host [redacted] are Currently not able to accept new boookings or sent messages until you accept our new Privacy Policy.

Airbnb has updated his Privacy Policy for European users on 18 Apr 2018.

This update is mandatory because of the new changes in the EU Digital privacy legislation that acts upon United States based companies, like Airbnb in order to protect European citizens and companies.

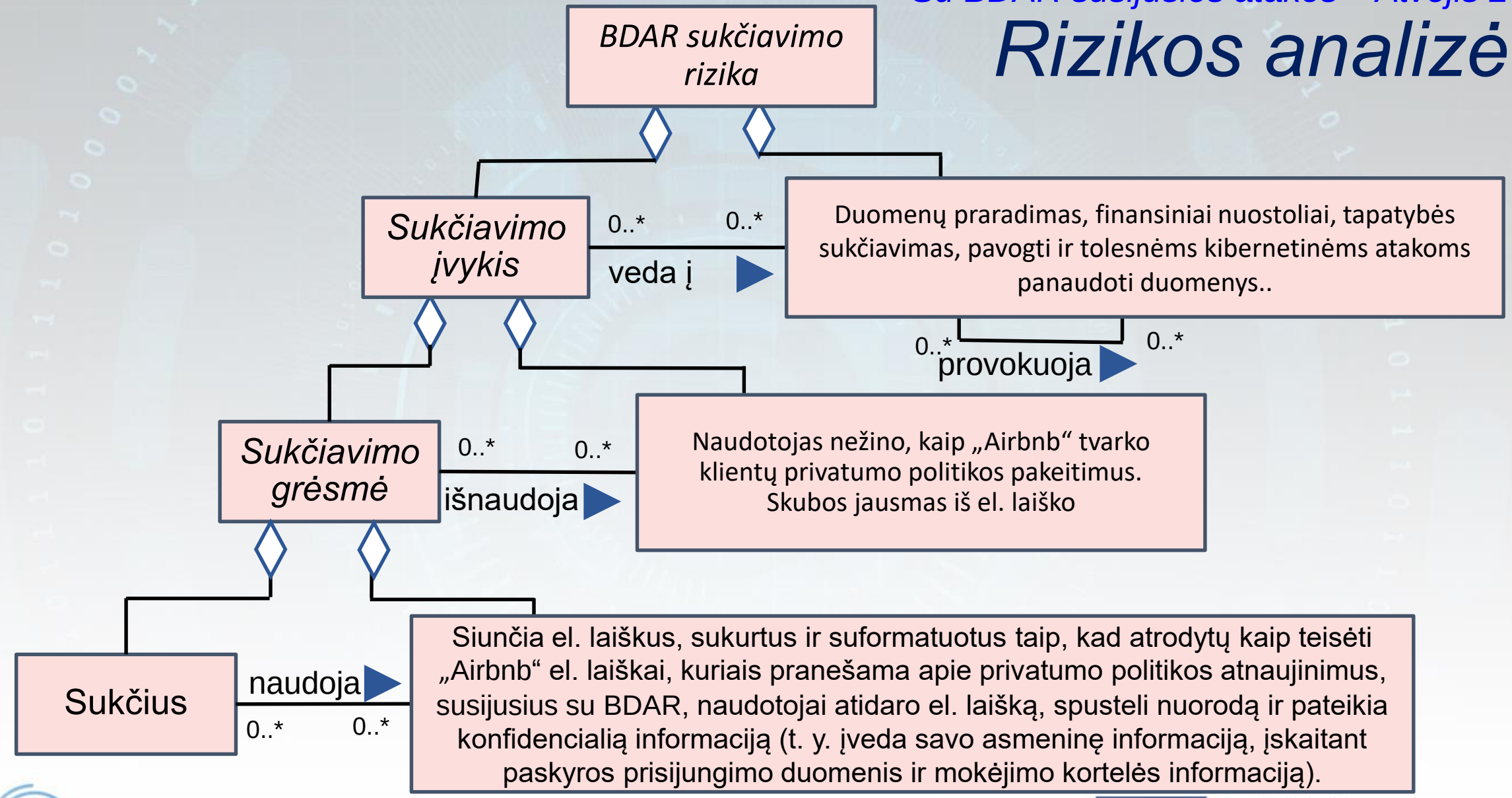
In order ro log back in, you need to accept our new Privacy Policy

Click here to accept the new Privacy Policy

Enviado con desdo Airbnb
Airbnb. Inc. 888. Brannan St. San Francisco, CA 94103

BDAR sukčiavimo laiškas (Šaltinis: Securityaffairs

Rizikos analizė



Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą ir išanalizuotumėte, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: El. laiškas
Sukčiavimo žinutės anatomija
a. Kas siunčia laišką? *BDAR atnaujinimas paskyrai*
b. Ar yra hipersaitų / priedų? *Taip*

3. Atpažinkite pagrindinius požymius
3.1 Teisėtos įmonės privatumo politikos susitarimus tvarko tiesiogiai interneto svetainėje arba programėlėje.
3.2 Įmonių klientams siunčiamuose BDAR pranešimuose neprašoma naudotojų prisijungimo duomenų

4. Kritinis mąstymas
4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio
4.2 Būkite atsargūs su hipersaitais / priedais; juose gali būti nuoroda į kenkėjišką šaltinį
4.3 Patikrinkite siuntėjo el. pašto adresą, ar jame nėra sukčiavimo požymių (žiūrėkite Airbnb list)
4.4 Daugiau informacijos apie el. laiško turinį rasite oficialioje „Airbnb“ svetainėje
4.5 Patikrinkite galimai apgaulingus URL adresus naudodamiesi nemokamomis apgaulės aptikimo priemonėmis
4.5 Ištrinkite gautą el. laišką, jei esate pagrįstai įsitikinę, kad tai sukčiavimas

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

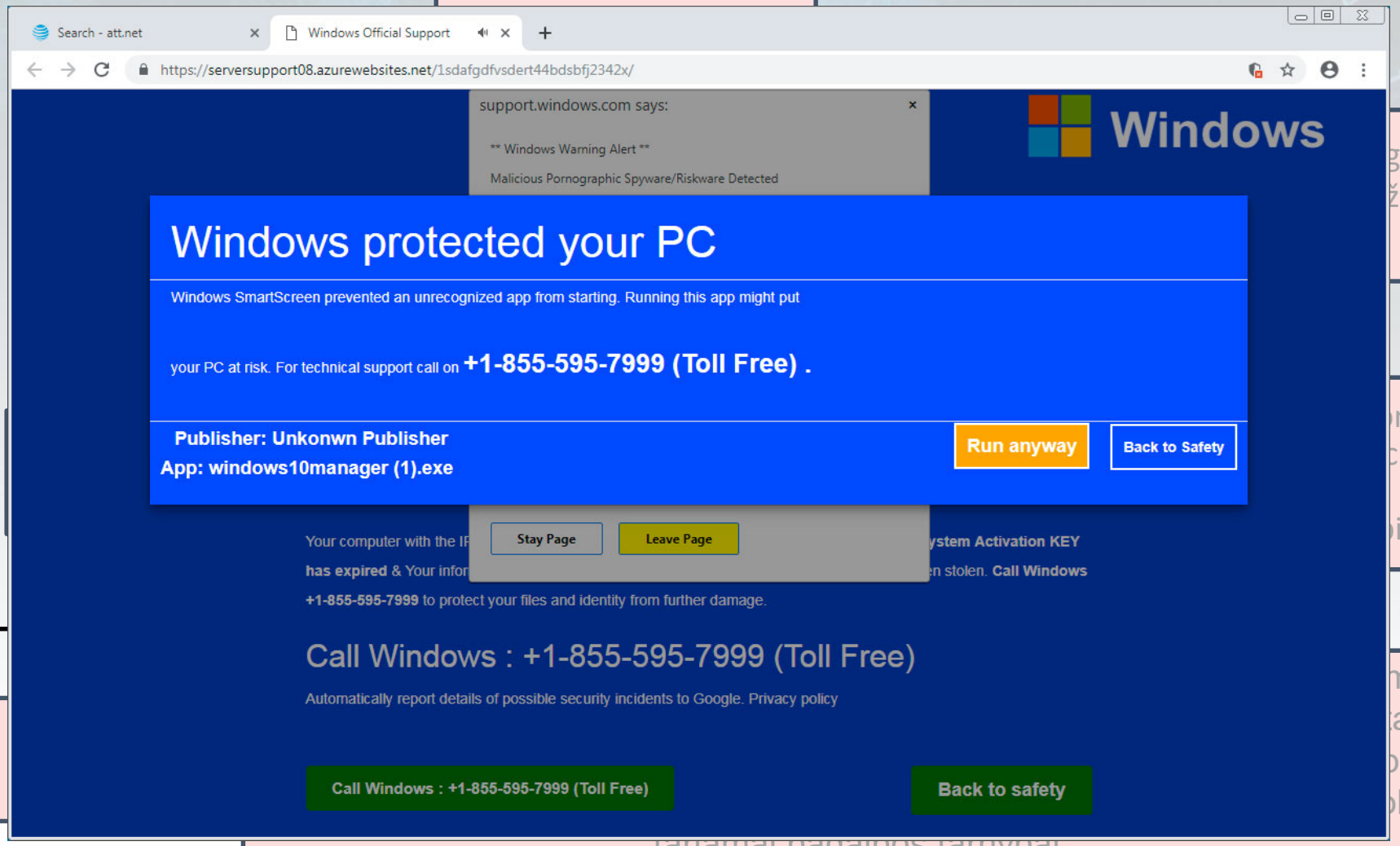
Techninės pagalbos atakos

- Techninės pagalbos sukčiai teigia, kad siūlo teisėtą techninės pagalbos paslaugą, ir gali naudoti įvairias taktikas, kad atkreiptų aukų dėmesį, įskaitant šaltus skambučius (angl. *cold call*), interneto svetainių iššokančius langus, el. pašto žinutes ir SMS žinutes.
- Populiariausios naudojamos taktikos
  - *iššokantys svetainės langai, įspėjantys naudotoją apie kompiuterinį virusą*
  - *Techninių paslaugų sukčiavimo el. aiškiai*

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė

Tech. pagalbos sukčiavimo rizika



gta asmeninė
žkrėtimas

mis kaip
crosoft“
biuterio

Sukčius

mos,
ą
ą,
kėti

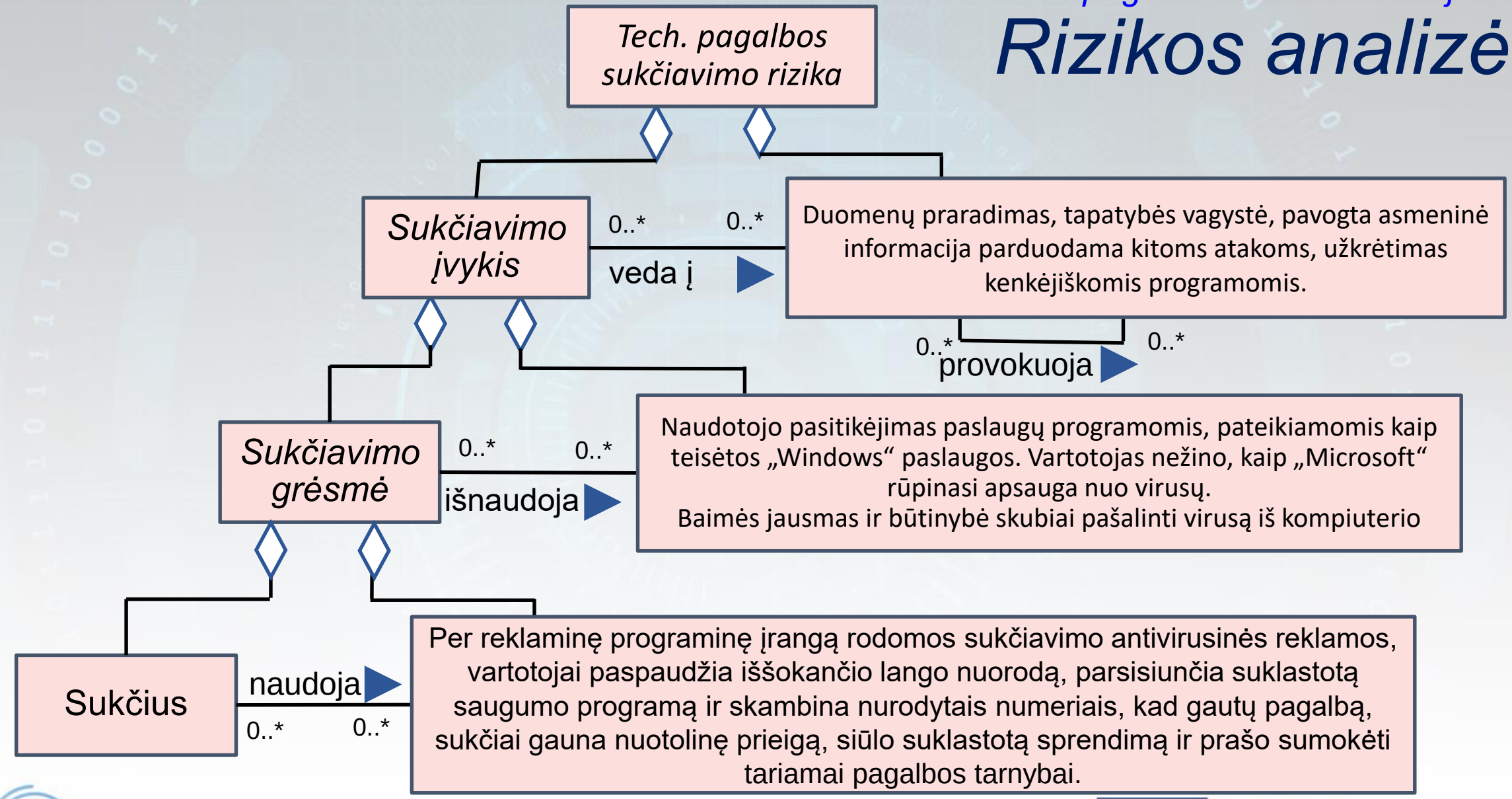
tiesiami pagalbos tarnybai.

