Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakud: andmepüük ja sotsiaalsed ründed

Sotsiaalse ründe tehnikad ja manipuleerimine

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 mõjutamis- ja manipuleerimisvõtteid ning õppida neid ära tundma.
- Selgitada sotsiaalse ründe tehnoloogiaid ja selle psühholoogilisi aspekte.
- Tutvuda, kuidas otsuste tegemist mõjutavad emotsioonid, töökoormus ja keskkond meie ümber.
- Selgitada mõjutamis- ja manipuleerimisvõtteid ning õppida neid ära tundma

Funded by the Erasmus+ Programme of the European Union

Õppija töökoormus

Loengud	4 h
Audio- ja videomaterjal	2 h
Juhtumiuuringud	2 h
Lisalugemine	8 h
Eksamiks valmistumine	1 h

Funded by the Erasmus+ Programme of the European Union

Loenguteemad

- Inimfaktor
- Suhtlusrünne ehk sotsiaalne rünnak (*social engineering attack*)
- Otsuste tegemise protsess
- Suhtlusründe psühholoogilised aspektid
  - Emotsioonid
  - Mõjurelvad
- Pööratud suhtlusrünne
- Soovitused suhtlusründe ennetamiseks

Funded by the
Erasmus+ Programme
of the European Union

Inimfaktor

$ 400 BIL Organisatsioonide vastu suunatud küberrünnakute hinnanguline maksumus kogu maailmas

Organisatsioonid pööravad tähelepanu küberjulgeoleku inimlikku komponenti harva ja tegelevad sellega alles siis, kui rikkumine on aset leidnud. Suurte rikkumiste korral võib see maksma minna miljoneid dollareid.

35 % andmetega seotud rikkumisi seostati inimliku eksimuse või hooletusega

Küberohtude tüübid ja ennetusmeetodid muutuvad iga päev. Küberhuvi ja -teadlikkuse kultuuri juurutamine võimaldab organisatsioonil paremini toime tulla muutuvate küberjulgeolekuohtudega.

47 % IT-spetsialistid kirjeldavad koostööd turvariskide juhtimise ja äritegevuse vahel halvaks või olematuks

Paljud juhid arvavad, et küberturvalisuse eest vastutab IT; pigem on see igaühe enda vastutus. Töötajate teadlikkus peaks olema organisatsiooni digitaalsete varade kaitsmise esimene rida.

CyberPhish
Safeguarding your digital future

[Walker at al. 2017]

Funded by the Erasmus+ Programme of the European Union

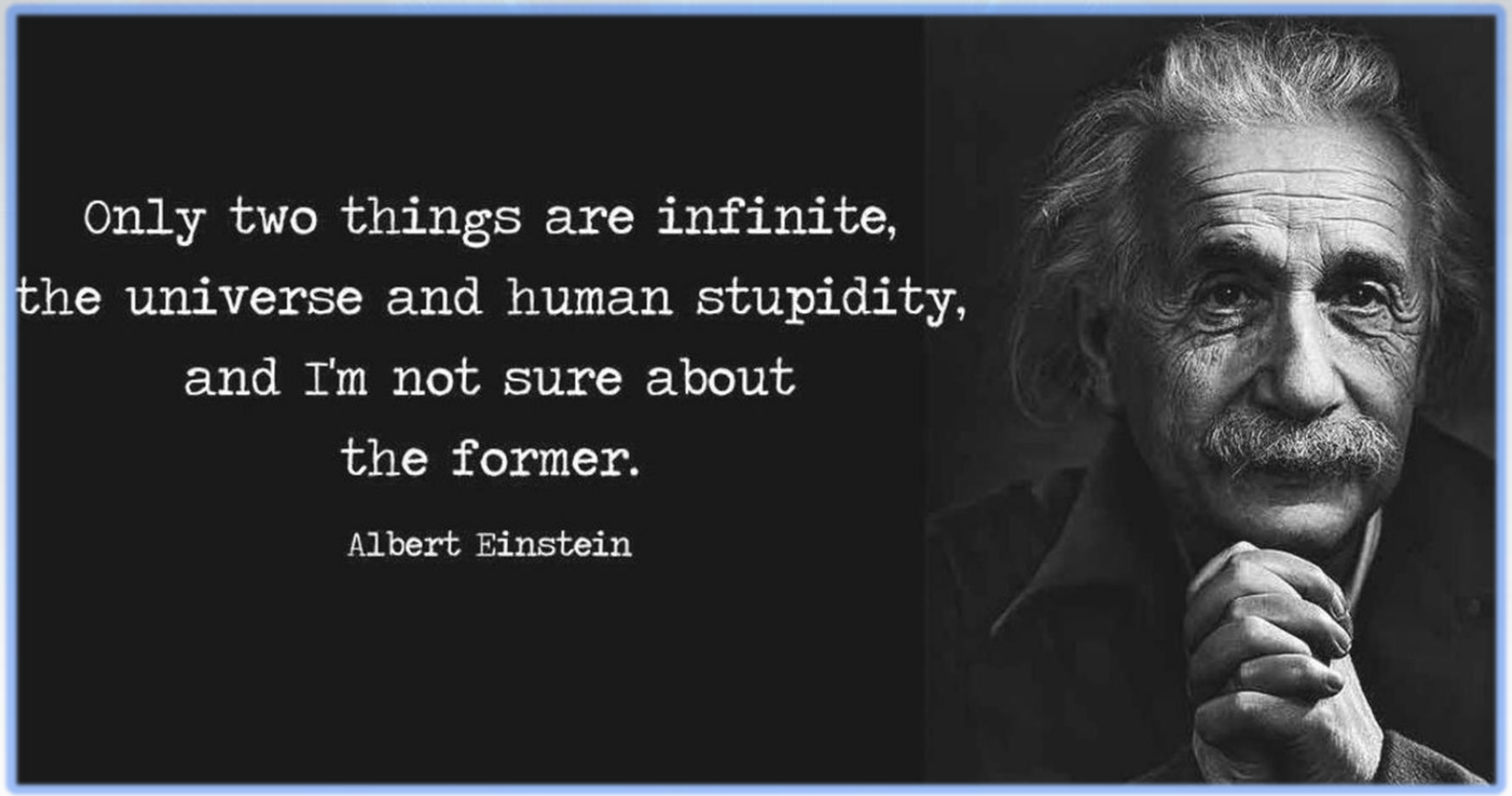
Inimfaktor

- Inimesed esindavad sageli turvaahela nõrgimat lüli ja on krooniliselt vastutavad turvasüsteemide rikete eest.

- Tehnilised turvameetmed arenevad pidevalt, kuid inimesed ei jõua muutustega kaasas käia ning jäävad infoturbe nõrgimaks lüliks oma nõrkuste, stereotüüpide ja hoiakutega

Funded by the
Erasmus+ Programme
of the European Union

Inimfaktor



Ainult kaks asja on lõpmatud universum ja inimeste **rumalus** ning esimeses pole ma kindel.

Source: https://iheartintelligence.com/

Mis on sotsiaalne rünne?

SOCIAL ENGINEERING

Social engineering is any act that influences a person to take an action that may or may not be in his or her interests

[Hadnagy, 2018]

Suhtlusrünne

- inimestega manipuleerimine eesmärgiga panna neid sooritama teatud toiminguid või avaldama konfidentsiaalset teavet

Funded by the Erasmus+ Programme of the European Union

Mis on sotsiaalne rünne?

- Sotsiaalset rünnet võib määratleda kui inimestega manipuleerimist, enamasti psühholoogilise veenmise abil, et saada juurdepääs süsteemidele, mis sisaldavad andmeid, dokumente ja teavet, mille hankimiseks sotsiaalinseneril ei tohiks olla juurdepääsu.
- Sotsiaalne manipulatsioon on inimpsühholoogia, mitte tehniliste häkkimistehnikate ärakasutamise kunst, et saada juurdepääs hoonetele, süsteemidele või andmetele.

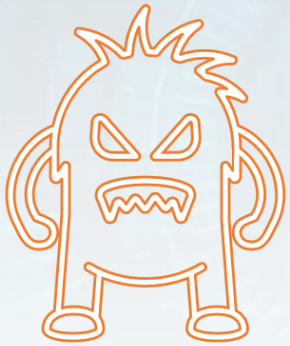
[Washo, 2021]

Funded by the Erasmus+ Programme of the European Union

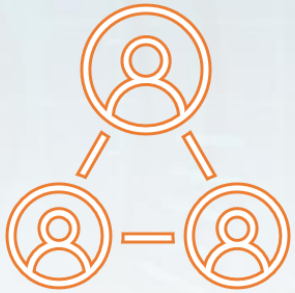
Suhtlusrünnete statistika

98% küberrünnakutest tuginevad sotsiaalsele manipuleerimisele

/



43% IT-spetsialistidest olid eelmisel aastal sotsiaalse manipu-leerimise sihikuks

