Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute mõistmise ja nendega toimetuleku ülevaade

Andmepüügirünnakute äratundmine

Andmepüügirünnakute ja -võtete juhtumiuuringud

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

Õppe-eesmärgid

Selgitada erinevaid andmepüügi-rünnakute tagajärgi ning kuidas andmepüügirünnakuid ära tunda ja nendega toime tulla.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Õpilase töökoormus

Loengud	3 h
Audio- ja videomaterjal	3 h
Juhtumiuuringud	3 h
Lisalugemine	6 h
Eksamiks valmistumine	3 h

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Loenguteemad

- Mis on andmepüügirünnakud ja -riskid?
- Andmepüügirünnakute juhtumiuuringute analüüs
  - Millised on andmepüügiohud ja -riskid erinevate juhtumite puhul?
  - Kuidas andmepüügiriske ära tunda ja nendega toime tulla?

Funded by the
Erasmus+ Programme
of the European Union

Mis on andmepüügirünnak?

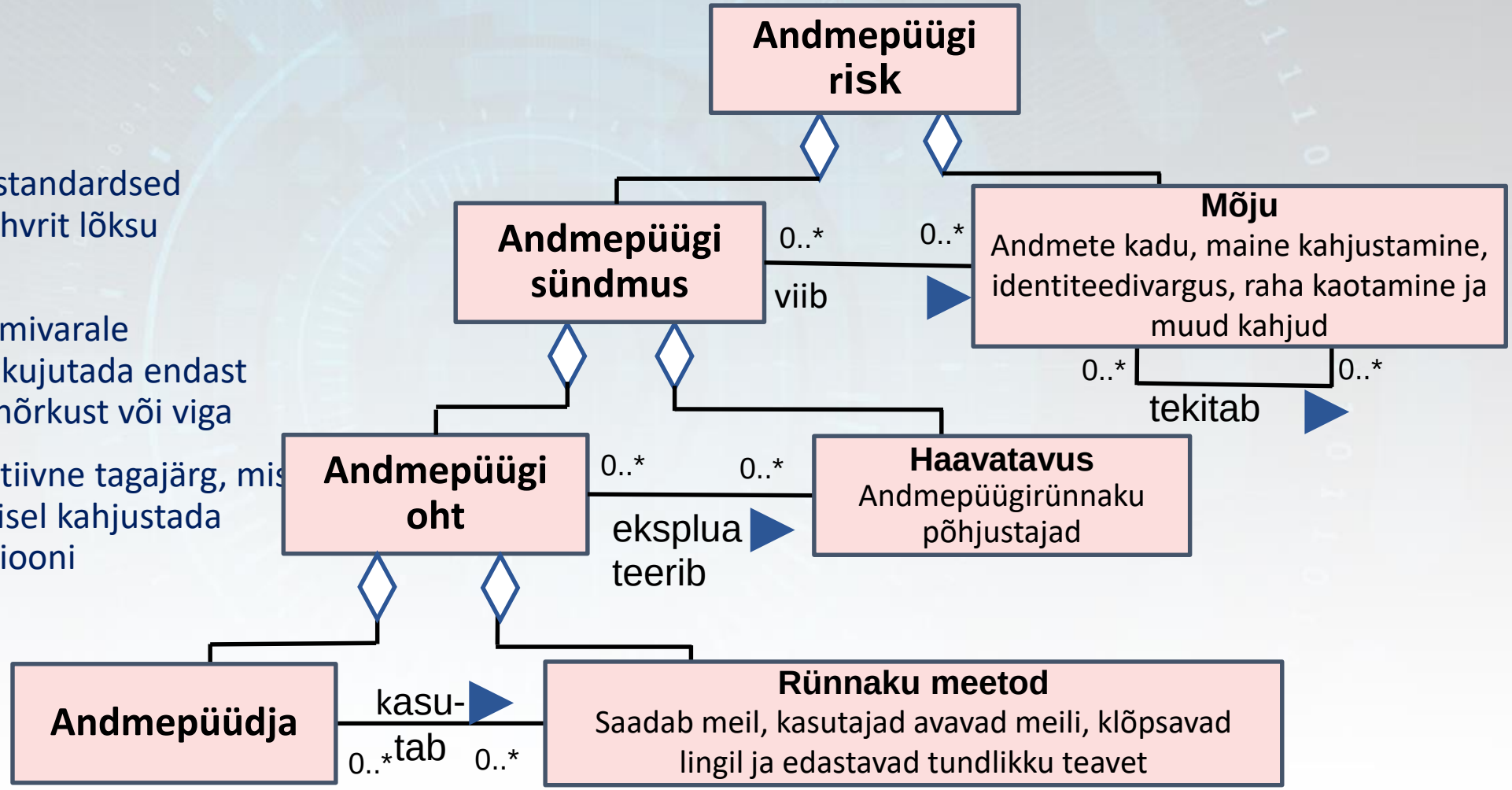
Andmepüük *on sotsiaalse manipuleerimise pettus, mille tagajärjeks võib olla andmete kadu, maine kahjustamine, identiteedivargus, rahakaotus ja palju muud kahju inimestele ja organisatsioonidele. Andmepüügipettus algab tavaliselt e-kirjaga, mis püüab võita potentsiaalse ohvri usaldust ja veenda teda ründaja soovitud toiminguid tegema.*

[*Abroshan, 2021*]

Funded by the
Erasmus+ Programme
of the European Union

Mis on andmepüügirisk?

- **Rünnaku meetod** – standardsed vahendid, mille abil ohvrit lõksu meelitatakse
- **Haavatavus** – süsteemivarale iseloomulik, mis võib kujutada endast süsteemi turvalisuse nõrkust või viga
- **Mõju** - võimalik negatiivne tagajärg, mis võib ohu realiseerumisel kahjustada varasid või organisatsiooni

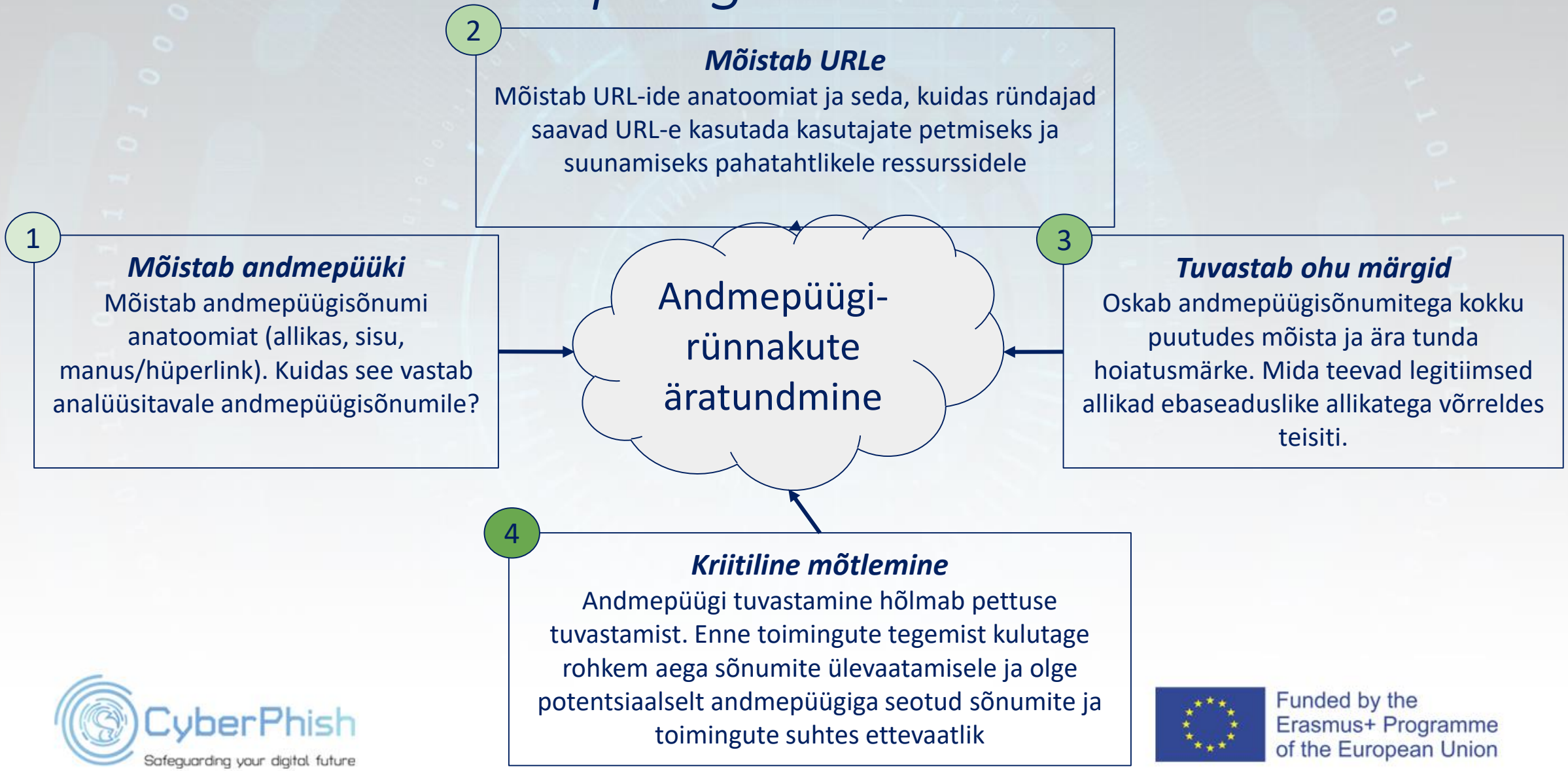


[*Dubois at al., 2010*]

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Andmepüügirünnakute äratundmine



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Juhtumiuuringud

Käsitletavad juhtumid

- COVID-iga seotud rünnakud
- GDPR-iga seotud rünnakud
- Tehnilise toe rünnakud
- Krüptovaluuta pettused
- Väljapressimispettused
- Ettemaksupettused
- Sotsiaalmeedia pettused

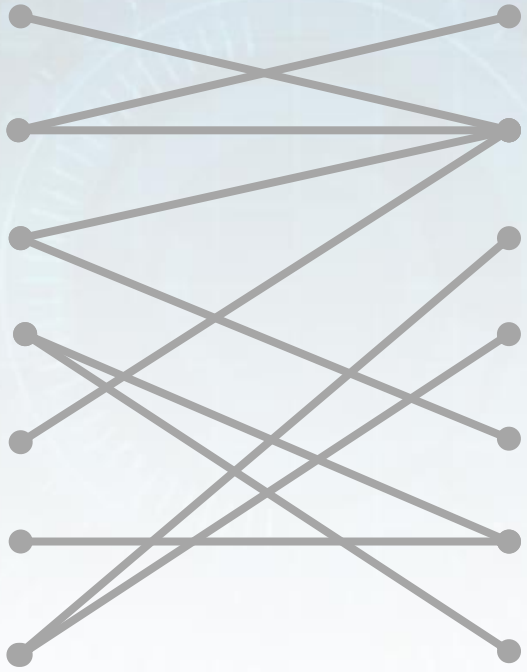
CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Juhtumiuuringud

Juhtumid

- COVID-iga seotud rünnakud
- GDPR-iga seotud rünnakud
- Tehnilise toe rünnakud
- Krüptovaluuta pettused
- Väljapressimispettused
- Ettemaksupettused
- Sotsiaalmeedia pettused



- GDPR-iga seotud rünnakud
- Meilid
- Kiirsõnumid
- Sotsiaalsed võrgustikud
- Veebisaidid
- Loterii pettused
- SMS

COVID-iga seotud rünnakud

- COVID-19 ajal märkasime pandeemiaga seotud petuskeemide tõusu e-kirjade ja SMS-ide kaudu, nagu võltsitud haiguste tõrje ja ennetamise keskused (CDC) või tervishoiuorganisatsioonide teatised vaktsiiniga hõlmatuse kohta, kust saate vaktsiini, vaktsiinide statistikat, töötajate vaktsineerimise info jne
- Levinud rünnakute hulka kuuluvad COVID-i tervisenõustamise meilipettused

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs

COVID phishing risk

get access
, Infected
vare etc.)

Phish
thre

Phisher

uses

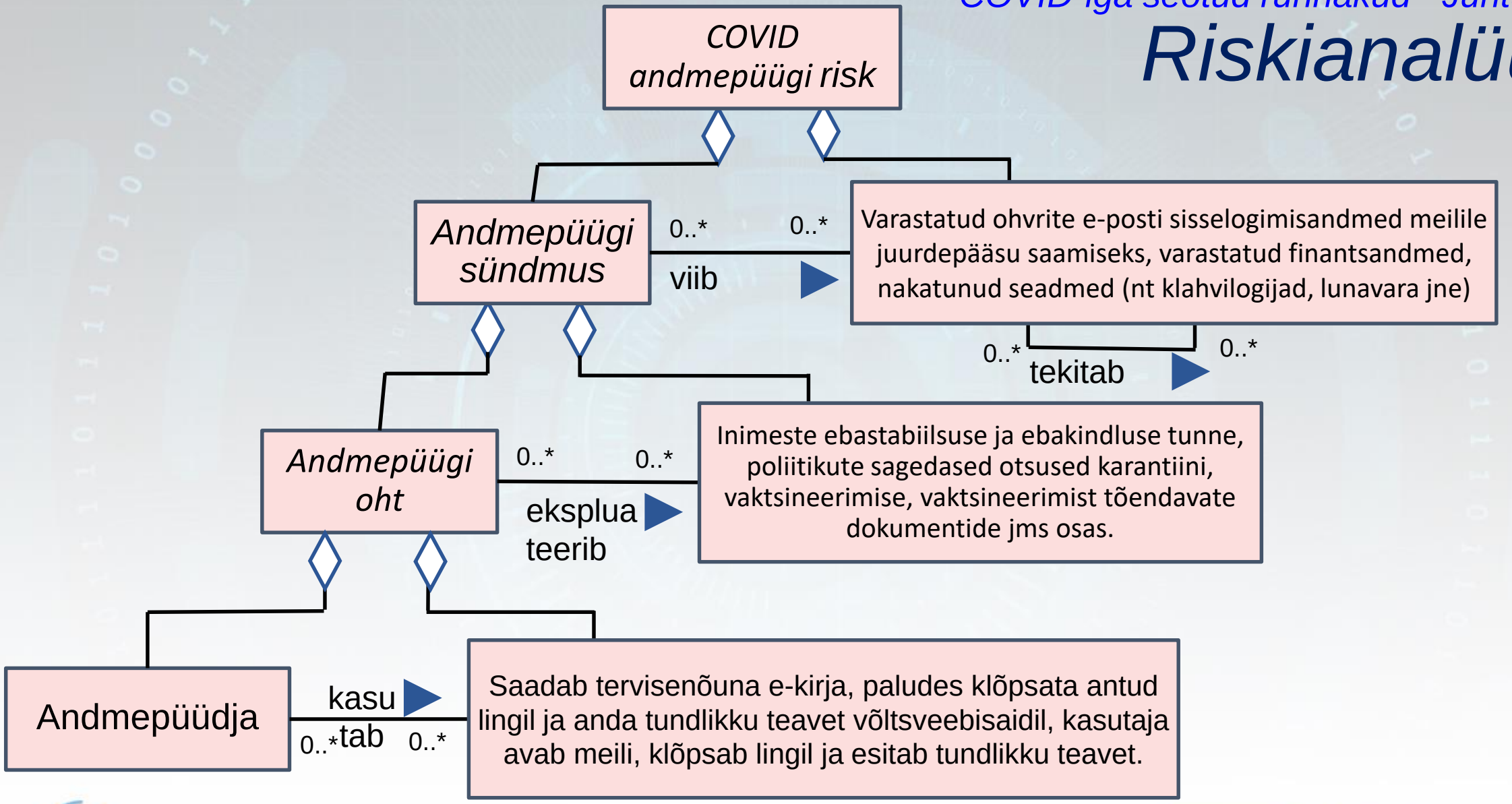
0..*

Coronavirus Phishing Email (Source: Wired)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