CyberPhish
Safeguarding your digital future

Techninės pagalbos sukčiavimo el. laiškas (Šaltinis: Bleepingcomputer)

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



CyberPhish
Safeguarding your digital future

Coronavirus Phishing Email (Source: Wired)

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių iššokančių raginimo imtis veiksmų mygtukų ar nuorodų.

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: Svetainė
Sukčiavimo žinutės anatomija:
a. Kas siunčia žinutę? *Iššokantis langas*
b. Koks žinutės turinys? *Antivirusinė apsauga*
c. Ar yra raginimų imtis veiksmų? *Taip*

3. Atpažinkite pagrindinius požymius
3.1 Teisėtą "Windows" apsaugą tvarko „Windows Defender“, o ne svetainė.
3.2 „Microsoft“ nesiunčia nepageidaujamų iššokančiųjų langų svetainėse
3.3 Negalite paskambinti „Windows“ telefonu

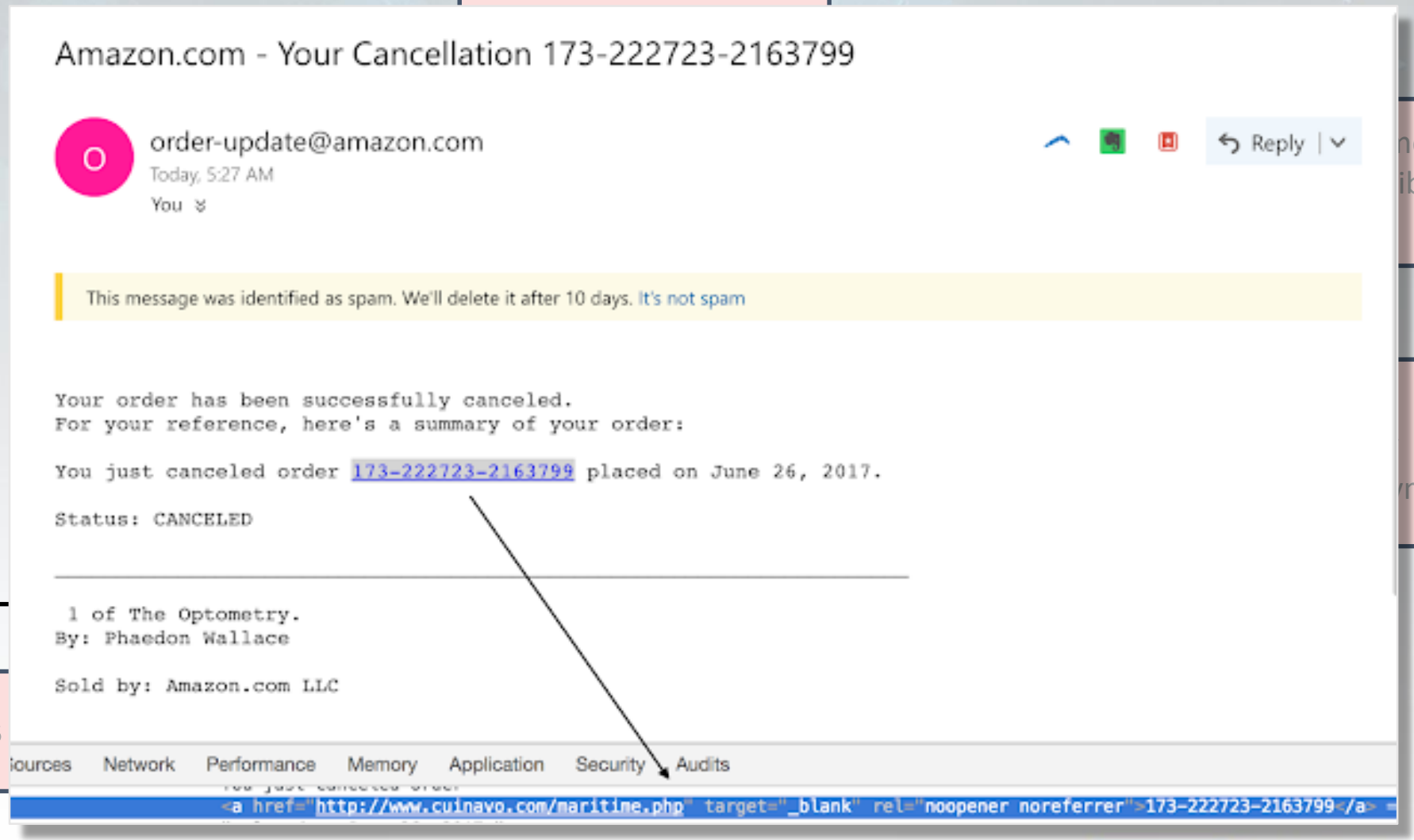
4. Kritinis mąstymas
4.1 Būkite atsargūs dėl visų netikėtų iššokančių langų svetainėse, nespauskite netikėtai iššokančių langų ir, jei įmanoma, blokuokite iššokančius langus
4.2 Būkite atsargūs, kai iššokančiuose languose prašoma atlikti veiksmus su skubos / baimės jausmu
4.3 Niekada nenurodykite paskyros slaptažodžio ar prisijungimo informacijos, kad gautumėte „patvirtinimą“ telefonu ar el. paštu
4.4 Uždarykite svetainę, kuri generuoja įtartiną iššokantį langą

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė

Tech. pagalbos sukčiavimo rizika



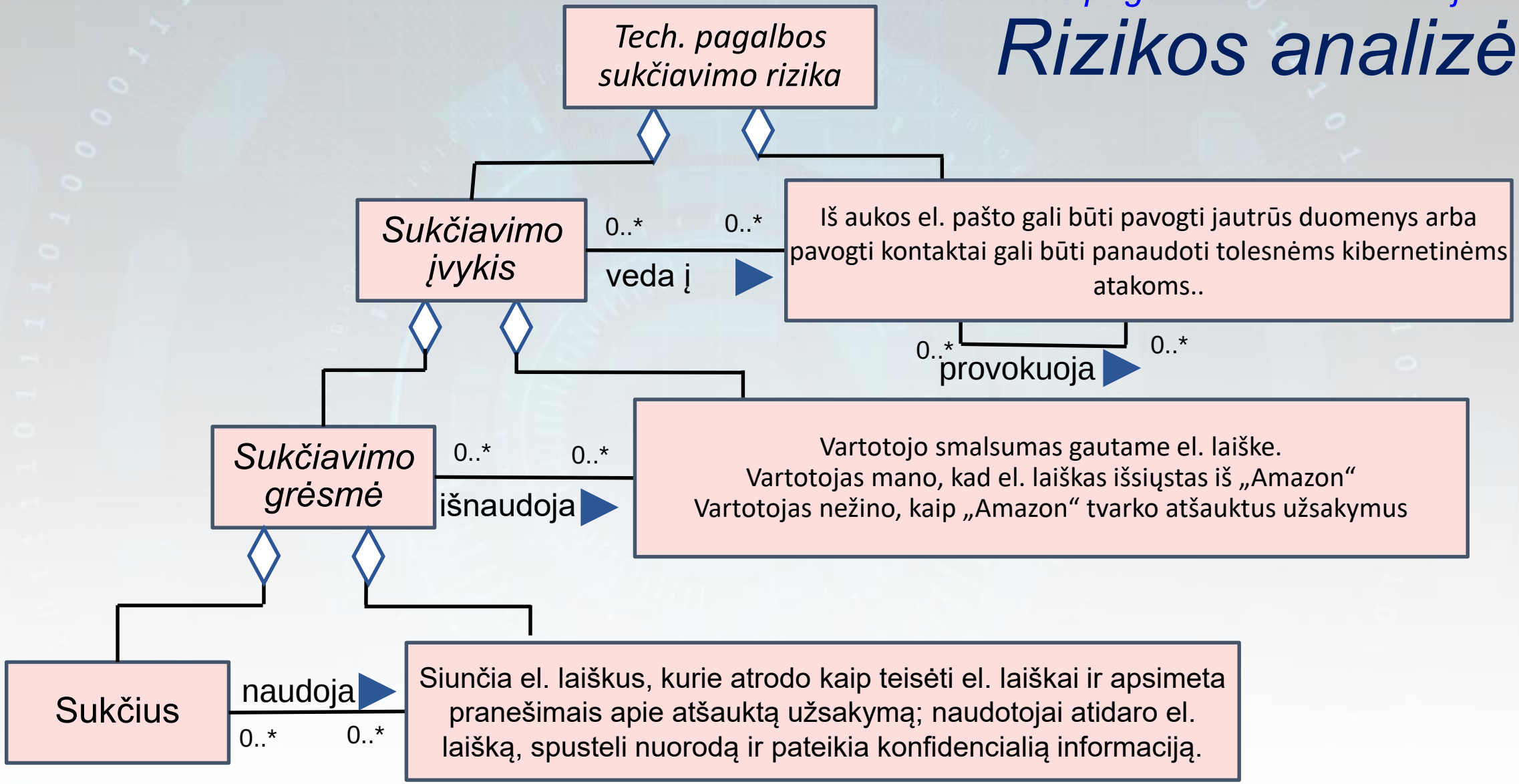
...nenys arba ...ibernetinėms

...mus

Sukčius

CyberPhish
Safeguarding your digital future
Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą ir išanalizuotumėte, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukčiavimą

Sukčiavimo šaltinis: El. laiškas
Sukčiavimo žinutės anatomija:
a. Kas siunčia el. laišką? *order-update@amazon.com*
b. Koks laiško turinys? *Atšauktas „Amazon“ užsakymas*
c. Ar yra hipersaitų / priedų? *Taip*

Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius

3.1 Teisėtuose „Amazon“ el. pašto laiškuose kriepiamasi vardu ir pavarde
3.2. Teisėti paslaugų el. laiškai yra profesionalūs ir vienodo formato.
3.3. Atkreipkite dėmesį, kad URL kelias nukreipia į **http://*www.cuinavo.com/maritime.php*** o ne į „Amazon“ šaltinį
3.4 „Amazon" siunčia užsakymo atšaukimo el. laišką iš *order-update@amazon.com* teisėto „Amazon“ el. pašto, tačiau el. pašto formatas nėra profesionalus. Tikėtina, kad pranešimo el. paštas yra suklastotas

4. Kritinis mąstymas

4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio
4.2 Net jei jis atrodo teisėtas, nueikite į savo tikrąją paskyrą teisėtoje bendrovės svetainėje, pvz., amazon.com, kad patikrintumėte bet kokias abejones.
4.3. Būkite atsargūs, nes šie el. pašto sukčių tipai gali pasinaudoti jūsų smalsumu ir godumu
4.4 Peržiūrėkite galimai apgaulingus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.5. Paskyros slaptažodį arba prisijungimo informaciją „verifikavimui“ pateikite tik saugiose teisėtų svetainių dalyse
4.6 Ištrinkite jums atsiųstą el. laišką, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų

2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą ir išanalizuotumėte, ar jis kenkėjiškas

2.3 Būkite atsargūs, jei URL kelias neatitinka turini

1. Supraskite sukčiavimą

Sukčiavimo šaltinis: El. laiškas

Sukčiavimo žinutės anatomija:

a. Kas siunčia el. laišką? *order-update@amazon.com*

b. Koks laiško turinys? *Atšauktas „Amazon“ užsakymas*

c. Ar yra hipersaitų / priedų? *Taip*

3. Atpažinkite pagrindinius požymius

3.1 Teisėtuose „Amazon“ el. pašto laiškuose kreipiamasi vardu ir pavarde

3.2. Teisėti paslaugų el. laiškai yra profesionalūs ir vienodo formato.

3.3. Atkreipkite dėmesį, kad URL kelias nukreipia į **http://www.cuinavo.com/maritime.php** o ne į „Amazon“ šaltinį

3.4 „Amazon" siunčia užsakymo atšaukimo el. laišką iš *order-update@amazon.com* teisėto „Amazon“ el. pašto, tačiau el. pašto formatas nėra profesionalus. Tikėtina, kad pranešimo el. paštas yra suklastotas

4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio

4.2 Net jei jis atrodo teisėtas, nueikite į savo tikrąją paskyrą teisėtoje bendrovės svetainėje, pvz., amazon.com, kad patikrintumėte bet kokias abejones.

