Funded by the
Erasmus+ Programme
of the European Union

Pārskats par kiberuzbrukumu izpratni un apiešanos ar tiem

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

Gadījumu izpēte

Pikšķerēšanas uzbrukumu un metožu analīze

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

Apmācību mērķis

Izskaidrot dažādus pikšķerēšanas uzbrukumus, kas izraisa uzbrukumu sekas un kā atpazīt un rīkoties ar šiem pikšķerēšanas uzbrukumiem

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kursantu darba slodze

Lekcija	3 st.
Audio un video materiāli	3 st.
Pētījumi	3 st.
Papildu lasīšana	6 st.
Sagatavošanās eksāmenam	3 st.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saturs

- Kas ir pikšķerēšanas uzbrukumi un riski?
- Pikšķerēšanas uzbrukumu un gadījumu izpētes analīze
  - Kādi ir pikšķerēšanas draudi un riski katrā gadījumā?
  - Kā atpazīt un novērst šos pikšķerēšanas riskus?

Funded by the
Erasmus+ Programme
of the European Union

Kas ir pikšķerēšanas uzbrukums?

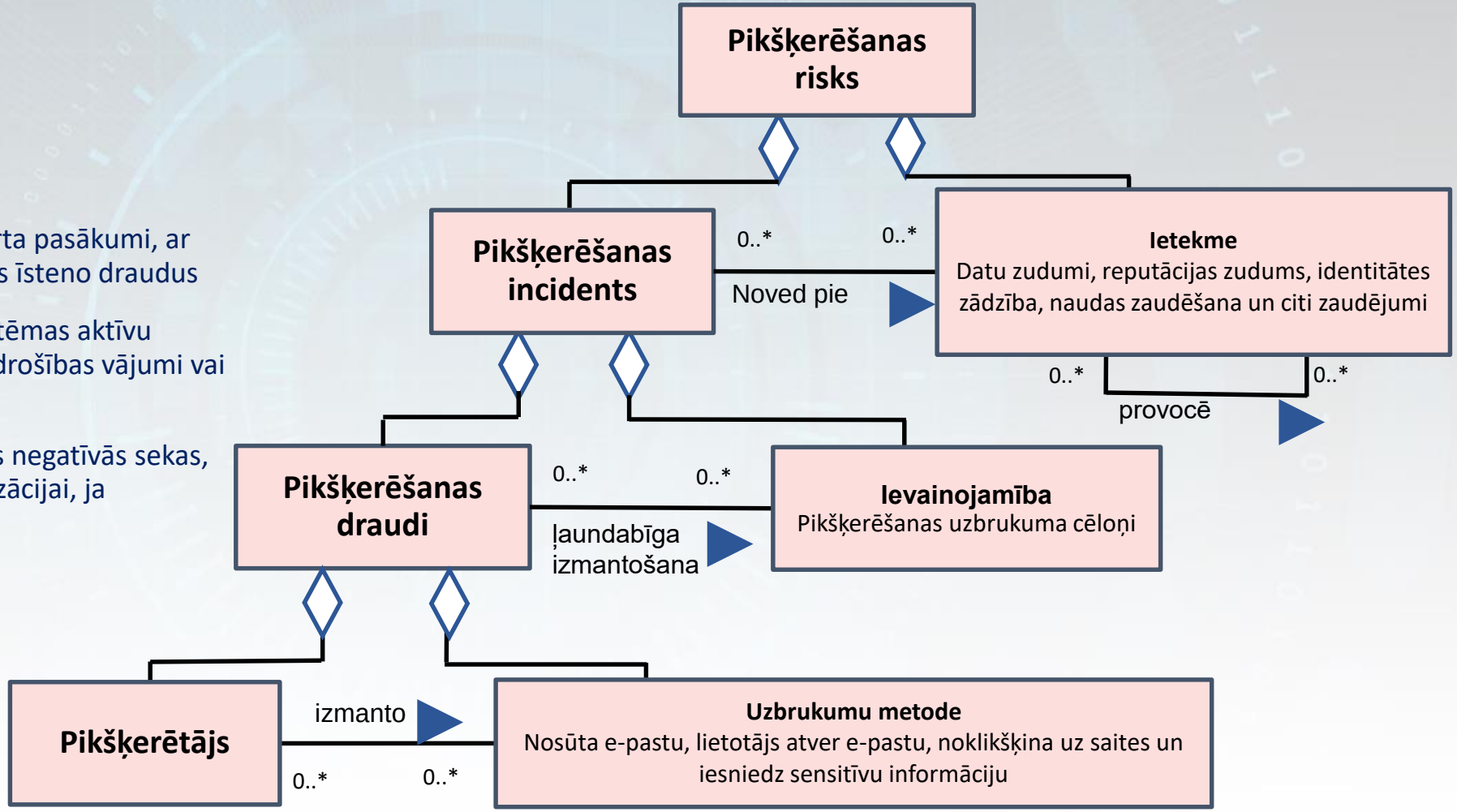
Pikšķerēšana jeb personas datu izmānīšana *ir sociālās inženierijas krāpniecība, kas var izraisīt datu zudumu, reputācijas bojājumus, identitātes zādzību, naudas zaudējumus un daudzus citus negatīvus efektus indivīdiem un organizācijām. Pikšķerēšanas krāpniecība parasti sākas ar e-pasta ziņojumu, kurā tiek mēģināts iegūt potenciālā upura uzticību un pārliecināt viņu veikt uzbrucējam vēlamās darbības.*

[Abrošans [Abroshan], 2021. gads]

Funded by the Erasmus+ Programme of the European Union

Kas ir pikšķerēšanas risks?

- **Uzbrukuma metode** – standarta pasākumi, ar kuriem draudu līdzeklis vai aģents īsteno draudus
- **Ievainojamība** – raksturīgie sistēmas aktīvu apsvērumi, kas var būt sistēmas drošības vājumi vai trūkumi
- **Ietekme** jeb efekts – iespējamās negatīvās sekas, kas var kaitēt aktīviem vai organizācijai, ja apdraudējums tiek izpildīts

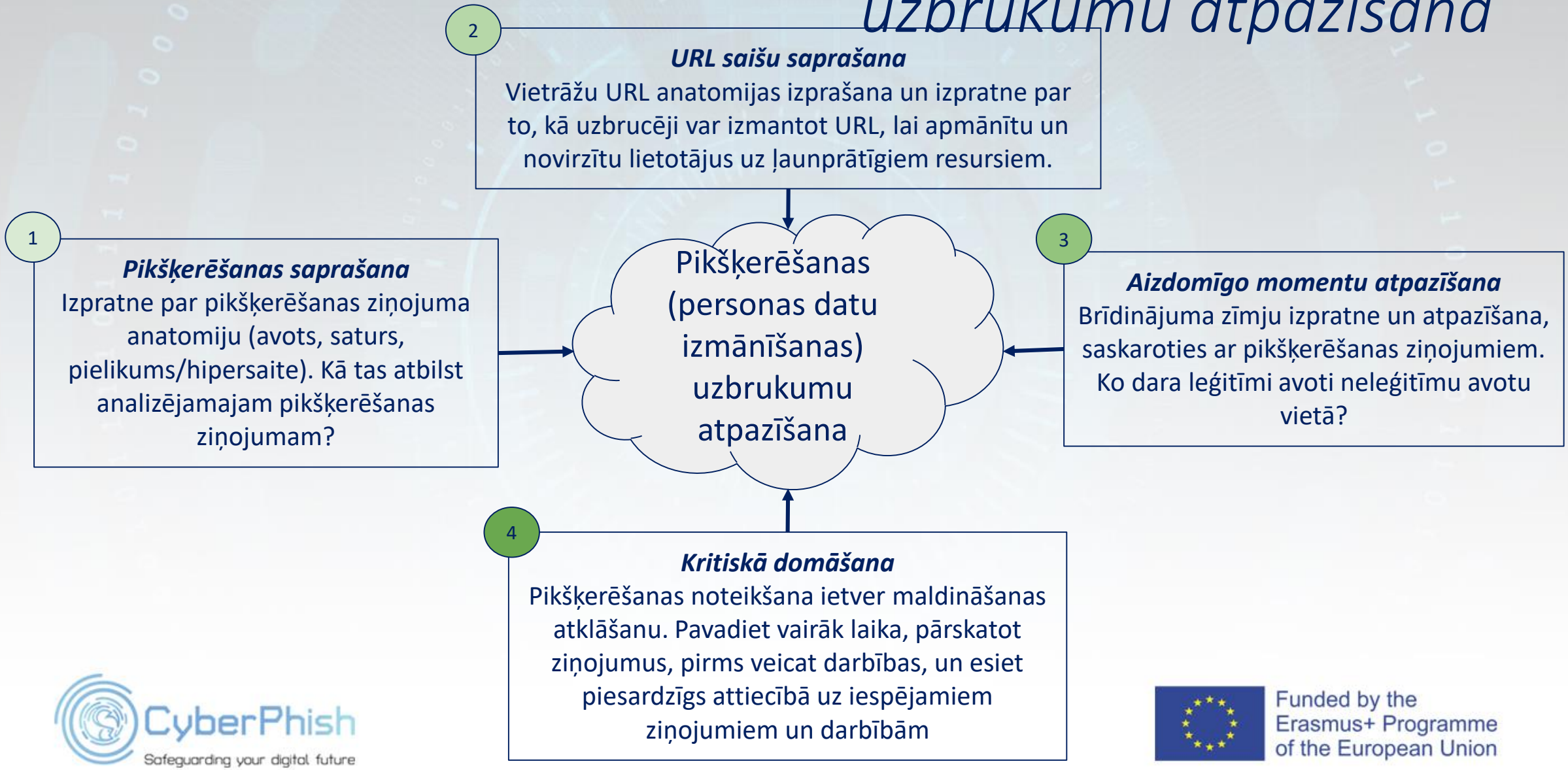


[*Dubuā [Dubois] un citi, 2010. gads*]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pētījumi

Izvēlēti gadījumi

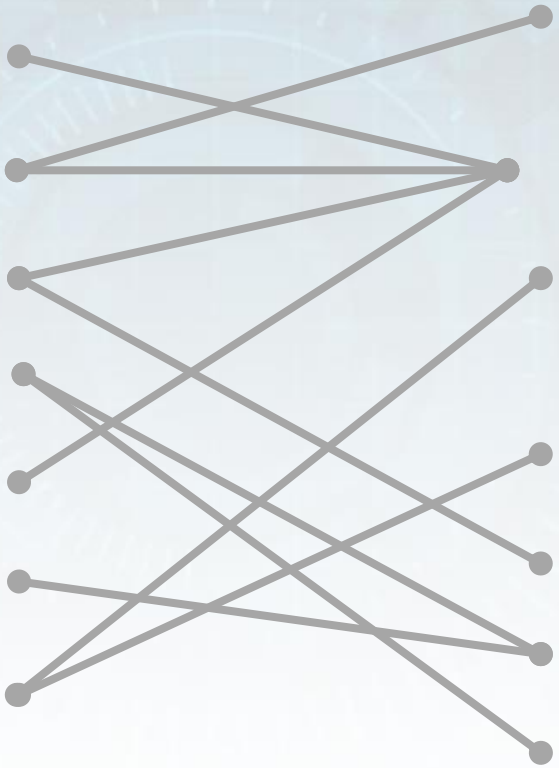
- Ar COVID saistīti uzbrukumi
- Ar COVID saistīti uzbrukumi
- Tehniskā atbalsta uzbrukumi
- Kriptovalūtu izkrāpšana
- Izspiešanas krāpniecība
- Avansa maksas izkrāpšana
- Sociālo mediju krāpniecība

Funded by the
Erasmus+ Programme
of the European Union

Pētījumi

Izvēlēti gadījumi

- Ar COVID saistīti uzbrukumi
- Ar COVID saistīti uzbrukumi
- Tehniskā atbalsta uzbrukumi
- Kriptovalūtu izkrāpšana
- Izspiešanas krāpniecība
- Avansa maksas izkrāpšana
- Sociālo mediju krāpniecība



Ar COVID saistīti uzbrukumi

E-pasti

Tūlītējā ziņapmaiņa (mirkļsaziņa)

Sociālie tīkli

Mājaslapas

Viltus loterijas

SMS (īsziņas)

Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni

Funded by the Erasmus+ Programme of the European Union

Ar COVID saistīti uzbrukumi

- Covid-19 laikā tika novērots ar pandēmiju saistītu krāpniecību un epastu, SMS sūtījumu pieaugums, piemēram, viltoti Slimību kontroles un profilakses centra (CDC) vai veselības organizāciju e-pasta ziņojumi, e-pasti vai ziņojumi par vakcinācijas segumu, kur var iegūt vakcīnu, vakcinācijas statistiku, darbinieku vakcinācijas statusu utt.
- Izplatītie uzbrukumi ietver COVID veselības ieteikumu e-pasta krāpniecību

Funded by the Erasmus+ Programme of the European Union

Riska analīze

Covid pikšķerēšanas

ai piekļūtu e-
es (t.i., taustiņu
ūra utt.)

Pikšķer
dra

Pikšķerētājs

izmant

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

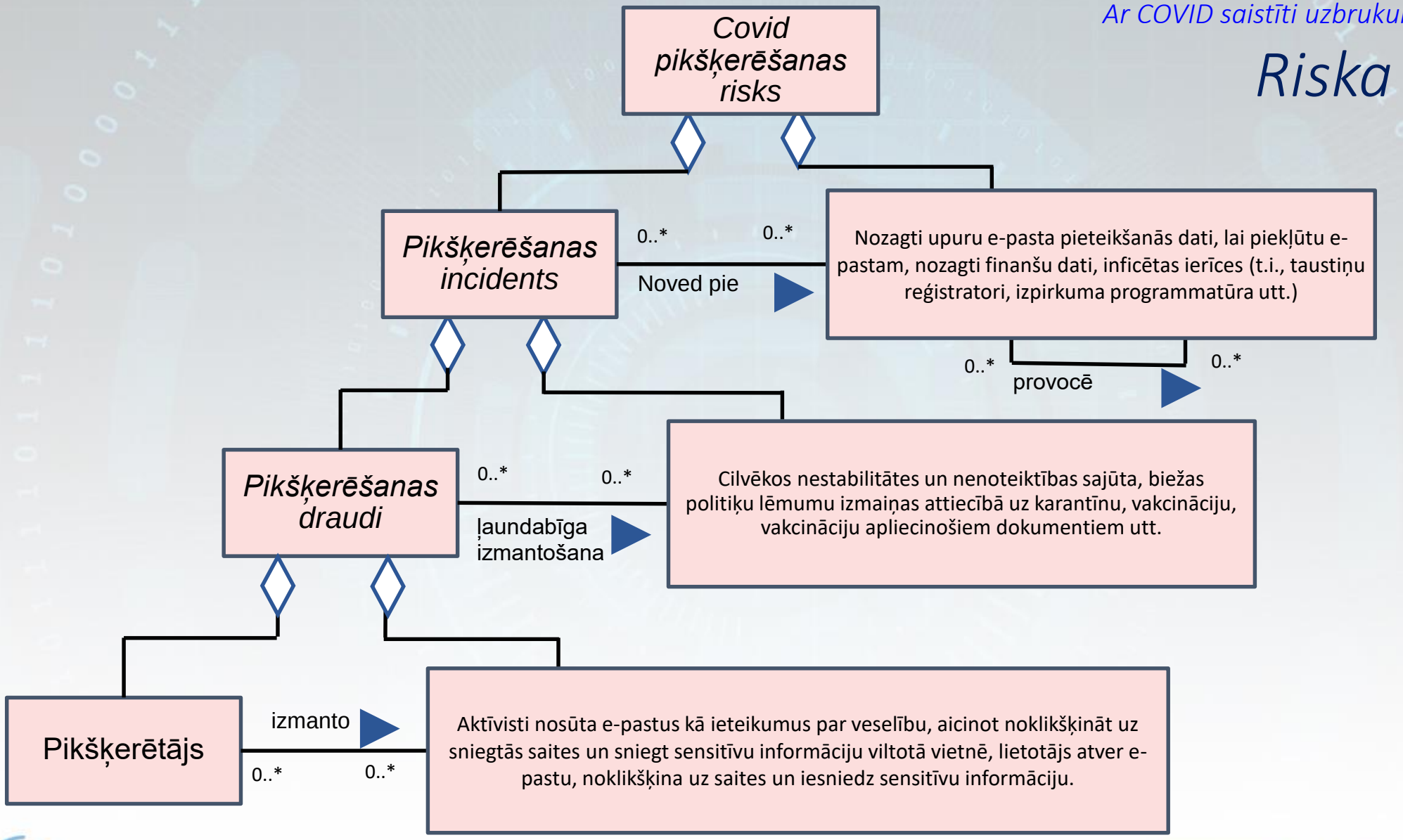
Safety Measures.pdf

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

Regards
Dr
Specialist wuhan-virus-advisory

Koronavīrusa pikšķerēšanas e-pasts (avots: Wired)

Riska analīze



Koronavīrusa pikšķerēšanas e-pasts (avots: Wired)

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *[Rediģēts]*
b. Kas ir ietvers ziņas saturā? *Koronavīrusa drošības pasākumi*
c. Vai ir hipersaites/pielikumi? *Jā*