CyberPhish
Safeguarding your digital future

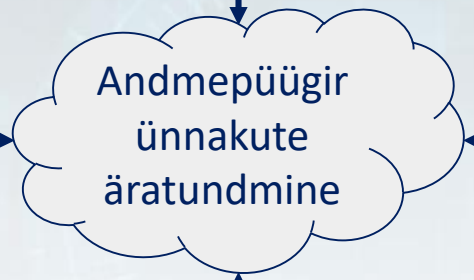
Coronavirus Phishing Email (Source: Wired)

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit linkide kohal ja analüüsige, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti nähtava sisuga

1. Mõistab andmepüüki
Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum tuleb? *[Peidetud]*
b. Mis on sõnumi sisu? *Koroonaviiruse ohutuse nõuanded*
c. Kas sisaldab linke/manuseid? *Jah*



3. Tuvastab ohu märke
3.1 Usaldusväärsed COVID-i teabeallikad ei saada soovimatuid e-kirju
3.2 Õigeted meilid kutsuvad teid tavaliselt teie nime järgi (st mitte "sir")
3.3 Õigetel e-kirjadel ei ole probleeme õigekirja ja grammatikag

4. Kriitiline mõtlemine
4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Olge hüperlinkide/manuste suhtes ettevaatlik; nad võivad viidata pahatahtlikule ressursile
4.3 Olge ettevaatlik, kui meilid nõuavad kiireloomulisuse/hirmuga toiminguid
4.4 Enne sõnumi usaldamist kasutage e-kirja sisu kohta lisateabe saamiseks otsingumootorit
4.5 Kontrollige potentsiaalselt andmepüügiga seotud URL-id, kasutades tasuta andmepüügi tuvastamise tööriistu
4.6 Kustutage teile saadetud meil, kui olete kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs

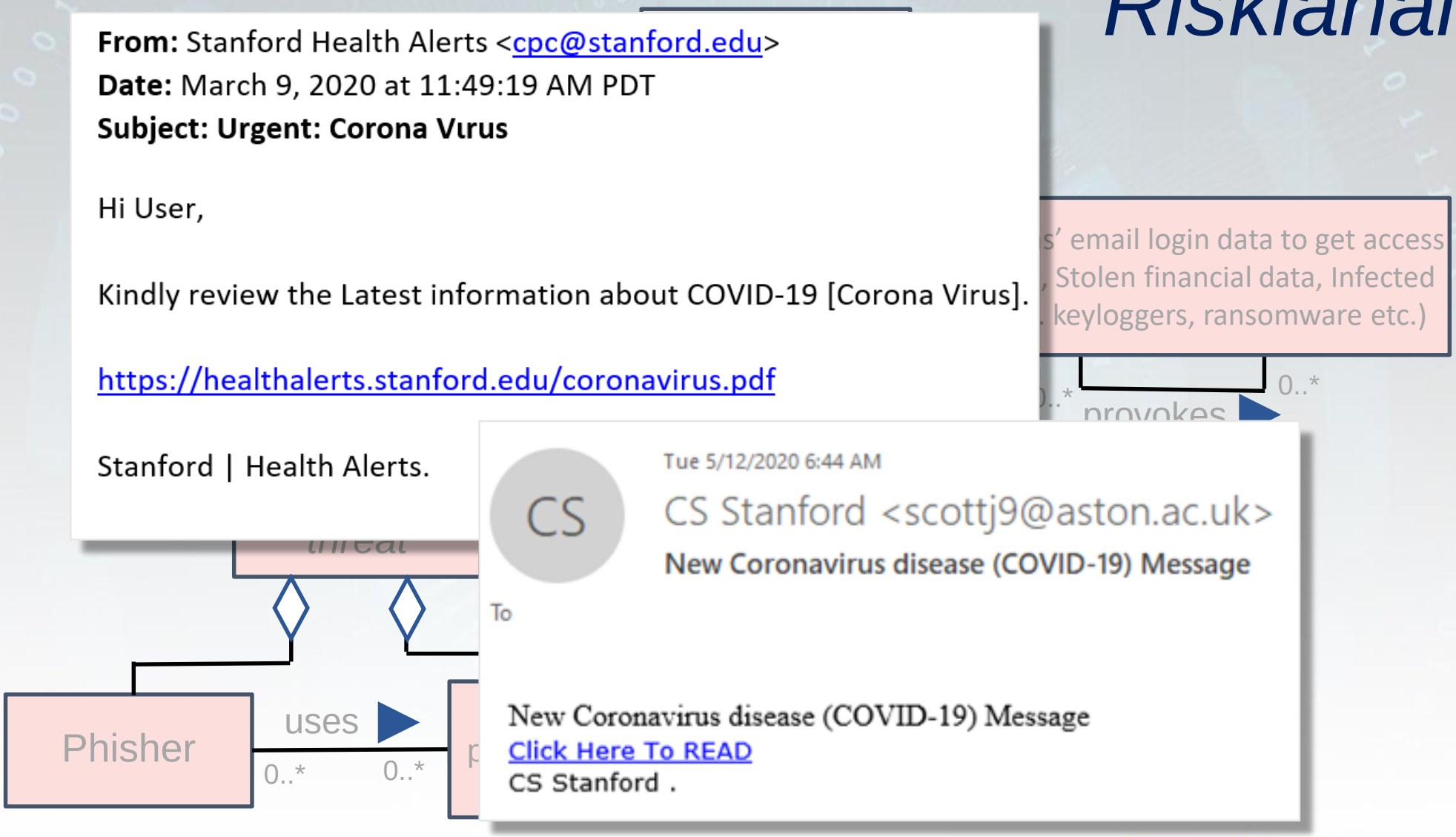
From: Stanford Health Alerts <cpc@stanford.edu>
Date: March 9, 2020 at 11:49:19 AM PDT
Subject: Urgent: Corona Vırus

Hi User,

Kindly review the Latest information about COVID-19 [Corona Virus].

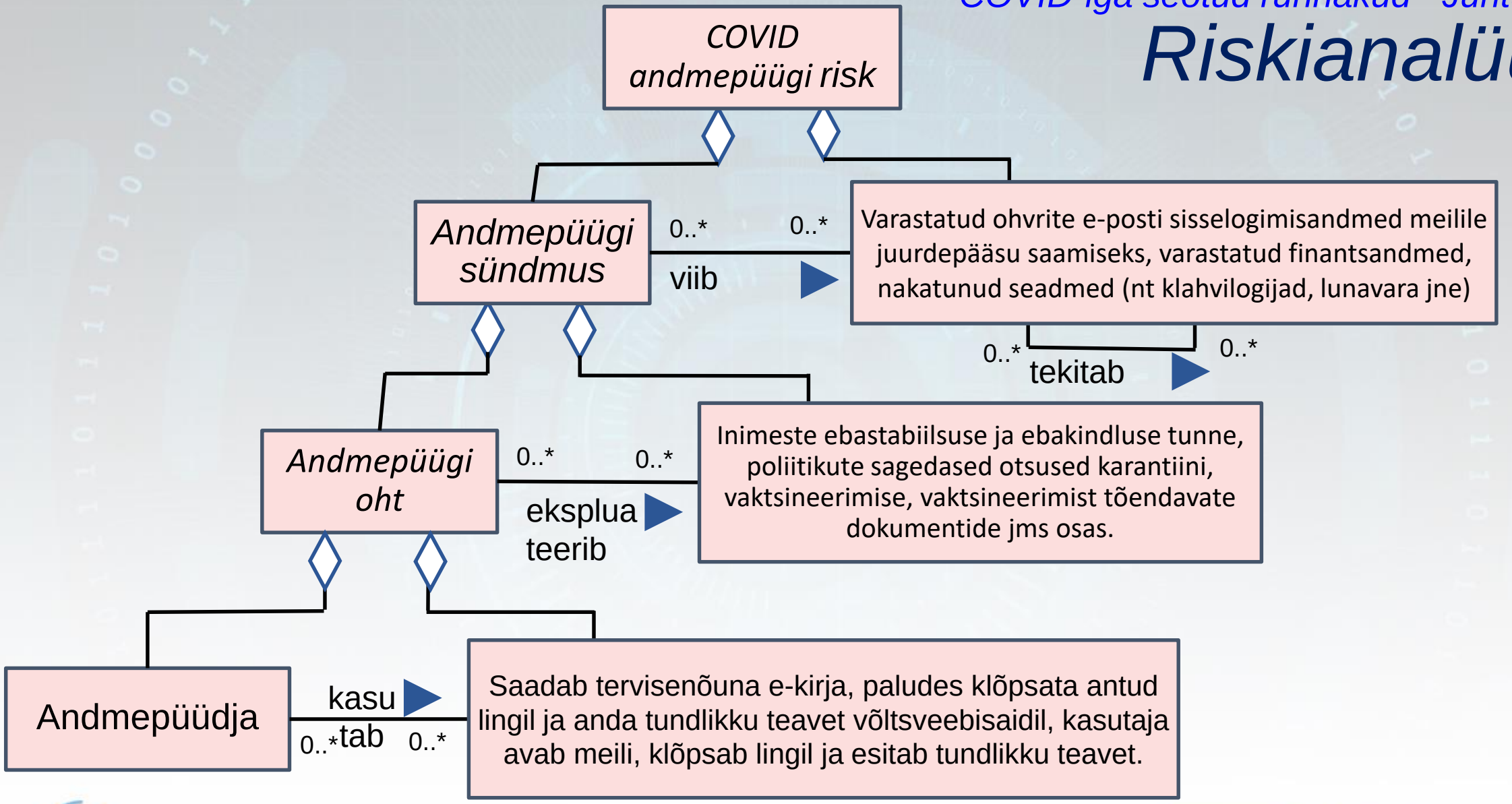
https://healthalerts.stanford.edu/coronavirus.pdf

Stanford | Health Alerts.



Coronavirus Phishing Email (Source: Stanford.edu, Stanford.edu)

Riskianalüüs



CyberPhish
Safeguarding your digital future

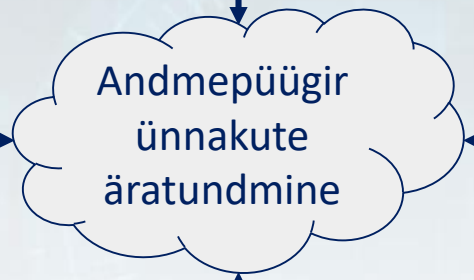
Coronavirus Phishing Email (Source: Wired)

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit linkide kohal ja analüüsige, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti nähtava sisuga

1. Mõistab andmepüüki
Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum tuleb? *cpc@stanford.edu, scottj9@aston.ac.uk*
b. Mis on sõnumi sisu? *Koroonaviirus*
c. Kas sisaldab linke/manuseid? *Jah*



3. Tuvastab ohu märke
3.1 Usaldusväärsed COVID-i teabeallikad ei saada soovimatuid e-kirju
3.2 Õigeted meilid kutsuvad teid tavaliselt teie nime järgi (st mitte "sir")
3.3 Õigetel e-kirjadel ei ole probleeme õigekirja ja grammatikag

4. Kriitiline mõtlemine
4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Olge hüperlinkide/manuste suhtes ettevaatlik; nad võivad viidata pahatahtlikule ressursile
4.3 Olge ettevaatlik, kui meilid nõuavad kiireloomulisuse/hirmuga toiminguid
4.4 Enne sõnumi usaldamist kasutage e-kirja sisu kohta lisateabe saamiseks otsingumootorit
4.5 Kontrollige potentsiaalselt andmepüügiga seotud URL-id, kasutades tasuta andmepüügi tuvastamise tööriistu
4.6 Kustutage teile saadetud meil, kui olete kindel, et tegemist on andmepüügiga

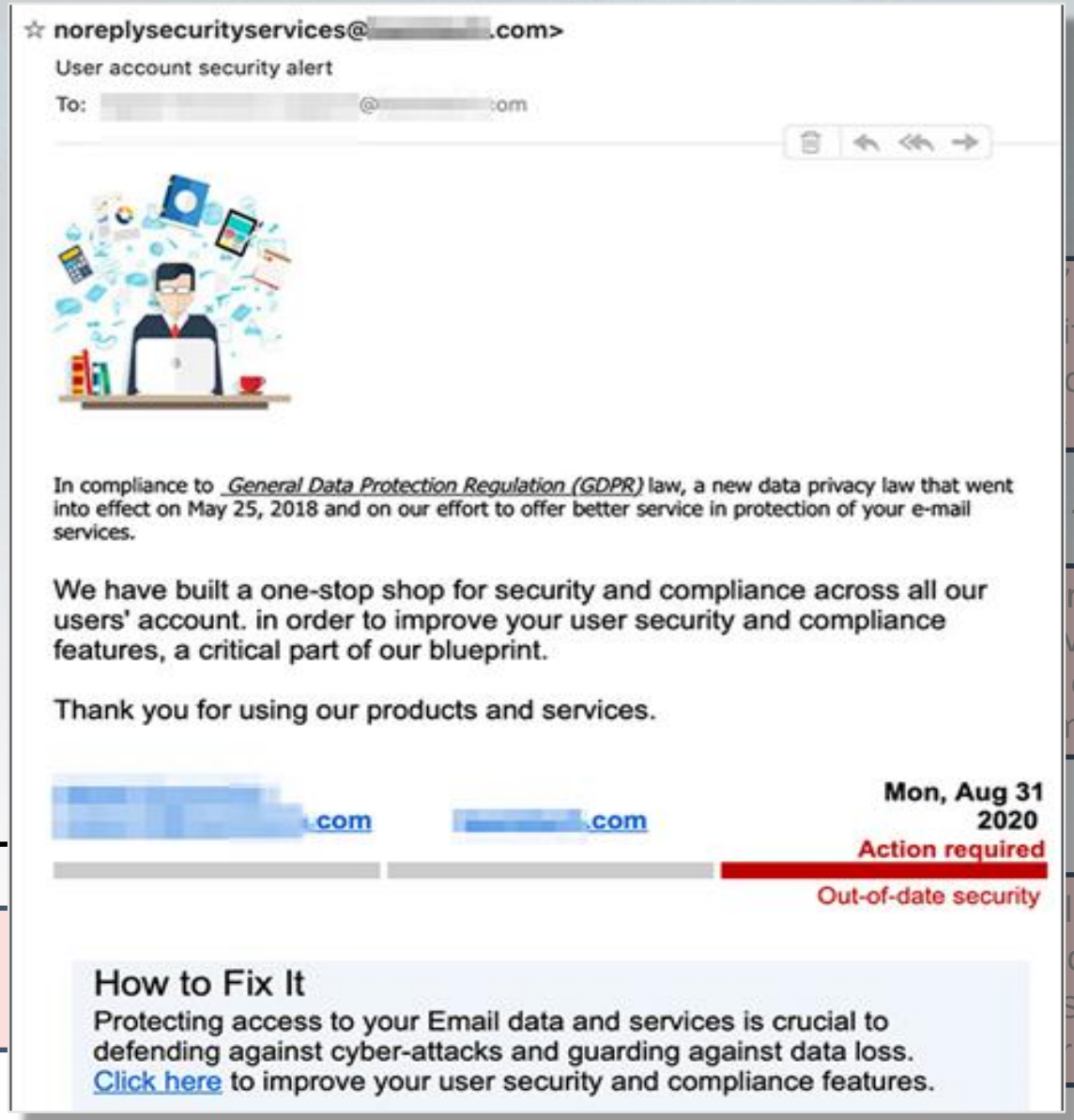
Funded by the Erasmus+ Programme of the European Union

GDPR-iga seotud rünnakud

- 2018. aastal leidis aset palju GDPR-iga seotud andmepüügirünnakuid, kuna kõik EL ettevõtted ja organisatsioonid olid kohustatud rakendama GDPR-i oma organisatsioonides
- Ründaja taktika võib hõlmata saatmist
  - võltskirjad ettekäändel, et ettevõte aitab GDPR-i tegevustes eesmärgiga teavet varastada
  - võltskirjad ettekäändel, et ettevõtted pakuvad klientidele teavet andmepoliitika muudatuste kohta