4.3. Būkite atsargūs, nes šie el. pašto sukčių tipai gali pasinaudoti jūsų smalsumu ir godumu

4.4 Peržiūrėkite galimai apgaulingus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis

4.5. Paskyros slaptažodį arba prisijungimo informaciją „verifikavimui“ pateikite tik saugiose teisėtų svetainių dalyse

4.6 Ištrinkite jums atsiųstą el. laišką, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų

2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL adresą ir išanalizuotumėte, ar jis kenkėjiškas

2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukč

Sukčiavimo šaltinis: El. laiškas

Sukčiavimo žinutės anatomija:

a. Kas siunčia el. laišką? *order-update@amazon.com*

b. Koks laiško turinys? *Atšauktas „Amazon“ užsakymas*

c. Ar yra hipersaitų / priedų? *Taip*

Sukčiavimo atakų atpažinimas

ius

3.1 Teisėtuose „Amazon“ el. pašto laiškuose kriepiamasi vardu ir pavarde

3.2. Teisėti paslaugų el. laiškai yra profesionalūs ir vienodo formato.

3.3. Atkreipkite dėmesį, kad URL kelias nukreipia į **http://*www.cuinavo.com/maritime.php*** o ne į „Amazon“ šaltinį

3.4 „Amazon" siunčia užsakymo atšaukimo el. laišką iš *order-update@amazon.com*

4. Kritinis mąstymas

4.1 Patikrinkite, ar el. laiškas yra iš patikimo ir laukiamo šaltinio

4.2 Net jei jis atrodo teisėtas, nueikite į savo tikrąją paskyrą teisėtoje bendrovės svetainėje, pvz., amazon.com, kad patikrintumėte bet kokias abejones.

4.3. Būkite atsargūs, nes šie el. pašto sukčių tipai gali pasinaudoti jūsų smalsumu ir godumu

4.4 Peržiūrėkite galimai apgaulingus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis

4.5. Paskyros slaptažodį arba prisijungimo informaciją „verifikavimui“ pateikite tik saugiose teisėtų svetainių dalyse

4.6 Ištrinkite jums atsiųstą el. laišką, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

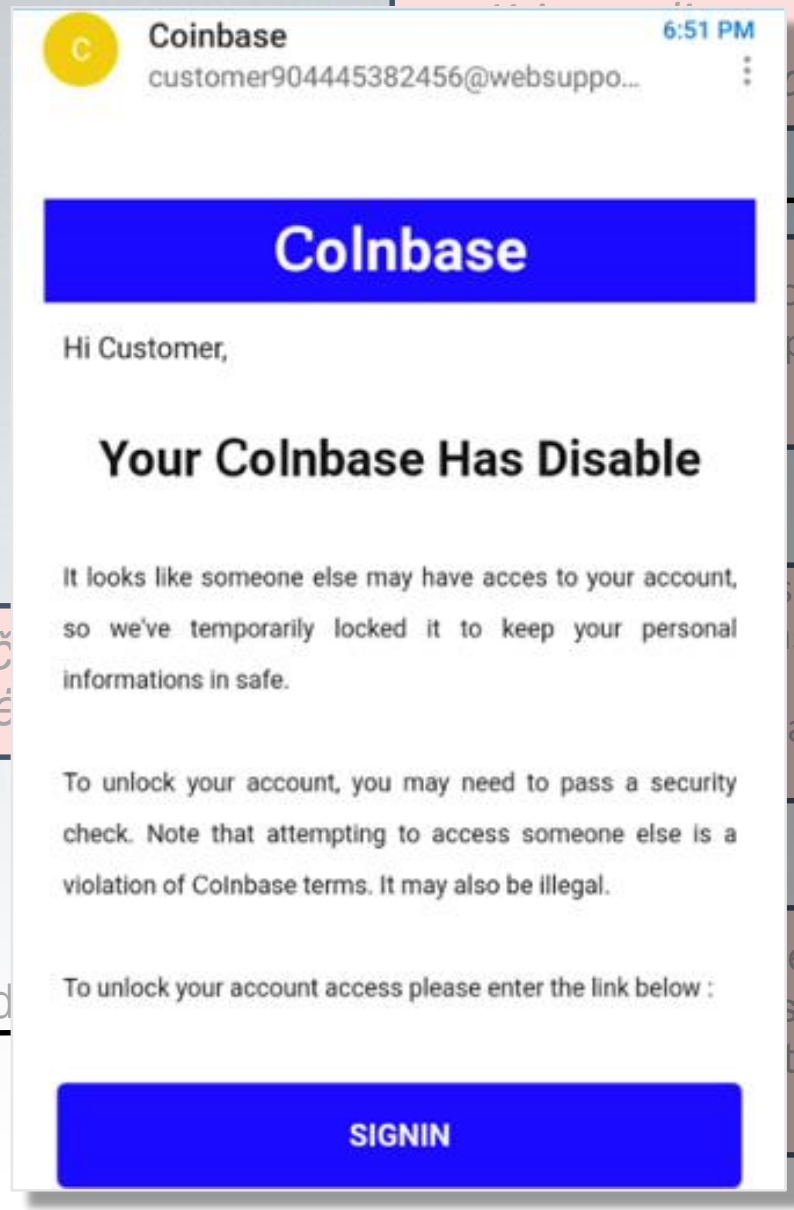
Funded by the Erasmus+ Programme of the European Union

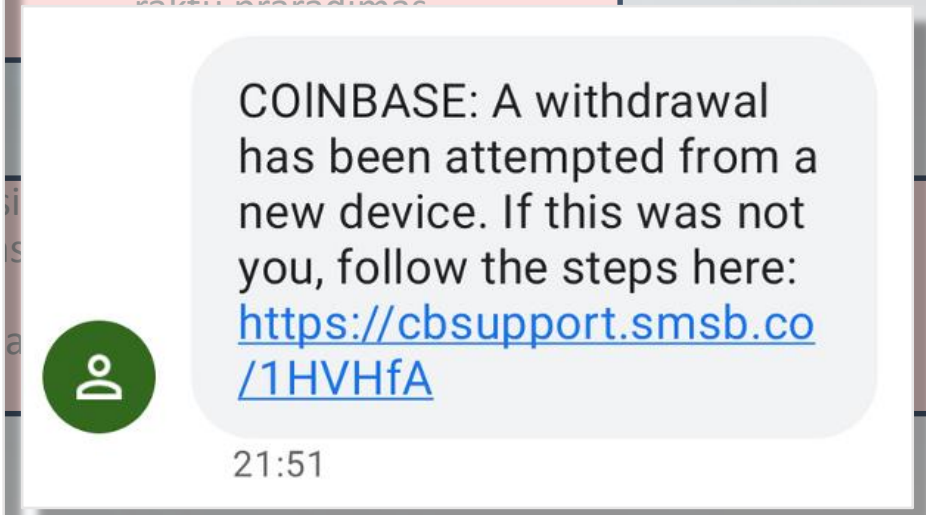
Kriptovaliutų sukčiavimai

- Bitkoinui ir kitoms kriptovaliutoms sparčiai brangstant ir populiarėjant, programišiai ir kibernetiniai nusikaltėliai ėmė labiau domėtis jų vagystėmis
- Užpuolikai gali naudoti sukčiavimą ir apsimesti populiarių kriptovaliutų biržų, tokių kaip „Binance“, „Huobi Global“ ar „Coinbase“, atstovais.

Funded by the
Erasmus+ Programme
of the European Union

Rizikos analizė





omenų praradimas, žala reputacijai, patybės vagystė, pinigų ar privačių

ėjančius naudotoją apie neįprastą veiklą jo paskyroje, spusteli nuorodą, prisijungia prie netikro prisijungimo tojo vardą ir slaptažodį bei pateiktų konfidencialią informaciją.

Sukč
grė

Sukčius

naud

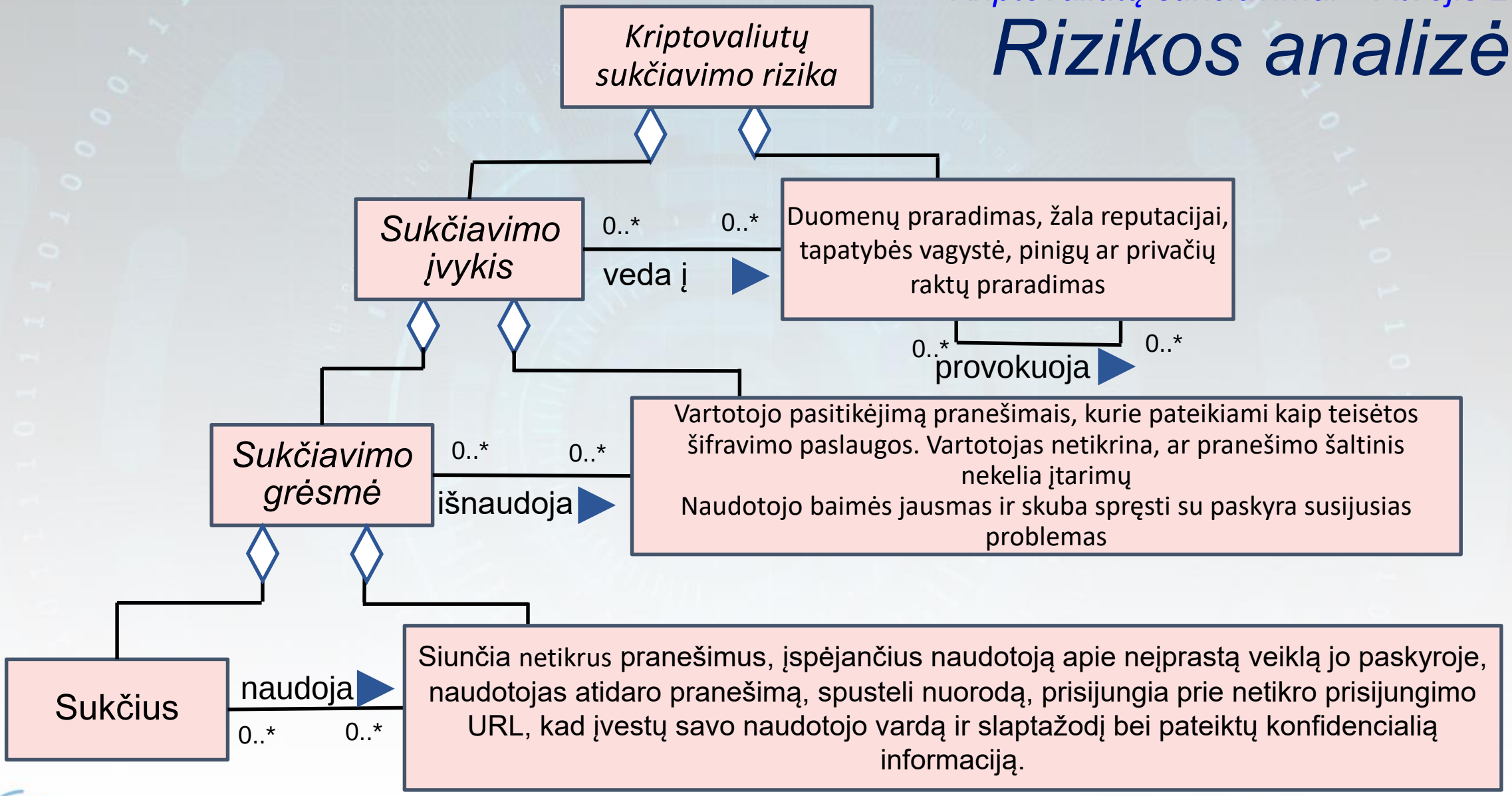
0..*

Cryptocurrency phishing email. Source: Reddit
Cryptocurrency phishing text message. Source: Reddit

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Cryptocurrency phishing email. Source: Reddit
Cryptocurrency phishing text message. Source: Reddit

Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukčiavimą

Sukčiavimo šaltinis: El. paštas, SMS žinutė
Sukčiavimo žinutės anatomija:
a. Iš ko siunčiama žinutė? *...@websupport.com, SMS telefono numeris*
b. Koks yra žinutės turinys? *Pranešimas apie sąskaitos išjungimą; pranešimas apie pinigų atsiėmimą*
c. Ar yra hipersaitų / priedų? *Taip*

Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius

3.1 Žinutėse iš teisėtų programėlių kreipiamasi į jus vardu
3.2. Teisėti pranešimai yra profesionalūs ir gerai suformatuoti
3.3. Teisėtose žinutėse nėra gramatikos klaidų, t. y. vietoj *„Coinbase“* naudojama *„CoInbase“*, *„Your CoInbase Has Disable“* arba *„SIGNIN“*.
3.4. Teisėtas „Coinbase“ el. pašto domenas yra *...@coinbase.com*, o ne *...@websupport.com*.