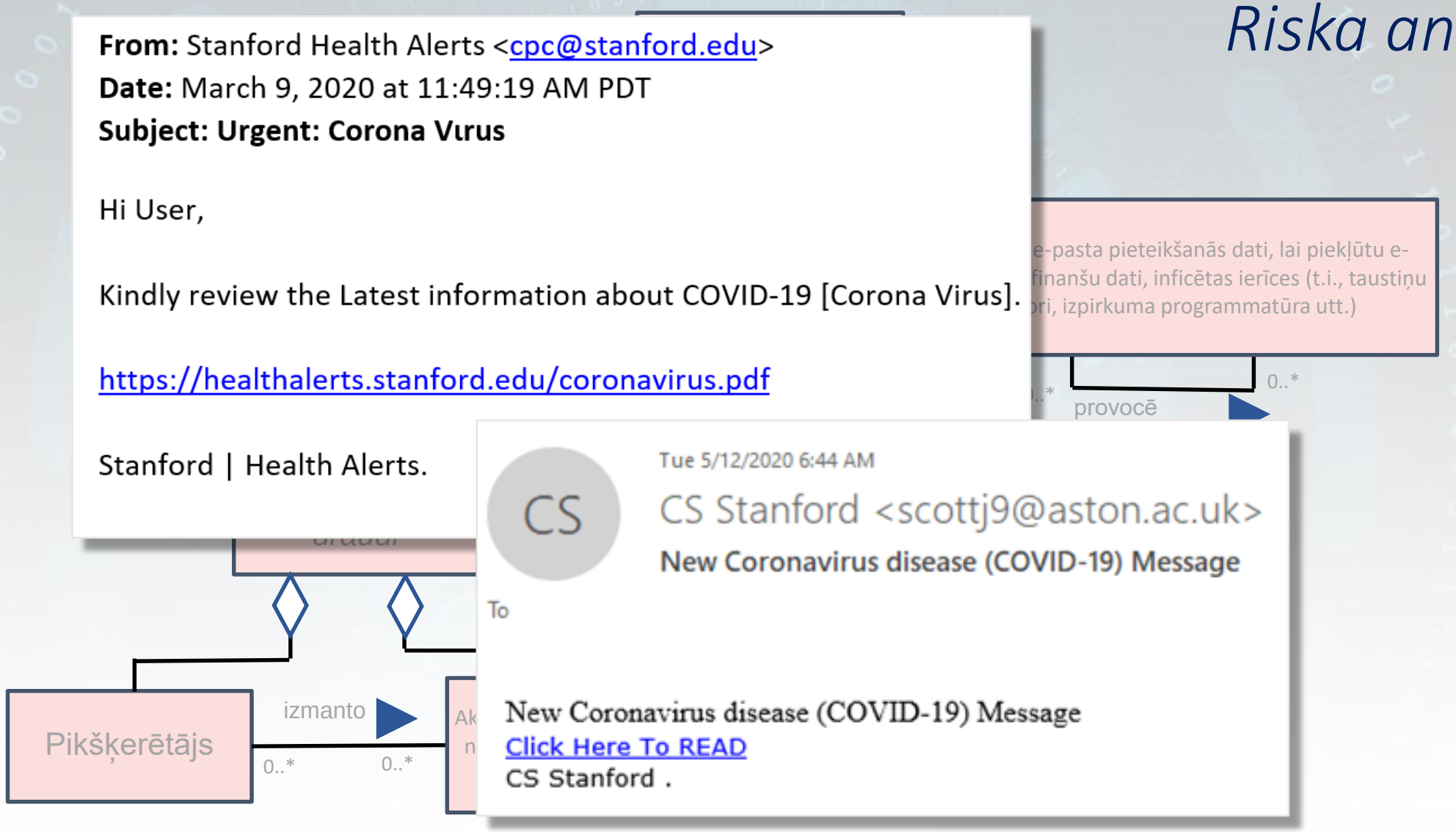
Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Uzticami COVID informācijas avoti nesūta nevēlamus e-pasta ziņojumus
3.2 Leģitīmi e-pasta ziņojumi parasti tiek uzrunāti jūsu vārdā (t.i., nevis "Kungs").
3.3 Leģitīmiem e-pasta ziņojumiem nav pareizrakstības un gramatikas problēmu, t.i., "Simptomi Biežākie simptomi"

4. Kritiskā domāšana
4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Esiet piesardzīgs attiecībā uz hipersaitēm/pielikumiem; tie var izveidot saiti uz ļaunprātīgu resursu
4.3 Esiet piesardzīgs, ja e-pastā tiek pieprasītas darbības ar steidzamības/baiļu sajūtu
4.4 Izmantojiet meklētājprogrammu, lai uzzinātu vairāk par e-pasta saturu, pirms uzticaties ziņojumam
4.5 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.6 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Riska analīze

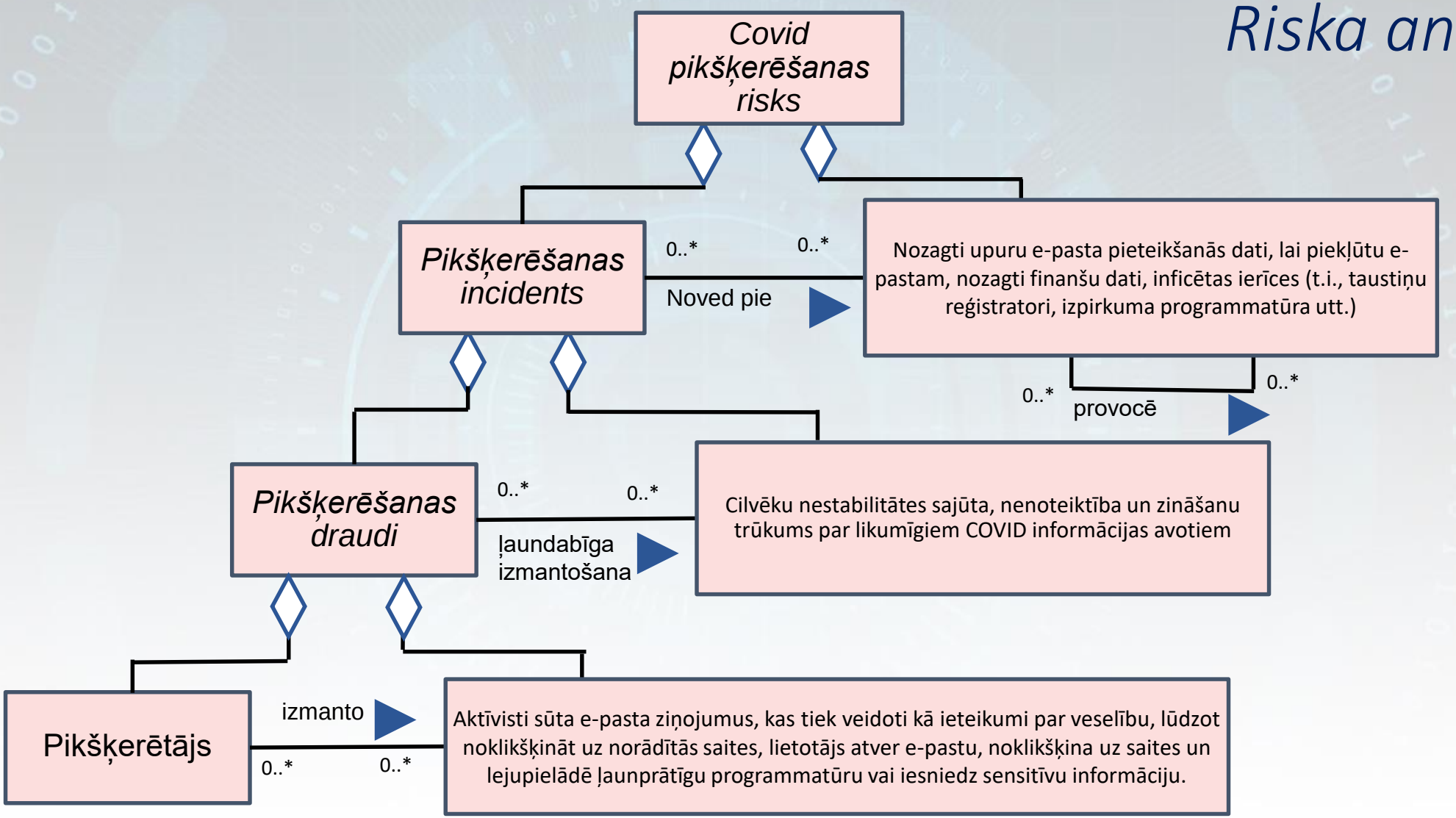


CyberPhish
Safeguarding your digital future

Koronavīrusa pikšķerēšanas e-pasts (avots: Stanford.edu, Stanford.edu)

Funded by the Erasmus+ Programme of the European Union

Riska analīze



Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa?
cpc@stanford.edu, scottj9@aston.ac.uk
b. Kas ir ietvers ziņas saturā? *Koronavīruss*
c. Vai ir hipersaites/pielikumi? *Jā*

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Uzticami COVID informācijas avoti nesūta nevēlamus e-pasta ziņojumus
3.2 Leģitīmas e-pasta vēstules parasti uzrunā jūs vārdā
3.3 Likumīgi e-pasta ziņojumi ir profesionāli, un tiem ir vienots veidnes formāts

4. Kritiskā domāšana
4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Esiet piesardzīgs attiecībā uz hipersaitēm/pielikumiem; tie var izveidot saiti uz ļaunprātīgu resursu
4.3 Izmantojiet meklētājprogrammu, lai uzzinātu vairāk par e-pasta saturu, pirms uzticaties ziņojumam
4.4 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

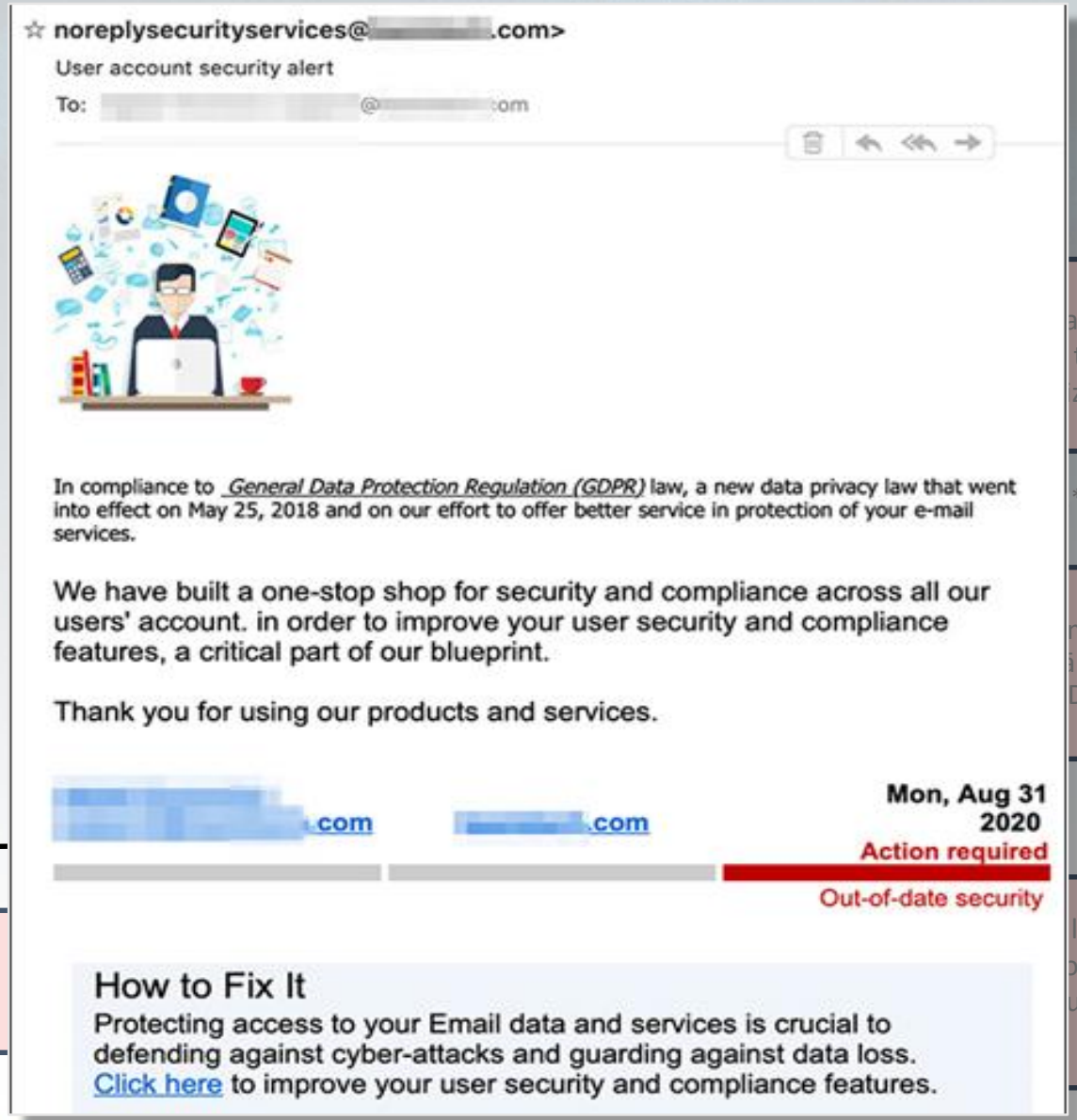
Funded by the Erasmus+ Programme of the European Union

Ar COVID saistīti uzbrukumi

- 2018. gadā notika daudzi ar GDPR saistīti pikšķerēšanas uzbrukumi, jo visiem uzņēmumiem un organizācijām bija obligāti jāievieš GDPR savās organizācijās.
- Uzbrucēju taktika var ietvert
  - *viltotu e-pasta ziņojumu sūtīšanu, izliekoties, ka uzņēmums palīdz GDPR darbībās, lai nozagtu informāciju.*
  - *viltus e-pasta vēstules, aizbildinoties vai uzdodoties par uzņēmumiem, kas klientiem sniedz informāciju par datu politikas izmaiņām*

Funded by the Erasmus+ Programme of the European Union

Riska analīze



asta pieteikšanās dati, lai piekļūtu e-pastam
tikt nozagti no upura e-pasta vai nozagtie
zmantoti turpmākiem kiberuzbrukumiem

* provocē 0..*

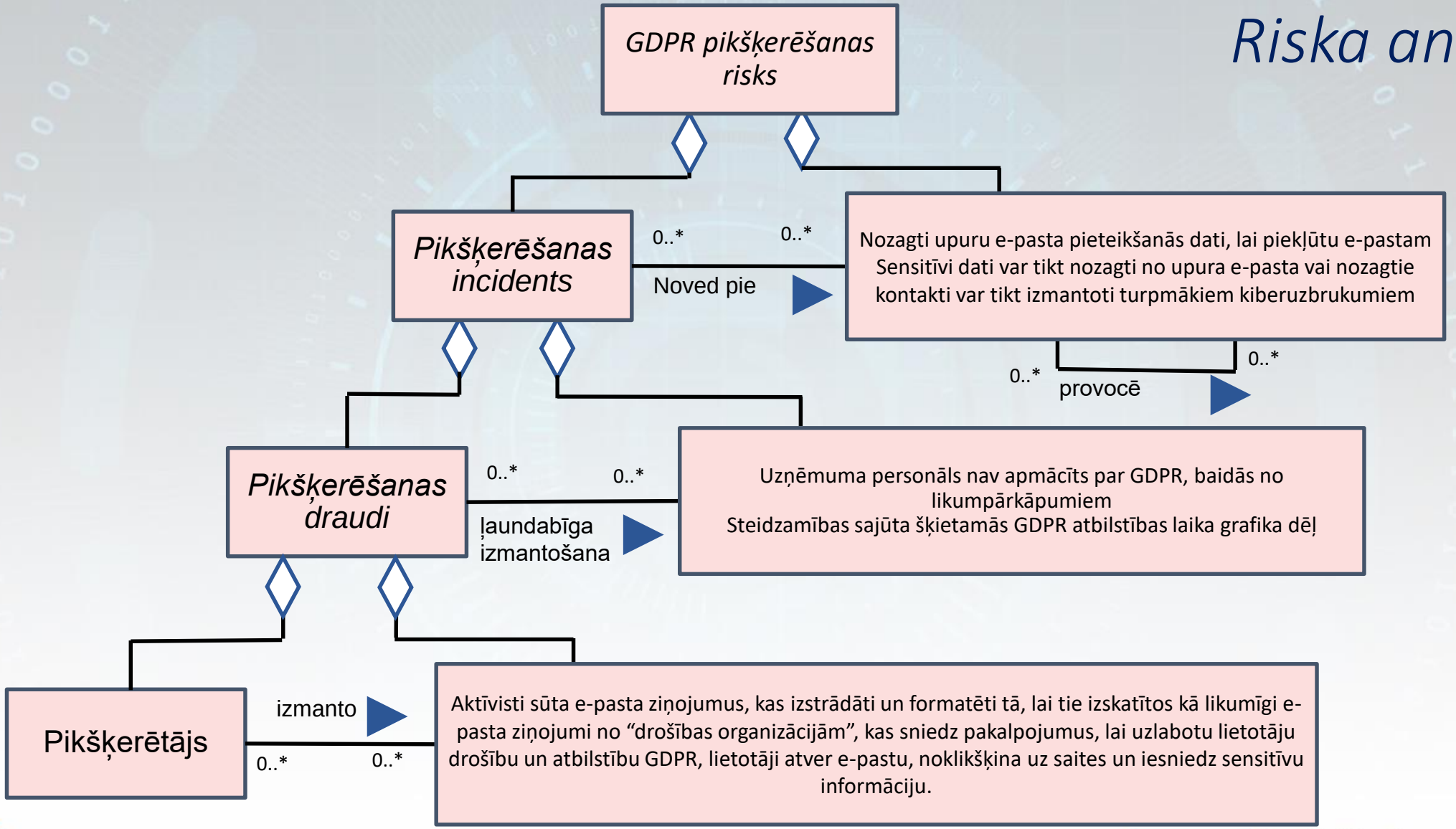
mācīts par GDPR, baidās no
ipumiem
DPR atbilstības laika grafika dēļ