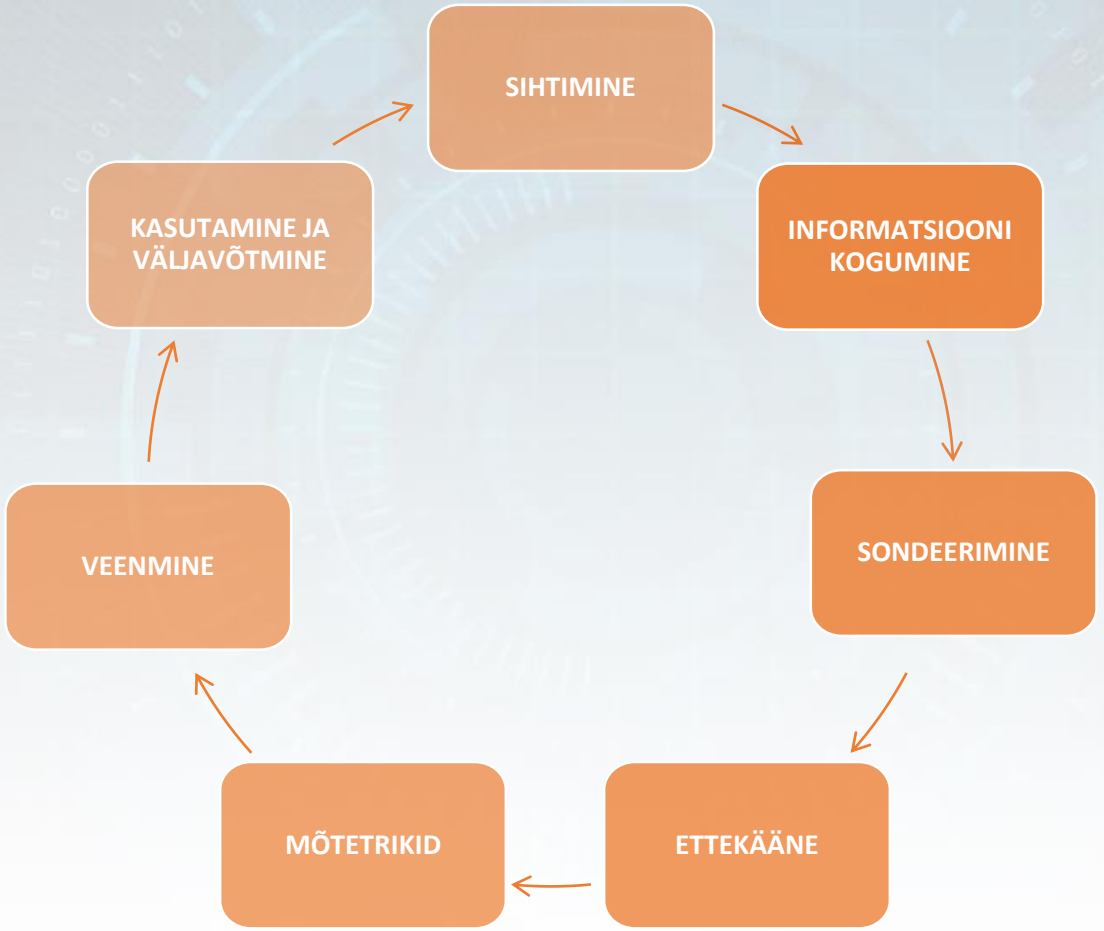


21% praegustest või endistest töötajatest kasutab sotsiaalset manipuleerimist

Sotsiaalse manipuleerimise katsed kasvasid 2018. aastal enam kui 500%.

Source: https://purplesec.us/resources/cyber-security-statistics

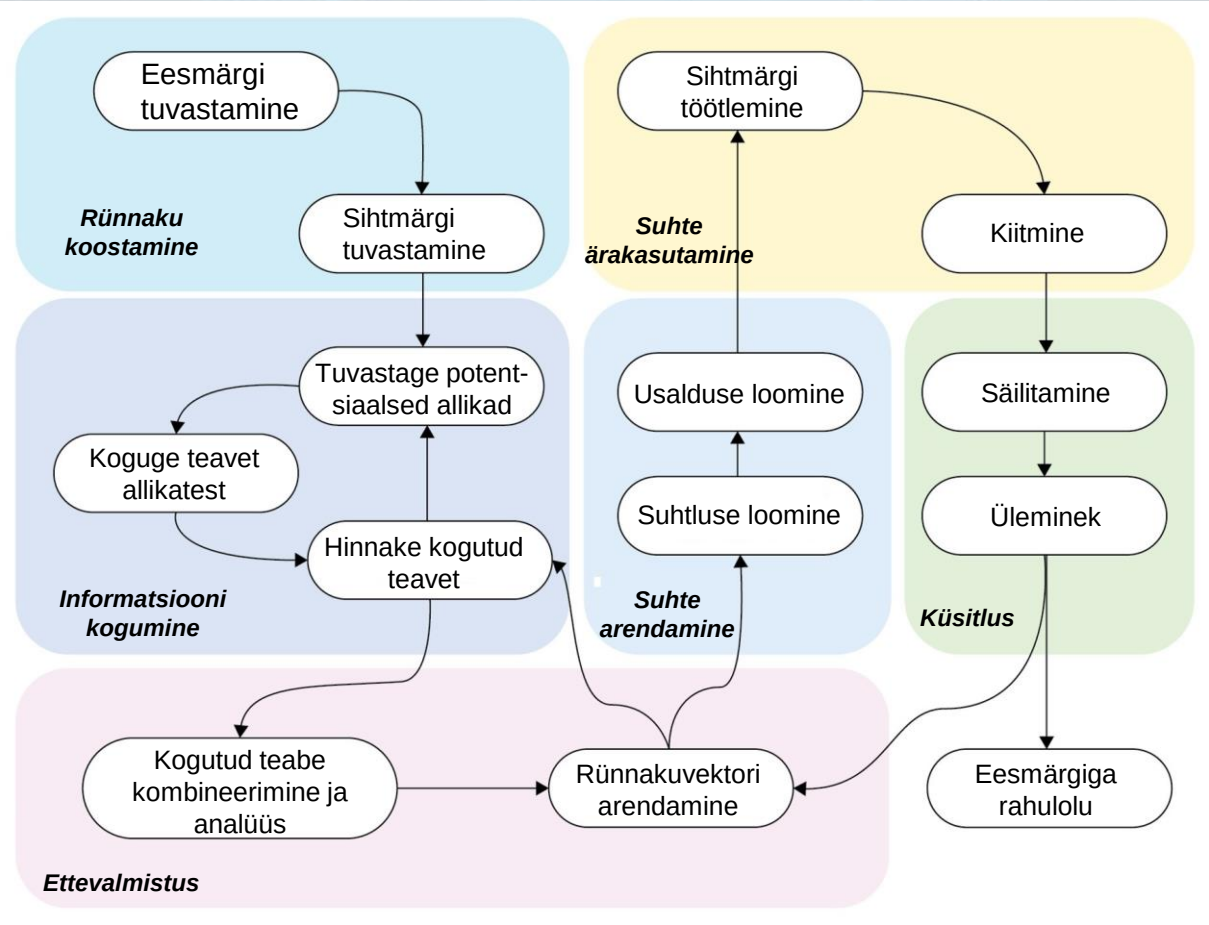
Sotsiaalse ründe raamistik



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sotsiaalse rünnaku "teekaart"



Source: Dr. Erdal Ozkaya "Learn Social Engineering", 2018

Samm 1: Sihtimine

- Sotsiaalne manipuleerimine – sihtmärgipõhine
- Sihtmärgi valimine lõplike "tulemuste" (nt teave, raha jne) põhjal

Funded by the Erasmus+ Programme of the European Union

Samm 2: Informatsiooni kogumine

- Kõige keerulisem samm kogu sotsiaalse manipuleerimise protsessis
- Võib kesta mõnest tunnist mõne aastani
- Teavet kogutakse harva korraga
- Sotsiaalmeedia platvormide, spetsiaalse tarkvara, pehmete oskuste kasutamine
- Andmete kogumiseks on kaks võimalust:
  - Mittetehnilised / mehaanilised meetodid
  - Tehnilised meetodid

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Samm 3: Sondeerimine

***Elicitation** – Sondeerimine - kaudteadmust või eelteavet koguma ehk püüdma salateavet märkamatult välja meelitada.*

Tegurid, mis muudavad sondeerimise tõhusaks:

- Enamik inimesi püüab võõraga vesteldes olla viisakad
- Spetsialistid, kui neilt küsitletakse, tahavad näida asjatundlikud
- Enamik inimesi ei valetaks kellelegi, kes näib olevat tõeliselt mures
- On tõenäolisem, et keegi vastab enda kohta hästi esitatud küsimustele