4. Kritinis mąstymas

4.1 Dukart patikrinkite siuntėjo adresą, teisėtų „Coinbase“ el. pašto adresų galūnė turėtų būti *.coinbase.com*.
4.2 Dėl problemų, susijusių su jūsų sąskaita arba mokėjimu, kreipkitės tiesiogiai į „Coinbase“ klientų aptarnavimo skyrių
4.3 Būkite atsargūs, nes šie sukčiai naudojasi jūsų baime ir skuba
4.4 Kryžminiu būdu patikrinkite saugumo informaciją teisėtų paslaugų svetainėje
4.5 Niekada nespauskite nuorodų / priedų iš nežinomų šaltinių, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.6 Paskyros slaptažodį arba prisijungimo informaciją „verifikavimui“ pateikite tik saugiose teisėtų svetainių dalyse
4.7 Ištrinkite atsiųstą el. laišką, jei pagrįstai įsitikinote, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

1. Supraskite sukčiavimą

Sukčiavimo šaltinis: El. paštas, SMS žinutė

Sukčiavimo žinutės anatomija:

a. Iš ko siunčiama žinutė? *...@websupport.com*, *SMS telefono numeris*

b. Koks yra žinutės turinys? *Pranešimas apie sąskaitos išjungimą; pranešimas apie pinigų atsiėmimą*

c. Ar yra hipersaitų / priedų? *Taip*

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų

2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas

2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

3. Atpažinkite pagrindinius požymius

3.1 Žinutėse iš teisėtų programėlių kreipiamasi į jus vardu

3.2. Teisėti pranešimai yra profesionalūs ir gerai suformatuoti

3.3. Teisėtose žinutėse nėra gramatikos klaidų, t. y. vietoj „Coinbase“ naudojama „CoInbase“, „Your CoInbase Has Disable“ arba „SIGNIN“.

3.4. Teisėtas „Coinbase“ el. pašto domenas yra *...@coinbase.com*, o ne *...@websupport.com*.

4.1 Dukart patikrinkite siuntėjo adresą, teisėtų „Coinbase“ el. pašto adresų galūnė turėtų būti *.coinbase.com*.

4.2 Dėl problemų, susijusių su jūsų sąskaita arba mokėjimu, kreipkitės tiesiogiai į „Coinbase“ klientų aptarnavimo skyrių

4.3 Būkite atsargūs, nes šie sukčiai naudojasi jūsų baime ir skuba

4.4 Kryžminiu būdu patikrinkite saugumo informaciją teisėtų paslaugų svetainėje

4.5 Niekada nespauskite nuorodų / priedų iš nežinomų šaltinių, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis

4.6 Paskyros slaptažodį arba prisijungimo informaciją „verifikavimui“ pateikite tik saugiose teisėtų svetainių dalyse

4.7 Ištrinkite atsiųstą el. laišką, jei pagrįstai įsitikinote, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukči
Sukčiavimo šaltinis: El. pašta
Sukčiavimo žinutės anatomija:
a. Iš ko siunčiama žinutė? *...@websupport.com, SMS telefono numeris*
b. Koks yra žinutės turinys? *Pranešimas apie sąskaitos išjungimą; pranešimas apie pinigų atsiėmimą*
c. Ar yra hipersaitų / priedų? *Taip*

Sukčiavimo atakų atpažinimas

ymius
j jus vardu
3.2. Teisėti pranešimai yra profesionalūs ir gerai suformatuoti
3.3. Teisėtose žinutėse nėra gramatikos klaidų, t. y. vietoj *„Coinbase“* naudojama *„CoInbase“*, *„Your CoInbase Has Disable“* arba *„SIGNIN“*.
3.4. Teisėtas „Coinbase“ el. pašto domenas yra *...@coinbase.com*, o ne *...@websupport.com*.

4. Kritinis mąstymas
4.1 Dukart patikrinkite siuntėjo adresą, teisėtų „Coinbase“ el. pašto adresų galūnė turėtų būti *.coinbase.com*.
4.2 Dėl problemų, susijusių su jūsų sąskaita arba mokėjimu, kreipkitės tiesiogiai į „Coinbase“ klientų aptarnavimo skyrių
4.3 Būkite atsargūs, nes šie sukčiai naudojasi jūsų baime ir skuba
4.4 Kryžminiu būdu patikrinkite saugumo informaciją teisėtų paslaugų svetainėje
4.5 Niekada nespauskite nuorodų / priedų iš nežinomų šaltinių, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.6 Paskyros slaptažodį arba prisijungimo informaciją „verifikavimui“ pateikite tik saugiose teisėtų svetainių dalyse
4.7 Ištrinkite atsiųstą el. laišką, jei pagrįstai įsitikinote, kad tai yra sukčiavimas

Išviliojimo sukčiavimai

- Deja, vis dažniau pasitaiko išviliojimo sukčiavimo atvejų, kai sukčiai ir įsilaužėliai gali gauti prisijungimo duomenis iš pažeistų duomenų ir grasinti aukoms „žinau tavo slaptažodį“.
- Užpuolikai taip pat gali teigti, kad prisijungė prie jūsų kompiuterio ir jo kameros, gavo jūsų seksualinio pobūdžio vaizdo įrašų ar nuotraukų ir netgi gali priversti jus sumokėti Bitkoinais.

Funded by the
Erasmus+ Programme
of the European Union

Rizikos analizė

Išviliojimo sukčiavimo rizika

Suk… gr…

Sukčius

nau…

0..*

…dėl

…kra

From: Beitris Englert <hbeleonoretvi@outlook.com>
Date: July 12, 2018

Subject:

It seems that, xxxxxxxxx, is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

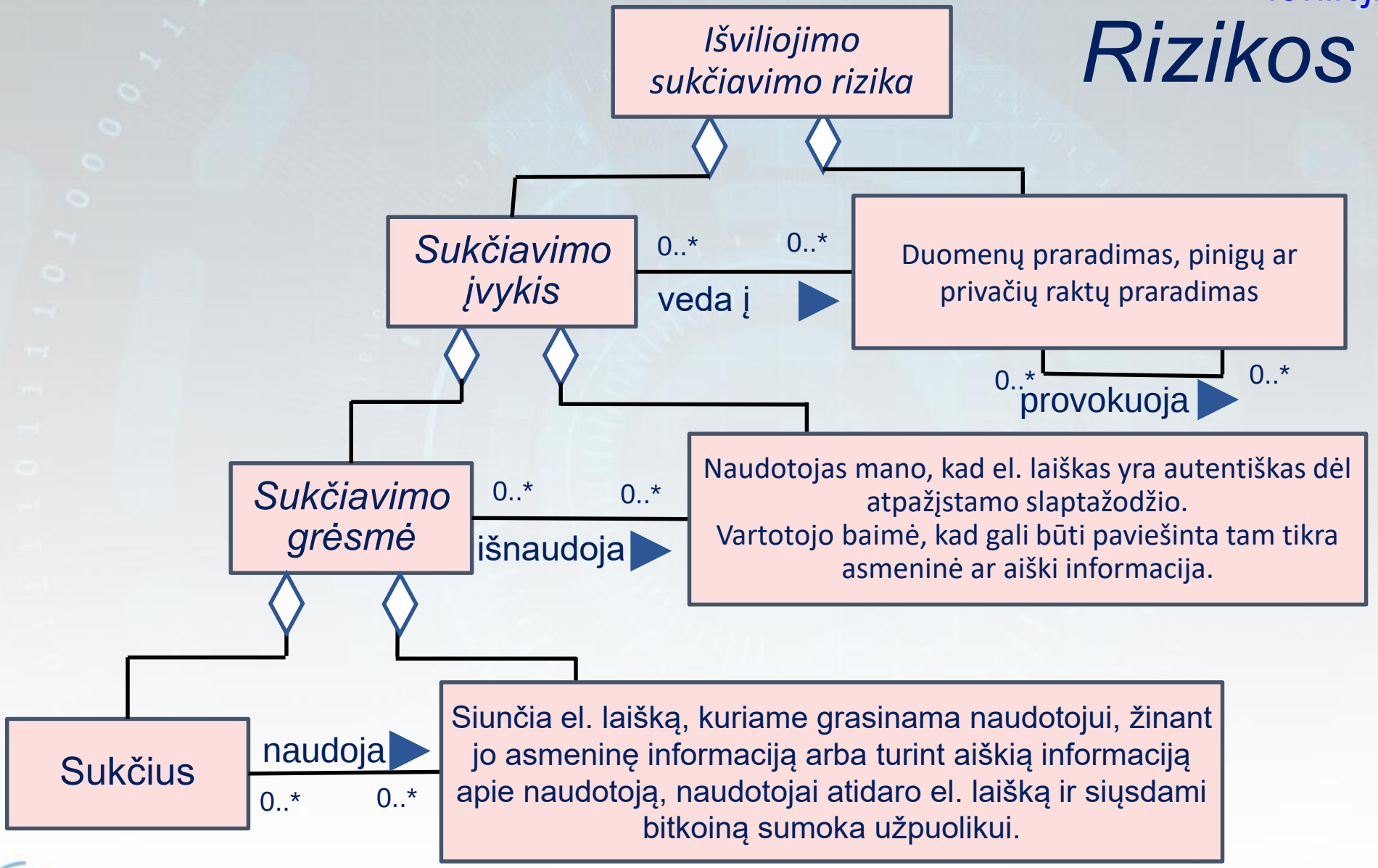
Well, in my opinion, $2900 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
(It is cAsE sensitive, so copy and paste it)

Cryptocurrency phishing email. Source: Reddit
Cryptocurrency phishing text message. Source: Reddit

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Cryptocurrency phishing email. Source: Reddit
Cryptocurrency phishing text message. Source: Reddit

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias neatitinka turinio

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: El. laiškas
Sukčiavimo žinutės anatomija:
a. Kas siunčia el. laišką? *...@outlook.com*
b. Koks laiško turinys? *Seksualinis išviliojimas*
c. Ar yra hipersaitų / nuorodų? *Taip*

3. Atpažinkite pagrindinius požymius
3.1 Daugeliu atvejų el. laiškai yra tušti grasinimai, o ne dėl to, kad vartotojas buvo „nulaužtas“
3.2 Užpuolikas galėjo gauti neskelbtinos informacijos dėl duomenų pažeidimo (angl. breach), nutekėjimo arba viešai prieinamos informacijos internete

4. Kritinis mąstymas
4.1 Būkite atsargūs, nes šie el. pašto sukčiai gali pasinaudoti jūsų baime ir gėda.
4.2 Patikrinkite, ar jūsų el. paštas nebuvo pažeistas interneto svetainėse, pvz., *haveibeenpwned*.com arba *dehashed*.com
4.3 Jei slaptažodis vis dar naudojamas, svarbu apsaugoti šias paskyras
4.4 Ištrinkite jums atsiųstą el. laišką, jei esate pagrįstai įsitikinę, kad tai sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Išankstinių mokesčių sukčiavimai

- Išankstinių mokesčių sukčiai vis dar stiprūs COVID pandemijos metu, nes žmonės susidūrė su sunkumais. Šios sukčiavimo atakos įvykdomos, kai užsienyje nusikaltėlis siūlo dalį didelės pinigų sumos už pagalbą pervedant pinigus iš savo šalies
- Norėdami tai padaryti, jie paprašys jūsų banko informacijos arba paprašys sumokėti mokesčius, rinkliavas ar įmokas.