Pikšķerētājs

lai tie izskatītos kā likumīgi e-
jumus, lai uzlabotu lietotāju
uz saites un iesniedz sensitīvu

GDPR pikšķerēšanas e-pasts (avots: Databreachtoday)

Riska analīze



GDPR pikšķerēšanas e-pasts (avots: Databreachtoday)

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *noreplysecurityservices*
b. Kas ir ietvers ziņas saturā? *Konta drošības brīdinājums*
c. Vai ir hipersaites/pielikumi? *Jā*

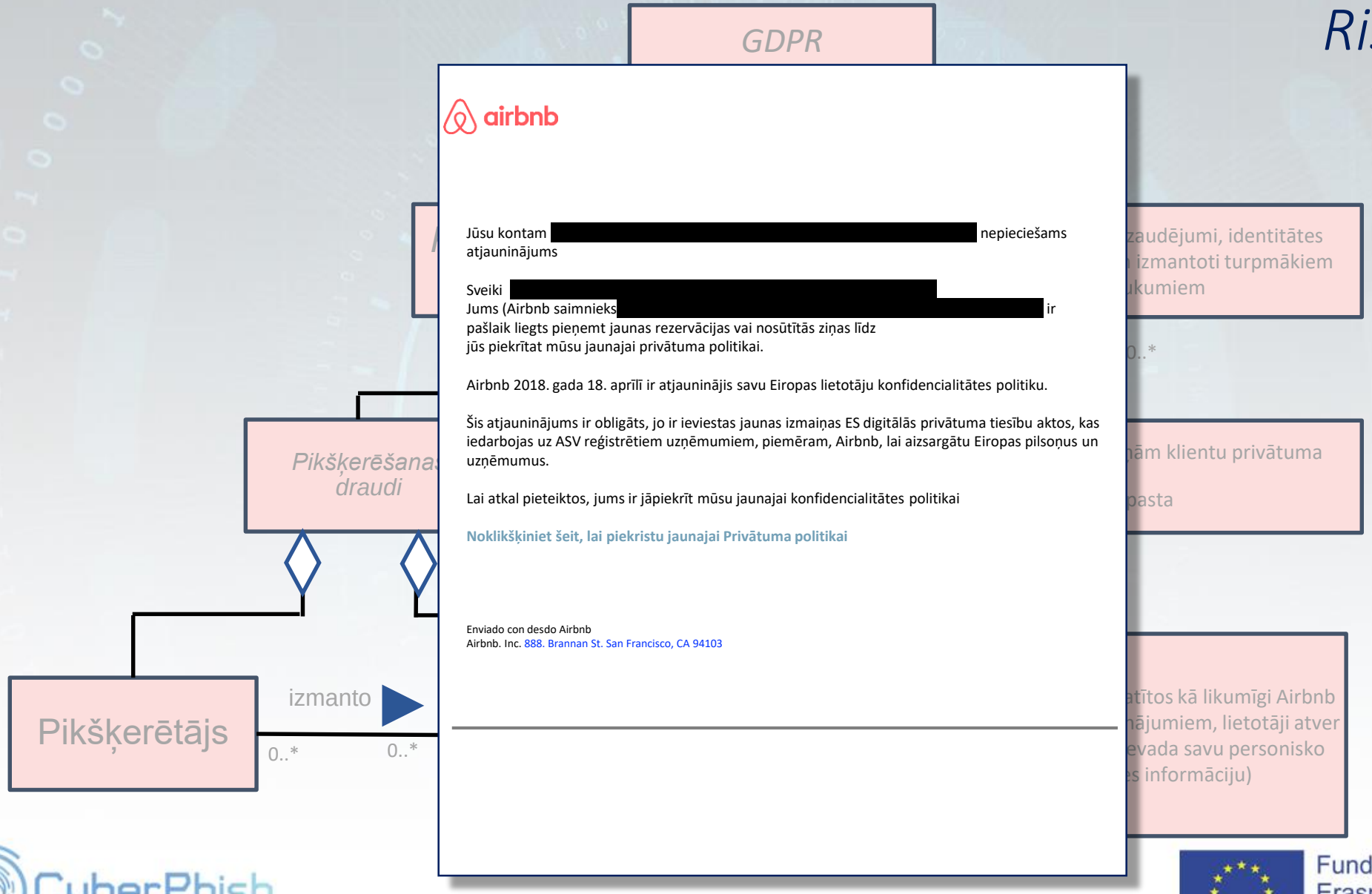
Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Leģitīmiem e-pasta ziņojumiem nav pretrunīga satura, piemēram, "GDPR" un "Novecojusi drošība".
3.2 Likumīgi e-pasta ziņojumi ir profesionāli, un tiem ir vienots formāts

4. Kritiskā domāšana
4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Esiet piesardzīgs attiecībā uz hipersaitēm/pielikumiem; tie var izveidot saiti uz ļaunprātīgu resursu
4.3 Esiet piesardzīgs, ja e-pastā tiek pieprasītas darbības ar steidzamības/baiļu sajūtu
4.4 Izmantojiet meklētājprogrammu, lai uzzinātu vairāk par organizāciju, kas sniedz iedomāto pakalpojumu
4.5 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.6 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

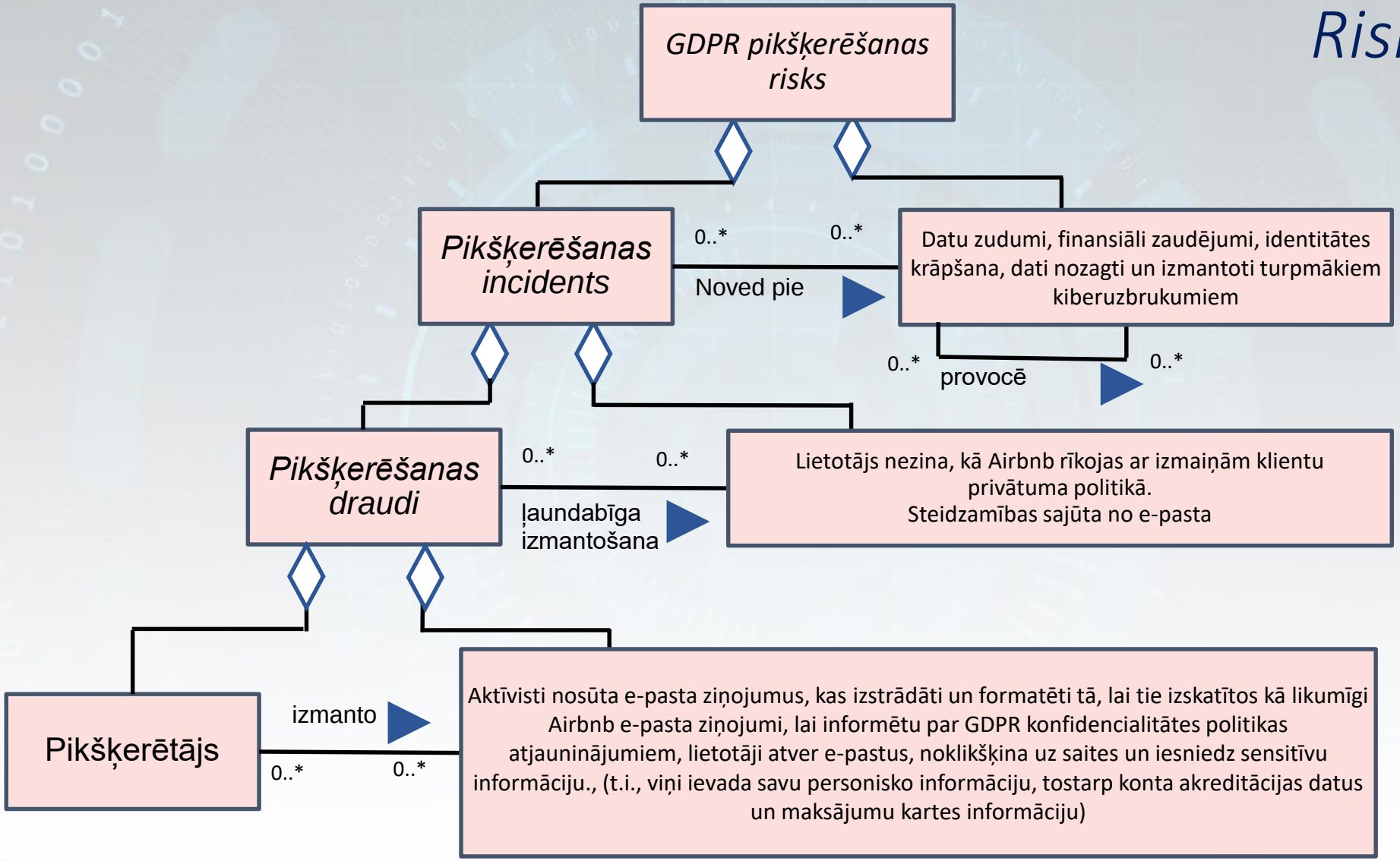
Funded by the Erasmus+ Programme of the European Union

Riska analīze



GDPR pikšķerēšanas e-pasts (avots: Securityaffairs)

Riska analīze

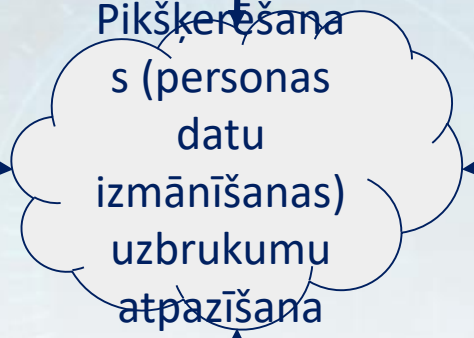


GDPR pikšķerēšanas e-pasts (avots: Securityaffairs)

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst ziņojuma saturam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. Kāds ir sūtītā ziņojuma saturs? *GDPR atjauninājums kontam*
b. Vai ir hipersaites/pielikumi? *Jā*



3. Aizdomīgo momentu atpazīšana
3.1 Likumīgi uzņēmumi apstrādā privātuma politikas līgumus tieši vietnē vai lietojumprogrammā
3.2 GDPR paziņojumos, ko uzņēmumi nosūta saviem klientiem, lietotāju akreditācijas dati netiek pieprasīti

4. Kritiskā domāšana
4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Esiet piesardzīgs attiecībā uz hipersaitēm/pielikumiem; tie var izveidot saiti uz ļaunprātīgu resursu
4.3 Pārbaudiet, vai sūtītāja e-pasta adresē nav neatbilstību, kas liecina par krāpšanu (skat. Airbnb sarakstu)
4.4 Plašāku informāciju par e-pasta saturu skatiet oficiālajā Airbnb vietnē
4.5 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.6 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

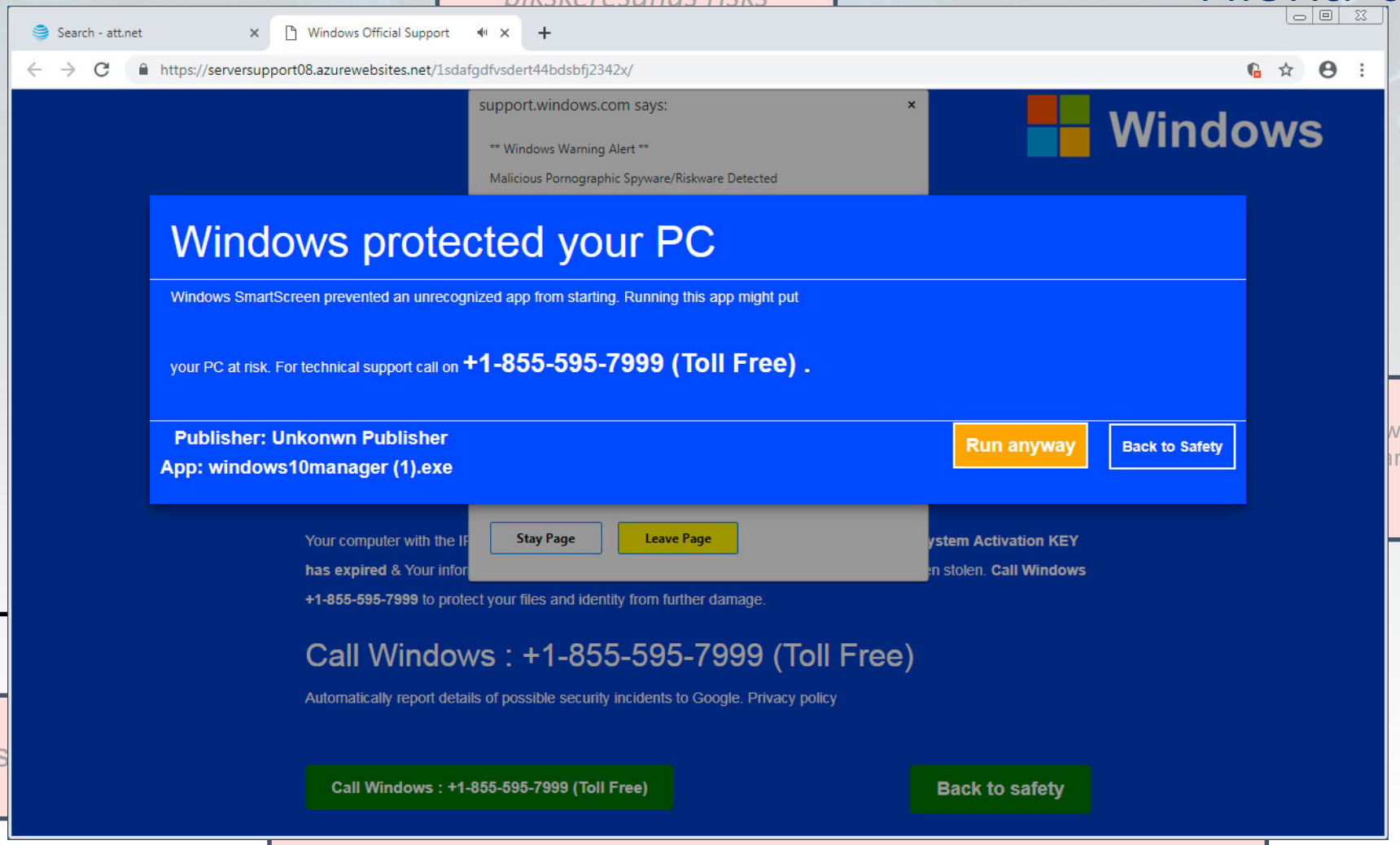
Tehniskā atbalsta uzbrukumi

- Tehniskā atbalsta krāpniecībā krāpnieks apgalvo, ka piedāvā likumīgu tehniskā atbalsta pakalpojumu, un var izmantot dažādas taktikas, lai pievērstu upuru uzmanību, tostarp nesagatavotus zvanus, vietņu uznirstošos logus, e-pasta ziņas un SMS.
- Populārākās izmantotās taktikas ietver sekojošo:
  - *vietnes uznirstošie logi brīdina lietotāju par datorvīrusu*
  - *tehnisko pakalpojumu e-pasta krāpniecība*

Funded by the Erasmus+ Programme of the European Union

Riska analīze

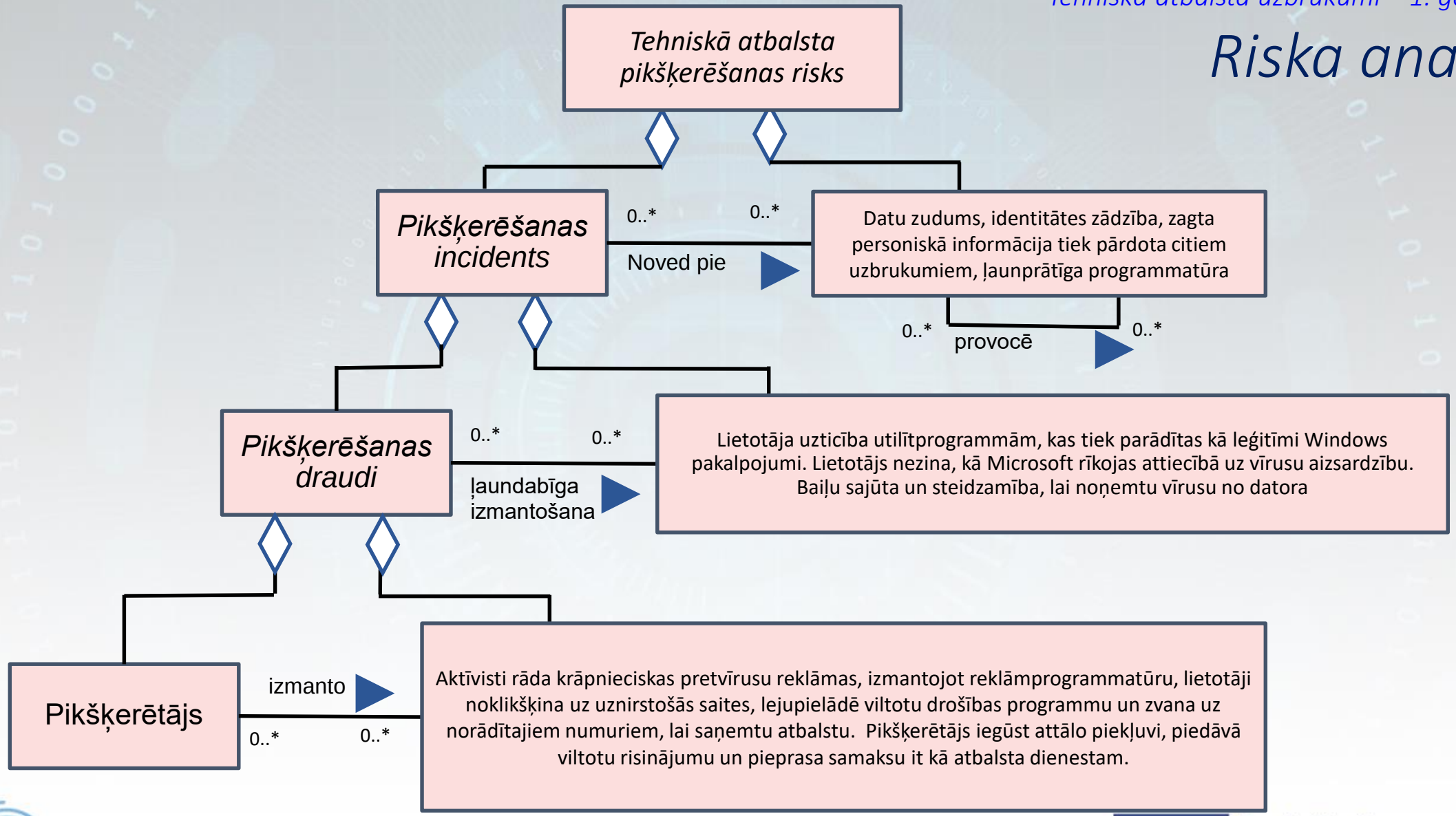
Tehniskā atbalsta pikšķerēšanas risks



Pikšķerētājs

ws
ardzību.