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



email login data to get access to
itive data could be stolen from
or stolen contacts could be used
further cyber attacks

0..*

.* provokes

rained about GDPR, fear
violations
of timeline for supposed
npliance

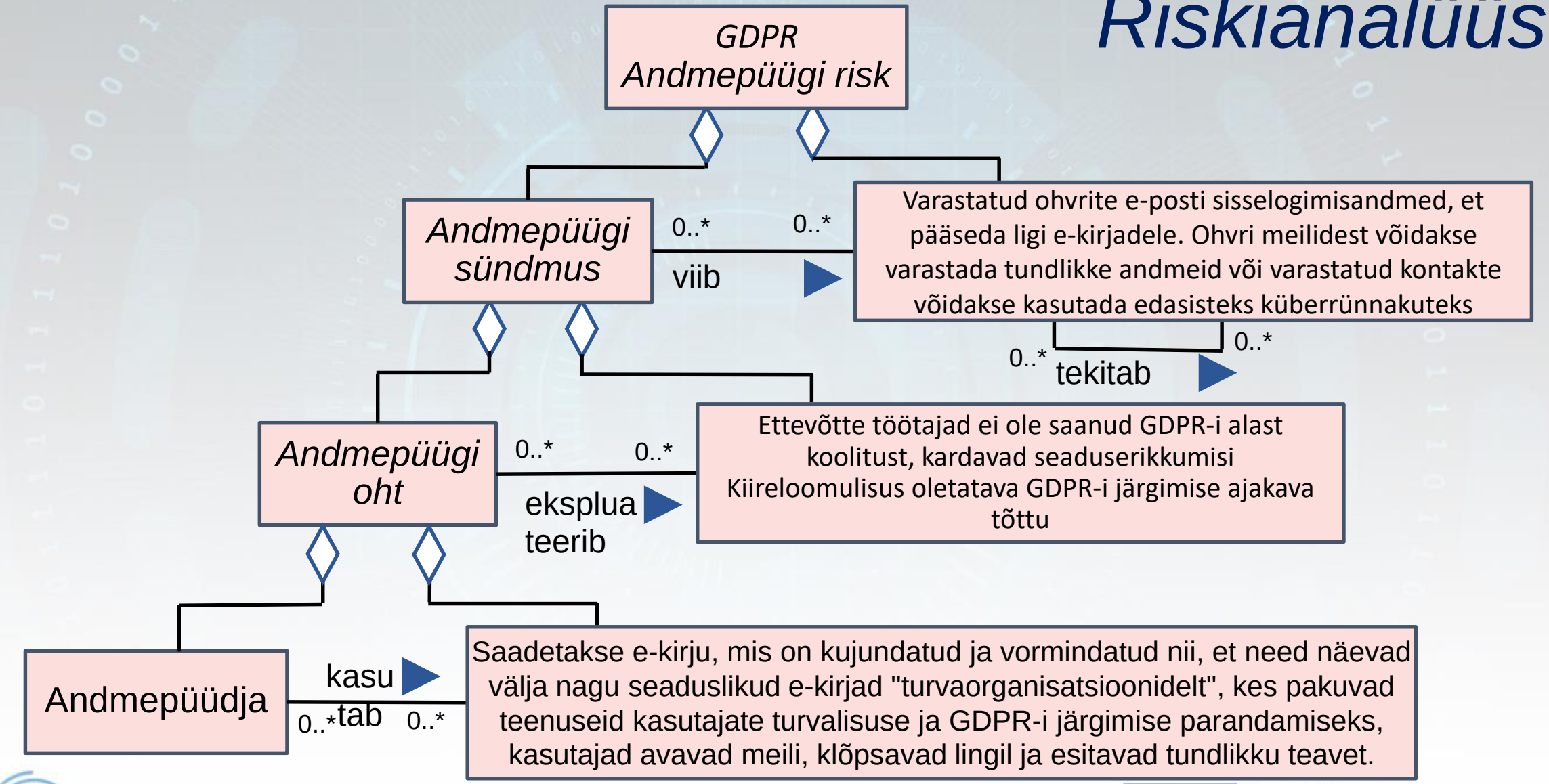
Phisher

like legitimate emails
ces to improve user
s email, clicks on the
rmation

GDPR Phishing Email (Source: Databreachtoday)

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



CyberPhish
Safeguarding your digital future

GDPR Phishing Email (Source: Databreachtoday)

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit linkide kohal ja analüüsige, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti nähtava sisuga

1. Mõistab andmepüüki
Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum tuleb? *noreplysecurityservices*
b. Mis on sõnumi sisu? Konto turvalisus
c. Kas sisaldab linke/manuseid? *Jah*

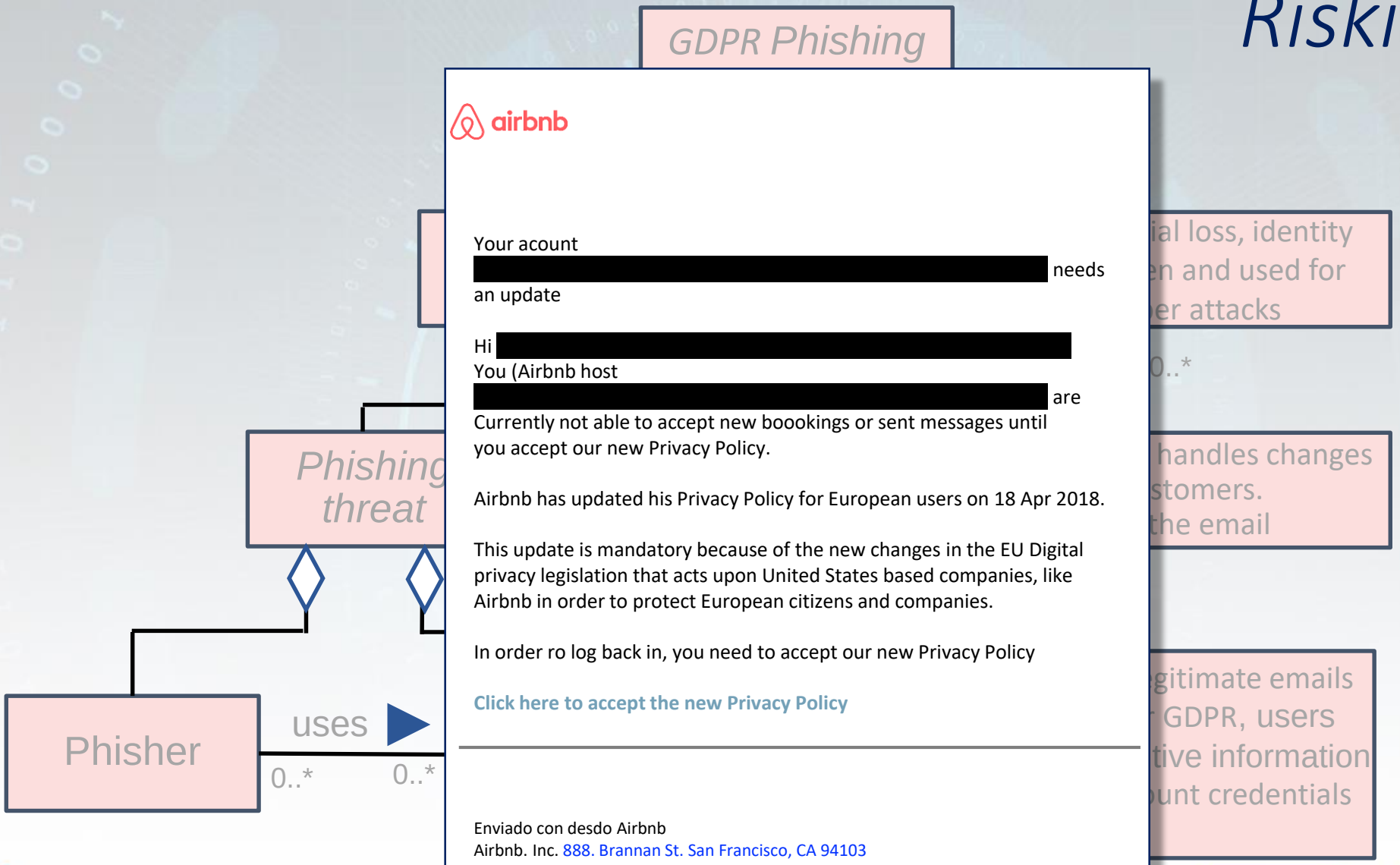
Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märke
3.1 Õigustatud meilisõnumitel ei ole vastuolulist sisu, nt „GDPR" vs „Aegunud turvalisus"
3.2 Õiguspärased teenusemeilid on professionaalsed ja ühtse vorminguga

4. Kriitiline mõtlemine
4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Olge hüperlinkide/manuste suhtes ettevaatlik; nad võivad viidata pahatahtlikule ressursile
4.3 Olge ettevaatlik, kui meilid nõuavad kiireloomulisuse/hirmuga toiminguid
4.4 Enne sõnumi usaldamist kasutage e-kirja sisu kohta lisateabe saamiseks otsingumootorit
4.5 Kontrollige potentsiaalselt andmepüügiga seotud URL-id, kasutades tasuta andmepüügi tuvastamise tööriistu
4.6 Kustutage teile saadetud meil, kui olete kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs

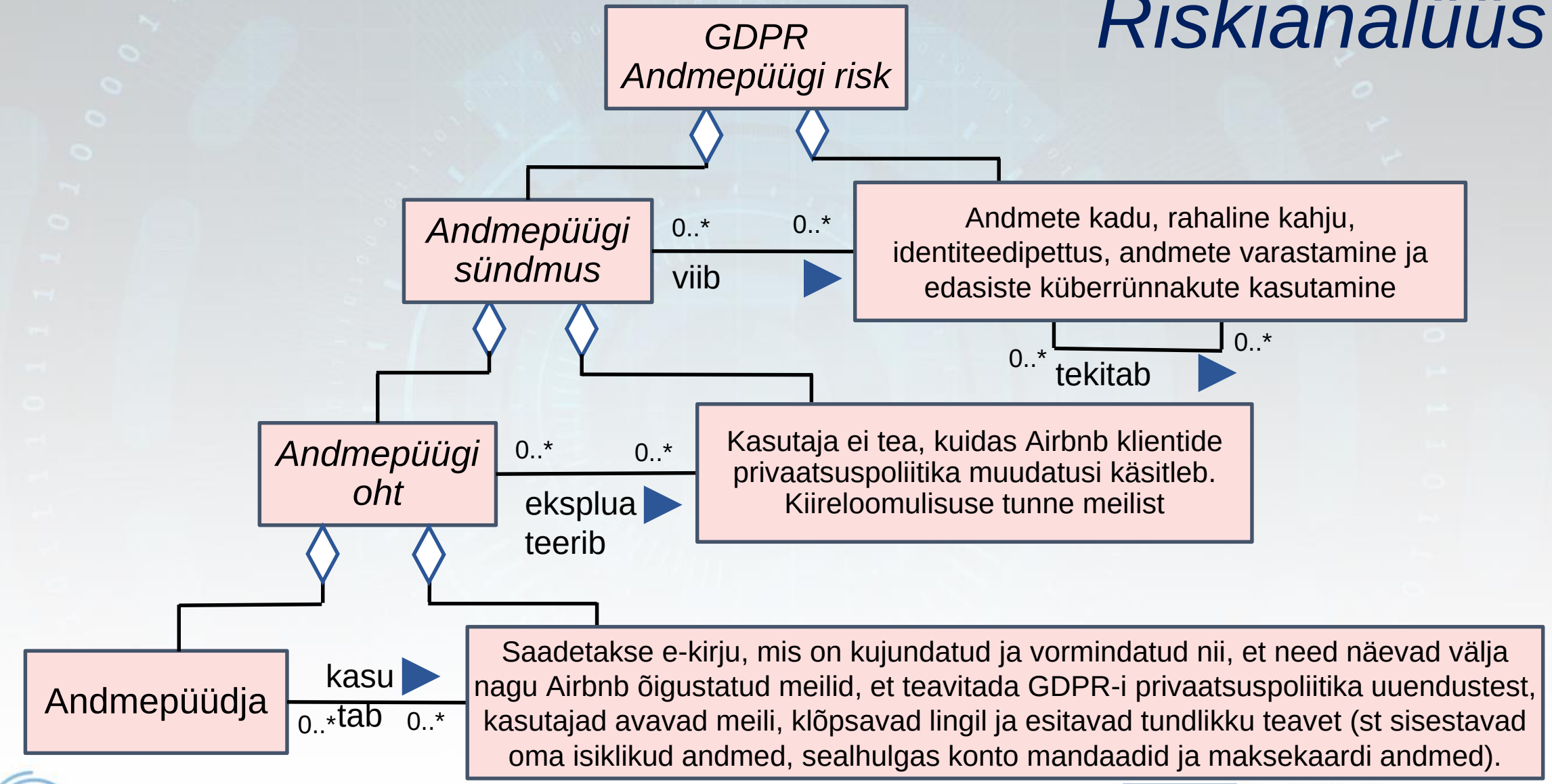


GDPR Phishing Email (Source: Securityaffairs)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



GDPR Phishing Email (Source: Databreachtoday)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit linkide kohal ja analüüsige, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti nähtava sisuga

1. Mõistab andmepüüki
Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum tuleb? [teadmata]
b. Mis on sõnumi sisu? GDPR uuendused
c. Kas sisaldab linke/manuseid? *Jah*

Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märke
3.1 Seaduslikud ettevõtted käsitlevad privaatsus-poliitika lepinguid otse veebisaidil või rakenduses
3.2 Ettevõtted oma klientidele saadavad GDPR-i teatised ei küsi kasutaja sisselogimise andmeid.