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė

[SPAM]ATN International Credit Settlement

Central Bank of Nigeria [printer@brandmelloon.co.uk]

Sent: Sat 10/13/2012 5:20 AM

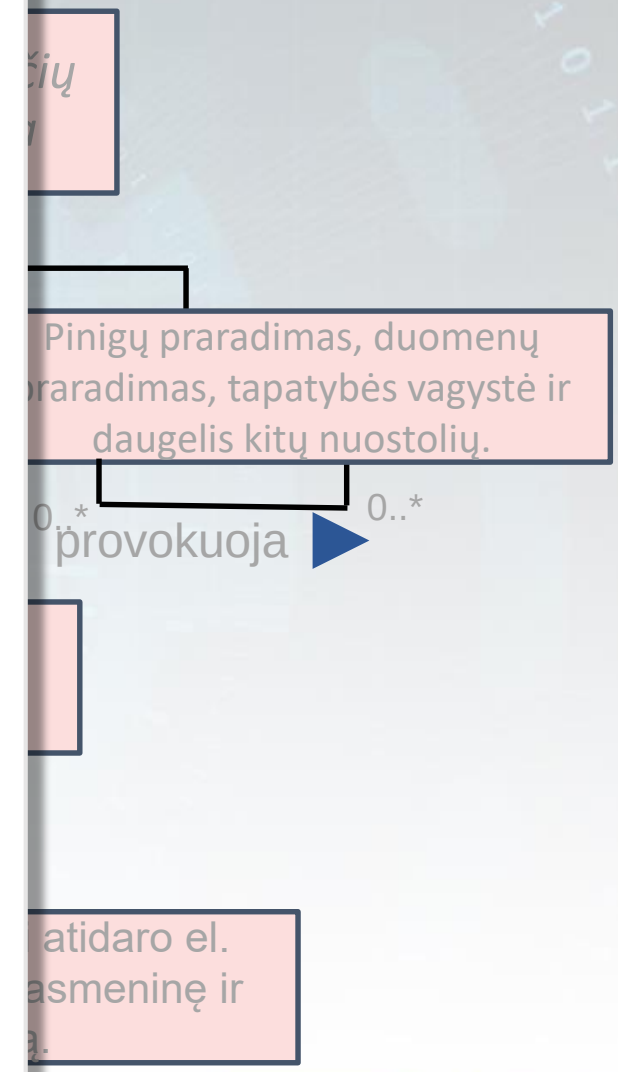
To: dave@d

Central Bank of Nigeria.
ATM International Credit Settlement,
Directorate of International Payment.

This is to officially notiify yoou about your Fund that was supposed to be rendered to you via numeroous ways i.e. Coourier Companies, Western Union Money Transfer and Banks. Due to this lost of Funds oof yours which was suppose to be given to you but failed to. So in this case, a beneficial meeting was held on the 25th of August 2012 at the World Bank iin Switzerland, which top officials and Central Bank Governors froom different countries in the world were present at the meeting. Which they discussed on how your Fund can be giiven to you withoout any loss at this time, which yoou have to stop any further communication with any other person(s) or office(s) to avoid any hitches in receiving your ATM payment.

In conclusion at the meeting., The President of World Bank Mr. Jim Yong Kim has strictly authorized 6 Banks in the World to deliver all Funds through courier companies. Your Fund which is truly $3.5 Million USD (Three Million, Five Hundred Thousand United States of America Dollars) to all beneficiaries in various countries in the world as an ATM MASTER CARD. Below are the authorized Banks;

Daiwa Bank R/Osaka/Japan.
Caja De Madrid/Madrid/Spain.
Lloyds Bank R /London/England.
Central Bank of Nigeria/Lagos/Nigeria.
Banco di Santo Spirito/Rome/Italy.
Bank of New York Mellon Corp/New York/USA.

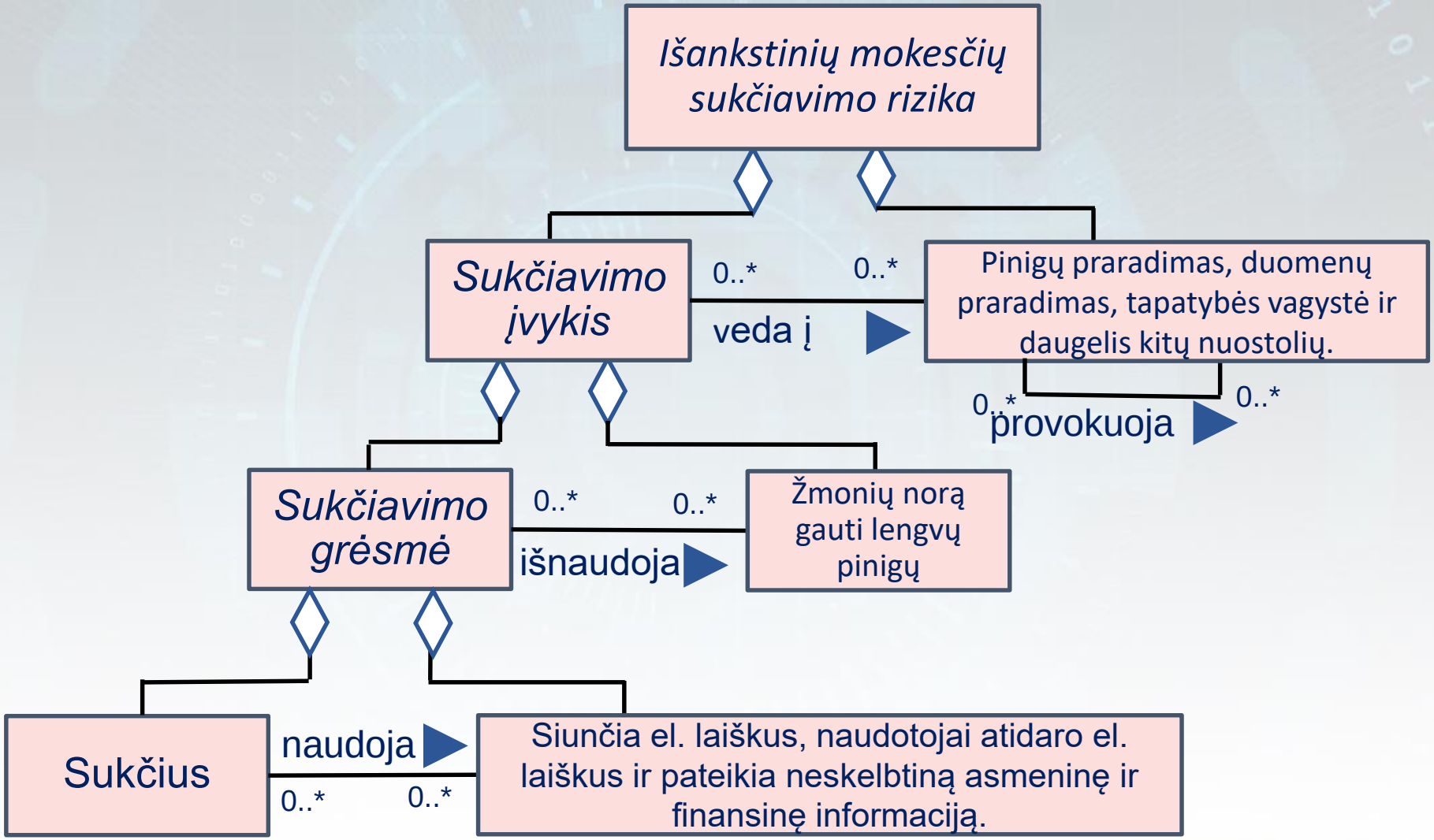


Extortion Phishing Email (Source: Massmoola)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Extortion Phishing Email (Source: Massmoola)

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nesivadovaukite jokiais el. pašto žinutėje pateiktais nurodymais.

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: El. laiškas
Sukčiavimo žinutės anatomija
a. Kas siunčia laišką? *Nigerijos centrinis bankas*
b. Koks yra žinutės turinys?
Atsiskaitymas už kreditą
c. Ar yra hipersaitų / priedų? *Ne*

Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius
3.1 Jei kas nors jums siūlo nemokamų pinigų, paprastai tai pernelyg gerai, kad būtų tiesa.
3.2. Teisėti bankų tarnybiniai el. laiškai yra profesionalūs, turi vienodą šablono formatą ir nesiunčia nepageidaujamų el. laiškų

4. Kritinis mąstymas
4.1 Niekada neteikite bankininkystės informacijos nepažįstamam asmeniui.
4.2. Būkite atsargūs, nes šie el. pašto sukčiai gali pasinaudoti jūsų smalsumu ir godumu
4.3 Ištrinkite jums atsiųstą el. laišką, jei esate pagrįstai įsitikinę, kad tai sukčiavimas

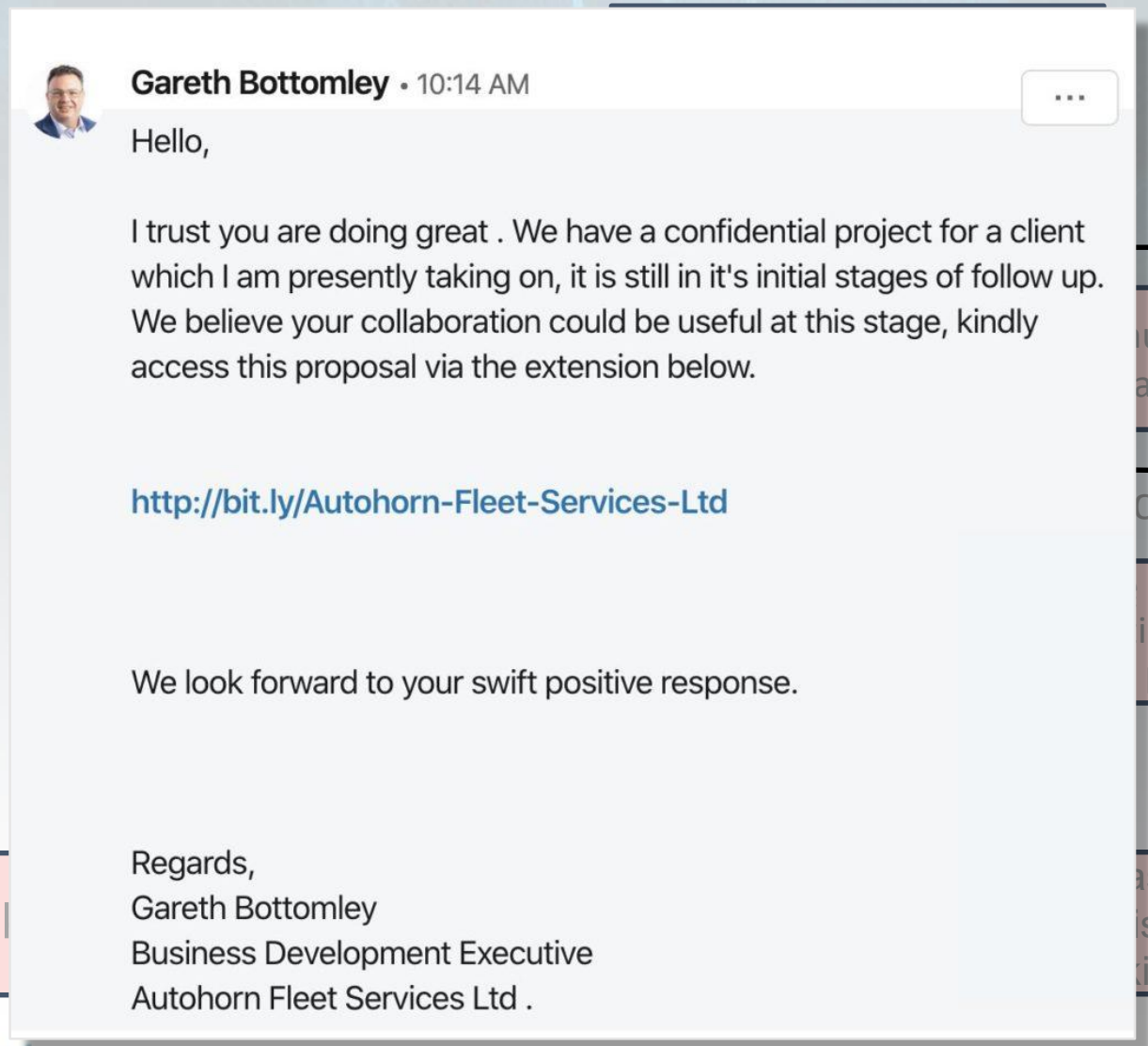
Funded by the Erasmus+ Programme of the European Union

Sukčiavimai socialiniuose tinkluose

- Užpuolikai naudojasi socialinių tinklais tokiais kaip „Facebook“, „LinkedIn“ ar „Twitter“, kad įkalbėtų naudotojus spustelėti kenkėjiškas nuorodas arba atskleistų asmeninę informaciją.
- Užpuolikai socialiniuose tinkluose taip pat gali rasti daugybę informacijos apie potencialias aukas, kad galėtų pradėti tikslinę ataką.