Riska analīze



Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz uznirstošajām pogām vai saitēm ar aicinājumu uz darbību

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: Tīmekļa vietne
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *Uznirstošs logs*
b. Kas ir ietvers ziņas saturā? *Pretvīrusu aizsardzība*
c. Vai ir sniegti aicinājumi uz darbību? *Jā*

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

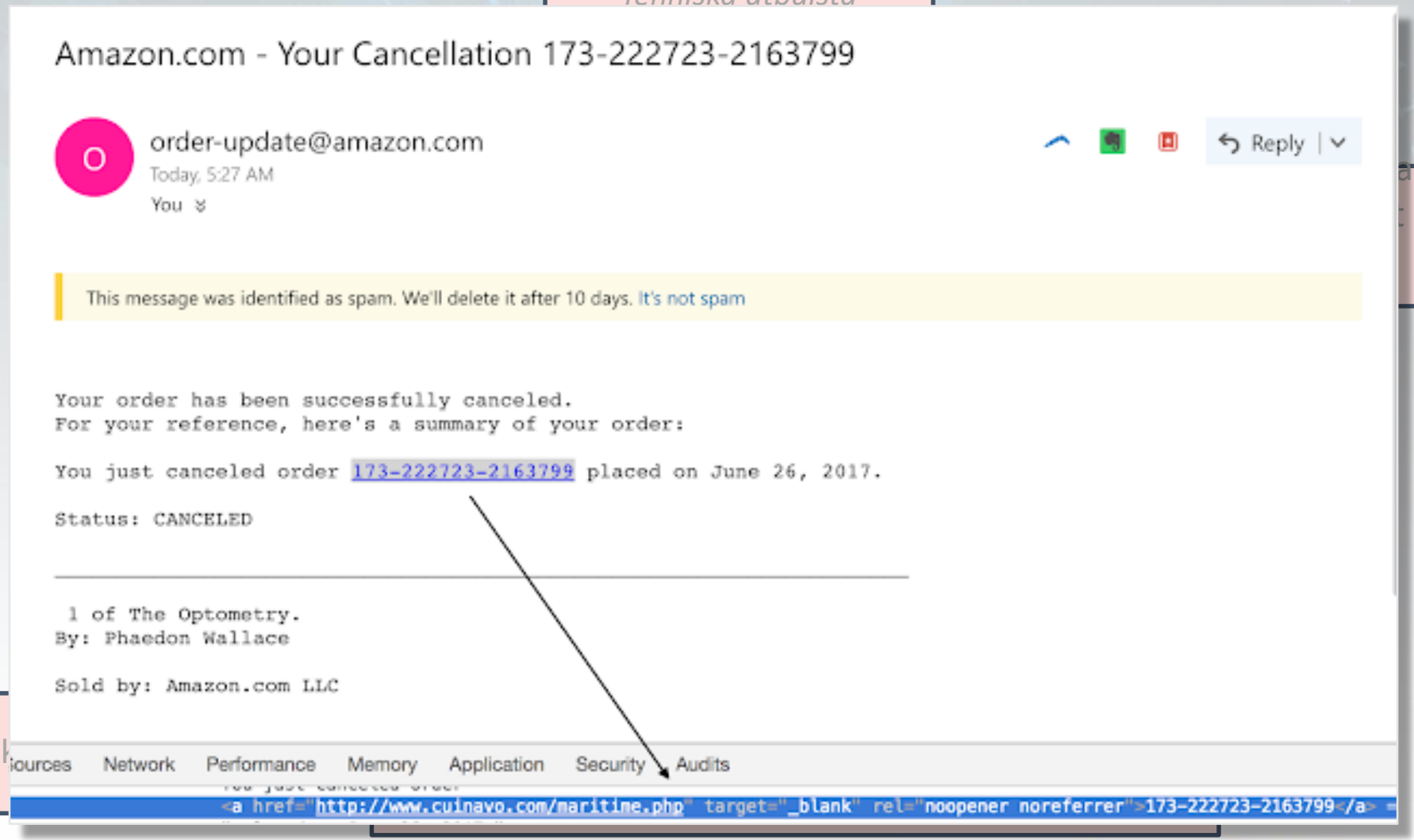
3. Aizdomīgo momentu atpazīšana
3.1 Patieso Windows aizsardzību risinās un nodrošinās vietējais Windows Defender, nevis tīmekļa vietnē
3.2 Microsoft nesūta nevēlamus uznirstošos logus uz vietnēm
3.3 Nav iespējams *piezvanīt* uz "Windows" tālruņa numuru

4. Kritiskā domāšana
4.1 Esiet piesardzīgs attiecībā uz visiem negaidītiem uznirstošajiem logiem vietnēs, neklikšķiniet uz negaidītiem uznirstošajiem logiem un, ja iespējams, bloķējiet uznirstošos logus.
4.2 Esiet piesardzīgs, ja uznirstošos logos pieprasītas darbības ar steidzamības/baiļu sajūtu
4.3 Nekad nenorādiet konta paroli vai pieteikšanās informāciju "pārbaudei" pa tālruni vai e-pastā
4.4 Aizveriet vietni, kurā tiek ģenerēts aizdomīgs uznirstošais logs

Funded by the Erasmus+ Programme of the European Union

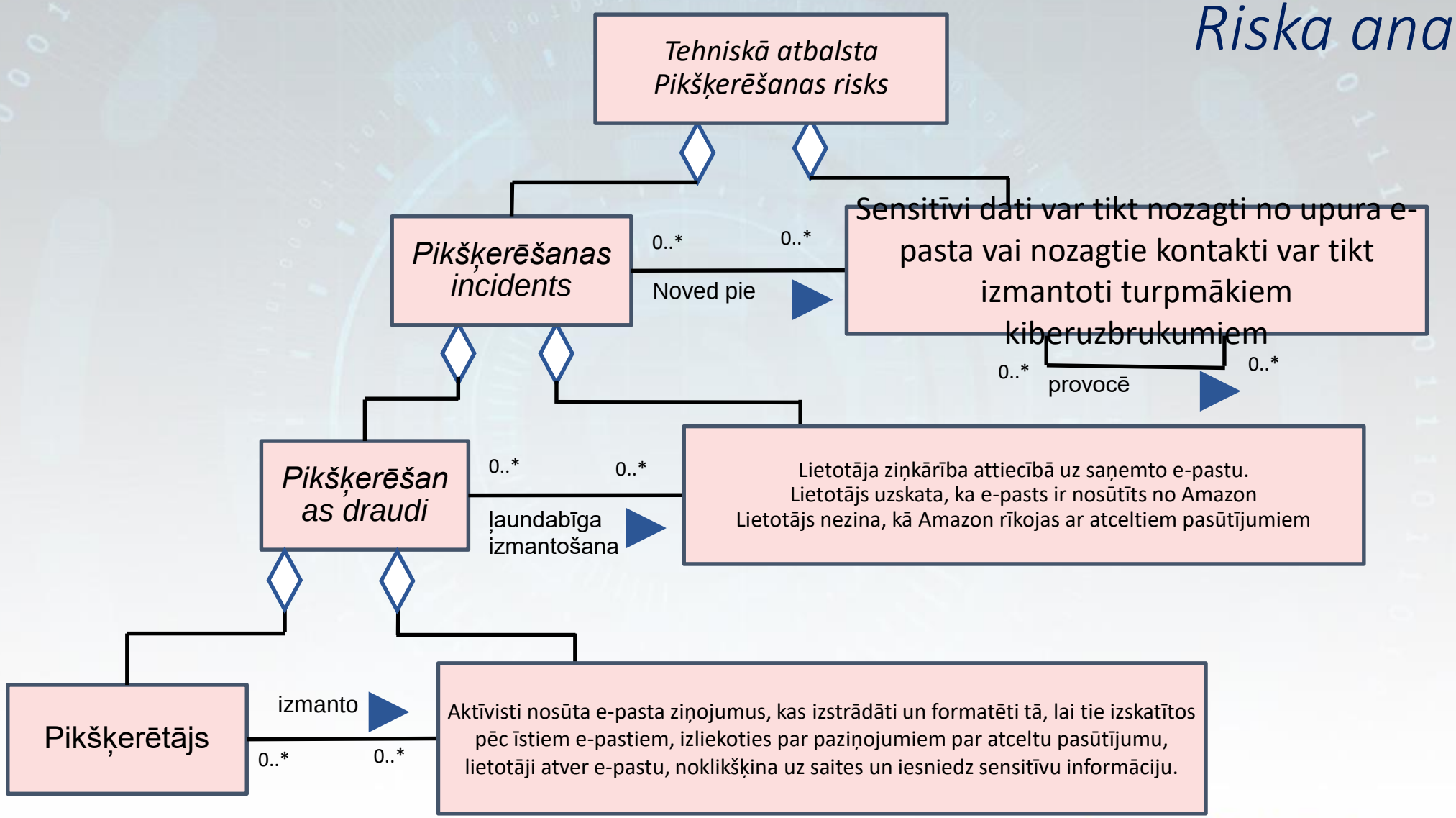
Riska analīze

Tehniskā atbalsta



Tehniskā atbalsta pikšķerēšanas e-pasta ziņojumi (Avots: vk-intel)

Riska analīze



Tehniskā atbalsta pikšķerēšanas e-pasta ziņojumi (Avots: vk-intel)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana

2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*order-update@amazon.com*"
b. Kas ir ietvers ziņas saturā? *Atcelts Amazon pasūtījums*
c. Vai ir hipersaites/pielikumi? *Jā*

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana

3.1 Leģitīmas e-pasta vēstules no uzņēmuma Amazon uzrunās jūs vārdā
3.2 Likumīgi e-pasta ziņojumi ir profesionāli, un tiem ir vienots formāts
3.3 Ņemiet vērā, ka URL ceļš novirza uz "**http://*www.cuinavo.com/maritime.php***" un nevis uz Amazon resursu vai vietni
3.4 Amazon nosūta pasūtījumu atcelšanas e-pastu no "*order-update@amazon.com*", kas ir leģitīms uzņēmuma Amazon e-pasts, bet e-pasta formāts nav profesionāls. Ziņojuma e-pasts, iespējams, ir viltots

4. Kritiskā domāšana

4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Pat ja e-pasts šķiet reāls, dodieties uz savu faktisko kontu uzņēmuma likumīgajā vietnē, piemēram, "*amazon.com*", lai pārbaudītu jebkādas bažas
4.3 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt saņēmēja ziņkāres un alkatības sajūtu
4.4 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.6 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana

2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*order-update@amazon.com*"
b. Kas ir ietvers ziņas saturā? *Atcelts Amazon pasūtījums*
c. Vai ir hipersaites/pielikumi? *Jā*

3. Aizdomīgo momentu atpazīšana

3.1 Leģitīmas e-pasta vēstules no uzņēmuma Amazon uzrunās jūs vārdā
3.2 Likumīgi e-pasta ziņojumi ir profesionāli, un tiem ir vienots formāts
3.3 Ņemiet vērā, ka URL ceļš novirza uz "**http://*www.cuinavo.com/maritime.php***" un nevis uz Amazon resursu vai vietni
3.4 Amazon nosūta pasūtījumu atcelšanas e-pastu no "*order-update@amazon.com*", kas ir leģitīms uzņēmuma Amazon e-pasts, bet e-pasta formāts nav profesionāls. Ziņojuma e-pasts, iespējams, ir viltots

uzbrukumu atpazīšana

4. Kritiskā domāšana

4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Pat ja e-pasts šķiet reāls, dodieties uz savu faktisko kontu uzņēmuma likumīgajā vietnē, piemēram, "*amazon.com*", lai pārbaudītu jebkādas bažas
4.3 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt saņēmēja ziņkāres un alkatības sajūtu
4.4 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.6 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana

2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*order-update@amazon.com*"
b. Kas ir ietvers ziņas saturā? *Atcelts Amazon pasūtījums*
c. Vai ir hipersaites/pielikumi? *Jā*

Pikšķerēšana
s (personas
datu
izmānīšanas)
uzbrukumu

3. Aizdomīgo momentu atpazīšana

3.1 Leģitīmas e-pasta vēstules no uzņēmuma Amazon uzrunās jūs vārdā
3.2 Likumīgi e-pasta ziņojumi ir profesionāli, un tiem ir vienots formāts
3.3 Ņemiet vērā, ka URL ceļš novirza uz "**http://*www.cuinavo.com/maritime.php***" un nevis uz Amazon resursu vai vietni
3.4 Amazon nosūta pasūtījumu atcelšanas e-pastu no "*order-update@amazon.com*", kas ir leģitīms uzņēmuma Amazon e-pasts, bet e-pasta formāts nav profesionāls. Ziņojuma e-pasts,

4. Kritiskā domāšana

4.1 Pārbaudiet, vai e-pasts ir no uzticama un sagaidāma avota
4.2 Pat ja e-pasts šķiet reāls, dodieties uz savu faktisko kontu uzņēmuma likumīgajā vietnē, piemēram, "*amazon.com*", lai pārbaudītu jebkādas bažas
4.3 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt saņēmēja ziņkāres un alkatības sajūtu
4.4 Meklējiet potenciāli pikšķerētus URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.6 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the
Erasmus+ Programme
of the European Union

Kriptovalūtu izkrāpšana

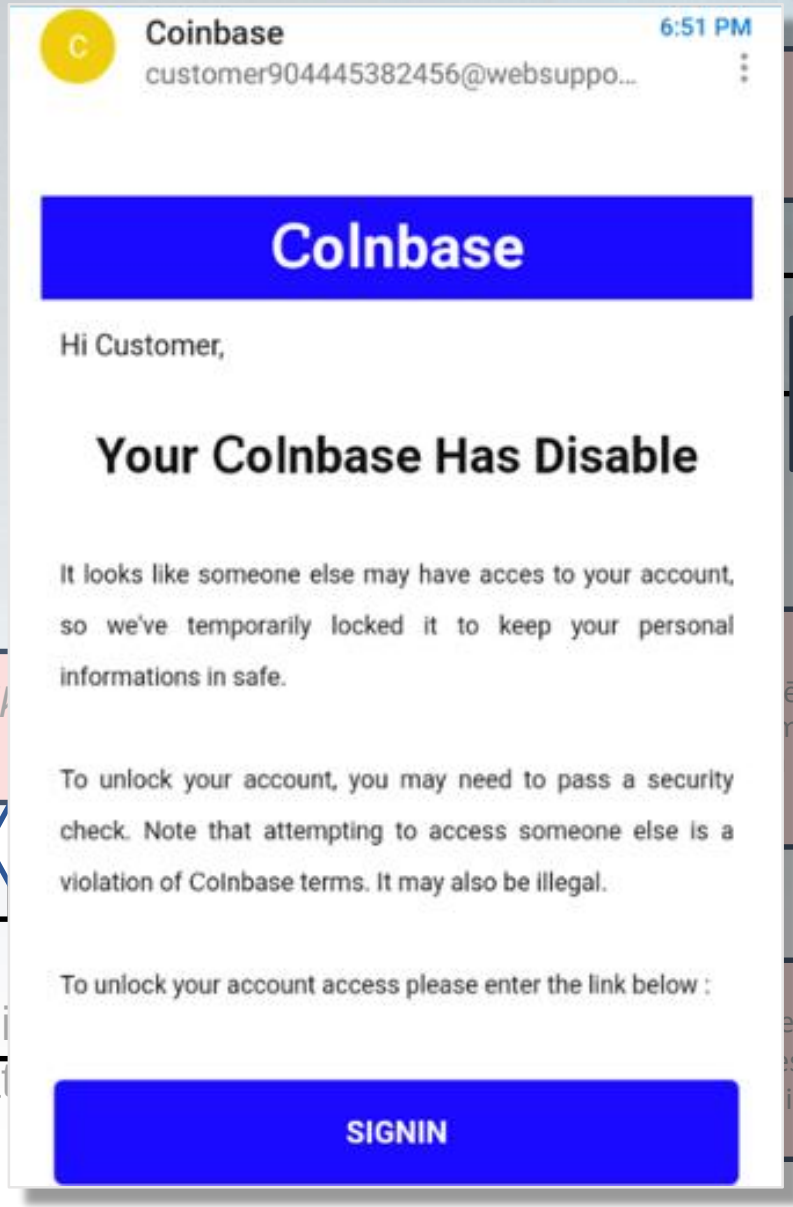
- Kad Bitcoin un citas kriptovalūtas piedzīvoja cenas un popularitātes pieaugumu, hakeri un kibernoziedznieki kļuva vairāk ieinteresēti to nozagšanā.
- Uzbrucēji var izmantot pikšķerēšanu, lai uzdotos par pārstāvjiem no populārām kriptovalūtu biržām, piemēram, Binance, Huobi Global vai Coinbase.