Funded by the Erasmus+ Programme of the European Union

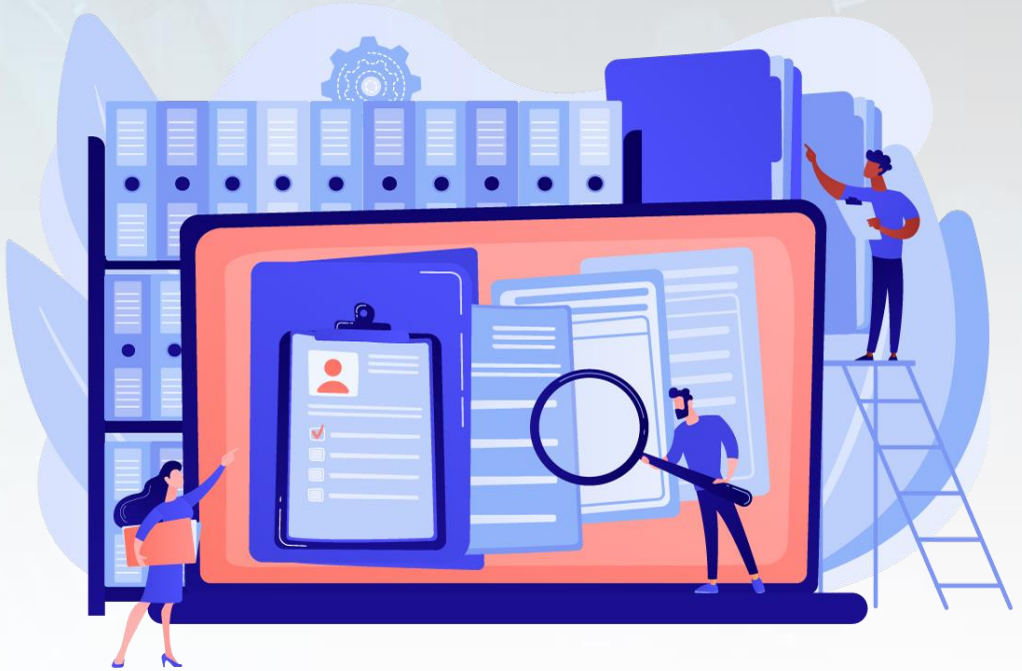
Samm 4: Ettekääne

Ettekääne on hädavajalik oskus, mida iga sotsiaalinsener vajab rünnaku sooritamiseks.

Ettekäände esitamine paneb inimese teise nahka.

Ettekäände esitamise üldpõhimõtted :

- Uurige rohkem
- Kasutage isiklikke huve
- Harjutage väljendeid või dialekte
- Kasutage lihtsamaid ettekäändeid
- Loogilised järeldused



Samm 5: Meeletrikid

Meeletrikid on pigem psühholoogiline asi ja neid kasutatakse sihtmärkide mõistuse avamiseks, jättes nad sotsiaalse ründaja kontrolli alla. .

MIND TRICKS ≠ SCIENCE

Inimesel on kolm mõtlemisviisi, mida saab ära kasutada:

1. **Visuaalne mõtlemine**
2. **Auditiivne mõtlemine**
3. **Kinesteetiline mõtlemine**

Samm 6: Veenmine

Sihtmärgi veenmiseks peab sotsiaalne ründaja kõigepealt lähtuma sihtmärgi huvidest. Veenmine toob sihtmärgid reageerima, mõtlema ja tegema täpselt nii, nagu sotsiaalinsener soovib.

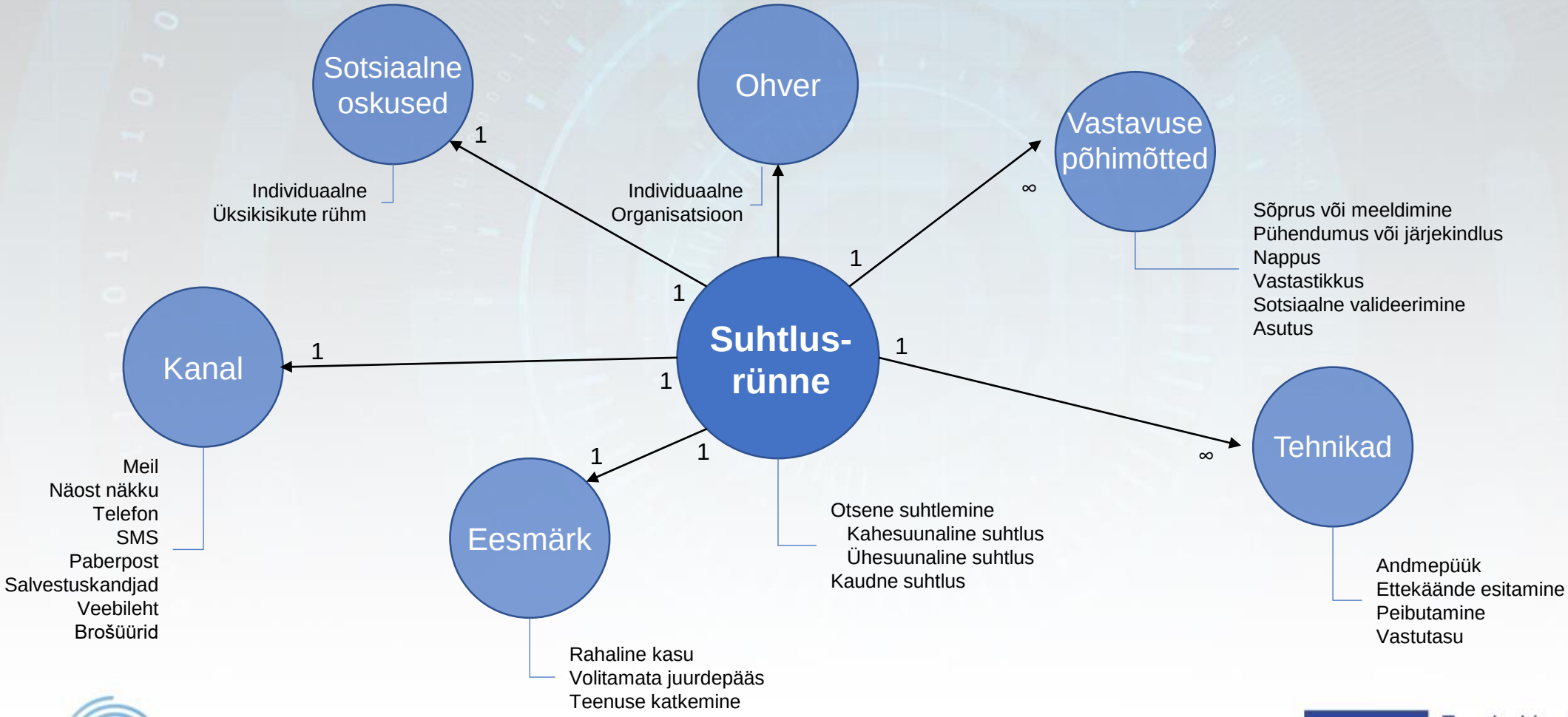
5 põhialust, mida sotsiaalinsenerid veenmisel kasutavad :

1. Selged eesmärgid
2. Empaatia
3. Õige meelsus
4. Paindlikkus
5. Vastutasu

Samm 7: Ärakasutamine ja lahtiühendamine

- Ohvri ärakasutamine, kui on tekkinud usaldus ja nõrkus rünnaku edendamiseks
- Väljalülitamine, kui kasutaja on soovitud toimingu teinud

Sotsiaalse rünnaku ontoloogiline mudel



[Merwe and Mouton, 2017]

Suhtlusrünnaku näide

Mitmed inimesed kaotasid pärast Ethereum Classicu veebisaidi häkkimist 2017. aastal tuhandeid dollareid krüptovaluutat. Sotsiaalse manipuleerimise abil esinesid häkkerid Classic Ether Walleti omanikuna, said juurdepääsu domeeniregistrile ja suunasid domeeni seejärel oma serverisse. Kurjategijad ekstraheerisid ohvritelt Ethereumi krüptovaluutat pärast veebisaidile koodi sisestamist, mis võimaldas neil vaadata tehinguteks kasutatavaid privaatvõtmeid.

Funded by the Erasmus+ Programme of the European Union

Suhtlusrünnaku näide

Shark Tanki televisioonikohtunik Barbara Corcoran sai 2020. aastal petta ligi 400 000 USA dollari suuruse andmepüügi ja sotsiaalse manipuleerimise pettuses. Küberkurjategija esines tema assistendina ja saatis raamatupidajale meili, milles taotles kinnisvarainvesteeringutega seotud pikendamismakset. Ta kasutas seaduslikuga sarnast e-posti aadressi. Pettus avastati alles pärast seda, kui raamatupidaja saatis assistendi õigele aadressile tehingu kohta e-kirja.

Funded by the Erasmus+ Programme of the European Union

Suhtlusrünnaku näide

Ühe suurima sotsiaalse manipuleerimise rünnaku pani toime Leedu kodanik Evaldas Rimasauskas kahe maailma suurima ettevõtte: Google'i ja Facebooki vastu.

Rimasauskas ja tema meeskond asutasid võltsfirma, teeseldes, et on arvutitootja, kes töötas Google'i ja Facebookiga. Rimsauskas lõi ka ettevõtte nimele pangakontod.

Seejärel saatsid petturid konkreetsetele Google'i ja Facebooki töötajatele andmepüügimeile, esitades neile arveid kaupade ja teenuste eest, mida tootja oli tõeliselt pakkunud, kuid suunates neid oma petturlikule kontole raha kandma. Aastatel 2013–2015 petsid Rimasauskas ja tema kaaslased kahelt tehnoloogiahiiglaselt enam kui 100 miljonit dollarit.

Funded by the Erasmus+ Programme of the European Union

Miks suhtlusrünnakud on edukad?

- Oleme loomult sotsiaalsed ;
  - Meie soov teistest silma paista
- Teised inimesed avaldavad meie otsustele suurt mõju ;
  - Meie soov olla abiks
  - Meie kalduvus usaldada inimesi, keda me ei tunne

Funded by the
Erasmus+ Programme
of the European Union

Miks suhtlusrünnakud on edukad?