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Gareth Bottomley • 10:14 AM

Hello,

I trust you are doing great . We have a confidential project for a client which I am presently taking on, it is still in it's initial stages of follow up. We believe your collaboration could be useful at this stage, kindly access this proposal via the extension below.

http://bit.ly/Autohorn-Fleet-Services-Ltd

We look forward to your swift positive response.

Regards,
Gareth Bottomley
Business Development Executive
Autohorn Fleet Services Ltd .

ų praradimas, tapatybės
agystė ir kita žala.

0..*

okuoja

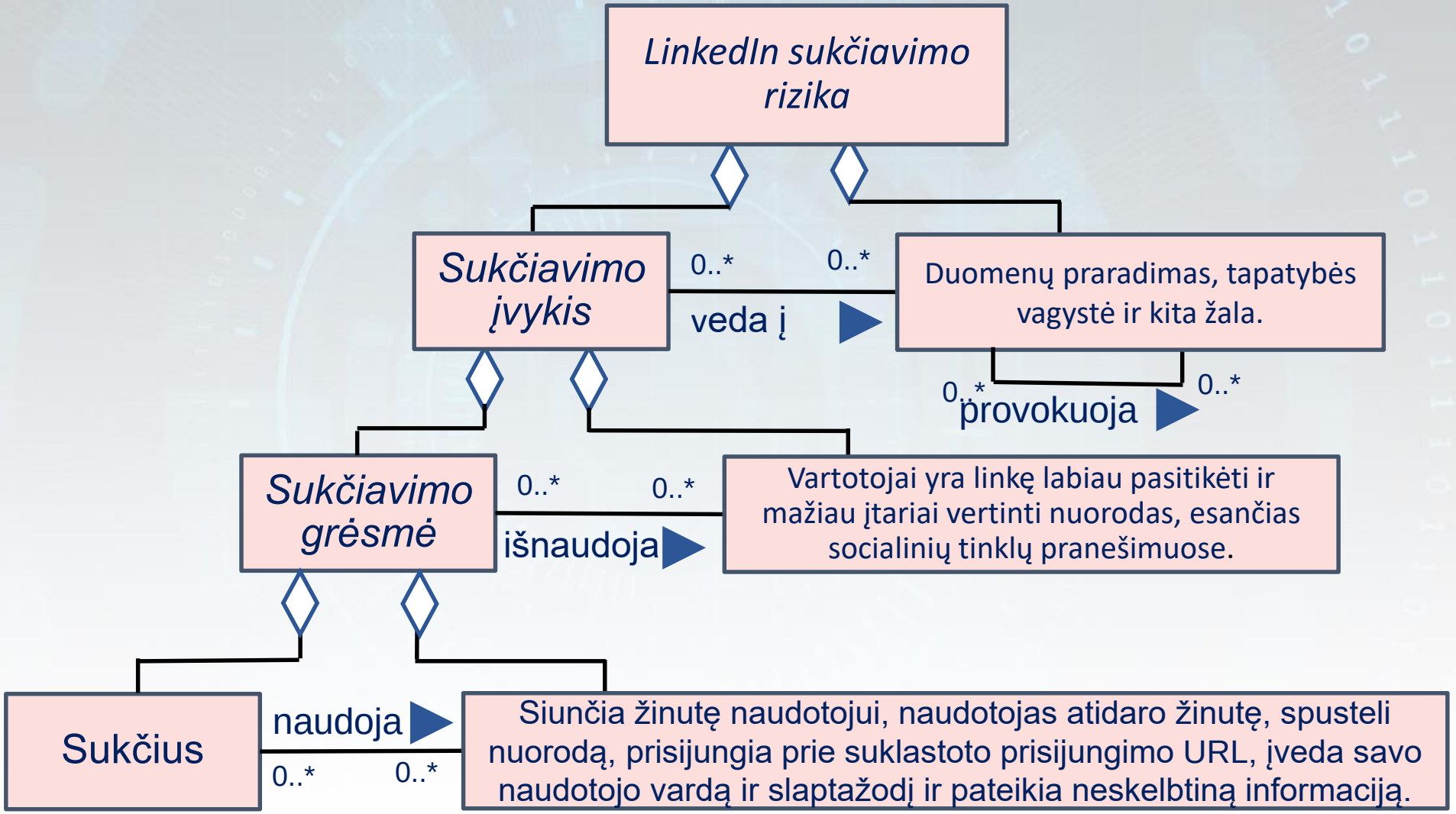
labiau pasitikėti ir
i nuorodas, esančias
pranešimuose.

Sul

as atidaro žinutę, spusteli
sijungimo URL, įveda savo
ia neskelbtiną informaciją.

Extortion Phishing Email (Source: Massmoola)

Rizikos analizė



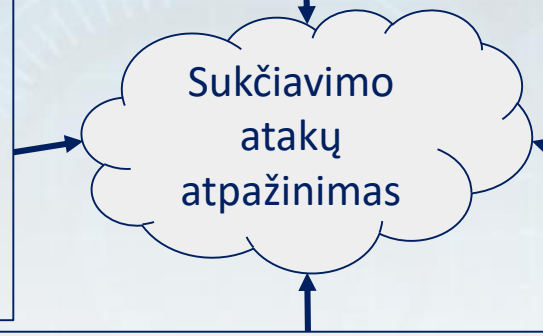
Extortion Phishing Email (Source: Massmoola)

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: Tiesioginė žinutė
Sukčiavimo žinutės anatomija:
a. Kas siunčia žinutę? *LinkedIn vartotojas*
b. Koks žinutės turinys? *Bendradarbiavimo pasiūlymas*
c. Ar yra hipersaitų / priedų? *Taip*

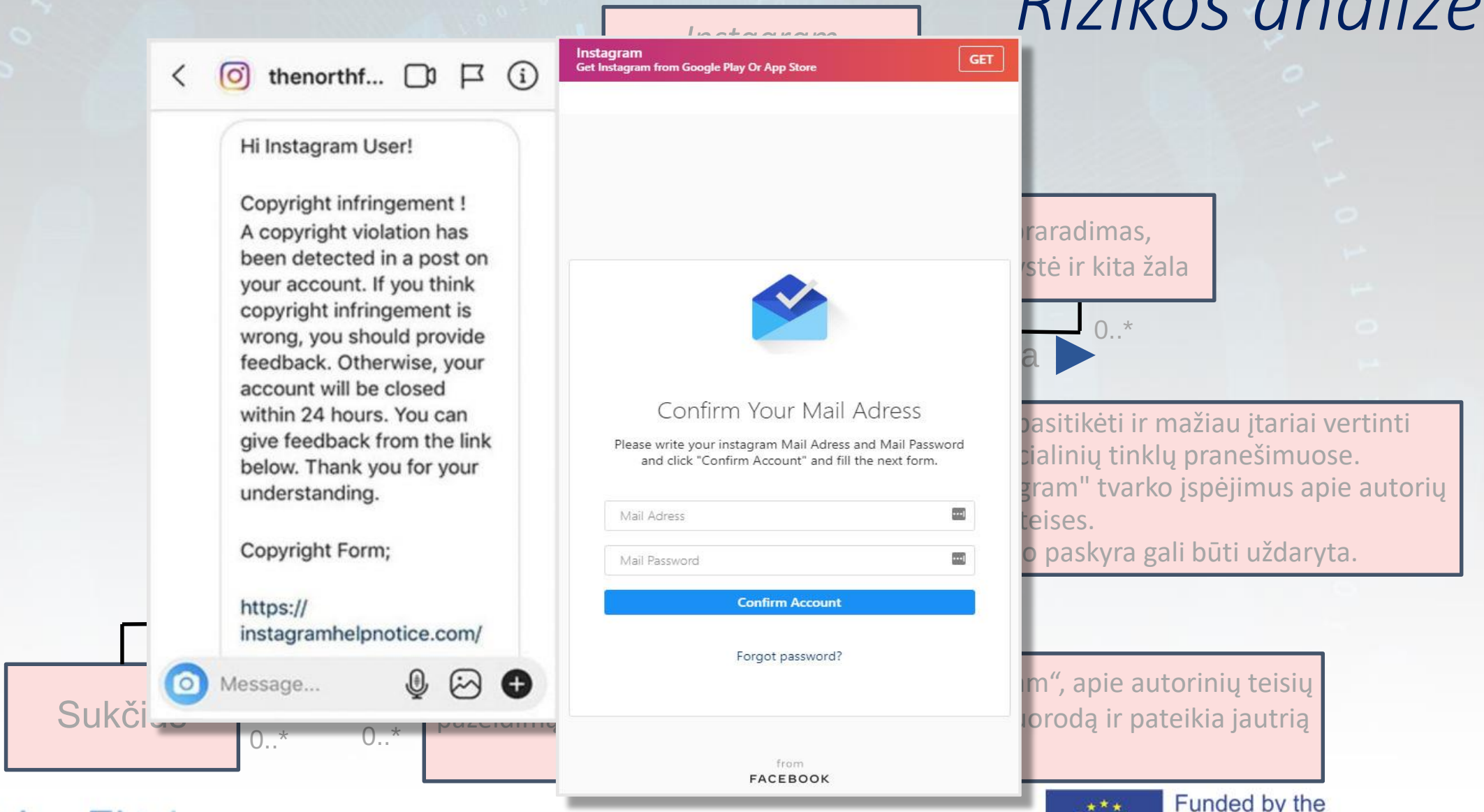


3. Atpažinkite pagrindinius požymius
3.1 Jei bendradarbiavimą siūlo nežinomas asmuo, tai gali būti įtartina.
3.2. Užpuolikai naudoja URL trumpinimo paslaugas, pavyzdžiui, „*bit.ly*“, kad sutrumpintų ir paslėptų sukčiavimo nuorodas

4. Kritinis mąstymas
4.1 paskyros slaptažodį arba prisijungimo informaciją pateikite tik saugiose teisėtų svetainių dalyse.
4.2. Net jei atrodo, kad žinutę siunčia asmuo, kuriuo pasitikite, yra tikimybė, kad į jo paskyrą buvo įsilaužta
4.3 Socialiniuose tinkluose visada naudokite sustiprintus privatumo nustatymus
4.4 Nespauskite ant įtartinų nuorodų tiesioginėse žinutėse, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.5. Niekada nepriimkite „LinkedIn“ prisijungimo prašymų iš nepažįstamo asmens
4.6 Būkite atsargūs ir socialiniuose tinkluose nesidalykite per daug asmeninės informacijos
4.7 Atšaukite / blokuokite įtartinas paskyras ir ištrinkite atsiųstą žinutę, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Funded by the
Erasmus+ Programme
of the European Union