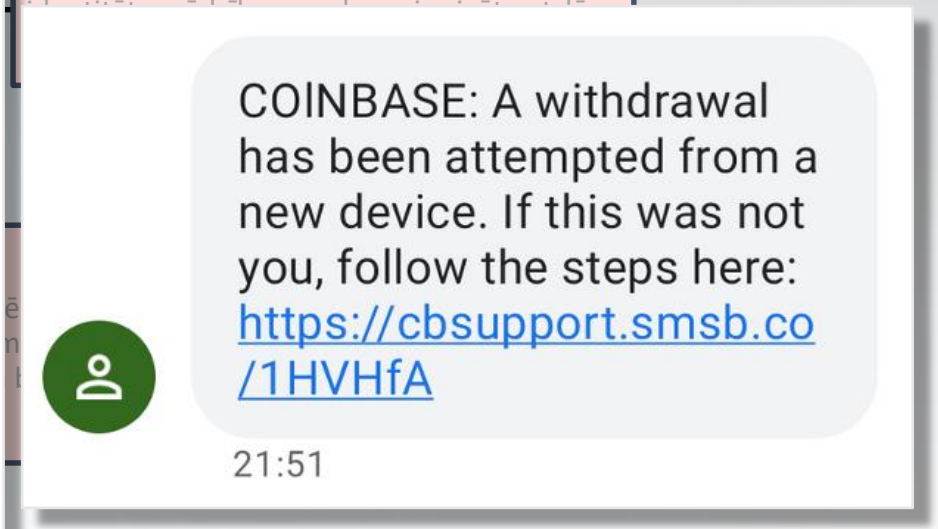
Funded by the
Erasmus+ Programme
of the European Union

Riska analīze

Pikšķerētājs

Datu zudums, reputācijas zaudējums,





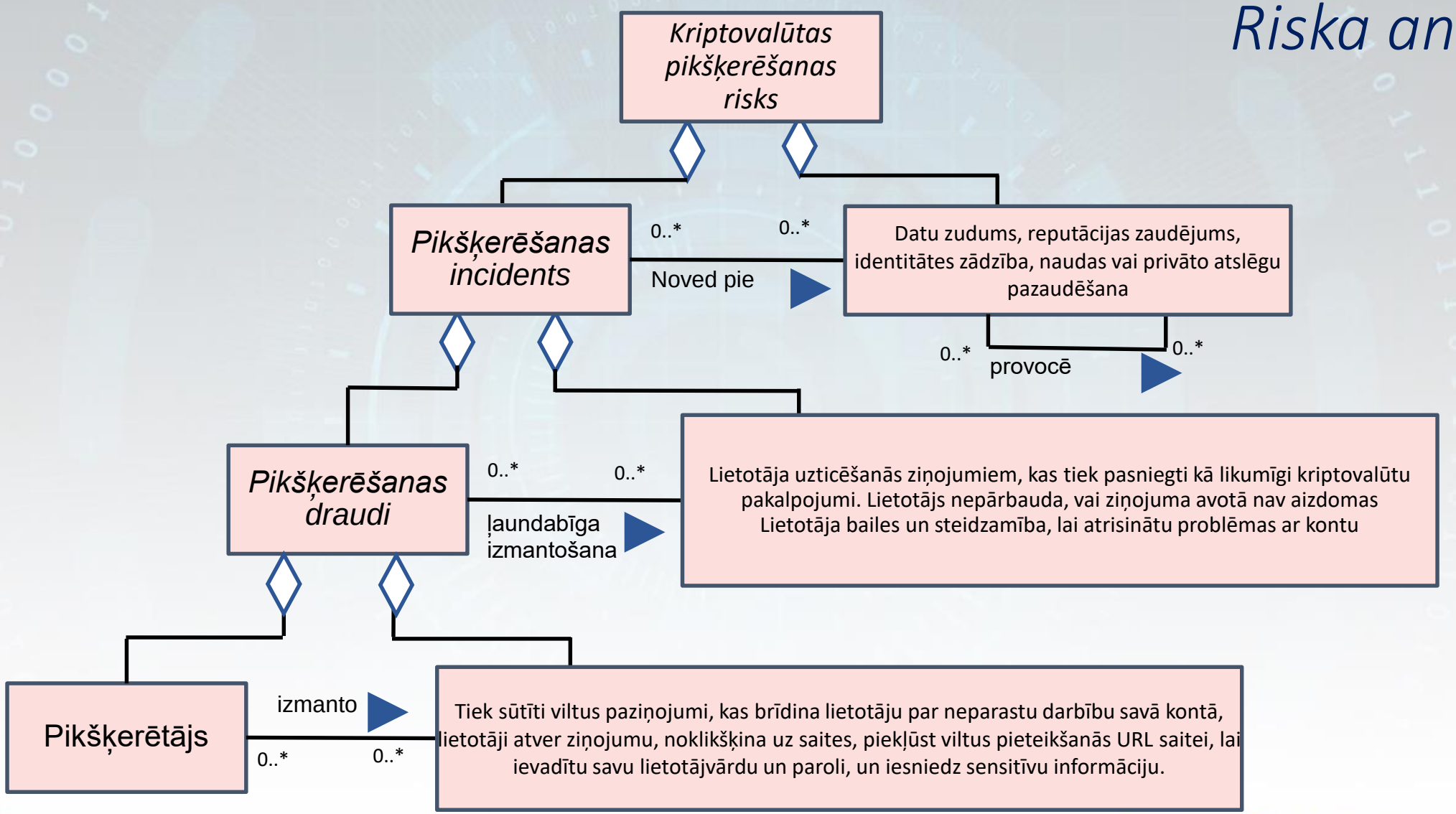
etotāju par neparastu darbību savā kontā, s, piekļūst viltus pieteikšanās URL saitei, lai i, un iesniedz sensitīvu informāciju.

Kriptovalūtas pikšķerēšanas e-pasts. Avots: Reddit
Kriptovalūtas pikšķerēšanas ziņojums. Avots: Reddit

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riska analīze



Kriptovalūtas pikšķerēšanas e-pasts. Avots: Reddit
Kriptovalūtas pikšķerēšanas ziņojums. Avots: Reddit

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana

2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots:
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*...@websupport.com*", *SMS tālruņa numurs*
b. Kas ir ietvers ziņas saturā? *Paziņojums par konta atspējošanu, paziņojums par līdzekļu izņemšanu*
c. Vai ir hipersaites/pielikumi? Jā

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana

3.1 Ziņojumi no likumīgām lietotnēm uzrunās jūs vārdā
3.2 Leģitīmi ziņojumi ir profesionāli un labi formatēti
3.3 Godprātīgos ziņojumos nav drukas kļūdu, t.i., lietojums "*CoInbase*" tā vietā, lai rakstītu "*Coinbase*", "*vai jūsu CoInbase ir bija atspējots*", vai "*REĢISTĒTIES*"
3.4 Leģitīmais e-pasta domēns, kas saistīts ar Coinbase, ir "*...@coinbase.com*" un nevis "*...@websupport.com*"

4. Kritiskā domāšana

4.1 Vēlreiz pārbaudiet sūtītāja adresi, leģitīmiem e-pastiem no Coinbase jābūt e-pasta adresēm, kas beidzas ar *.coinbase.com*
4.2 Sazinieties tieši ar Coinbase klientu atbalsta dienestu, ja rodas problēmas ar kontu vai maksājumu
4.3 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt saņēmēja bailes un steidzamības sajūtu
4.4 Pārbaudīt drošības informāciju likumīgā pakalpojuma vietnē
4.5 Nekad neklikšķiniet uz saitēm/pielikumiem no nezināmiem avotiem, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus.
4.6 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.7 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana

2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots: E-pasti, SMS
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*...@websupport.com*", *SMS tālruņa numurs*
b. Kas ir ietvers ziņas saturā? *Paziņojums par konta atspējošanu, paziņojums par līdzekļu izņemšanu*
c. Vai ir hipersaites/pielikumi? Jā

3. Aizdomīgo momentu atpazīšana

3.1 Ziņojumi no likumīgām lietotnēm uzrunās jūs vārdā
3.2 Leģitīmi ziņojumi ir profesionāli un labi formatēti
3.3 Godprātīgos ziņojumos nav drukas kļūdu, t.i., lietojums "*CoInbase*" tā vietā, lai rakstītu "*Coinbase*", "*vai jūsu CoInbase ir bija atspējots*", vai "*REĢISTĒTIES*"
3.4 Leģitīmais e-pasta domēns, kas saistīts ar Coinbase, ir "*...@coinbase.com*" un nevis "*...@websupport.com*"

4. Kritiskā domāšana

4.1 Vēlreiz pārbaudiet sūtītāja adresi, leģitīmiem e-pastiem no Coinbase jābūt e-pasta adresēm, kas beidzas ar *.coinbase.com*
4.2 Sazinieties tieši ar Coinbase klientu atbalsta dienestu, ja rodas problēmas ar kontu vai maksājumu
4.3 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt saņēmēja bailes un steidzamības sajūtu
4.4 Pārbaudīt drošības informāciju likumīgā pakalpojuma vietnē
4.5 Nekad neklikšķiniet uz saitēm/pielikumiem no nezināmiem avotiem, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus.
4.6 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.7 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots: E-pasti, SMS
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*...@websupport.com*", *SMS tālruņa numurs*
b. Kas ir ietvers ziņas saturā? *Paziņojums par konta atspējošanu, paziņojums par līdzekļu izņemšanu*
c. Vai ir hipersaites/pielikumi? Jā

Pikšķerēšana
s (personas datu izmānīšanas) uzbrukumu

3. Aizdomīgo momentu atpazīšana

3.1 Ziņojumi no likumīgām lietotnēm uzrunās jūs vārdā
3.2 Leģitīmi ziņojumi ir profesionāli un labi formatēti
3.3 Godprātīgos ziņojumos nav drukas kļūdu, t.i., lietojums "*CoInbase*" tā vietā, lai rakstītu "*Coinbase*", "*vai jūsu CoInbase ir bija atspējots*", vai "*REĢISTĒTIES*"
3.4 Leģitīmais e-pasta domēns, kas saistīts ar Coinbase, ir "*...@coinbase.com*" un

4. Kritiskā domāšana
4.1 Vēlreiz pārbaudiet sūtītāja adresi, leģitīmiem e-pastiem no Coinbase jābūt e-pasta adresēm, kas beidzas ar *.coinbase.com*
4.2 Sazinieties tieši ar Coinbase klientu atbalsta dienestu, ja rodas problēmas ar kontu vai maksājumu
4.3 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt saņēmēja bailes un steidzamības sajūtu
4.4 Pārbaudīt drošības informāciju likumīgā pakalpojuma vietnē
4.5 Nekad neklikšķiniet uz saitēm/pielikumiem no nezināmiem avotiem, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus.
4.6 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.7 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Izspiešanas krāpniecība

- Diemžēl izspiešanas krāpniecības paņēmieni atgriežas, kad krāpnieki un hakeri var piekļūt datiem no veikt uzbrukumus vai izteikt draudus "Es zinu jūsu paroli" saviem upuriem.
- Uzbrucēji var arī apgalvot, ka ir piekļuvuši jūsu datoram un tā kamerai, ieguvuši seksuāla rakstura videoklipus vai attēlus ar jums un var pat likt jums maksāt ar Bitcoin.

Funded by the
Erasmus+ Programme
of the European Union

Riska analīze

Izspiešanas pikšķerēšanas

roles dēļ.
cija var tikt

Pikšķerētājs

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.

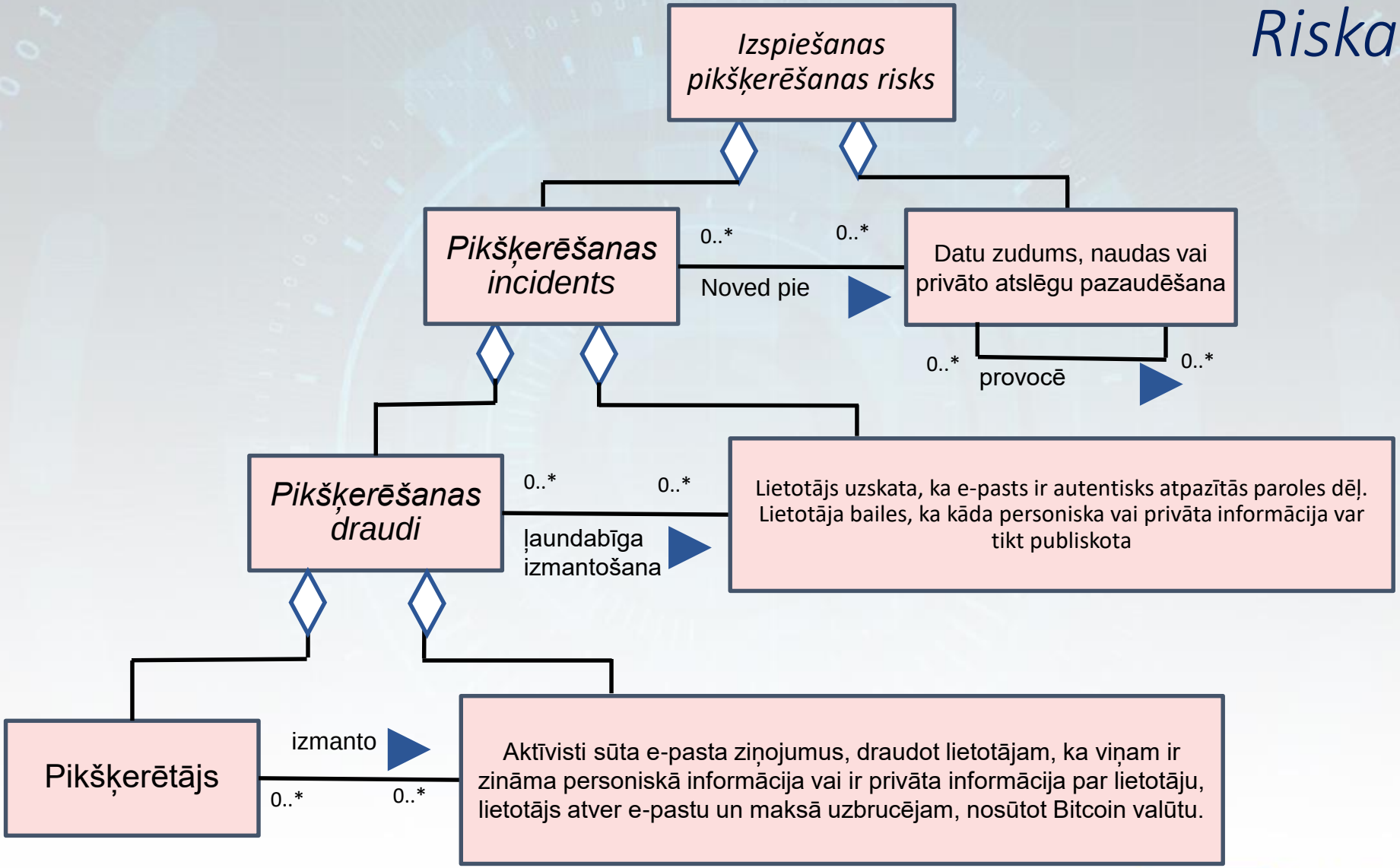
exactly what should you do?