4. Kriitiline mõtlemine
4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Olge hüperlinkide/manuste suhtes ettevaatlik; nad võivad viidata pahatahtlikule ressursile
4.3 Kontrollige saatja e-posti aadressi lahknevuste suhtes, mis viitavad pettusele (vt Airbnb loendit)
4.4 Vaadake lisateavet meili sisu kohta ametlikul Airbnb veebisaidil
4.5 Kontrollige potentsiaalselt andmepüügiga seotud URL-id, kasutades tasuta andmepüügi tuvastamise tööriistu
4.6 Kustutage teile saadetud meil, kui olete kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

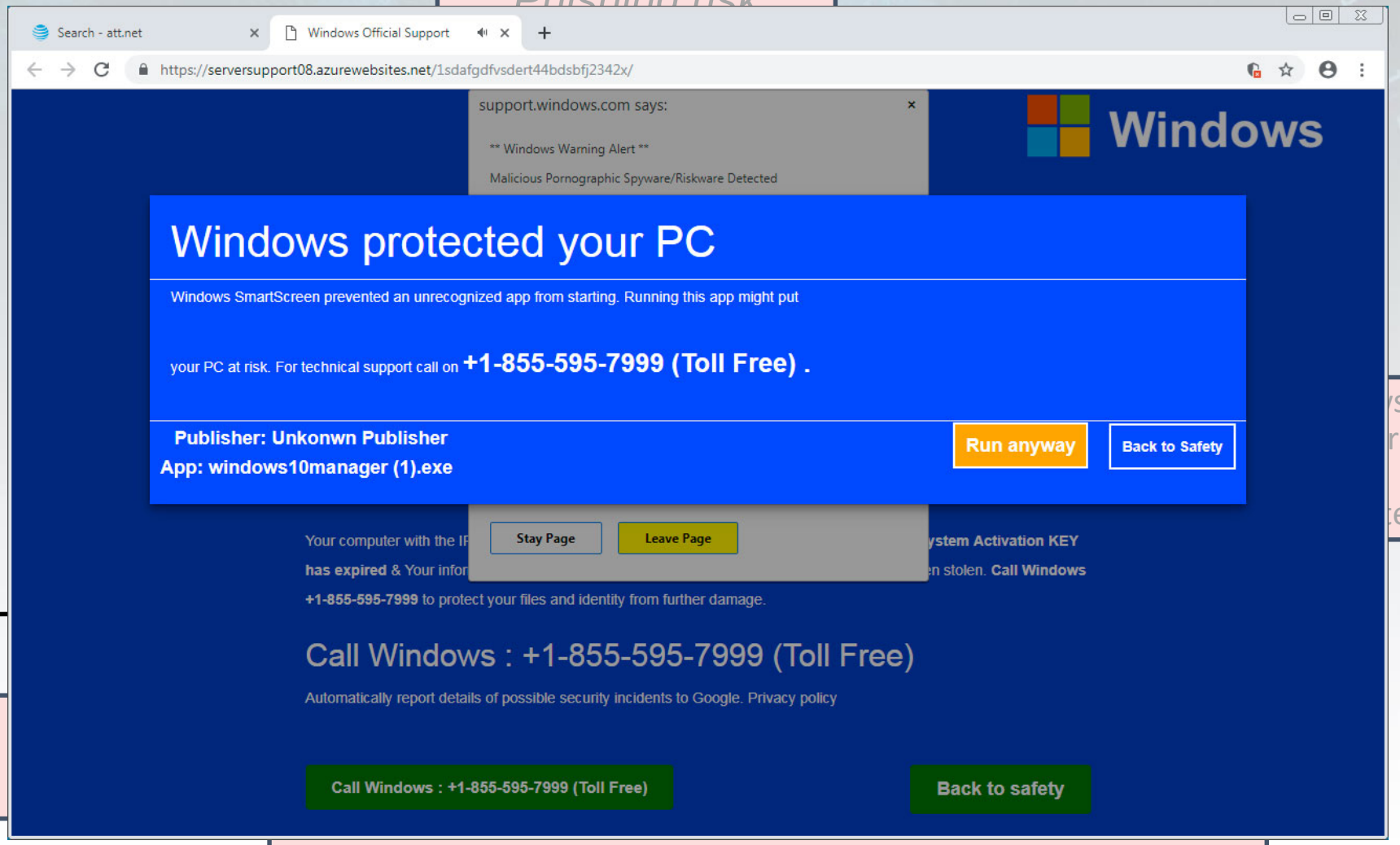
Tehnilise toe rünnakud

- Tehnilise toe pettuste puhul väidab pettur, et pakub seaduslikku tehnilise toe teenust ja võib ohvrite tähelepanu äratamiseks kasutada erinevaid taktikaid, sealhulgas külmkõnesid, veebisaidi hüpikaknaid, meilisõnumeid ja SMS-e.
- Kõige populaarsemad kasutatud taktikad, sealhulgas
  - veebisaidi hüpikaknad hoiatavad kasutajat arvutiviiruse eest
  - tehniliste teenuste meilipettused

Funded by the
Erasmus+ Programme
of the European Union

Riskianalüüs

Tech support
Phishing risk

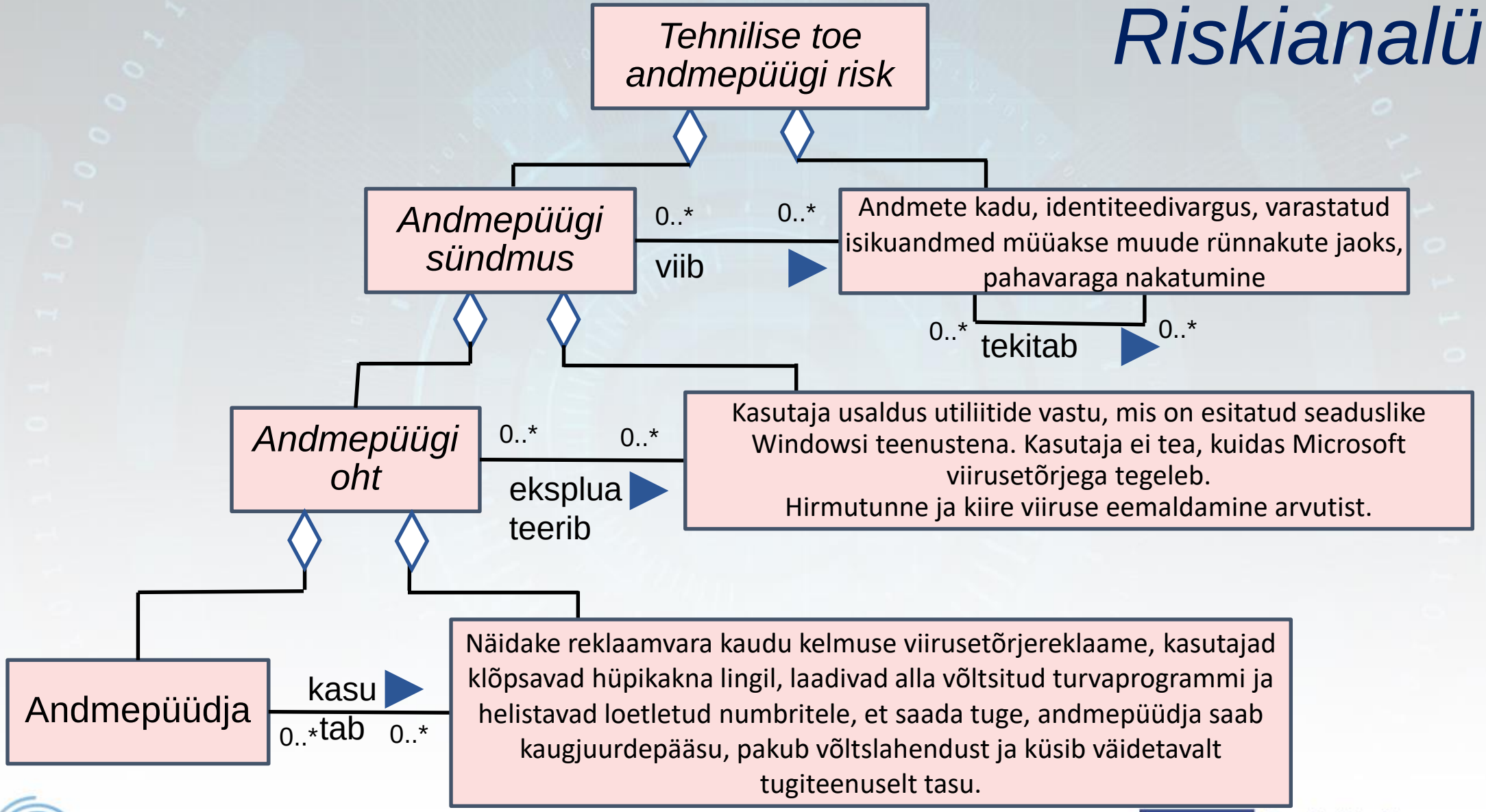


Phisher

Tech Support Phishing Email (Source: Bleepingcomputer)

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



CyberPhish
Safeguarding your digital future

Tech Support Phishing Email (Source: Bleepingcomputer)

Funded by the Erasmus+ Programme of the European Union

Risk tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake tegevusele kutsuvatel hüpikakende nuppudel ega linkidel

1. Mõistab andmepüüki
Andmeüügi allikas: veebileht
Phishing message anatomy:
a. Kellelt sõnum pärineb? *hüpikaken*
b. Mis on teate sisu? *Antiviiruse kaitse*
c. Kas palutakse kasutajal midagi teha? *JAH*

Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märke
3.1 Windowsi kaitsega tegeleb kohalik Windows Defender, mitte veebilehekülg
3.2 Microsoft ei saada veebisaitidele soovimatuid hüpikaknaid
3.3 Te ei saa telefoninumbril Windowsile helistada

4. Kriitiline mõtlemine
4.1 Olge ettevaatlik kõigi ootamatute hüpikakende suhtes veebisaitidel, ärge klõpsake ootamatutel hüpikakendel ja blokeerige hüpikaknad võimaluse korral
4.2 Olge ettevaatlik, kui hüpikaknad nõuavad kiireloomulisuse/hirmuga toiminguid
4.3 Ärge kunagi andke telefoni või meili teel "kinnitamiseks" konto parooli ega sisselogimisandmeid
4.4 Sulgege kahtlase hüpikakna genereeriv veebisait

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs

Tech support

Amazon.com - Your Cancellation 173-222723-2163799

order-update@amazon.com
Today, 5:27 AM
You

Reply

This message was identified as spam. We'll delete it after 10 days. It's not spam

Your order has been successfully canceled.
For your reference, here's a summary of your order:

You just canceled order 173-222723-2163799 placed on June 26, 2017.

Status: CANCELED

1 of The Optometry.
By: Phaedon Wallace

Sold by: Amazon.com LLC

Sources Network Performance Memory Application Security Audits

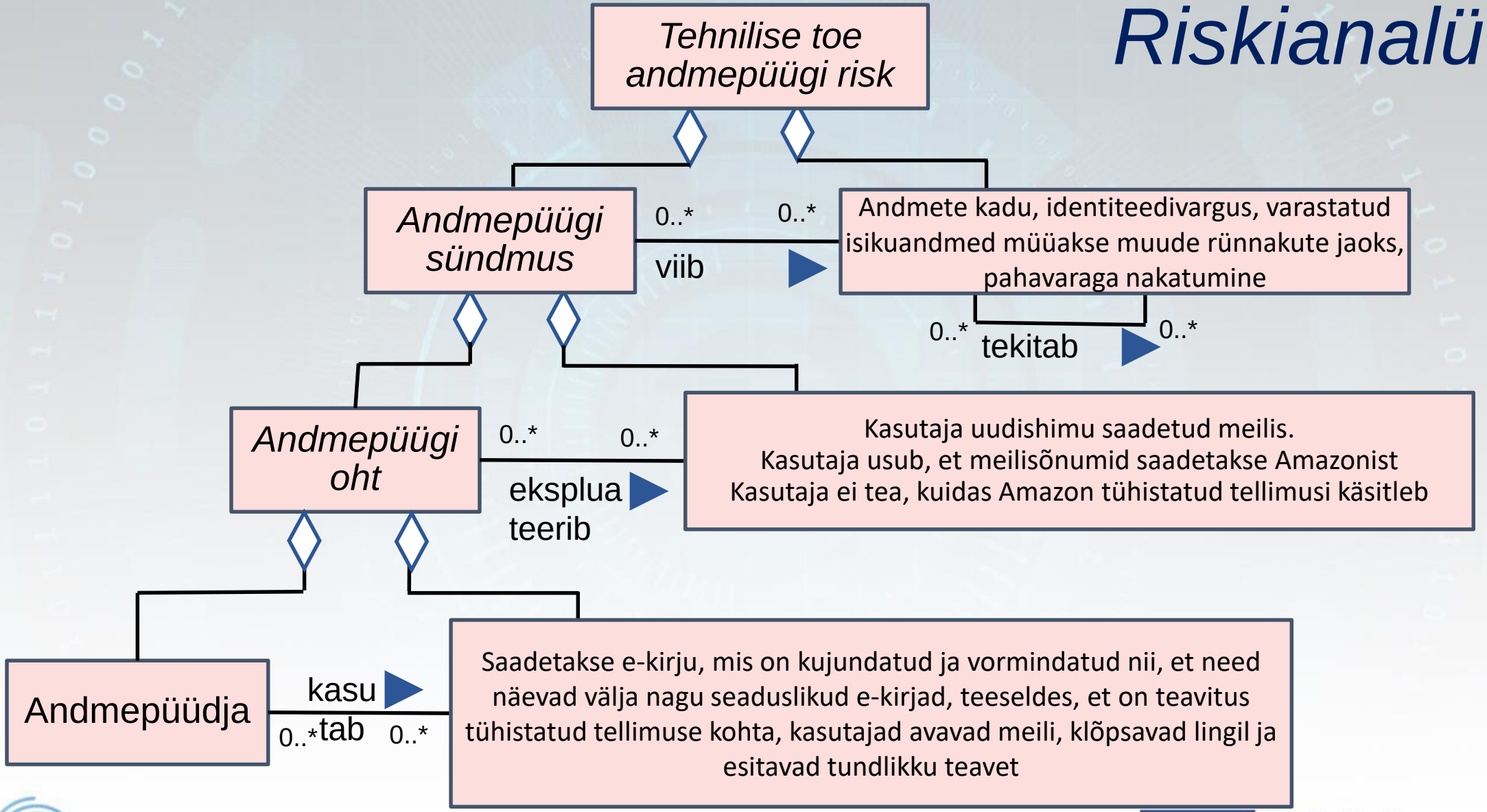
173-222723-2163799

Tech Support Phishing Email (Source: vk-intel)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



Tech Support Phishing Email (Source: Bleepingcomputer)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti sisuga

1. Mõistab andmepüüki

Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? "*order-update@amazon.com*"
b. Mis on sõnumi sisu? *Cancelled Amazon order*
c. Kas sõnum sisaldab hüperlinke/manuseid? *JAH*

Andmepüügir ünnakute äratundmine

3. Ohu märkide tuvastamine

3.1 Amazoni seaduslikud meilid kutsuvad teid teie nime järgi
3.2 Õiguspärased teenusemeilid on professionaalsed ja ühtse vorminguga.
3.3 Pange tähele, et URL-i tee viitab aadressile „http://www.cuinavo.com/maritime.php", mitte Amazoni ressursile
3.4 Amazon saadab tellimuse tühistamise meili aadressilt „order-update@amazon.com" seadusliku Amazoni meili, kuid meilivorming pole professionaalne. Tõenäoliselt on meilisõnum võltsitud

4. Kriitiline mõtlemine

4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Isegi kui see tundub olevat õigustatud, minge oma tegelikule kontole ettevõtte seaduslikul veebisaidil, nt „amazon.com", et kontrollida kõiki probleeme.
4.3 Olge ettevaatlik, kuna sellised meilipetturid võivad ära kasutada teie uudishimu ja ahnust
4.4 Otsige üles potentsiaalselt andmepüügiga seotud URL-e, kasutades tasuta andmepüügi tuvastamise tööriistu
4.5 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".
4.6 Kustutage teile saadetud meil, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik

1. Mõistab andmepüüki

Andmepüügi allikas: Email

Andmepüügi sõnumi anatoomia:

a. Kellelt sõnum pärineb? "*order-update@amazon.com*"
b. Mis on sõnumi sisu? *Cancelled Amazon order*
c. Kas sõnum sisaldab hüperlinke/manuseid? *JAH*

3. Ohu märkide tuvastamine

3.1 Amazoni seaduslikud meilid kutsuvad teid teie nime järgi
3.2 Õiguspärased teenusemeilid on professionaalsed ja ühtse vorminguga.
3.3 Pange tähele, et URL-i tee viitab aadressile „http://www.cuinavo.com/maritime.php", mitte Amazoni ressursile
3.4 Amazon saadab tellimuse tühistamise meili aadressilt „order-update@amazon.com" seadusliku Amazoni meili, kuid meilivorming pole professionaalne. Tõenäoliselt on meilisõnum võltsitud

4. Kriitiline mõtlemine

4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Isegi kui see tundub olevat õigustatud, minge oma tegelikule konto kõiki probleeme.
4.3 Olge ettevaatlik, kuna sellised meilipetturid võivad ära kasutada tei
4.4 Otsige üles potentsiaalselt andmepüügiga seotud URL-e, kasutades tasuta andmepüügi tuvastamise tööriistu
4.5 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".
4.6 Kustutage teile saadetud meil, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manustel ega linkidel
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti sisuga

1. Mõistab an
Andmepüügi allika
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? "*order-update@amazon.com*"
b. Mis on sõnumi sisu? *Cancelled Amazon ord*
c. k
JAI
? Ye

ünnakute äratundmine

ime järgi
3.2 Olgusparased teenusemeilid on professionaalsed ja ühtse vorminguga.
3.3 Pange tähele, et URL-i tee viitab aadressile „http://www.cuinavo.com/maritime.php", mitte Amazoni ressursile
ole