- Oleme teabega üle koormatud ja otsime aja säästmiseks otseteid .
  - Meie soov, et kõik head asjad juhtuksid kiiresti ja ilma pingutusteta
  - Meie hirm hätta sattuda
- Turvaalaste teadmiste puudumine;
- Isikliku teabe liigjagamine sotsiaalmeedias;

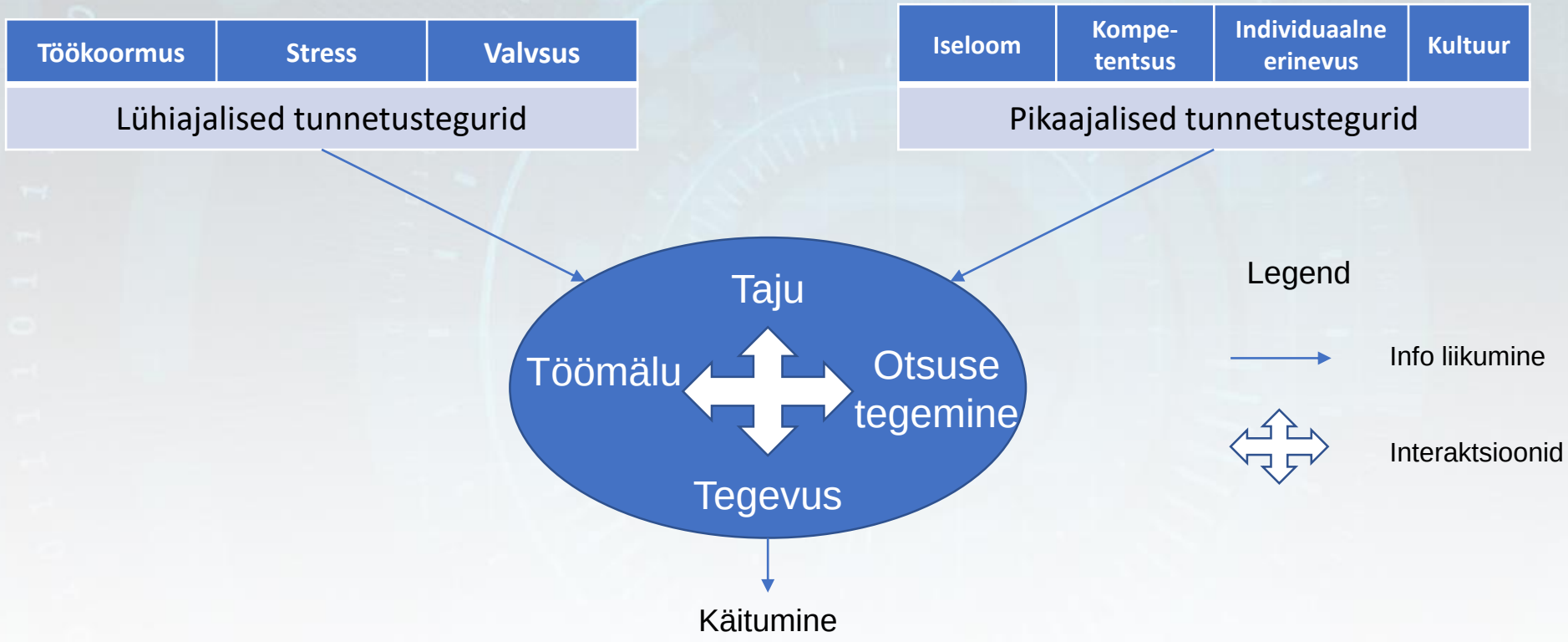
Funded by the Erasmus+ Programme of the European Union

Sotsiaalse ründe psühholoogilised aspektid

Mõned autorid pooldavad sotsiaalsete küberrünnakute käsitlemist teatud tüüpi psühholoogilise rünnakuna.

[Montañez at al. 2020]

Inimese kognitiivsed funktsioonid



suur kognitiivne töökoormus, kõrge stressitase, vähene tähelepanelikkus, valdkonnaalaste teadmiste puudumine ja/või varasemate kogemuste puudumine muudavad inimese vastuvõtlikumaks sotsiaalsetele küberrünnakutele

[Montañez at al. 2020]

Veebipõhise veenmise psühholoogia

"Praegune Interneti-tarbijate põlvkond elab kohese rahulduse ja kiirete lahenduste maailmas, mis toob kaasa kannatlikkuse kaotuse ja sügava mõtlemise puudumise." - Rob Weatherhead, The Guardian

Meie käitumist, mõtteid ja uskumusi kujundavad pidevalt meid ümbritsev keskkond ja ka meie enda kogemused.

Mõjutamine ja veenmise kunst on protsess, mille käigus pannakse keegi teine tahtma teha, reageerida, mõelda või uskuda nii, nagu sina tahad.

Funded by the Erasmus+ Programme of the European Union

Kõrgendatud emotsioonid

- Emotsionaalne manipuleerimine annab ründajatele igas suhtluses ülekaalu. Suurenenud emotsionaalses seisundis teete palju tõenäolisemalt irratsionaalseid või riskantseid tegevusi.

[Montañez at al. 2020]

Funded by the Erasmus+ Programme of the European Union

Kõrgendatud emotsioonid

[Montañez at al. 2020]

Hirm

COVID-19

N

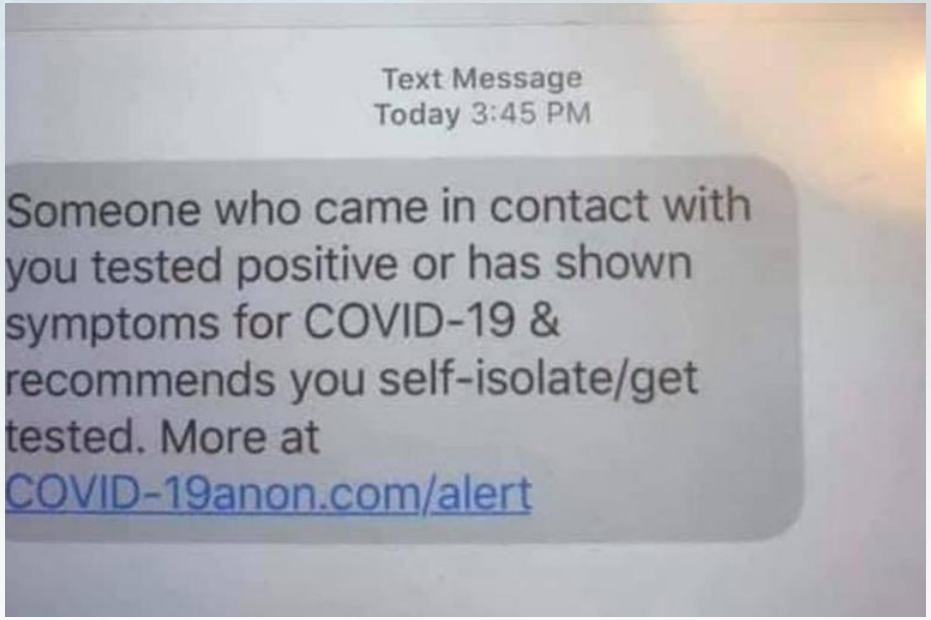
nicholsschoolorg@alsummers.com <nicholsschoolorg@alsummers.com>

To: jullrich@dshield.org

Hi, neighbor.
Tests confirmed that I was sick with a coronavirus.
Doctors said that in the week I will leave the world.
My parents will be left without my support.
And at this time you will live enjoying.
I think this is unfair, and I suggest you pay me.
What I am sitting at home and don't try to infect your home.
Life or money.
Hurry up! Every hour, I hate you more and more.

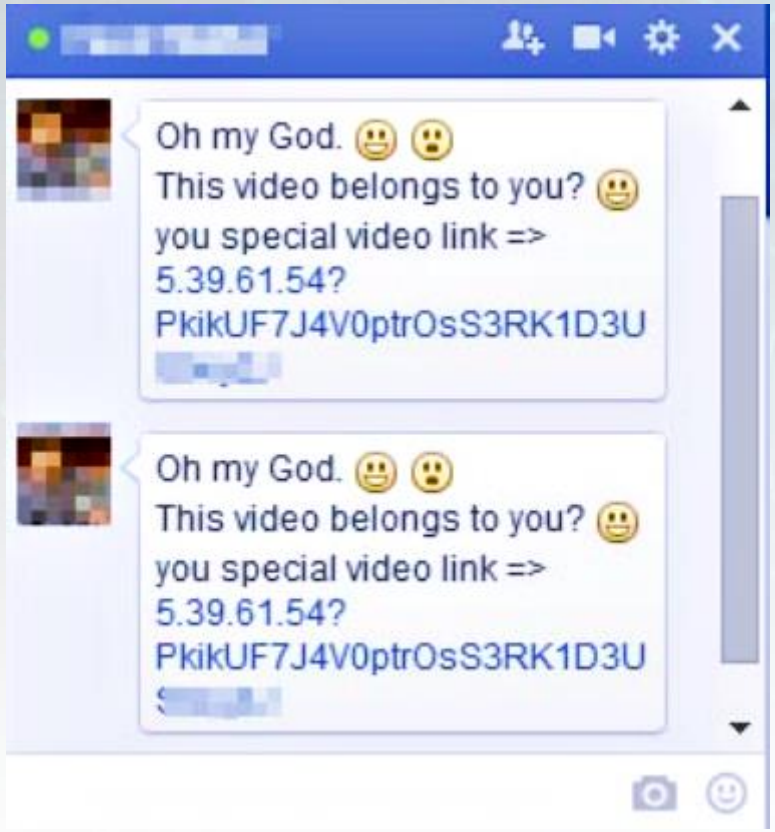
My bitcoin address (BTC Wallet) 18P3S6DuNUpW2WLozsrrW6rRd6xh24Rc7N