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)

Izspiešanas pikšķerēšanas e-pasts (avots: MailOnline)

Riska analīze



Izspiešanas pikšķerēšanas e-pasts (avots: MailOnline)

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst saturam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: E-pasts
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? "*...@outlook.com*"
b. Kas ir ietvers ziņas saturā? *Seksuāla rakstura izspiešana*
c. Vai ir hipersaites/pielikumi? *Jā*

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Vairumā gadījumu e-pastu ziņojumi ir tukši draudi, nevis tāpēc, ka lietotāja dati tika uzlauzti
3.2 Iespējams, ka uzbrucējs ir ieguvis sensitīvu informāciju no datu pārkāpuma, noplūdes vai publiski pieejamus datus internetā

4. Kritiskā domāšana
4.1 Esiet piesardzīgs, jo šie e-pasta krāpniecības veidi var ekspluatēt jūsu bailes un kaunu
4.2 Pārbaudiet, vai jūsu e-pasts nav uzlauzts vietnēs, t.i., *haveibeenpwned.com* vai *dehashed.com*
4.3 Ja parole joprojām tiek izmantota, ir svarīgi aizsargāt šos kontus
4.4 Izdzēsiet nosūtīto e-pasta ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Avansa maksas izkrāpšana

- Covid pandēmijas laikā joprojām ir spēcīgi izteiktas avansa maksas izkrāpšanas, jo cilvēki ir nonākuši grūtos laikos. Šie pikšķerēšanas uzbrukumi notiek, kad noziedznieks ārvalstīs piedāvā daļu no lielas naudas summas, lai palīdzētu viņam pārskaitīt naudu no savas valsts
- Lai to izdarītu, viņi pieprasīs jūsu bankas informāciju vai lūgs jums samaksāt nodevas, nodevas vai nodokļus

Funded by the Erasmus+ Programme of the European Union

Riska analīze

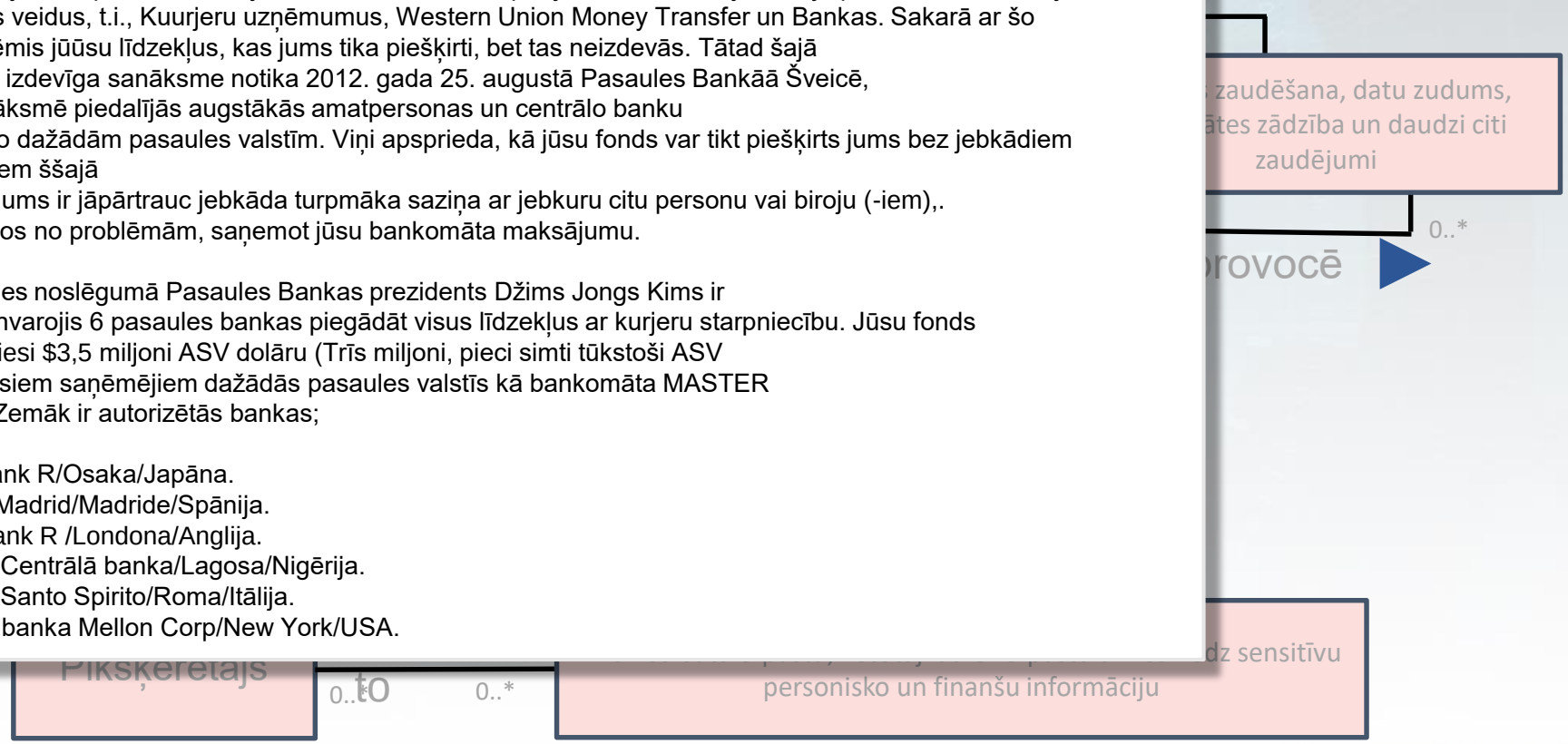
[SUROGĀTPASTS] ATN Starptautiskie kredītu norēķini
Nigērijas Centrālā banka [printer@brandmelloon.co.uk]
Nosūtīšanas datums: Sest., 10.13.2012. plkst. 5:20 AM
Saņēmējs: dave@d

Nigērijas Centrāla banka
ATM Starptautiskie kredītu norēķini
Starptautisko maksājumu direktorāts.

Šis paziņojums ir paredzēts, lai jūūūs oficiāli informētu par jūsu fondu, kas jums bija paredzēts, izmantojot dažādus veidus, t.i., Kuurjeru uzņēmumus, Western Union Money Transfer un Bankas. Sakarā ar šo esat saņēmis jūūsu līdzekļus, kas jums tika piešķirti, bet tas neizdevās. Tātad šajā gadījumā izdevīga sanāksme notika 2012. gada 25. augustā Pasaules Bankāā Šveicē, kurā sanāksmē piedalījās augstākās amatpersonas un centrālo banku vadītāji no dažādām pasaules valstīm. Viņi apsprieda, kā jūsu fonds var tikt piešķirts jums bez jebkādiem zaudējumiem šajā laikā, un jums ir jāpārtrauc jebkāda turpmāka saziņa ar jebkuru citu personu vai biroju (-iem),. lai izvairītos no problēmām, saņemot jūsu bankomāta maksājumu.

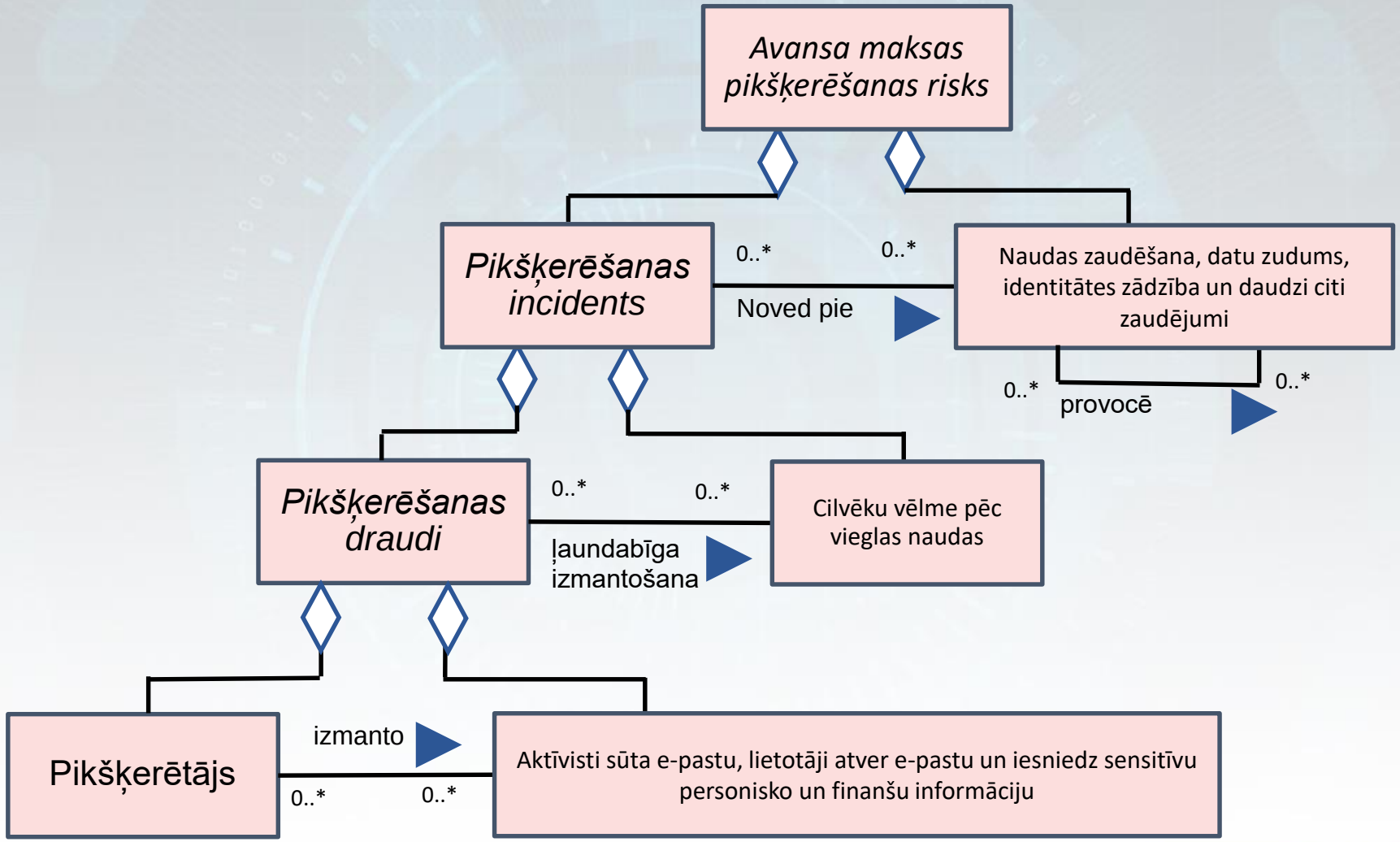
Sanāksmes noslēgumā Pasaules Bankas prezidents Džims Jongs Kims ir stingri pilnvarojis 6 pasaules bankas piegādāt visus līdzekļus ar kurjeru starpniecību. Jūsu fonds kas ir patiesi $3,5 miljoni ASV dolāru (Trīs miljoni, pieci simti tūkstoši ASV dolāru) visiem saņēmējiem dažādās pasaules valstīs kā bankomāta MASTER KARTE. Zemāk ir autorizētās bankas;

Daiwa Bank R/Osaka/Japāna.
Caja De Madrid/Madride/Spānija.
Lloyds Bank R /Londona/Anglija.
Nigērijas Centrālā banka/Lagosa/Nigērija.
Banco di Santo Spirito/Roma/Itālija.
Ņujorkas banka Mellon Corp/New York/USA.



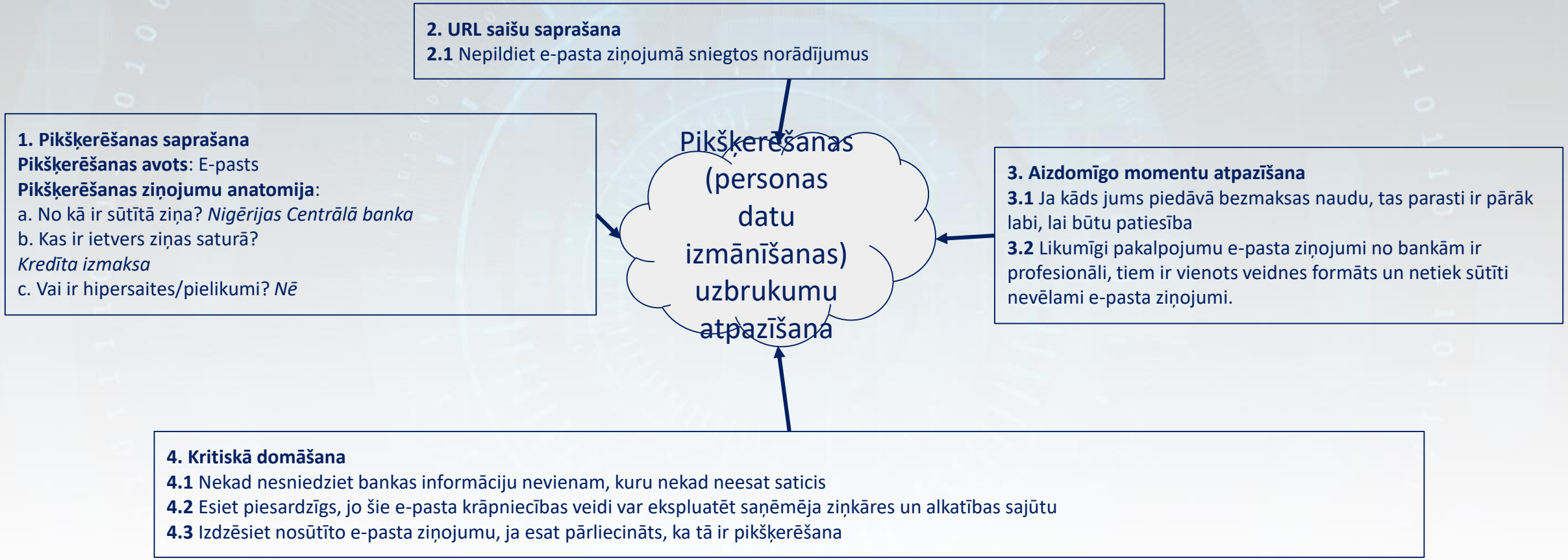
Izspiešanas pikšķerēšanas e-pasts (avots: Massmoola)

Riska analīze



Izspiešanas pikšķerēšanas e-pasts (avots: Massmoola)

Riska atpazīšana

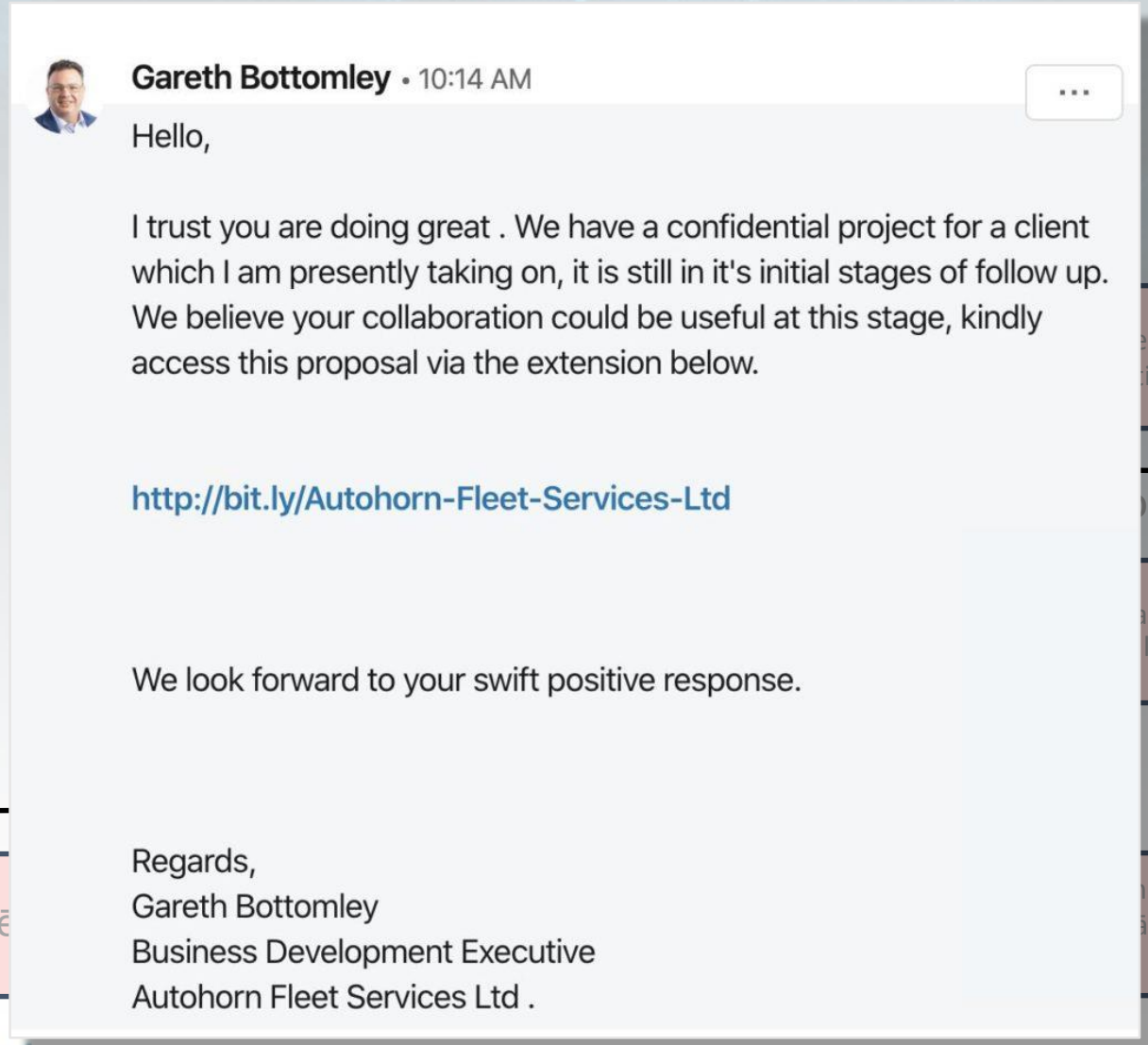


Sociālo mediju krāpniecība

- Šeit uzbrucēji izmanto sociālo mediju vietnes, piemēram, Facebook, LinkedIn vai Twitter, lai maldinātu lietotājus noklikšķināt uz ļaunprātīgām saitēm vai atklāt personas informāciju.
- Uzbrucēji var arī atrast daudz informācijas par potenciālajiem upuriem sociālajos medijos, lai uzsāktu mērķtiecīgu uzbrukumu

Funded by the Erasmus+ Programme of the European Union

Riska analīze



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.