4. Kriitiline mõtlemine

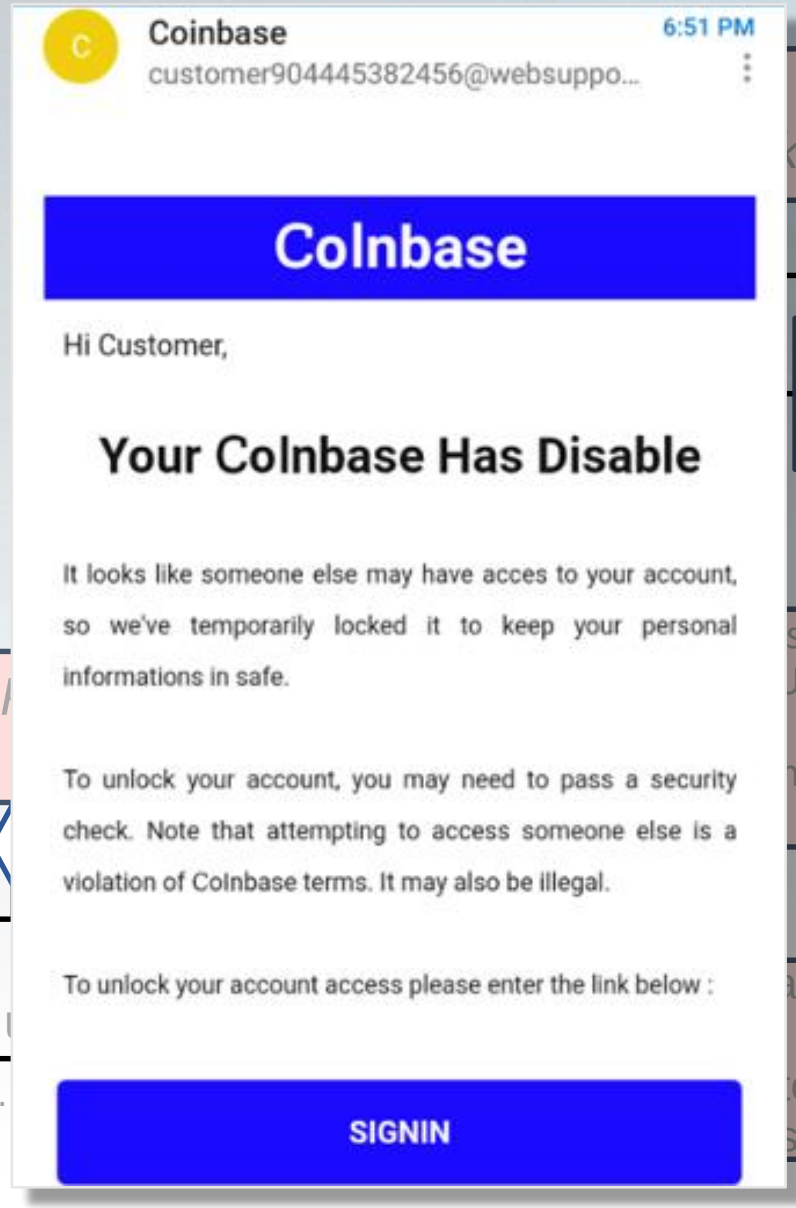
4.1 Veenduge, et e-kiri pärineb usaldusväärsest ja oodatud allikast
4.2 Isegi kui see tundub olevat õigustatud, minge oma tegelikule kontole ettevõtte seaduslikul veebisaidil, nt „amazon.com", et kontrollida kõiki probleeme.
4.3 Olge ettevaatlik, kuna sellised meilipetturid võivad ära kasutada teie uudishimu ja ahnust
4.4 Otsige üles potentsiaalselt andmepüügiga seotud URL-e, kasutades tasuta andmepüügi tuvastamise tööriistu
4.5 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".
4.6 Kustutage teile saadetud meil, kui olete piisavalt kindel, et tegemist on andmepüügiga

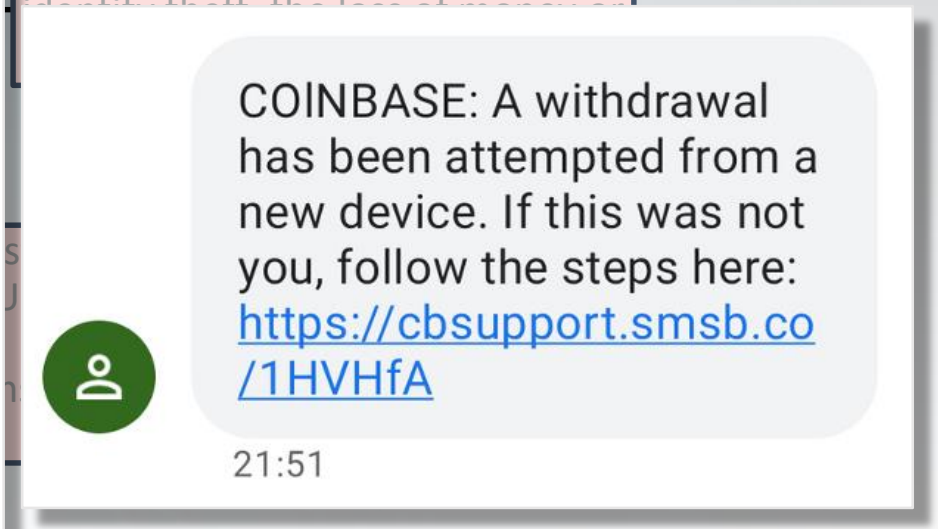
Krüptovaluuta pettused

- Kuna Bitcoini ja teiste krüptovaluutade hind ja populaarsus tõusid, tekkis häkkerite ja küberkurjategijate huvi selle varastamise vastu.
- Ründajad saavad andmepüügi abil kehastuda populaarsete krüptovaluutabörside (nt Binance, Huobi Global või Coinbase) esindajatena

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs





Data loss, reputational damage,

Phisher

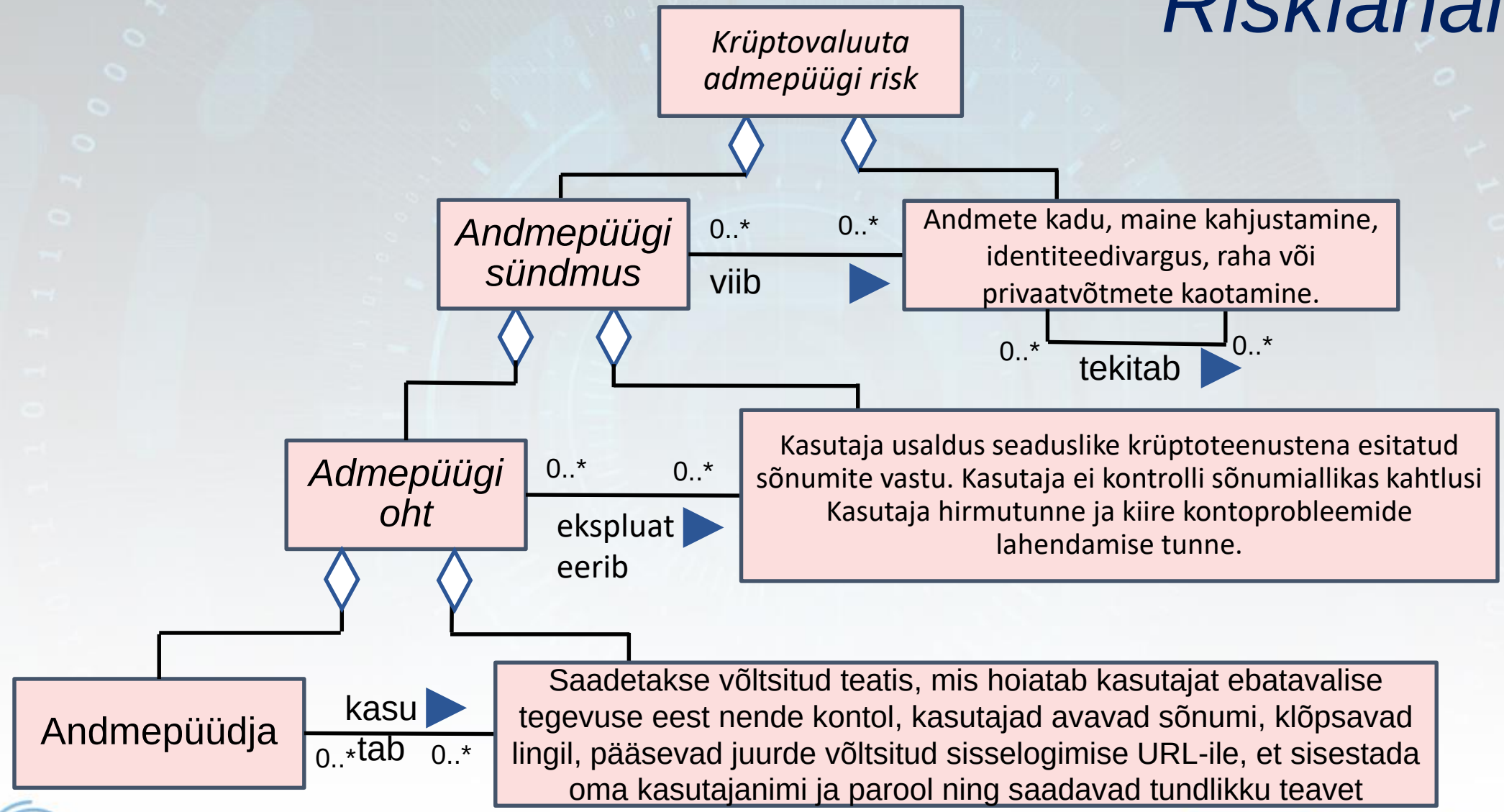
rns user of unusual activity in message, clicks on the link, o enter their username and sensitive information

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

Riskianalüüs



CyberPhish
Safeguarding your digital future

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

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manuseid ega linke
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti sisuga

1. Mõistab andmepüüki

Andmepüügi allikas: Email, SMS
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? *"...@websupport.com", SMS telefoni number*
b. Mis on sõnumi sisu? *Account disable notification, Withdrawal notice (mure kontoga, oht raha kaotada)*
c. Kas sisaldab hüperlinke/manuseid? JAH

Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märgid

3.1 Õiguspärastest rakendustest pärinevad sõnumid kutsuvad teid teie nime järgi
3.2 Õiguspärased sõnumid on professionaalsed ja hästi vormindatud
3.3 Õiguspärased sõnumid ei sisalda kirjavigu, st "Coinbase" asemel kasutatakse "CoInbase", "Teie CoInbase on keelatud" või "SIGNIN".
3.4 Coinbase'i seaduslik meilidomeen on "...@coinbase.com", mitte "...@websupport.com"

4. Kriitiline mõtlemine

4.1 Kontrollige veelkord saatja aadressi, Coinbase'i seaduslike e-kirjade e-posti aadressid peaksid lõppema .coinbase.com
4.2 Konto või maksega seotud probleemide korral pöörduge otse Coinbase'i klienditoe poole
4.3 Olge ettevaatlik, kuna seda tüüpi petturid kasutavad ära teie hirmu ja kiireloomulisust
4.4 Turvateabe ristkontrollimine seadusliku teenuse veebisaidil
4.5 Ärge kunagi klõpsake tundmatutest allikatest pärinevatel linkidel/manustel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil
4.6 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".
4.7 Kustutage teile saadetud meil, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

1. Mõistab andmepüüki

Andmepüügi allikas: Email, SMS

Andmepüügi sõnumi anatoomia:

a. Kellelt sõnum pärineb? *"...@websupport.com", SMS telefoni number*

b. Mis on sõnumi sisu? *Account disable notification, Withdrawal notice (mure kontoga, oht raha kaotada)*

c. Kas sisaldab hüperlinke/manuseid? JAH

2. Mõistab URLe

2.1 Ärge klõpsake manuseid ega linke

2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik

3. Tuvastab ohu märgid

3.1 Õiguspärastest rakendustest pärinevad sõnumid kutsuvad teid teie nime järgi

3.2 Õiguspärased sõnumid on professionaalsed ja hästi vormindatud

3.3 Õiguspärased sõnumid ei sisalda kirjavigu, st "Coinbase" asemel kasutatakse "CoInbase", "Teie CoInbase on keelatud" või "SIGNIN".

3.4 Coinbase'i seaduslik meilidomeen on "...@coinbase.com", mitte "...@websupport.com"

4.3 Olge ettevaatlik, kuna seda tüüpi petturid kasutavad ära teie hirmu

4.4 Turvateabe ristkontrollimine seadusliku teenuse veebisaidil

4.5 Ärge kunagi klõpsake tundmatutest allikatest pärinevatel linkidel/manustel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil

4.6 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".

4.7 Kustutage teile saadetud meil, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manuseid ega linke
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti sisuga

1. Mõistab andm
Andmepüügi allikas: Em
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? "*...@websupport.com*", *SMS telefoni number*
b. Mis on sõnumi sisu? *Account disable notification, Withdrawal notice (mure kontoga, oht raha kaotada)*
c. Kas

ünnakute äratundmine

sõnumid kutsuvad teid teie
hiime järgi
3.2 Õiguspärased sõnumid on professionaalsed ja hästi vormindatud
3.3 Õiguspärased sõnumid ei sisalda kirjavigu, st "Coinbase" asemel kasutatakse "CoInbase", "Teie CoInbase on keelatud" või "SIGNIN".
3.4 Coinbase'i seaduslik meilidomeen on "...@coinbase.com", mitte

4. Kriitiline mõtlemine
4.1 Kontrollige veelkord saatja aadressi, Coinbase'i seaduslike e-kirjade e-posti aadressid peaksid lõppema .coinbase.com
4.2 Konto või maksega seotud probleemide korral pöörduge otse Coinbase'i klienditoe poole
4.3 Olge ettevaatlik, kuna seda tüüpi petturid kasutavad ära teie hirmu ja kiireloomulisust
4.4 Turvateabe ristkontrollimine seadusliku teenuse veebisaidil
4.5 Ärge kunagi klõpsake tundmatutest allikatest pärinevatel linkidel/manustel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil
4.6 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks**".**
4.7 Kustutage teile saadetud meil, kui olete piisavalt kindel, et tegemist on andmepüügiga

Väljapressimispettused

- Väljapressimispettused on kahjuks tulemas tagasi, kus petturid ja häkkerid pääsevad ligi rikkumiste andmetele ja ohustavad ohvreid "Ma tean teie parooli".
- Ründajad võivad ka väita, et on pääsenud juurde teie arvutile ja selle kaamerale, hankinud teist seksuaalselt vulgaarset videot või pilte ning isegi panna teid maksma Bitcoiniga.