Source: Vilnius University Kaunas faculty internal phishing database

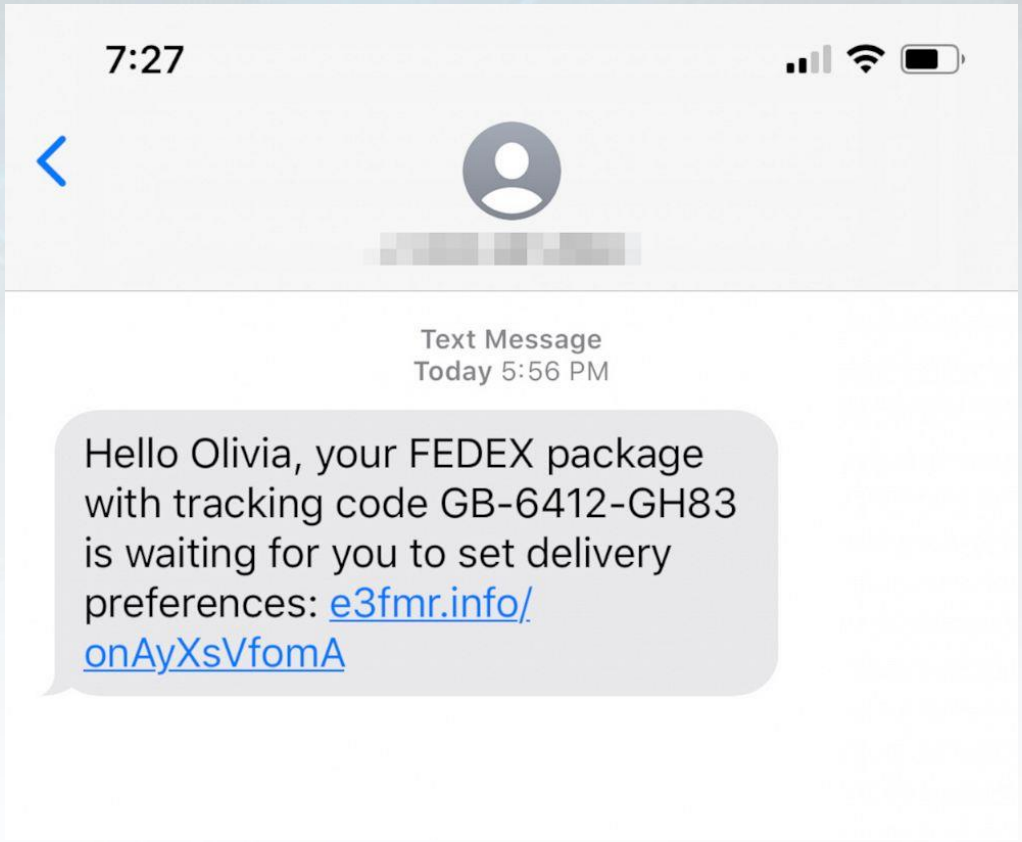


Source: https://www.thesun.co.uk/news/11422572/scam-message-hoax-tricks-americans-exposed-to-coronavirus-must-self-isolate/

Uudishimu

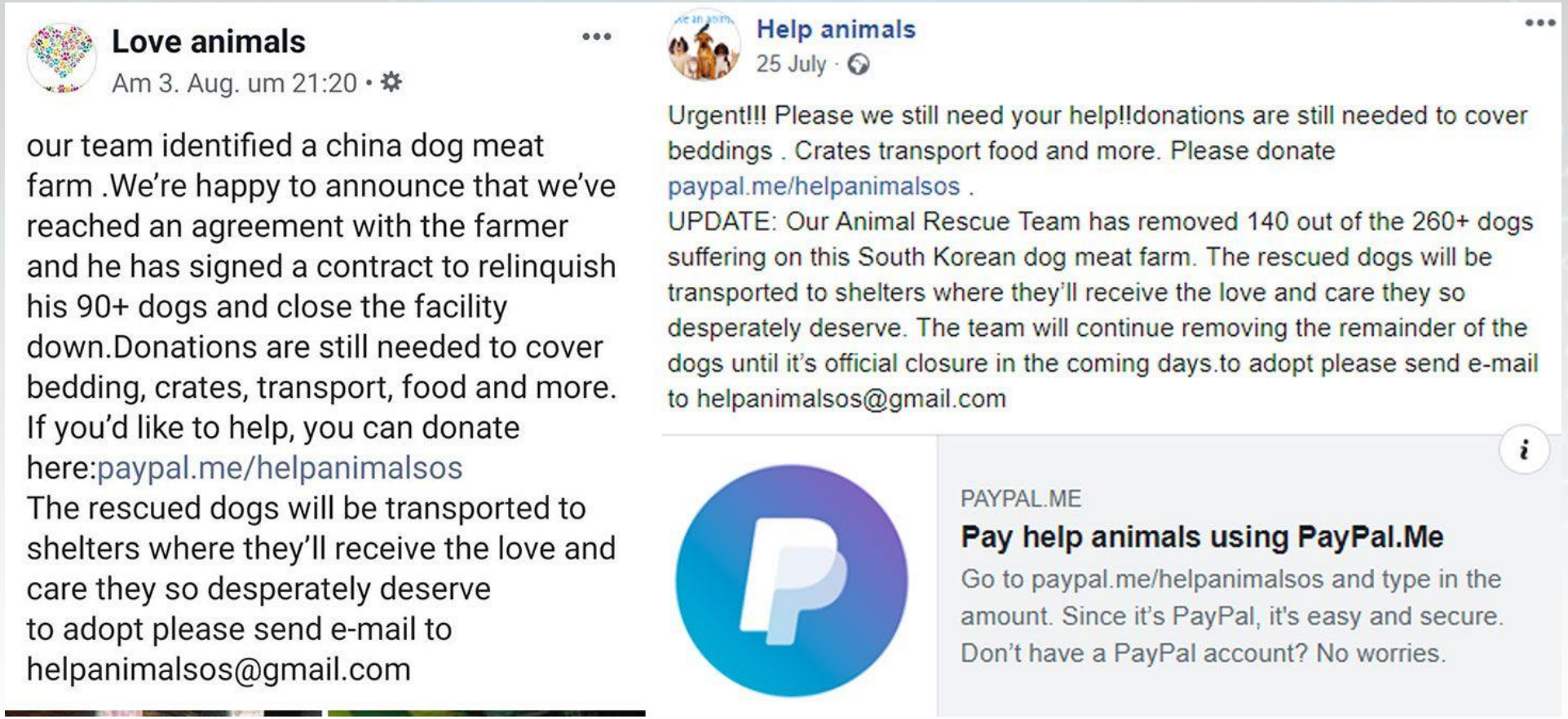


Source: https://soravjain.com/cyber-security-for-women-in-social-media/



Source: https://www.scamadviser.com/scam-reports/scam-trends/4293/delivery-scams-all-in-one-dhl-fedex-usps-and-dpd

Abivalmidus



Love animals
Am 3. Aug. um 21:20 •

our team identified a china dog meat farm .We're happy to announce that we've reached an agreement with the farmer and he has signed a contract to relinquish his 90+ dogs and close the facility down.Donations are still needed to cover bedding, crates, transport, food and more. If you'd like to help, you can donate here:paypal.me/helpanimalsos
The rescued dogs will be transported to shelters where they'll receive the love and care they so desperately deserve
to adopt please send e-mail to helpanimalsos@gmail.com

Help animals
25 July ·

Urgent!!! Please we still need your help!!donations are still needed to cover beddings . Crates transport food and more. Please donate paypal.me/helpanimalsos .
UPDATE: Our Animal Rescue Team has removed 140 out of the 260+ dogs suffering on this South Korean dog meat farm. The rescued dogs will be transported to shelters where they'll receive the love and care they so desperately deserve. The team will continue removing the remainder of the dogs until it's official closure in the coming days.to adopt please send e-mail to helpanimalsos@gmail.com

PAYPAL.ME
Pay help animals using PayPal.Me
Go to paypal.me/helpanimalsos and type in the amount. Since it's PayPal, it's easy and secure. Don't have a PayPal account? No worries.

Source: https://usa.kaspersky.com/blog/fake-charity-scam/18580/

Kiireloomuline

Ajatundlikud võimalused või taotlused on veel üks usaldusväärne tööriist ründaja arsenalis.

Võite olla motiveeritud end kompromiteerima tõsise probleemi varjus, mis vajab kohest tähelepanu.

Teise võimalusena võite saada auhinna või preemia, mis võib kaduda, kui te kiiresti ei tegutse.

Kumbki lähenemisviis tühistab teie kriitilise mõtlemise võime.