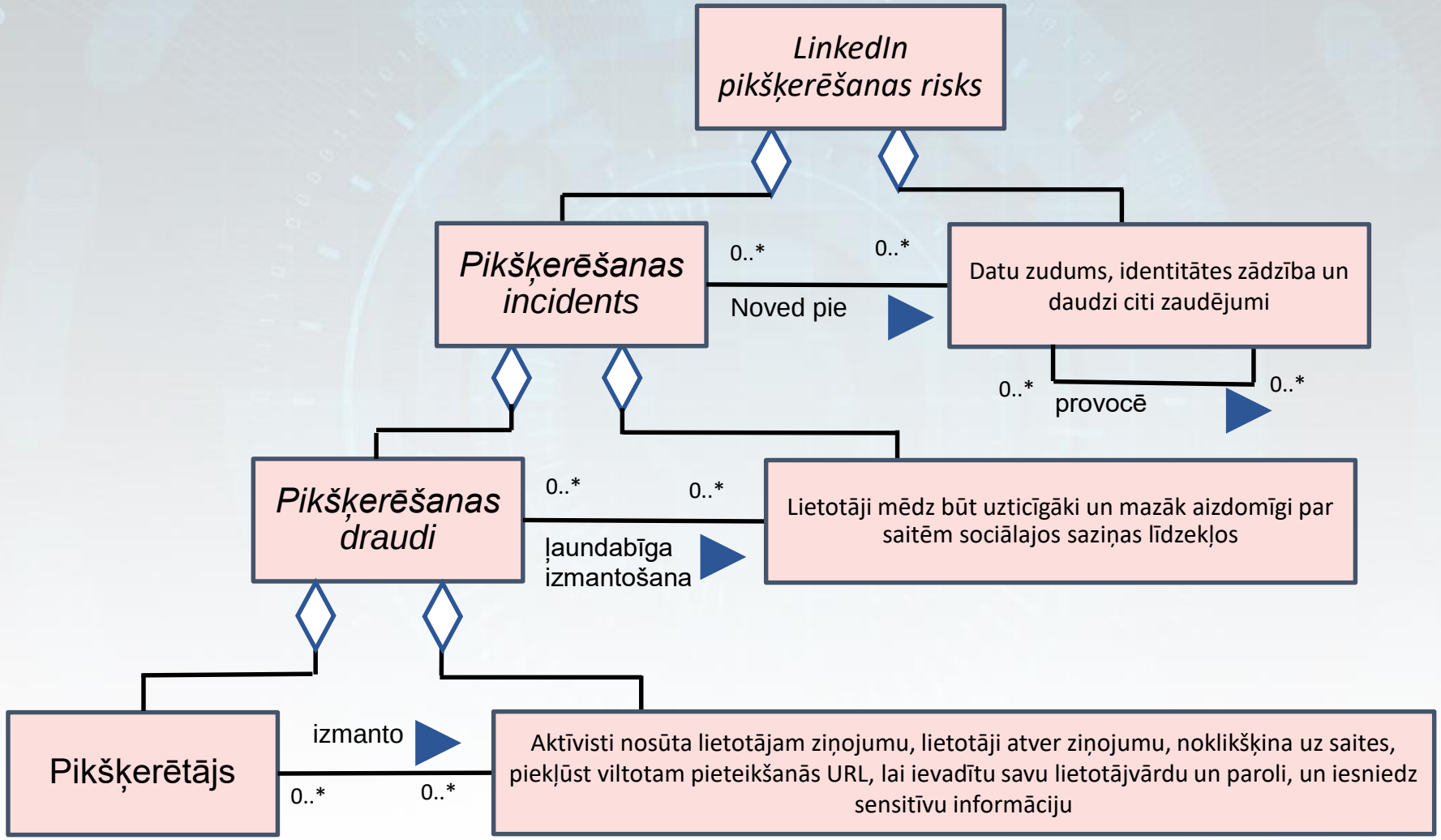
http://bit.ly/Autohorn-Fleet-Services-Ltd

We look forward to your swift positive response.

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

Izspiešanas pikšķerēšanas e-pasts (avots: LinkedInTraining)

Riska analīze



Izspiešanas pikšķerēšanas e-pasts (avots: LinkedInTraining)

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: Tiešais paziņojums
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *LinkedIn lietotājs*
b. Kas ir ietvers ziņas saturā? *Sadarbības priekšlikums*
c. Vai ir hipersaites/pielikumi? *Jā*

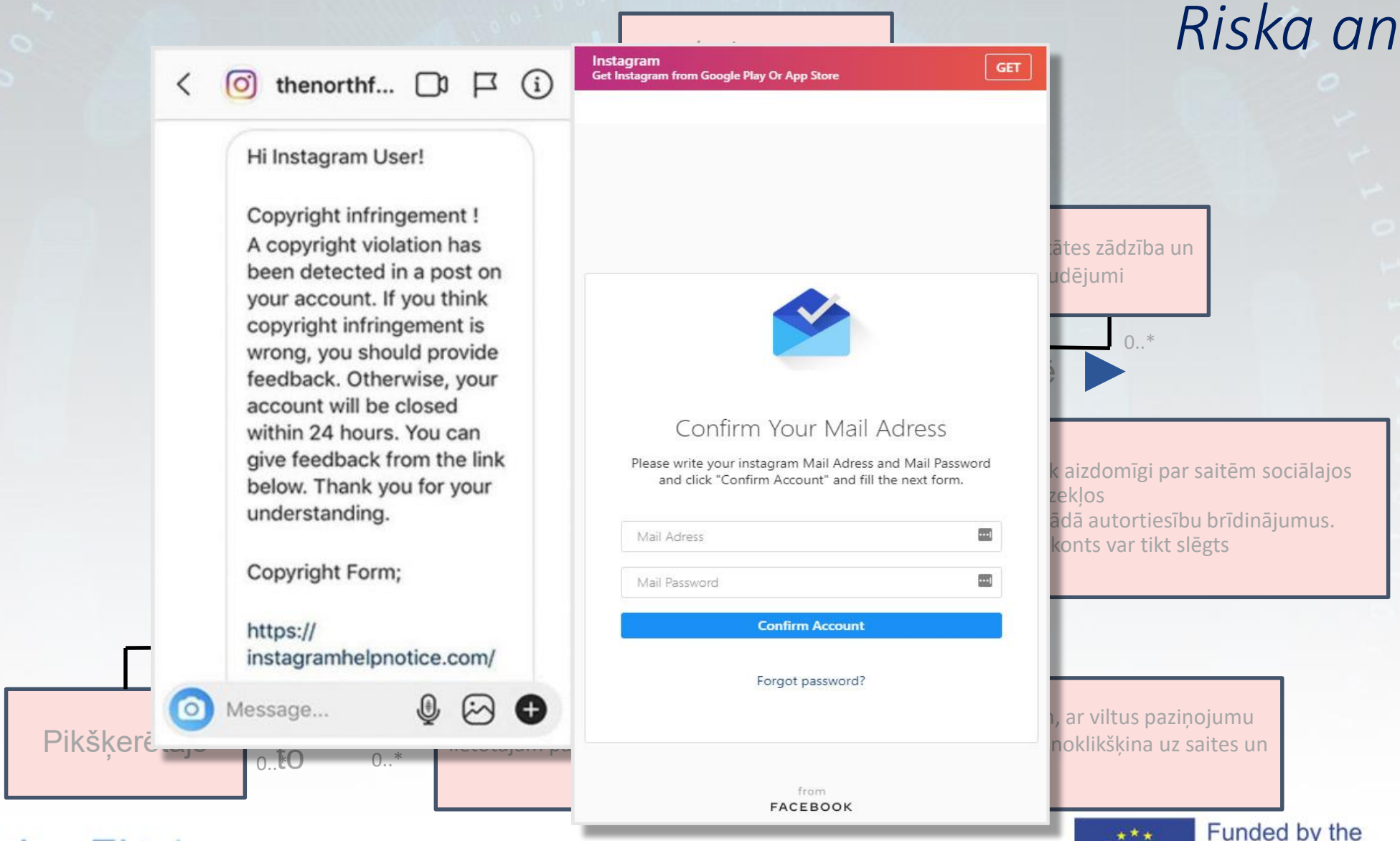
Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Ja kāda nezināms persona piedāvā sadarbību, tas, iespējams, ir aizdomīgs darījums.
3.2 Uzbrucēji izmanto URL saīsināšanas pakalpojumus, piemēram "*bit.ly*", lai saīsinātu un paslēptu pikšķerēšanas saites

4. Kritiskā domāšana
4.1 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.2 Pat ja šķiet, ka ziņojums ir no personas, kurai uzticaties, pastāv iespēja, ka šīs personas konts ir apdraudēts
4.3 Sociālajos saziņas līdzekļos vienmēr izmantojiet uzlabotus privātuma iestatījumus
4.4 Neklikšķiniet uz aizdomīgām saitēm DM (tiešās saziņas) ziņojumos, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Nekad nepieņemiet LinkedIn savienojuma pieprasījumus no nepazīstamas personas
4.6 Esiet piesardzīgs, kopīgojot pārāk daudz personiskās informācijas sociālajos medijos
4.7 Pārtrauciet sekošanu/bloķējiet aizdomīgus kontus un izdzēsiet jums nosūtīto ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

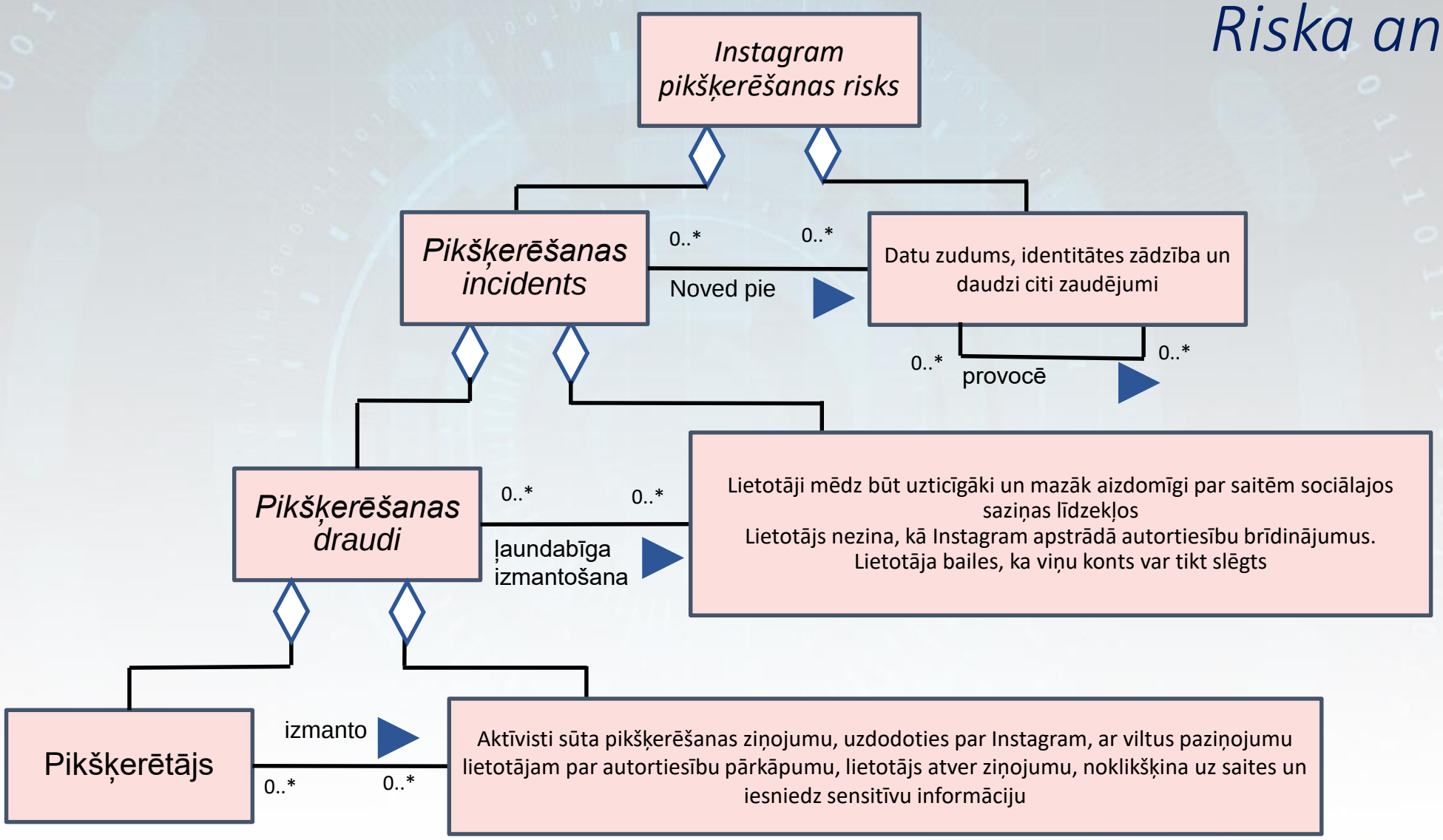
Funded by the Erasmus+ Programme of the European Union

Riska analīze



Sociālo mediju pikšķerēšanas e-pasts (Avots: Hackread)

Riska analīze



Sociālo mediju pikšķerēšanas e-pasts (Avots: Hackread)

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst platformas domēnam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: Tiešie ziņojumi
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *Instagram lietotājs*
b. Kas ir ietvers ziņas saturā? *Prasība par autortiesību pārkāpumu*
c. Vai ir hipersaites/pielikumi? *Jā*

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Likumīgus paziņojumus par autortiesību pretenzijām Instagram nosūtīs personīgi
3.2 Lai uzrunātu jūs, Instagram vienmēr izmantos jūsu kontā reģistrēto vārdu
3.3 Norādītajai saitei ir jāatbilst platformas domēnam t.i., *"instagram.com"* nevis *"instagram**helpnotice**.com"*

4. Kritiskā domāšana
4.1 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.2 Pat ja šķiet, ka ziņojums ir no personas, kurai uzticaties, pastāv iespēja, ka šīs personas konts ir apdraudēts
4.3 Sociālajos saziņas līdzekļos vienmēr izmantojiet uzlabotus privātuma iestatījumus
4.4 Neklikšķiniet uz aizdomīgām saitēm DM (tiešās saziņas) ziņojumos, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Esiet piesardzīgs, sūtot ziņojumus lietotājiem, kurus nepazīstat un kuriem nesekojat
4.6 Pārtrauciet sekošanu/bloķējiet aizdomīgus kontus un izdzēsiet jums nosūtīto ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst platformas domēnam

1. Pikšķerēšanas saprašana

Pikšķerēšanas avots: Tiešais paziņojums
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *Instagram lietotājs*
b. Kas ir ietvers ziņas saturā? *Prasība par autortiesību pārkāpumu*
c. Vai ir hipersaites/pielikumi? *Jā*

3. Aizdomīgo momentu atpazīšana

3.1 Likumīgus paziņojumus par autortiesību pretenzijām Instagram nosūtīs personīgi
3.2 Lai uzrunātu jūs, Instagram vienmēr izmantos jūsu kontā reģistrēto vārdu
3.3 Norādītajai saitei ir jāatbilst platformas domēnam t.i., "*instagram.com*" , nevis "*instagram**helpnotice**.com*"

4. Kritiskā domāšana
4.1 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.2 Pat ja šķiet, ka ziņojums ir no personas, kurai uzticaties, pastāv iespēja, ka šīs personas konts ir apdraudēts
4.3 Sociālajos saziņas līdzekļos vienmēr izmantojiet uzlabotus privātuma iestatījumus
4.4 Neklikšķiniet uz aizdomīgām saitēm DM (tiešās saziņas) ziņojumos, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Esiet piesardzīgs, sūtot ziņojumus lietotājiem, kurus nepazīstat un kuriem nesekojat
4.6 Pārtrauciet sekošanu/bloķējiet aizdomīgus kontus un izdzēsiet jums nosūtīto ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

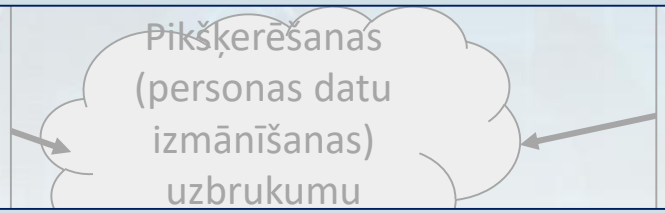
Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana

2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst platformas domēnam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: Tiešie ziņojumi
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *Instagram lietotājs*
b. Kas ir ietvers ziņas saturā? *Prasība par autortiesību pārkāpumu*
c. Vai ir h



3. Aizdomīgo momentu atpazīšana
3.1 Likumīgus paziņojumus par autortiesību pretenzijām Instagram nosūtīs personīgi
3.2 Lai uzrunātu jūs, Instagram vienmēr izmantos jūsu kontā reģistrēto vārdu
3.3 Norādītajai saitei ir jāatbilst platformas domēnam t.i., "*instagram.com*" nevis "*instagram**helpnotice**.com*"