Rizikos analizė

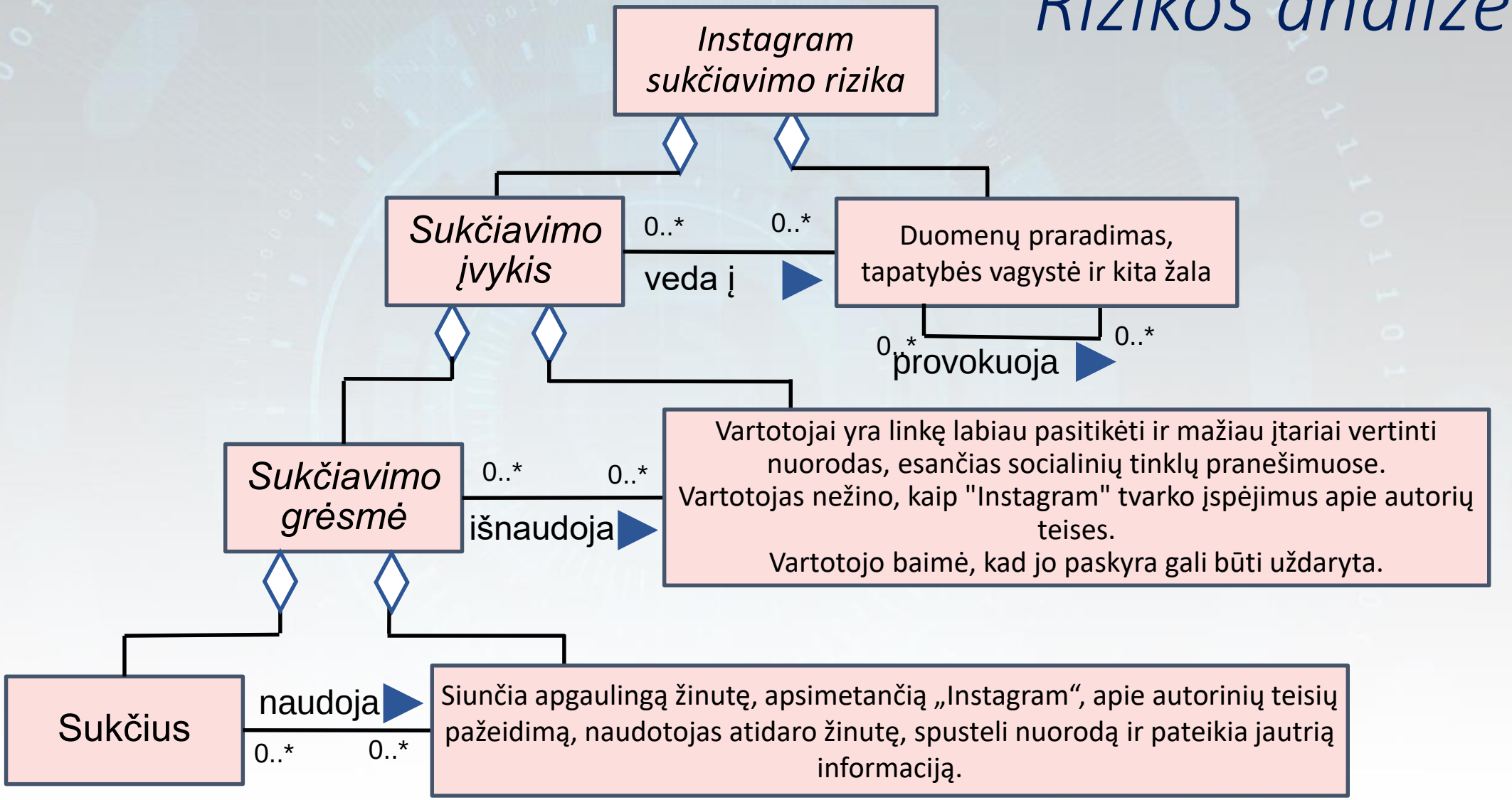


Socialiniųn tinklų sukčiavimo el. laiškas (Šaltinis: Hackread)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Rizikos analizė



Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias nesutampa su platformos domenu

1. Supraskite sukčiavimą

Sukčiavimo šaltinis: Tiesioginė žinutė
Sukčiavimo žinutės anatomija:
a. Kas siunčia žinutę? *Instagram vartotojas*
b. Koks žinutės turinys? *Pretenzija dėl autorių teisių pažeidimo*
c. Ar yra hipersaitų / nuorodų? *Taip*

Sukčiavimo atakų atpažinimas

3. Atpažinkite pagrindinius požymius

3.1 teisėtus pranešimus apie autorių teisių pretenzijas siunčia asmeniškai „Instagram“
3.2 „Instagram“, kreipdamasi į jus, visada naudos jūsų paskyroje registruotą vardą
3.3 Pateikta nuoroda turi atitikti platformos domeną, t. y. *instagram.com*, o ne *instagramhelpnotice.com*

4. Kritinis mąstymas

4.1 Paskyros slaptažodį arba prisijungimo informaciją pateikite tik saugiose teisėtų svetainių dalyse
4.2 Net jei atrodo, kad žinutė yra iš asmens, kuriuo pasitikite, yra tikimybė, kad į jo paskyrą buvo įsilaužta
4.3 Socialiniuose tinkluose visada naudokite sustiprintus privatumo nustatymus
4.4 Nespauskite ant įtartinų nuorodų tiesioginėse žinutėse, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.5 Būkite atsargūs, susirašinėdami žinutėmis su naudotojais, kurių nepažįstate ir kurių nesekate
4.6 Atšaukite / blokuokite įtartinas paskyras ir ištrinkite atsiųstą žinutę, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias nesutampa su platformos domenu

1. Supraskite sukčiavimą

Sukčiavimo šaltinis: *Tiesioginė žinutė*
Sukčiavimo žinutės anatomija:
a. Kas siunčia žinutę? *Instagram vartotojas*
b. Koks žinutės turinys? *Pretenzija dėl autorių teisių pažeidimo*
c. Ar yra hipersaitų / nuorodų? *Taip*

3. Atpažinkite pagrindinius požymius

3.1 teisėtus pranešimus apie autorių teisių pretenzijas siunčia asmeniškai „Instagram“
3.2 „Instagram“, kreipdamasi į jus, visada naudos jūsų paskyroje registruotą vardą
3.3 Pateikta nuoroda turi atitikti platformos domeną, t. y. *instagram.com*, o ne *instagram**helpnotice**.com*

4. Kritinis mąstymas

4.1 Paskyros slaptažodį arba prisijungimo informaciją pateikite tik saugiose teisėtų svetainių dalyse
4.2 Net jei atrodo, kad žinutė yra iš asmens, kuriuo pasitikite, yra tikimybė, kad į jo paskyrą buvo įsilaužta
4.3 Socialiniuose tinkluose visada naudokite sustiprintus privatumo nustatymus
4.4 Nespauskite ant įtartinų nuorodų tiesioginėse žinutėse, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.5 Būkite atsargūs, susirašinėdami žinutėmis su naudotojais, kurių nepažįstate ir kurių nesekate
4.6 Atšaukite / blokuokite įtartinas paskyras ir ištrinkite atsiųstą žinutę, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos atpažinimas

2. Supraskite URL adresus

2.1 Nespauskite jokių priedų ar nuorodų

2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas

2.3 Būkite atsargūs, jei URL kelias nesutampa su platformos domenu

1. Supraskite sukč

Sukčiavimo šaltinis: Tiesioginė žinutė

Sukčiavimo žinutės anatomija:

a. Kas siunčia žinutę? *Instagram vartotojas*

b. Koks žinutės turinys? *Pretenzija dėl autorių teisių pažeidim*

c. Ar yra

Sukčiavimo atakų atpažinimas

3.1 teisėtus pranešimus apie autorių teisių pretenzijas siunčia asmeniškai „Instagram“

3.2 „Instagram“, kreipdamasi į jus, visada naudos jūsų paskyroje registruotą vardą

.com,

4. Kritinis mąstymas

4.1 Paskyros slaptažodį arba prisijungimo informaciją pateikite tik saugiose teisėtų svetainių dalyse

4.2 Net jei atrodo, kad žinutė yra iš asmens, kuriuo pasitikite, yra tikimybė, kad į jo paskyrą buvo įsilaužta

4.3 Socialiniuose tinkluose visada naudokite sustiprintus privatumo nustatymus

4.4 Nespauskite ant įtartinų nuorodų tiesioginėse žinutėse, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis

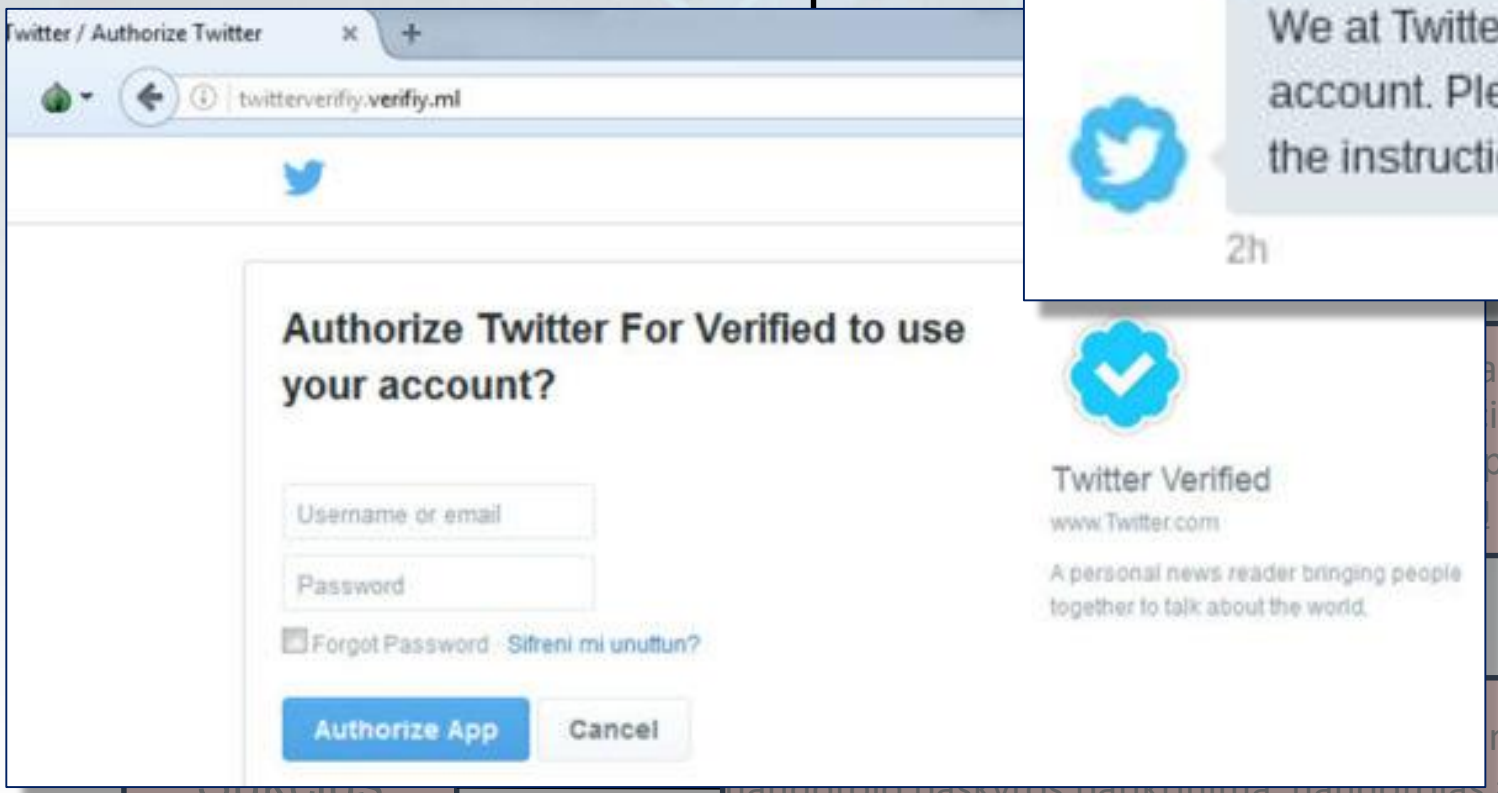
4.5 Būkite atsargūs, susirašinėdami žinutėmis su naudotojais, kurių nepažįstate ir kurių nesekate

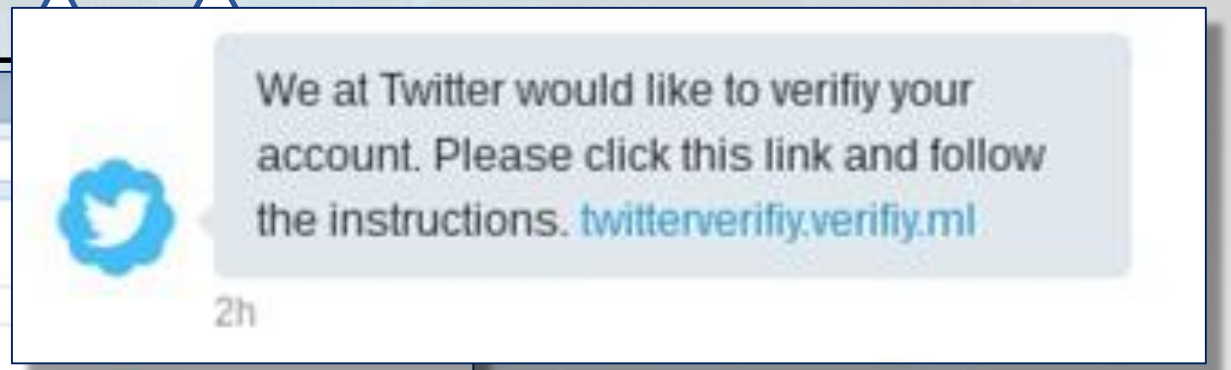
4.6 Atšaukite / blokuokite įtartinas paskyras ir ištrinkite atsiųstą žinutę, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Funded by the Erasmus+ Programme of the European Union