Funded by the Erasmus+ Programme of the European Union

Kiireloomulisus

Friday 02/02/19 4.18pm

[redacted]

URGENT: supplier will not complete an urgent order

To [redacted]

Hi Sandra

Sorry to spring this on you with late notice – I need you to make an urgent payment to AusTekno Logics' new bank account ASAP or they won't deliver on time.

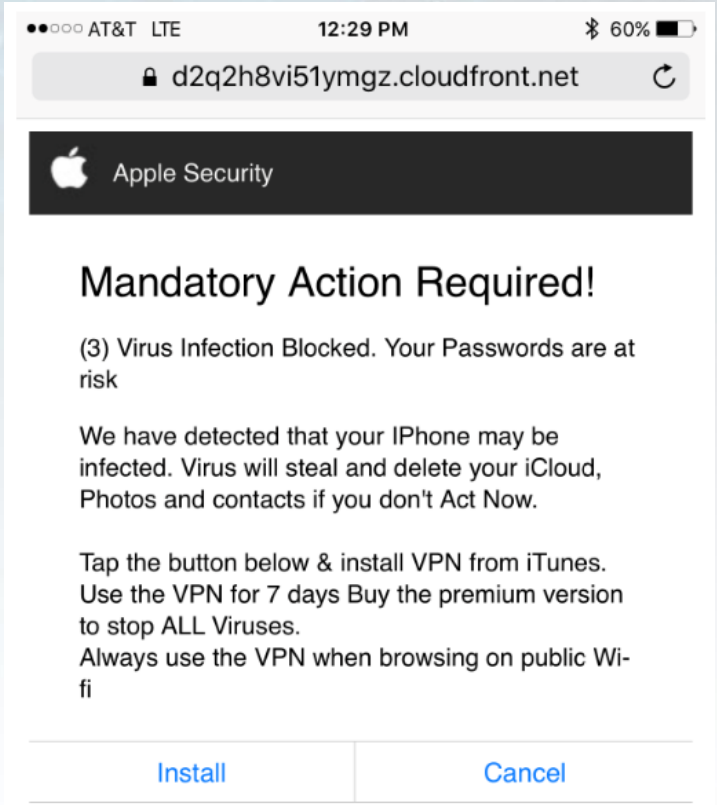
I'll be in a meeting all day.

AusTekno Logics
Account number: 123456789
Code: 11 22 33

Thanks,

John Doe
The Services Company
Chief Executive Officer
Email: john.doe@services.com.au

Source: https://www.scamwatch.gov.au/about-scamwatch/tools-resources/online-resources/spot-the-scam-signs



Source: https://www.reddit.com/r/jailbreak/comments/78b2tv/request_remove_this_fucking_vpn_ad_please_like/

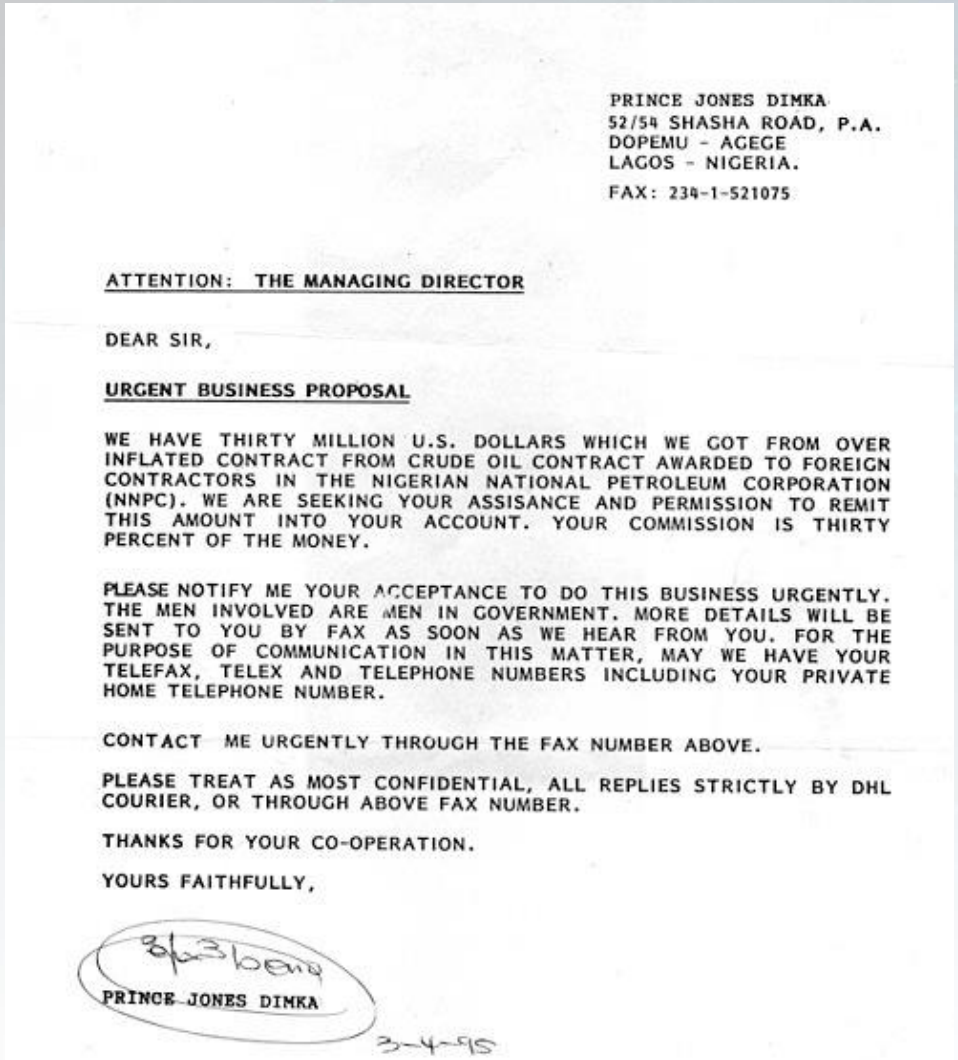
Viha

- Me väldime vihaseid inimesi
- Väldime konflikte

- Vihane "boss" helistab töötajale ja küsib parooli

Funded by the Erasmus+ Programme of the European Union

Saamahimu



PRINCE JONES DIMKA
52/54 SHASHA ROAD, P.A.
DOPEMU - AGEGE
LAGOS - NIGERIA.
FAX: 234-1-521075

ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

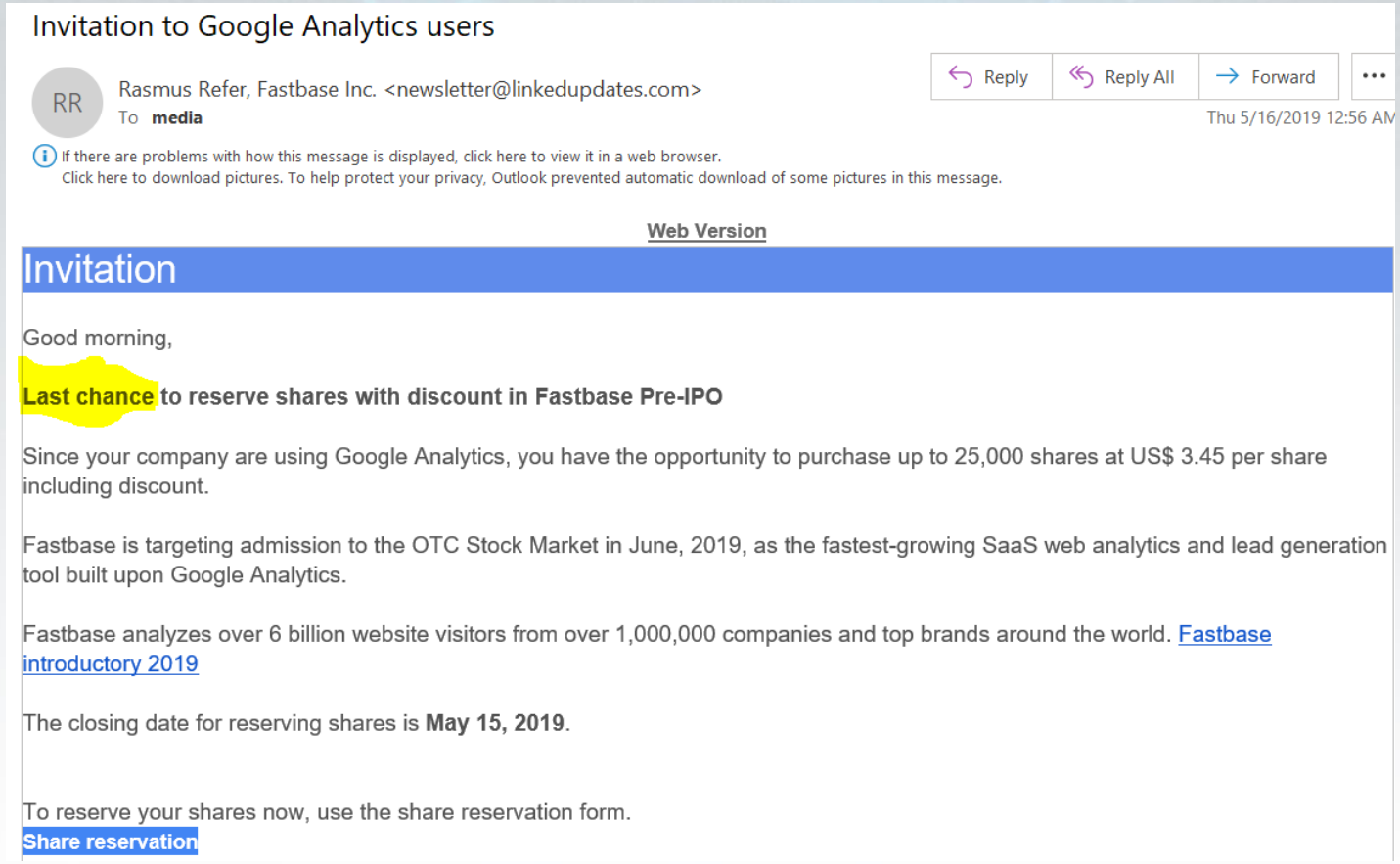
PRINCE JONES DIMKA

3-4-95

- Need on ühed vanimad petuskeemid – Nigeeria printside või sõjaväelaste rikkust tõotav varastatud varandust jagada.
- Mõnikord on selleks varakas lesknaine, kes sureb vähki, või Briti advokaat, kes annab teie osa pärandvarast.