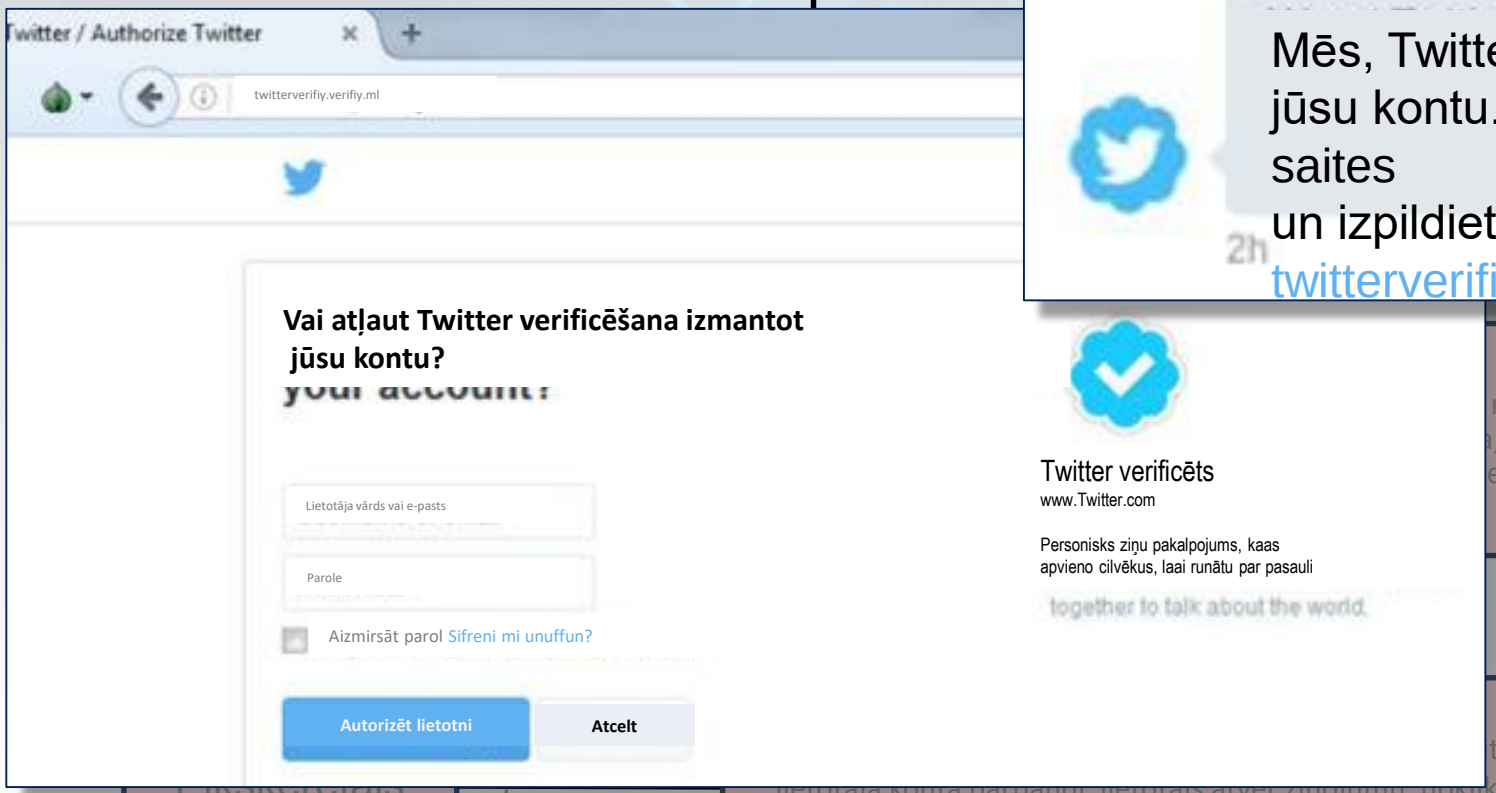
4. Kritiskā domāšana

4.1 Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās
4.2 Pat ja šķiet, ka ziņojums ir no personas, kurai uzticaties, pastāv iespēja, ka šīs personas konts ir apdraudēts
4.3 Sociālajos saziņas līdzekļos vienmēr izmantojiet uzlabotus privātuma iestatījumus
4.4 Neklikšķiniet uz aizdomīgām saitēm DM (tiešās saziņas) ziņojumos, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus
4.5 Esiet piesardzīgs, sūtot ziņojumus lietotājiem, kurus nepazīstat un kuriem nesekojat
4.6 Pārtrauciet sekošanu/bloķējiet aizdomīgus kontus un izdzēsiet jums nosūtīto ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana

Funded by the Erasmus+ Programme of the European Union

Riska analīze

Twitter pikšķerēšanas risks

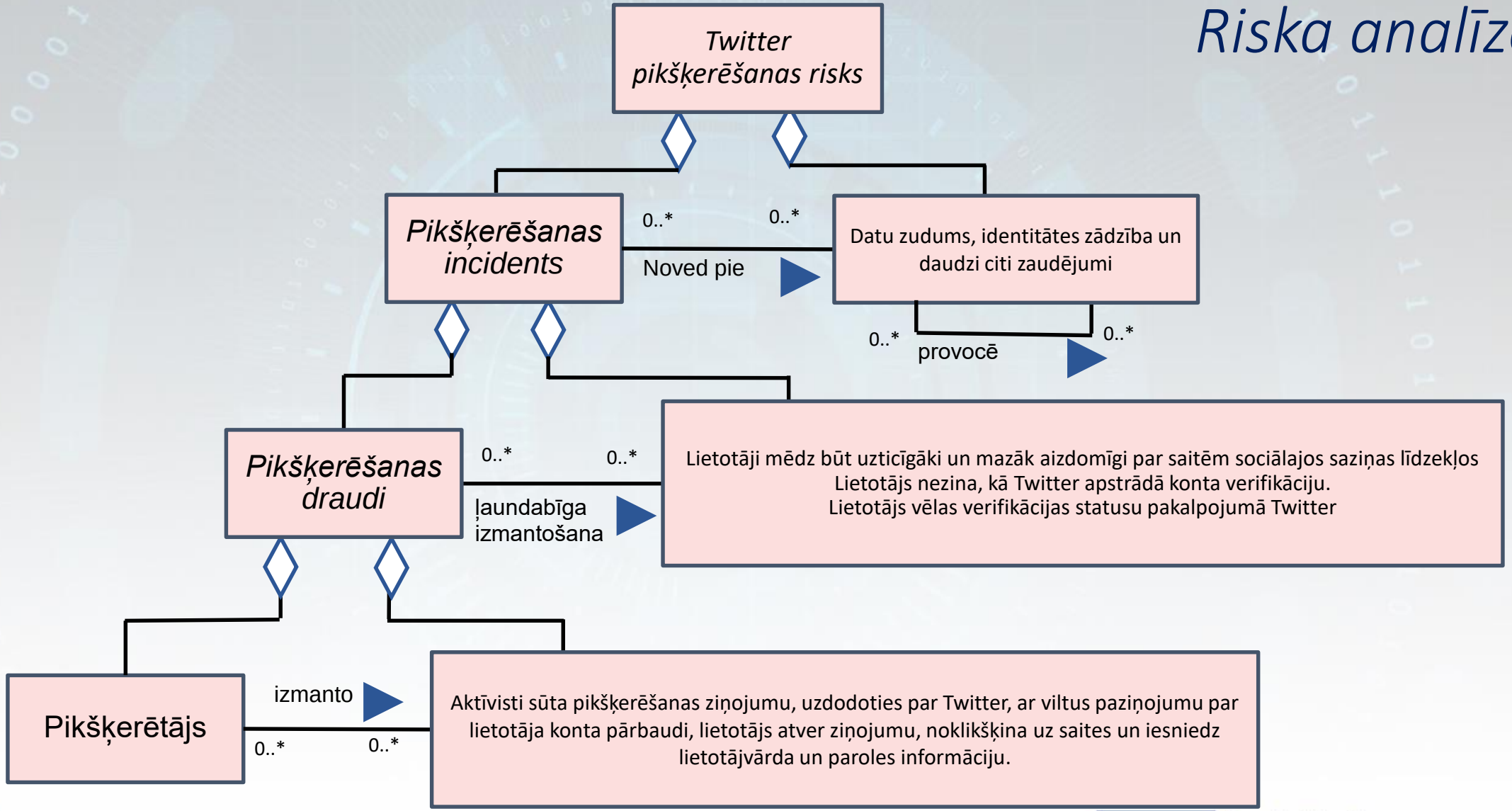


mazāk aizdomīgi par saitēm sociālajos saziņas līdzekļos
, kā Twitter apstrādā konta verifikāciju.
erifikācijas statusu pakalpojumā Twitter

tter, ar viltus paziņojumu par
ķina uz saites un iesniedz
lietotājvārda un paroles informāciju.

0..to 0..*

Riska analīze



Sociālo mediju pikšķerēšanas e-pasts (Avots: Malwarebytes)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riska atpazīšana

2. URL saišu saprašana
2.1 Neklikšķiniet uz pielikumiem vai saitēm
2.2 Virziet kursoru virs pielikuma, lai atklātu URL, un analizējiet, lai noteiktu, vai tas nav ļaunprātīgs
2.3 Esiet piesardzīgs, ja URL ceļš neatbilst platformas domēnam

1. Pikšķerēšanas saprašana
Pikšķerēšanas avots: Tiešais paziņojums
Pikšķerēšanas ziņojumu anatomija:
a. No kā ir sūtītā ziņa? *Twitter lietotājs*
b. Kas ir ietvers ziņas saturā? *Konta verifikācijas prasība*
c. Vai ir hipersaites/pielikumi? *Jā*

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumu atpazīšana

3. Aizdomīgo momentu atpazīšana
3.1 Leģitīms Twitter verifikācijas process tiek veikts, izmantojot lietotāja pieprasījuma procesu pakalpojumam Twitter (nevis otrādi)
3.2 Lai uzrunātu jūs, Twitter vienmēr izmantos jūsu kontā reģistrēto vārdu
3.3 Norādītajai saitei ir jāatbilst platformas domēnam t.i., *"twitter.com"* un nevis "***twitterverifiy.verifiy.ml***"

4. Kritiskā domāšana
4.1 *Norādiet konta paroli vai pieteikšanās informāciju "pārbaudei" tikai likumīgu vietņu drošās daļās, piem., twitter.com*
4.2 *Pat ja šķiet, ka ziņojums ir no personas, kurai uzticaties, pastāv iespēja, ka šīs personas konts ir apdraudēts*
4.3 *Sociālajos saziņas līdzekļos vienmēr izmantojiet uzlabotus privātuma iestatījumus*
4.4 *Neklikšķiniet uz aizdomīgām saitēm DM (tiešās saziņas) ziņojumos, pārbaudiet aizdomīgos URL, izmantojot bezmaksas pikšķerēšanas noteikšanas rīkus*
4.5 *Esiet piesardzīgs, sūtot ziņojumus lietotājiem, kurus nepazīstat un kuriem nesekojat*
4.6 *Pārtrauciet sekošanu/bloķējiet aizdomīgus kontus un izdzēsiet jums nosūtīto ziņojumu, ja esat pārliecināts, ka tā ir pikšķerēšana*

Funded by the Erasmus+ Programme of the European Union

Kopsavilkums

- Pikšķerēšanas gadījumu izpēte
- Izcelto pikšķerēšanas uzbrukumu un krāpniecības risku analīze
- Šo pikšķerēšanas uzbrukumu atpazīšana, lai novērstu pikšķerēšanas riskus

CyberPhish
Safeguarding your digital future

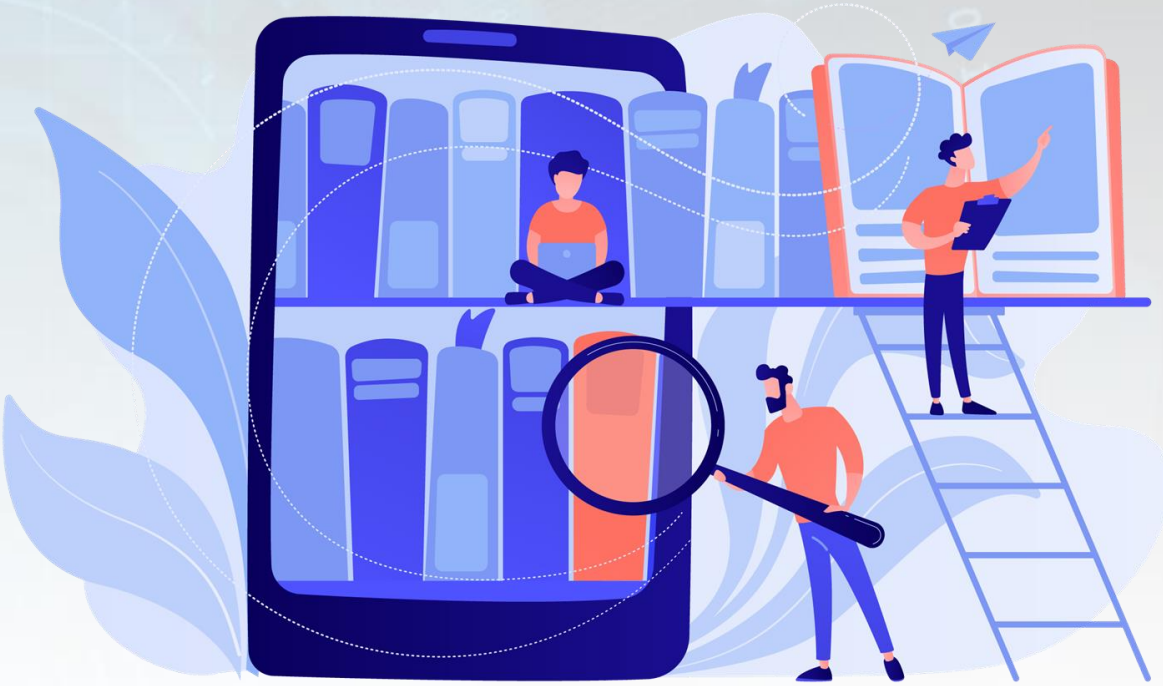
Funded by the Erasmus+ Programme of the European Union

Uzdevums

- Apspriediet 3 neminētus pikšķerēšanas uzbrukumus, kuri, jūsuprāt, ir izplatīti mūsdienās
- Izveidojiet riska analīzi šīm pikšķerēšanas krāpniecībām, izceļot uzbrukuma metodes, ievainojamības un pikšķerēšanas notikumus, kas rada pikšķerēšanas risku.
- Apspriediet, kā atpazīt šīs krāpniecības un novērst pikšķerēšanas riskus

Papildu lasīšana

- **Dubuā E.** *[Dubois E.]***, Heimanss P.** *[Heymans P.]***, Meijers N.** ***[Mayer N.]*****, Matulevičs R.** *[Matulevičius R.]* (2010. gads)
  Sistemātiska pieeja informācijas sistēmu drošības riska pārvaldības jomas definēšanai. *Apzinātas perspektīvas informācijas sistēmu inženierijā 2010: 289-306*
- **Abrošans H.** *[Abroshan H.]* (2021. gads)**:** Pikšķerēšanas upuru pamatcēloņi — cilvēka uzvedības, emociju un demogrāfijas ietekme, Promocijas darbs, Gentes Universitāte
- **Altobaiti K.** *[Althobaiti, K.]***, Mengs N.** *[Meng, N.]***, & Venīja K.** *[Vaniea, K.]* (2021. gads). Man nav vajadzīgs eksperts! URL pikšķerēšanas funkciju padarīšana cilvēkiem saprotama. Materiālā *2021. gada CHI konferences par cilvēciskajiem faktoriem skaitļošanas sistēmās* (1-17. lpp.).
- **Dreiks C. E.** *[Drake, C. E.]***, Oliver J. J.** *[Oliver, J. J.]* **un Kūncs E. J.** *[Koontz, E. J.]* (2004. gads). Pikšķerēšanas e-pasta anatomija. Materiālos CEAS.
- **Altobaiti K.** *[Althobaiti, K.]***, Mengs N.** *[Meng, N.]***, & Venīja K.** *[Vaniea, K.]* (2021. gada maijs). Man nav vajadzīgs eksperts! URL pikšķerēšanas funkciju padarīšana cilvēkiem saprotama. Materiālā *2021. gada CHI konferences par cilvēciskajiem faktoriem skaitļošanas sistēmās* (1-17. lpp.).
- **Dreiks C. E.** *[Drake, C. E.]***, Oliver J. J.** *[Oliver, J. J.]* **un Kūncs E. J.** *[Koontz, E. J.]* (2004. gads). Pikšķerēšanas e-pasta anatomija. Materiālos CEAS.



Īsi video

- Pikšķerēšanas e-pasta krāpniecības anatomija
  - ***https://youtu.be/3gpOM9c6mmA***
- Daži pikšķerēšanas uzbrukumu piemēri
  - ***https://youtu.be/lpGfxIAQhSo***
  - ***https://youtu.be/pGEAZdp0MAI***
- Pikšķerēšanas atpazīšana un aizsardzība pret to
  - ***https://youtu.be/R12_y2BhKbE***

Funded by the Erasmus+ Programme of the European Union

Pateicamies!