Rizikos Analizė

Twitter sukčiavimo rizika





abiau pasitikėti ir mažiau įtariai vertinti
ias socialinių tinklų pranešimuose.
o „Twitter“ atlieka paskyros patikrinimą.
gauti „Twitter“ patikrinimo statusą

Sukelia

0..*

0..*

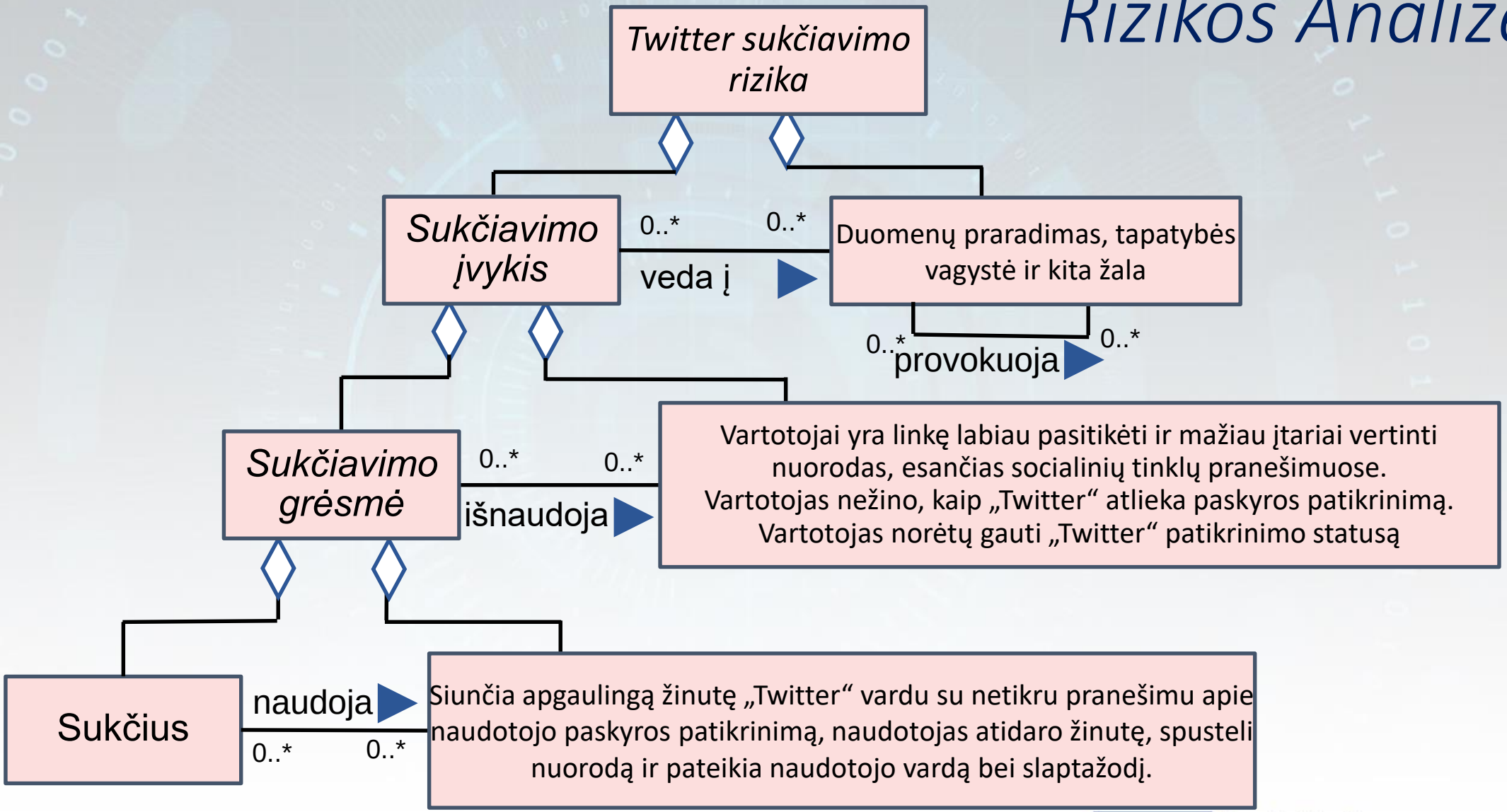
netikru pranešimu apie
atidaro žinutę, spusteli
nuorodą ir pateikia naudotojo vardą bei slaptažodį.

CyberPhish
Safeguarding your digital future

Sukčiavimai socialiniuose tinkluose (Šaltinis: Malwarebytes)

Funded by the Erasmus+ Programme of the European Union

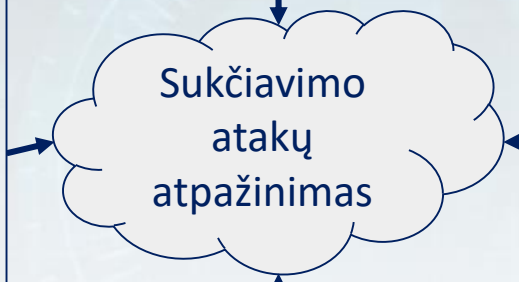
Rizikos Analizė



Rizikos atpažinimas

2. Supraskite URL adresus
2.1 Nespauskite jokių priedų ar nuorodų
2.2 Užveskite pelės žymeklį ant priedo, kad pamatytumėte URL, ir išanalizuokite, ar jis kenkėjiškas
2.3 Būkite atsargūs, jei URL kelias nesutampa su platformos domenu

1. Supraskite sukčiavimą
Sukčiavimo šaltinis: *Tiesioginė žinutė*
Sukčiavimo žinutės anatomija:
a. Kas siunčia žinutę? *Twitter vartotojas*
b. Koks žinutės turinys? *Reikalavimas patvirtinti paskyrą*
c. Ar yra hipersaitų / priedų? *Taip*



3. Atpažinkite pagrindinius požymius
3.1 Teisėtas „*Twitter*“ patvirtinimo procesas tvarkomas pateikiant užklausą „*Twitter*“ (o ne atvirkščiai)
3.2 „Twitter“ kreipintis į jus visada naudos jūsų paskyroje užregistruotą vardą
3.3 Pateikta nuoroda turi atitikti platformos domeną, t. y. *twitter.com, o ne* ***twitterverifiy.verifiy.ml***

4. Kritinis mąstymas
4.1 Paskyros slaptažodį arba prisijungimo informaciją pateikite tik saugiose teisėtų svetainių dalyse, pvz., *twitter.com*
4.2. Net jei atrodo, kad žinutę siunčia asmuo, kuriuo pasitikite, yra tikimybė, kad į jo paskyrą buvo įsilaužta
4.3 Socialiniuose tinkluose visada naudokite sustiprintus privatumo nustatymus
4.4 Nespauskite ant įtartinų nuorodų tiesioginėse žinutėse, patikrinkite įtartinus URL adresus naudodamiesi nemokamomis sukčiavimo aptikimo priemonėmis
4.5 Būkite atsargūs, kai siunčiate žinutes naudotojams, kurių nepažįstate ir kurių nesekiojate
4.6 Atšaukite / blokuokite įtartinas paskyras ir ištrinkite atsiųstą žinutę, jei esate pagrįstai įsitikinę, kad tai yra sukčiavimas

Santrauka

- Sukčiavimo atvejų analizė
- Išskirtų sukčiavimo atakų ir sukčiavimo atvejų rizikos analizė
- Šių sukčiavimo atakų atpažinimas, siekiant užkirsti kelią kylančiai sukčiavimo rizikai

Funded by the Erasmus+ Programme of the European Union

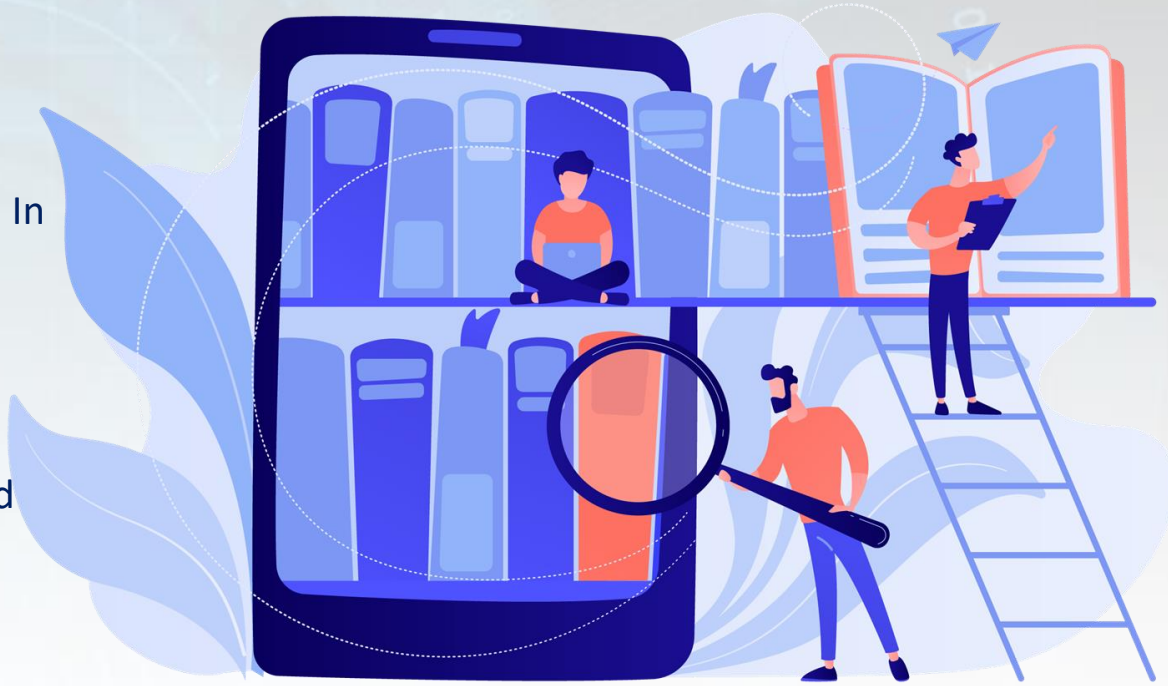
Užduotis

- Aptarkite 3 nepaminėtas sukčiavimo atakas, kurios, jūsų manymu, šiandien yra paplitusios.
- Sudarykite šių sukčiavimo atvejų rizikos analizę, pabrėždami atakos metodus, pažeidžiamumą ir sukčiavimo įvykius, kurie sudarė sukčiavimo riziką.
- Aptarkite, kaip galite atpažinti šiuos sukčiavimo atvejus ir užkirsti kelią dėl jų kylančiai sukčiavimo rizikai.

Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

- **Dubois E., Heymans P., Mayer N., Matulevičius R.** (2010) A Systematic Approach to Define the Domain of Information System Security Risk Management. *Intentional Perspectives on Information Systems Engineering 2010: 289-306*
- **Abroshan H.** (2021)**:** Root Causes of Falling Victim to Phishing – The Effects of Human Behavior, Emotions, and Demographics., *PhD thesis*, Ghent University.
- **Althobaiti, K., Meng, N., & Vaniea, K.** (2021). I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).
- **Drake, C. E., Oliver, J. J., & Koontz, E. J.** (2004). Anatomy of a Phishing Email. In CEAS.
- **Althobaiti, K., Meng, N., & Vaniea, K.** (2021, May). I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).
- **Drake, C. E., Oliver, J. J., & Koontz, E. J.** (2004). Anatomy of a Phishing Email. In CEAS.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Trumpi vaizdo įrašai

- Sukčiavimo el. laišku anatomija
  - ***https://youtu.be/3gpOM9c6mmA***
- Sukčiavimo atakų pavyzdžiai
  - ***https://youtu.be/lpGfxIAQhSo***
  - ***https://youtu.be/pGEAZdp0MAI***
- Sukčiavimo atpažinimas ir apsisaugojimas
  - ***https://youtu.be/R12_y2BhKbE***

Funded by the Erasmus+ Programme of the European Union

Dėkojame!