Source: https://www.businessinsider.com/online-scams-internet-phishing-2019-3

Saamahimu



Invitation to Google Analytics users

RR

Rasmus Refer, Fastbase Inc. <newsletter@linkedupdates.com>

To **media**

Reply | Reply All | Forward | ...

Thu 5/16/2019 12:56 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Web Version

Invitation

Good morning,

Last chance to reserve shares with discount in Fastbase Pre-IPO

Since your company are using Google Analytics, you have the opportunity to purchase up to 25,000 shares at US$ 3.45 per share including discount.

Fastbase is targeting admission to the OTC Stock Market in June, 2019, as the fastest-growing SaaS web analytics and lead generation tool built upon Google Analytics.

Fastbase analyzes over 6 billion website visitors from over 1,000,000 companies and top brands around the world. Fastbase introductory 2019

The closing date for reserving shares is **May 15, 2019**.

To reserve your shares now, use the share reservation form.

Share reservation

Source: Vilnius University Kaunas faculty internal phishing database

Mõjurelvad

[Cialdini, 2007]

*Reciprocity - **Vastastikkus***

- "... peaksime püüdma mitterahaliselt tagasi maksta selle, mida teine inimene meile on andnud."

- Tehnika 1: kui keegi teeb järeleandmise, oleme kohustatud vastama mööndusega. Mööndus tegemine annab teisele poolele vastutustunde tulemuse eest ja suurema rahulolu lahendusega.

[Cialdini, 2007]

Funded by the Erasmus+ Programme of the European Union

*Reciprocity - **Vastastikkus***

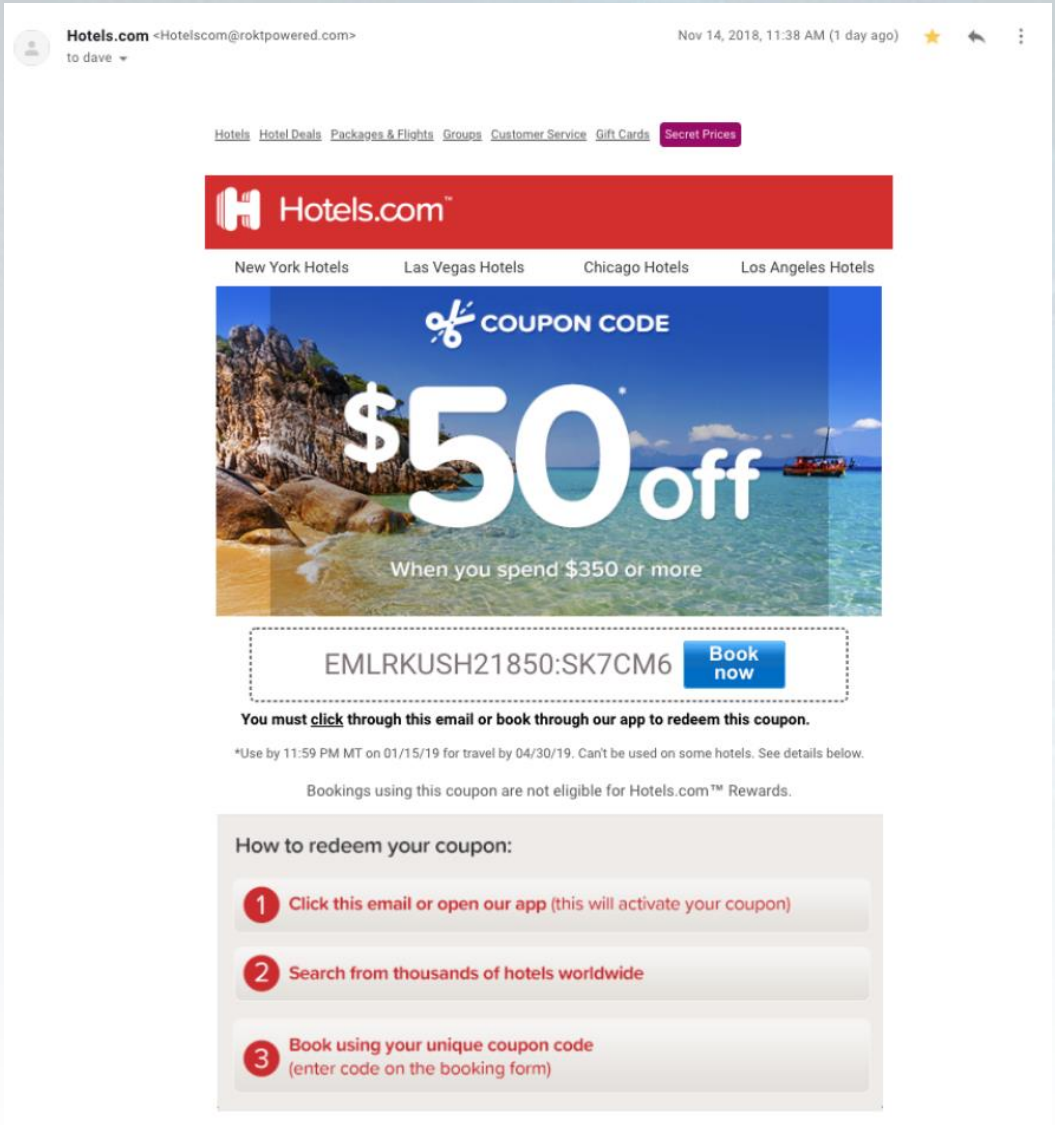
- Tehnika 2: tagasilükkamine ja taganemine: liialdatud taotlus lükati tagasi, soovitud väiksem taotlus rahuldatakse

- Tehnika3. : kontrasti põhimõte: müü esmalt kulukas ese; või esitage esmalt ebasoovitav valik

[Cialdini, 2007]

Funded by the Erasmus+ Programme of the European Union

Reciprocity
Vastastikkus



Source: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Consistency - Järjepidevus

- Meil on "peaaegu obsessiivne soov olla (ja näida) kooskõlas sellega, mida oleme juba teinud"

- Kui oleme teinud valiku või seisukoha võtnud, kogeme isiklikku ja inimestevahelist survet selle kohustusega järjekindlalt käituda.

[Cialdini, 2007]

Funded by the Erasmus+ Programme of the European Union

Consistency - Järjepidevus

- Jalg ukses tehnika: väikese taotlusega nõustumine suurendab tõenäosust, et nõustute teise, suurema taotlusega.

- Uks näos Tehnika: suurest taotlusest keeldumine suurendab tõenäosust, et nõustute teise, väiksema taotlusega.

[McLeod, 2014]

Funded by the Erasmus+ Programme of the European Union

Consistency - Järjepidevus

- Madala palli tehnika: veenja paneb inimese pühenduma madala palliga pakkumisele, millest tal pole kavatsust kinni pidada; siis tõstetakse järsku hinda. Kuna inimene on juba pühendunud, on uuest kõrgemast hinnanõudlusest raske ära öelda.

[McLeod, 2014]

Funded by the Erasmus+ Programme of the European Union

Consistency - Järjepidevus

From: Amazon.com <amazonorders@web7892.com>
To:
Sent: Thursday, April 25, 2019 3:40 PM
Subject: Action needed to complete your order

amazon.com

Dear

There was a problem with your recent order. The delivery addresses is invalid. Please click below to log in and correct the problem.

View or manage order

Best regards,

Amazom.com

Source: https://www.forbes.com/sites/barrycollins/2021/07/07/is-this-amazon-email-fake-how-to-spot-the-scams/?sh=605d881d119a

Funded by the Erasmus+ Programme of the European Union

Authority - Autoriteet

- Tunnustatud asutuselt saadud teave võib anda meile väärtusliku otsetee otsustamaks, kuidas olukorras tegutseda.

- Üha enam on meie ühendatud maailmas üha enam õigeks autoriteediks isik, bränd, organisatsioon või eesmärk, millel on suurim vaatajaskond.