Funded by the
Erasmus+ Programme
of the European Union

Riskianalüüs

Extortion

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)

cause of

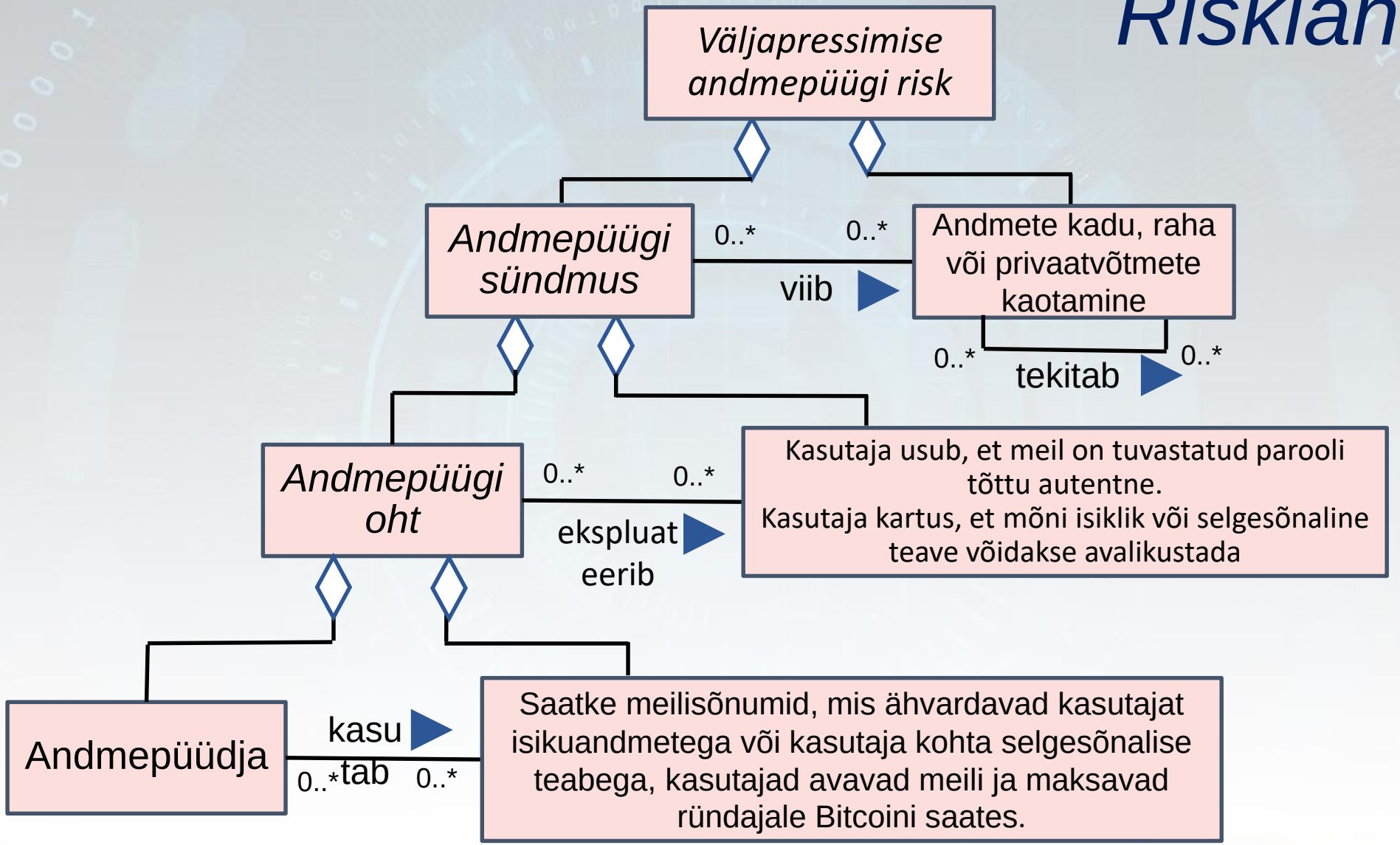
nal or
ublic

Phisher

Extortion Phishing Email (Source: MailOnline)

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



Extortion Phishing Email (Source: MailOnline)

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manuseid ega linke
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti sisuga

1. Mõistab andmepüüki
Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? "*...@outlook.com*"
b. Mis on sõnumi sisu? *Sex extortion*
c. Kas sisaldab hüperlinke/manuseid? *JAH*

3. Tuvastab ohu märgid
3.1 Enamasti on meilid tühjad ähvardused ja mitte kasutaja häkkimise tõttu
3.2 Ründaja võis hankida tundlikku teavet andmetega seotud rikkumise, lekke või Internetis avalikult kättesaadavatest andmebaasidest

4. Kriitiline mõtlemine
4.1 Olge ettevaatlik, kuna need meilipetturid võivad teie hirmu ja häbi ära kasutada
4.2 Kontrollige, kas teie e-posti aadressi on ohustatud veebisaitidel, nt haveibeenpwned.com või dehashed.com
4.3 Kui parool on endiselt kasutusel, on oluline neid kontosid kaitsta (muutke ära parool)
4.4 Kui olete piisavalt kindel, et tegemist on andmepüügiga, kustutage teile saadetud meil

Funded by the
Erasmus+ Programme
of the European Union

Ettemaksupettused

- Ettemaksupettused on COVID-pandeemia ajal endiselt tugevad, kuna inimesed on sattunud rasketesse aegadesse. Need andmepüügirünnakud leiavad aset siis, kui välismaal asuv kurjategija pakub osa suurest rahasummast, et aidata neil raha oma riigist välja kanda.
- Selleks küsivad nad teie pangateavet või teilt teenustasu, kompensatsiooni või maksude hüvitamist.

Funded by the
Erasmus+ Programme
of the European Union

Risk Analysis

[SPAM]ATN International Credit Settlement

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

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

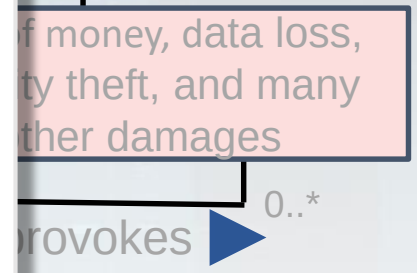
To: dave@d

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;

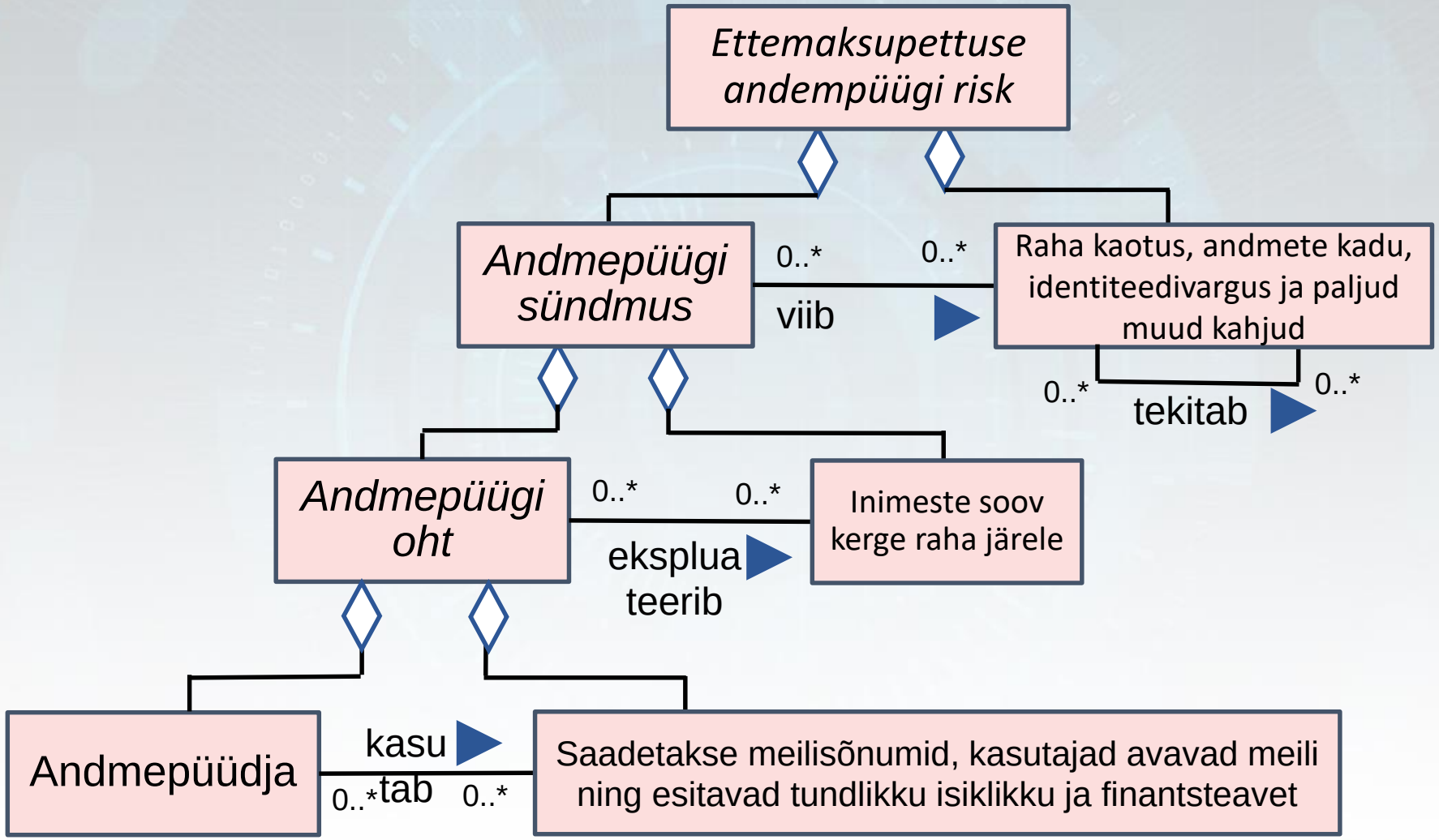
Daiwa Bank R/Osaka/Japan.
Caja De Madrid/Madrid/Spain.
Lloyds Bank R /London/England.
Central Bank of Nigeria/Lagos/Nigeria.
Banco di Santo Spirito/Rome/Italy.
Bank of New York Mellon Corp/New York/USA.



Extortion Phishing Email (Source: Massmoola)

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



CyberPhish
Safeguarding your digital future

Extortion Phishing Email (Source: Massmoola)

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge järgige e-kirjas olevaid juhiseid

1. Mõistab andmepüüki
Andmepüügi allikas: Email
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? *Central Bank of Nigeria*
b. Mis on sõnumi sisu?
Credit settlement
c. Kas sisaldab hüperlinke/manuseid? *EI*

Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märgid
3.1 Kui keegi pakub teile tasuta raha, on see tavaliselt liiga ilus, et tõsi olla
3.2 Pankade seaduslikud teenusemeilid on professionaalsed, ühtse mallivorminguga ja ei saada soovimatuid e-kirju

4. Kriitiline mõtlemine
4.1 Ärge kunagi andke pangateavet kellelegi, kellega te pole kunagi kohtunud
4.2 Olge ettevaatlik, kuna sellised meilipetturid võivad ära kasutada teie uudishimu ja ahnust
4.3 Kui olete piisavalt kindel, et tegemist on andmepüügiga, kustutage teile saadetud meil

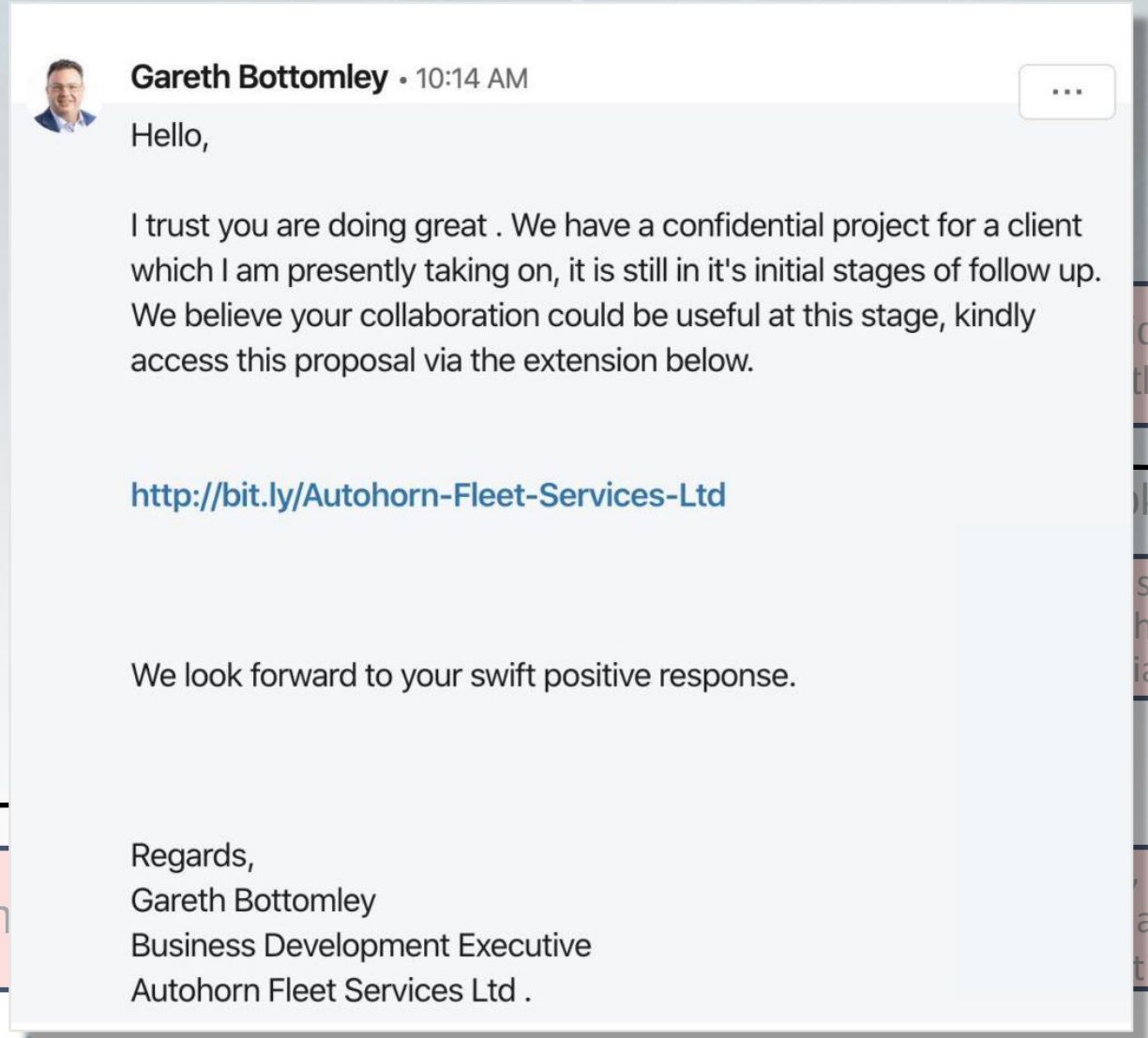
Funded by the Erasmus+ Programme of the European Union

Sotsiaalmeedia pettused

- Siin kasutavad ründajad sotsiaalmeedia saite, nagu Facebook, LinkedIn või Twitter, et meelitada kasutajaid klõpsama pahatahtlikel linkidel või avaldama isiklikku teavet.
- Samuti võivad ründajad leida sotsiaalmeediast ohtralt teavet potentsiaalsete ohvrite kohta, et alustada sihipärast rünnakut.

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



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 .

dentity theft,
ther damages

0..*

kes

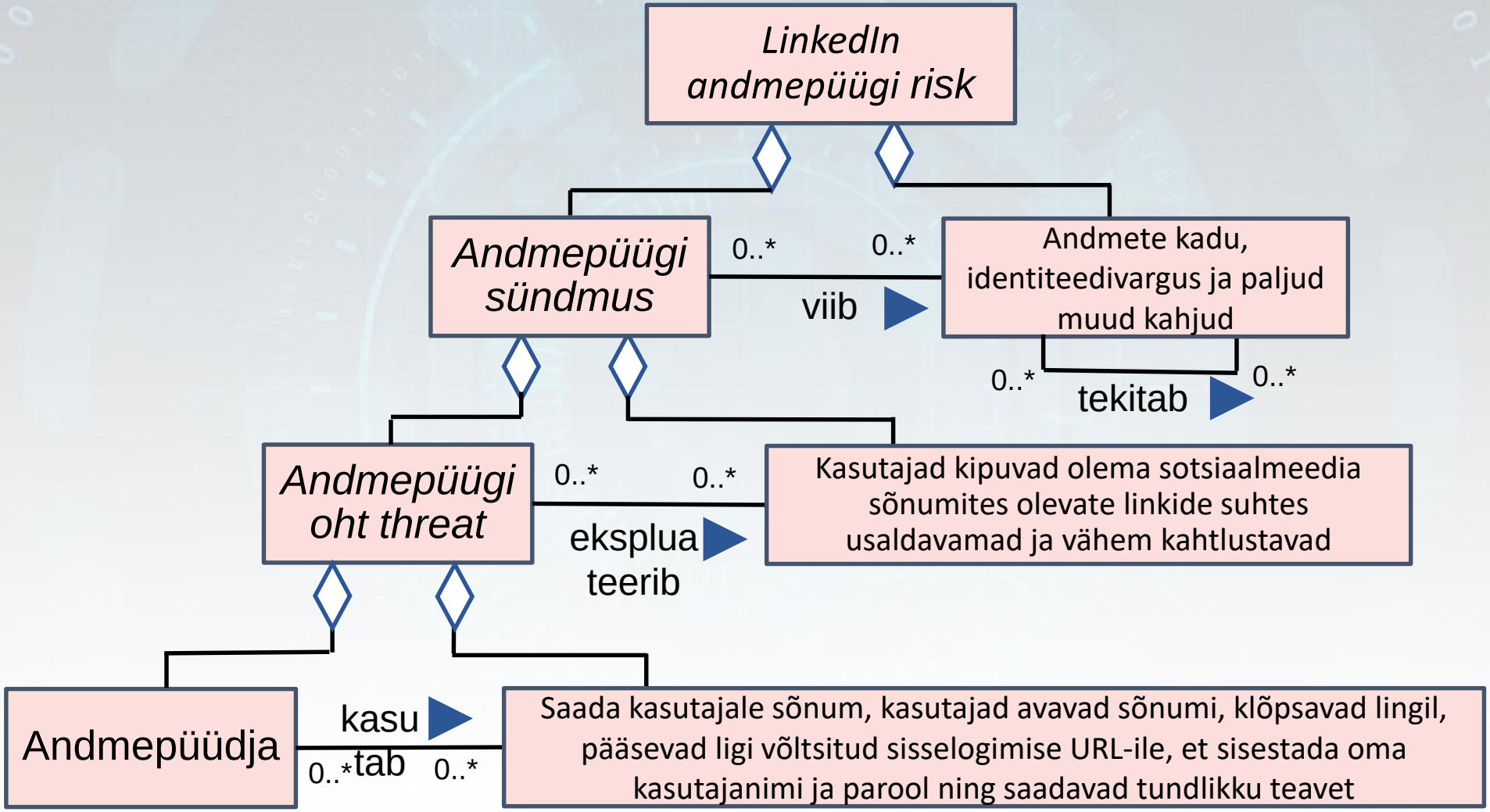
sting and less
hin messages
ia

Phish

, clicks on the link,
ame and password
tion

Extortion Phishing Email (Source: LinkedInTraining)

Riskianalüüs

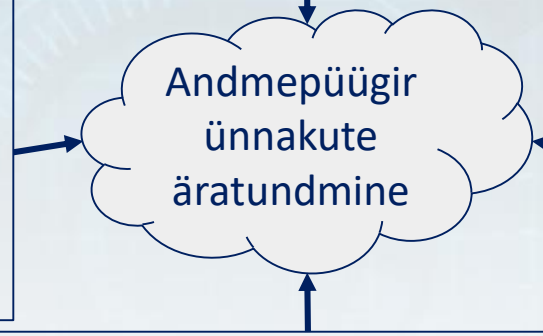


Extortion Phishing Email (Source: LinkedInTraining)

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manuseid ega linke
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtliks

1. Mõistab andmepüüki
Andmepüügi allikas: Sotsiaalmeedia sõnum
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? *LinkedIn Kasutaja*
b. Mis on sõnumi sisu? *Koostöö pakkumine*
c. Kas sisaldab hüperlinke/manuseid? *JAH*

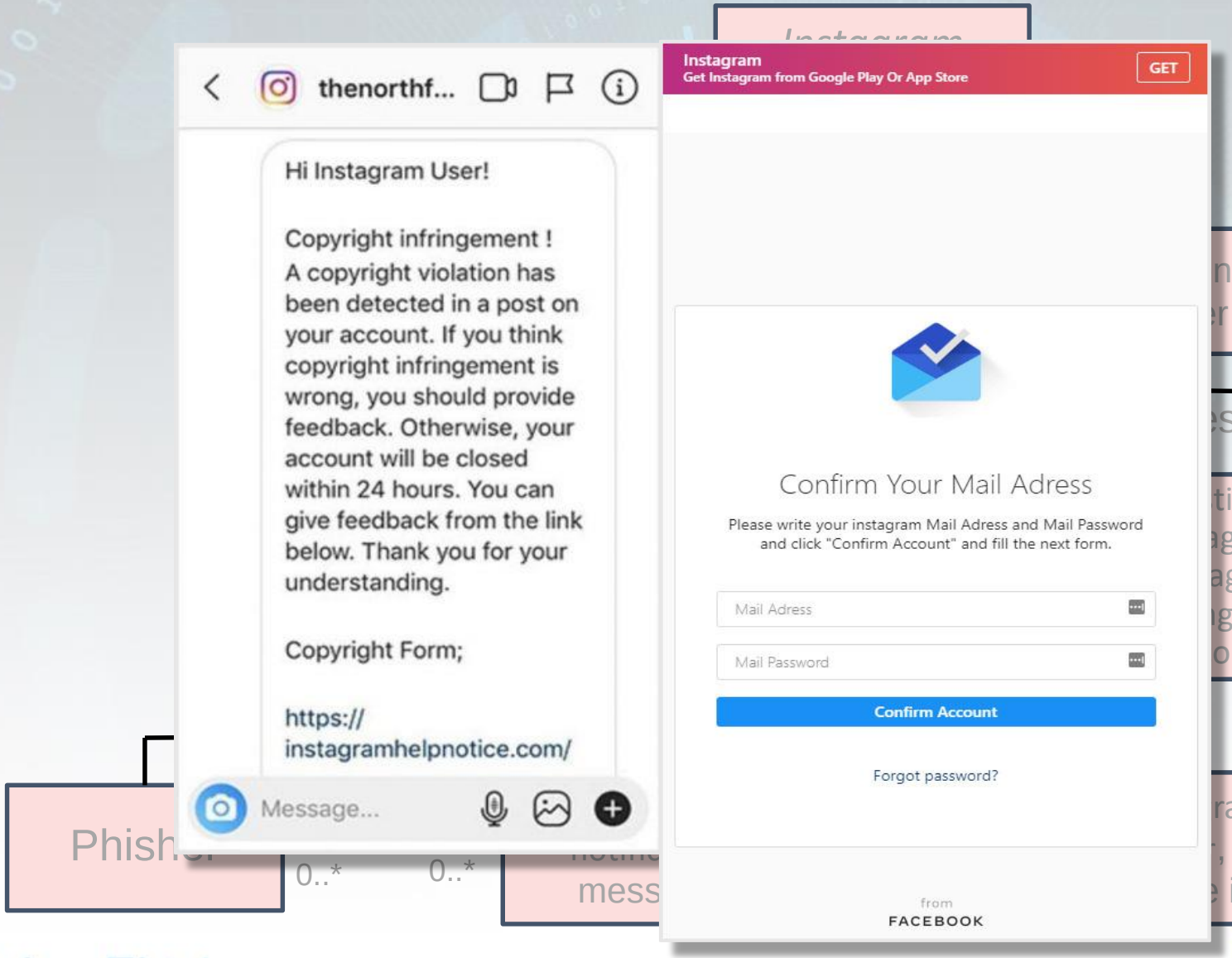


3. Tuvastab ohu märgid
3.1 Kui keegi tundmatu pakub koostööd, on see tõenäoliselt kahtlane
3.2 Ründajad kasutavad andmepüügilinkide lühendamiseks ja peitmiseks URL-i lühendamisteenuseid (nt bit.ly).

4. Kriitilien mõtlemine
4.1 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvaliste osade kinnitamiseks
4.2 Isegi kui tundub, et sõnum on pärit kelleltki, keda te usaldate, on tõenäoline, et tema konto on rünnatud
4.3 Kasutage sotsiaalmeedias alati täiustatud privaatsusseadeid
4.4 Ärge klõpsake DM-ides kahtlastel linkidel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil
4.5 Ärge kunagi võtke vastu LinkedIni ühenduse taotlusi kelleltki, kellega te pole tuttav
4.6 Olge ettevaatlik, kui jagate sotsiaalmeedias liiga palju isiklikku teavet
4.7 Katkestage/blokeerige kahtlased kontod ja kustutage teile saadetud sõnum, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the
Erasmus+ Programme
of the European Union

Riskianalüüs

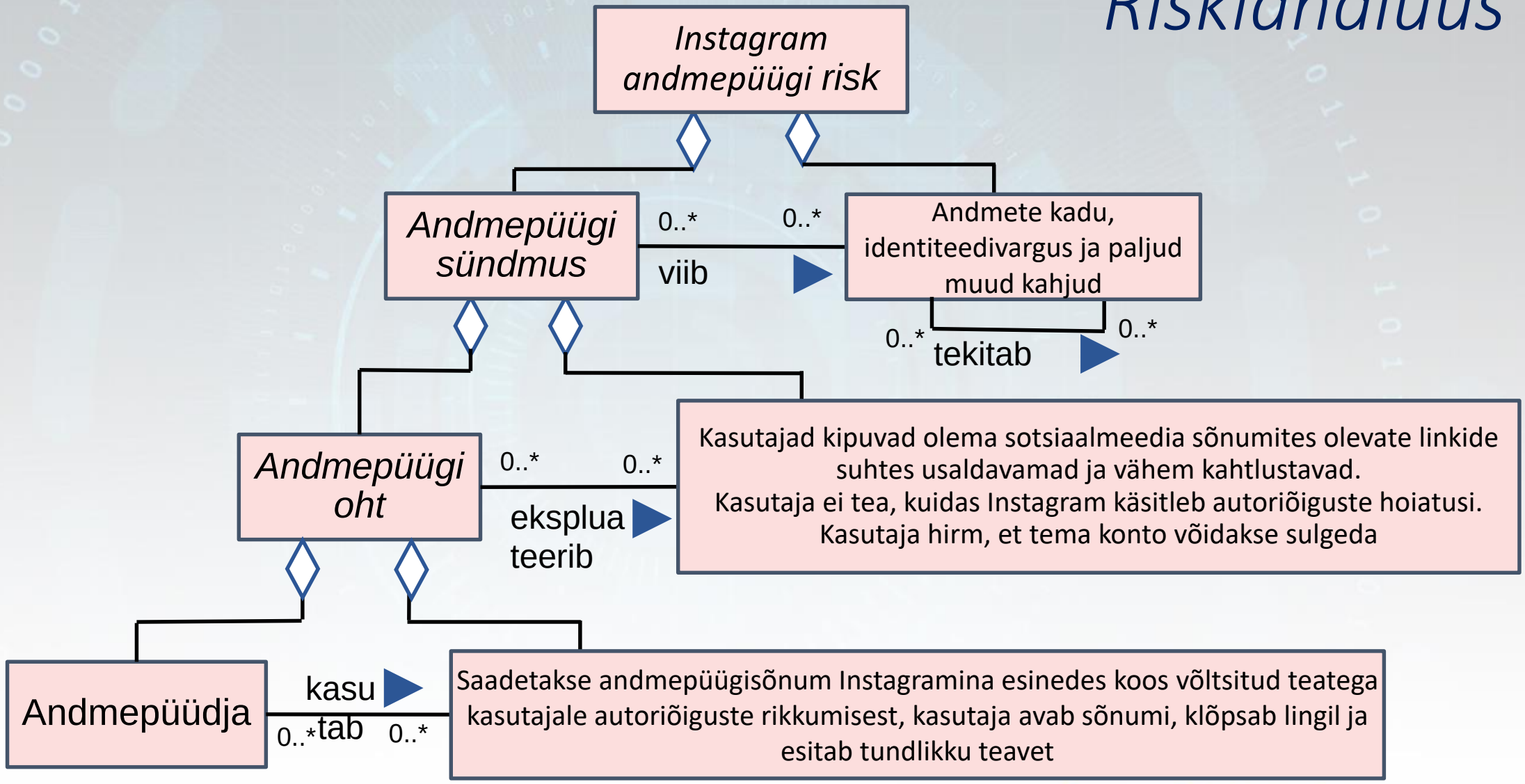


Social Media Phishing Email (Source: Hackread)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



CyberPhish
Safeguarding your digital future

Social Media Phishing Email (Source: Hackread)

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manuseid ega linke
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti platvormi domeeniga

1. Mõistab andmepüüki

Andmepüügi allikas: Direct message
Andmepüügi sõnumi anatoomia:
a. Kellelt sõnum pärineb? *Instagram kasutaja*
b. Mis on sõnumi sisu? *Copyright rikkumine*
c. Kas sisaldab hüperlinke/manuseid? *JAH*

Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märgid

3.1 Õigustatud autoriõiguse nõuete teatised saadab Instagram isiklikult
3.2 Instagram kasutab teie poole pöördumiseks alati teie kontole registreeritud nime
3.3 Esitatud link peaks ühtima platvormi domeeniga, st "instagram.com", mitte "instagramhelpnotice.com"

4. Kriitiline mõtlemine

4.1 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".
4.2 Isegi kui tundub, et sõnum on pärit kelleltki, keda te usaldate, on tõenäoline, et tema konto on rünnatud
4.3 Kasutage sotsiaalmeedias alati täiustatud privaatsusseadeid
4.4 Ärge klõpsake DM-ides kahtlastel linkidel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil
4.5 Olge ettevaatlik, kui saadate sõnumeid kasutajatele, keda te ei tunne ja keda te ei jälgi
4.6 Katkestage/blokeerige kahtlased kontod ja kustutage teile saadetud sõnum, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manuseid ega linke

2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik

2.3 Olge ettevaatlik, kui URL-i tee ei ühti platvormi domeeniga

1. Mõistab andmepüüki

Andmepüügi allikas: Direct message

Andmepüügi sõnumi anatoomia:

a. Kellelt sõnum pärineb? *Instagram kasutaja*

b. Mis on sõnumi sisu? *Copyright rikkumine*

c. Kas sisaldab hüperlinke/manuseid? *JAH*

3. Tuvastab ohu märgid

3.1 Õigustatud autoriõiguse nõuete teatised saadab Instagram isiklikult

3.2 Instagram kasutab teie poole pöördumiseks alati teie kontole registreeritud nime

3.3 Esitatud link peaks ühtima platvormi domeeniga, st "instagram.com", mitte "instagramhelpnotice.com"

4. Kriitiline mõtlemine

4.1 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".

4.2 Isegi kui tundub, et sõnum on pärit kelleltki, keda te usaldate, on tõenäoline, et tema konto on rünnatud

4.3 Kasutage sotsiaalmeedias alati täiustatud privaatsusseadeid

4.4 Ärge klõpsake DM-ides kahtlastel linkidel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil

4.5 Olge ettevaatlik, kui saadate sõnumeid kasutajatele, keda te ei tunne ja keda te ei jälgi

4.6 Katkestage/blokeerige kahtlased kontod ja kustutage teile saadetud sõnum, kui olete piisavalt kindel, et tegemist on andmepüügiga

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe

2.1 Ärge klõpsake manuseid ega linke

2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik

2.3 Olge ettevaatlik, kui URL-i tee ei ühti platvormi domeeniga

1. Mõistab andr

Andmepüügi allika

Andmepüügi sõnumi anatoomia:

a. Kellelt sõnum pärineb? *Instagram kasutaja*

b. Mis on sõnumi sisu? *Copyright rikkumine*

c. K

ünnakute äratundmine

aadab Instagram isikliikult

3.2 Instagram kasutab teie poole pöördumiseks alati teie kontole registreeritud nime

4. Kriitiline mõtlemine

4.1 Andke konto parool või sisselogimisandmed ainult seaduslike veebisaitide turvalistes osades "kinnitamiseks".

4.2 Isegi kui tundub, et sõnum on pärit kelleltki, keda te usaldate, on tõenäoline, et tema konto on rünnatud

4.3 Kasutage sotsiaalmeedias alati täiustatud privaatsusseadeid

4.4 Ärge klõpsake DM-ides kahtlastel linkidel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil

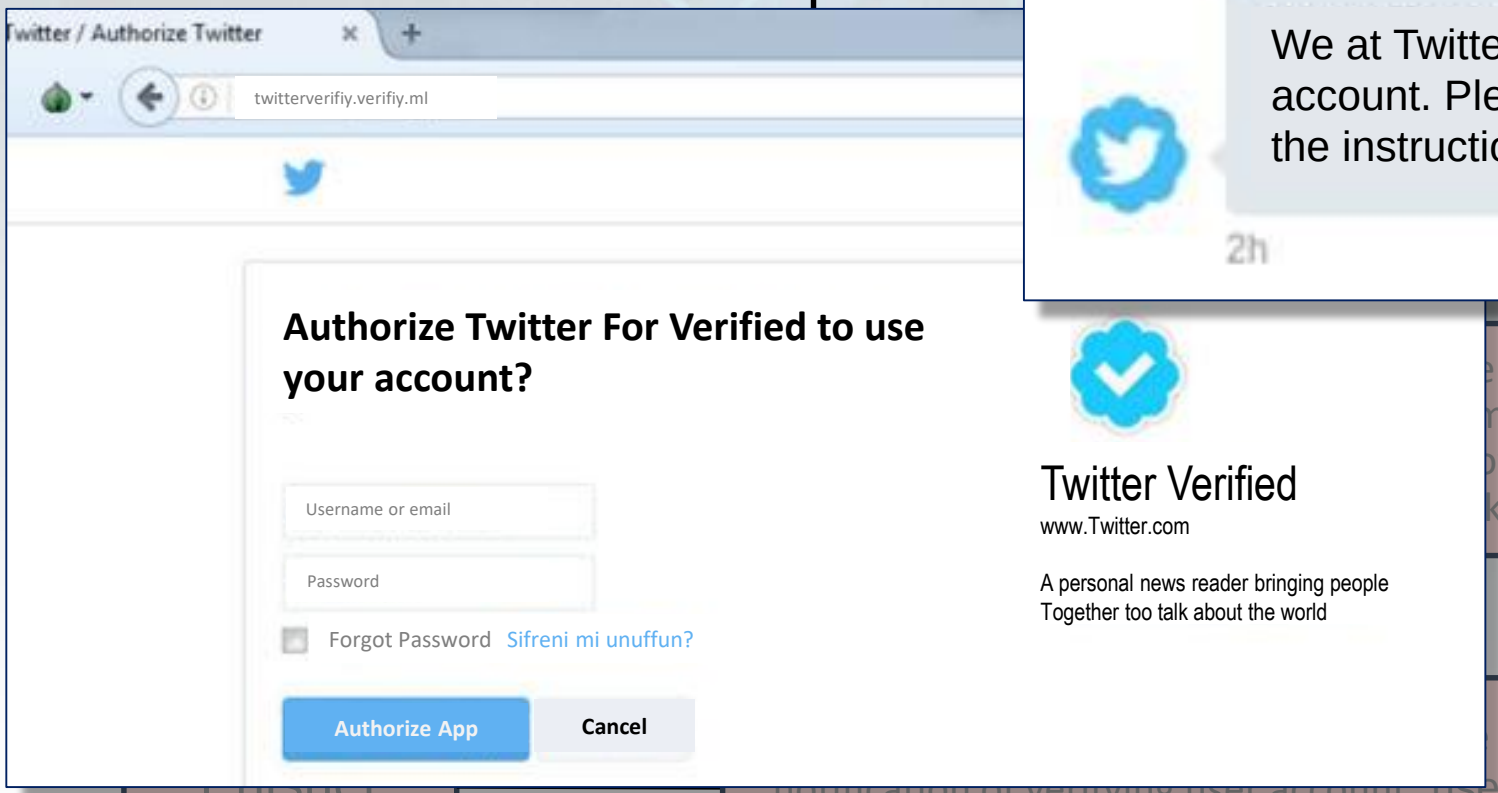
4.5 Olge ettevaatlik, kui saadate sõnumeid kasutajatele, keda te ei tunne ja keda te ei jälgi

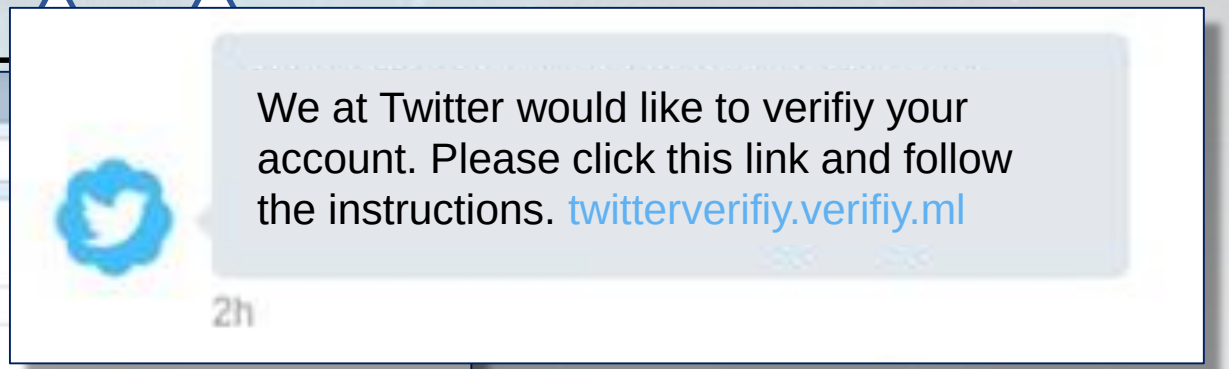
4.6 Katkestage/blokeerige kahtlased kontod ja kustutage teile saadetud sõnum, kui olete piisavalt kindel, et tegemist on andmepüügiga

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs

Twitter phishing risk





Twitter Verified
www.Twitter.com

A personal news reader bringing people
Together too talk about the world

trusting and less suspicious about links
messages on social media.
w twitter handles account verification.
ke verification status on Twitter

Twitter with a fake
r opens message,
clicks link and submit username and password information

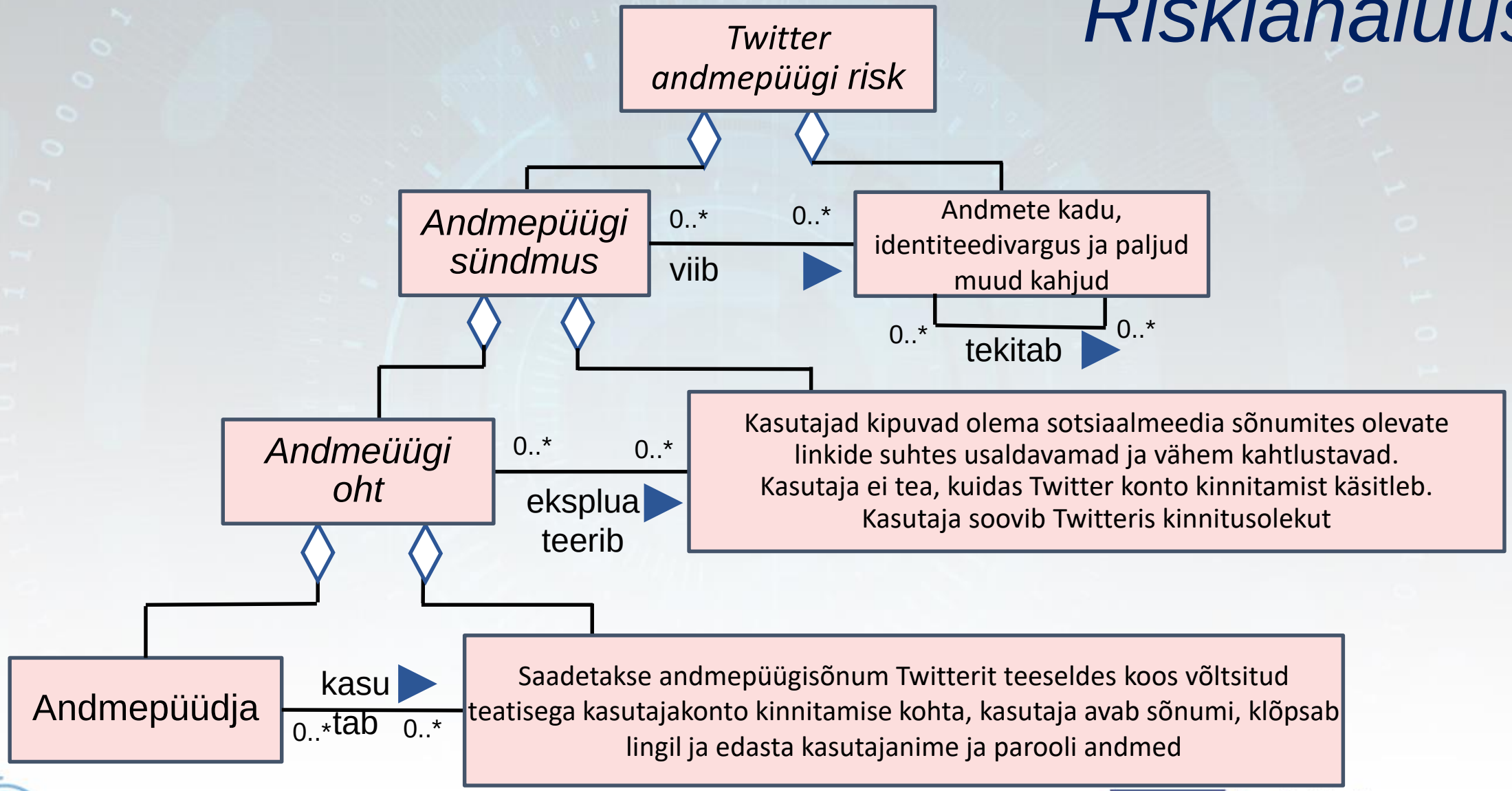
0..*

0..*

Social Media Phishing Email (Source: Malwarebytes)

Funded by the Erasmus+ Programme of the European Union

Riskianalüüs



CyberPhish
Safeguarding your digital future

Social Media Phishing Email (Source: Malwarebytes)

Funded by the Erasmus+ Programme of the European Union

Riski tuvastamine

2. Mõistab URLe
2.1 Ärge klõpsake manuseid ega linke
2.2 URL-i kuvamiseks hõljutage kursorit manuse kohal ja analüüsige, et teha kindlaks, kas see on pahatahtlik
2.3 Olge ettevaatlik, kui URL-i tee ei ühti platvormi domeeniga

1. Mõistab andmepüüki
Andmepüügi allikas: Twitteri sõnum
Andmepüügi sõnumi anatoomia:
a. Kellellt sõnum pärineb? *Twitter User*
b. Mis on sõnumi sisu? *Kontoga probleemid*
c. Kas sisaldab hüperlinke/manuseid? *JAH*

Andmepüügir ünnakute äratundmine

3. Tuvastab ohu märgid
3.1 Seadustatud Twitteri kinnitamise protsessi käsitleb Twitteri päringuprotsess (mitte vastupidi)
3.2 Twitter kasutab teie poole pöördumiseks alati teie kontole registreeritud nime
3.3 Esitatud link peaks ühtima platvormi domeeniga, st "twitter.com", mitte "twitterverifiy.verifiy.ml"

4. Kriitiline mõtlemine
4.1 *Andke konto parool või sisselogimisteave "kinnitamiseks" ainult seaduslike veebisaitide turvalistes osades, nt "twitter.com"*
4.2 *Isegi kui tundub, et sõnum on pärit kelleltki, keda te usaldate, on tõenäoline, et tema konto on rünnatud*
4.3 *Kasutage sotsiaalmeedias alati täiustatud privaatsusseadeid*
4.4 *Ärge klõpsake DM-ides kahtlastel linkidel, kontrollige kahtlasi URL-e tasuta andmepüügi tuvastamise tööriistade abil*
4.5 *Olge ettevaatlik, kui saadate sõnumeid kasutajatele, keda te ei tunne ja keda te ei jälgi*
4.6 *Katkestage/blokeerige kahtlased kontod ja kustutage teile saadetud sõnum, kui olete piisavalt kindel, et tegemist on andmepüügiga*

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte

- Andmepüügi juhtumiuuringud
- Esiletõstetud andmepüügirünnakute ja pettuste riskianalüüs
- Andmepüügirünnakute äratundmine, et vältida sellest tulenevaid andmepüügiriske.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

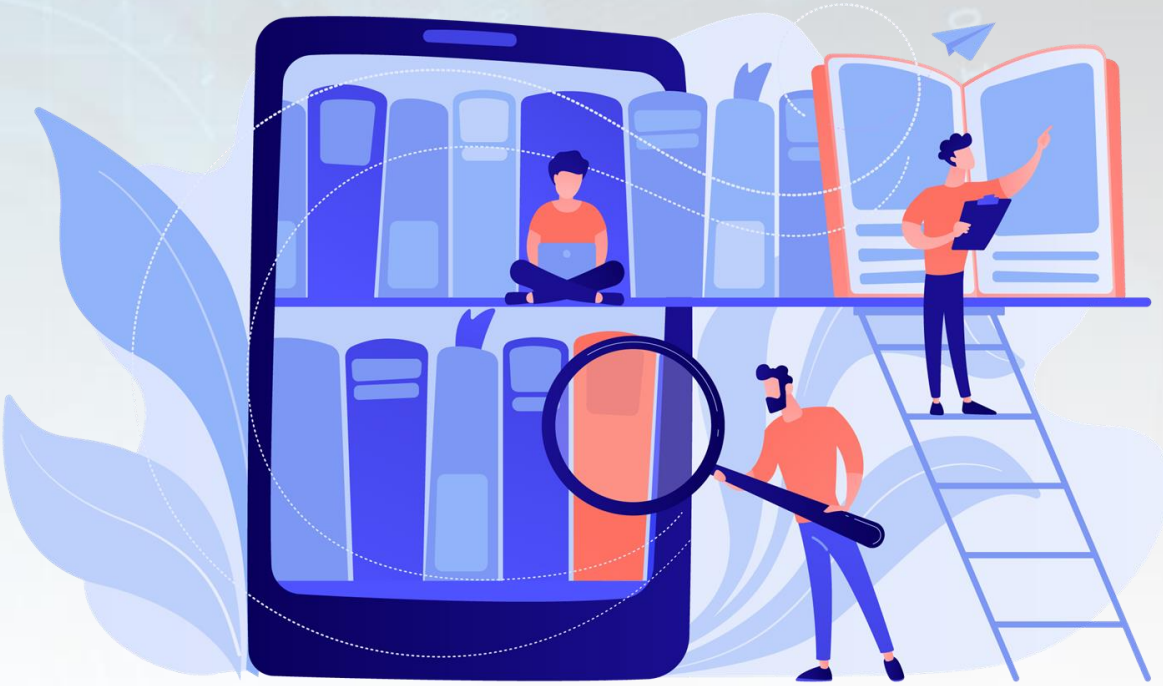
Ülesanne

- Arutage 3 mainimata andmepüügirünnakut, mis on teie arvates tänapäeval levinud
- Koostage nende andmepüügipettuste jaoks riskianalüüs, tuues esile ründemeetodid, haavatavused ja andmepüügijuhtumid, mis moodustavad andmepüügiriski
- Arutage, kuidas saate neid pettuseid ära tunda ja sellest tulenevaid andmepüügiriske ära hoida.

Funded by the Erasmus+ Programme of the European Union

Lisalugemine

- **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

Lühivideod

- Phishing email scam anatomy
  - ***https://youtu.be/3gpOM9c6mmA***
- Some phishing attack examples
  - ***https://youtu.be/lpGfxIAQhSo***
  - ***https://youtu.be/pGEAZdp0MAI***
- Recognising and staying safe from phishing
  - ***https://youtu.be/R12_y2BhKbE***

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tänan kuulamast!