[Cialdini, 2007]

Funded by the Erasmus+ Programme of the European Union

Authority - Autoriteet

- Pealkirjad
- Vormiriietus
- Riided
- Kaubamärgid

Source https://apkpure.com/nl/call-from-police/com.opik.fakegv.fyuukfg

Authority - Autoriteet

From: **Markus** <markusceo@eco1focus.com>
Date: Mon, Dec 7, 2020 at 11:38 AM
Subject: Invoice to be paid
To: Finance department <financedept@ecofocus.org>

Hi Gwen,

Could you do me a favour? Theres pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me bec ause I can't access the accounts from here.
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!) Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

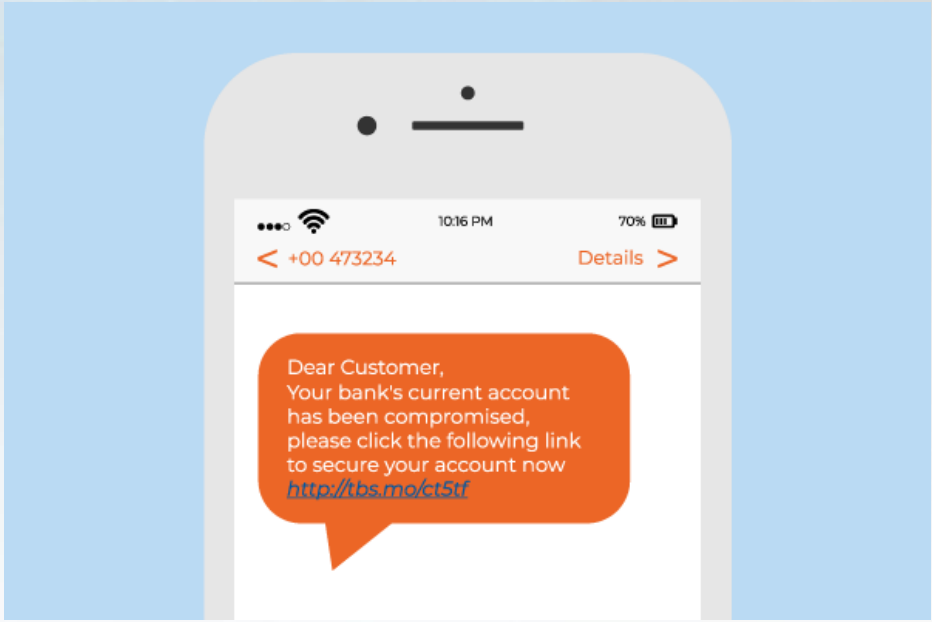
Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

Funded by the Erasmus+ Programme of the European Union

Authority - Autoriteet

Source: https://www.twitter.com



Source: https://rdcom.com/en/bulk-sms/what-is-sms-phishing-how-to-avoid-it/

Liking - meeltmööda

- Inimestele meeldivad need, kellele nad meeldivad, ja neid mõjutavad rohkem need, kes neile meeldivad.
- Meil on hea meel täita meile meeldivate inimeste soove.

Funded by the Erasmus+ Programme of the European Union

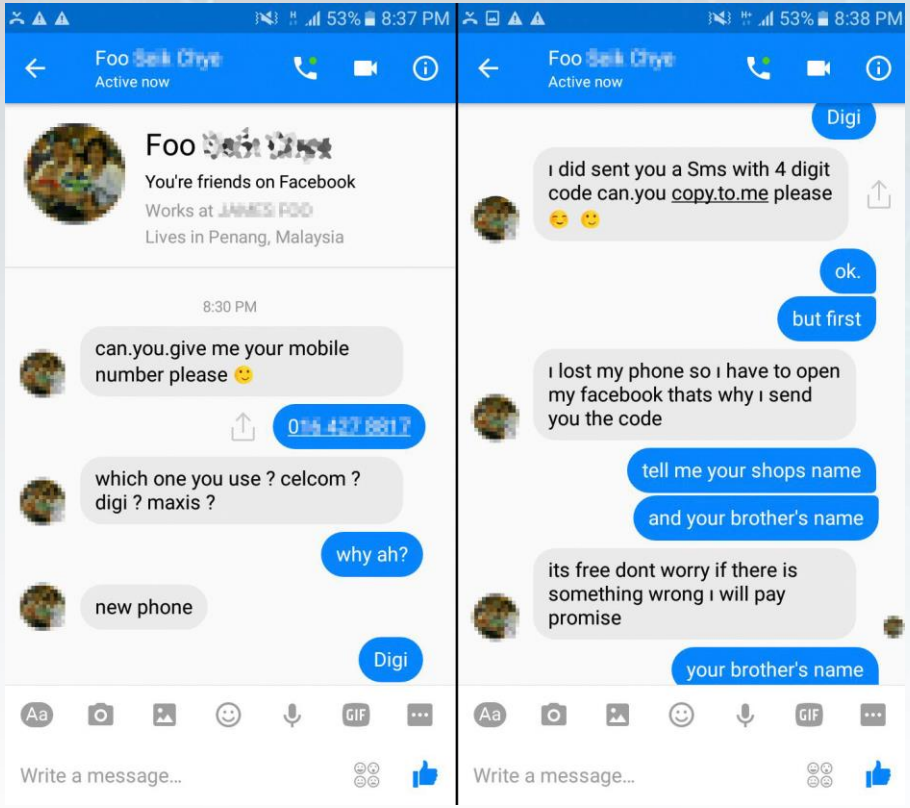
Liking - meeltmööda

- Inimesed kipuvad looma usaldust nendega, keda nad nii füüsiliselt kui ka emotsionaalselt köidavad:
  - Meile meeldivad inimesed, kes on meiega sarnased
  - Meile meeldivad inimesed, kes meile komplimente teevad
  - Meile meeldivad inimesed, kes teevad meiega koostööd ühiste eesmärkide nimel

[Cialdini, 2007]

Funded by the Erasmus+ Programme of the European Union

Liking - meeltmööda



Source: https://says.com/my/tech/scammers-are-using-this-hot-new-tactic-to-hack-into-your-facebook-profile/

---------- Forwarded message ----------
From: **Sally Jones** <sjones1234@aol.com>
Date: Sat, Aug 11, 2018 at 2:43 PM
Subject: Re: Hello
To: jsmith@gmail.com

Alright, I'm sorry I'm putting this to you. I'm currently in a meeting. Please I need you to purchase iTunes gift card 5 pieces - $100 each at the store? I would reimburse you when am through, Let me know if you can help with that right now. Thanks

Regards
Sally Jones

On Saturday, 11 August 2108, Joe Smith <jsmith@gmail.com> wrote:

Sorry had a 10:15 with my mentor.

On Sat, Aug 11, 2018 at 1:28 PM, Sally Jones <sjones1234@aol.com> wrote:

> Joe. Are you free at the moment?
>
> Regards
> Sally Jones
>
> Sent from my iPhone

Source: https://www.apa.org/about/division/digest/leader-resources/convention-email-scams/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

*Consensus - **Üksmeel***

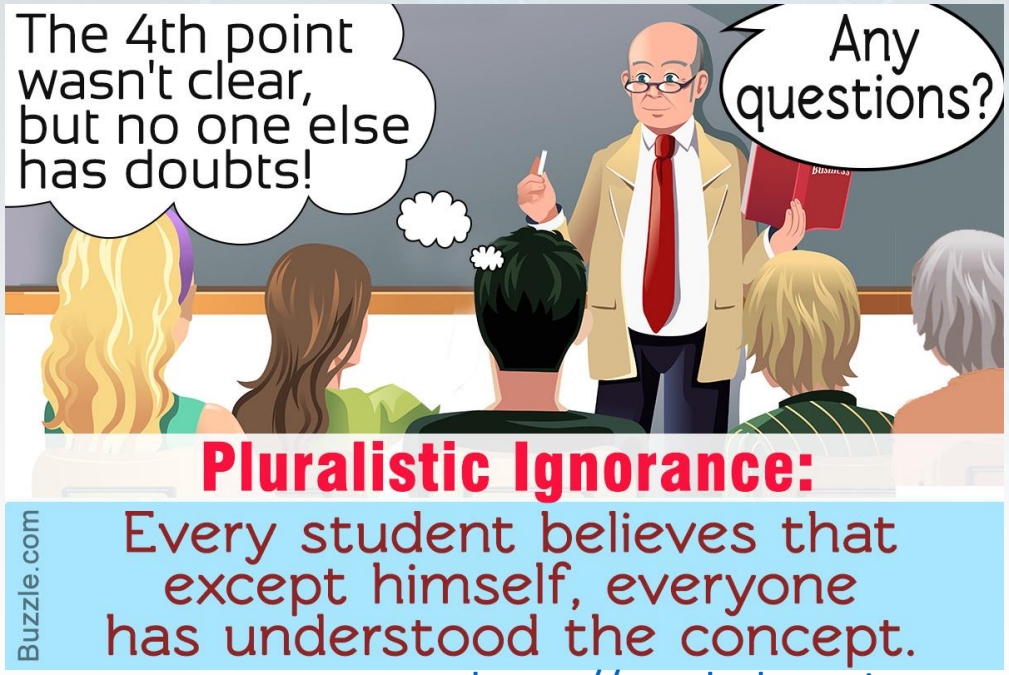
- Üks tööriistu, mida me kasutame õige kindlaksmääramiseks, on teada saada, mida teised inimesed õigeks peavad.
- Mida rohkem inimesi leiab, et idee on õige, seda õigem on idee (demokraatia).

[Cialdini, 2007]

Funded by the Erasmus+ Programme of the European Union

Consensus - Üksmeel

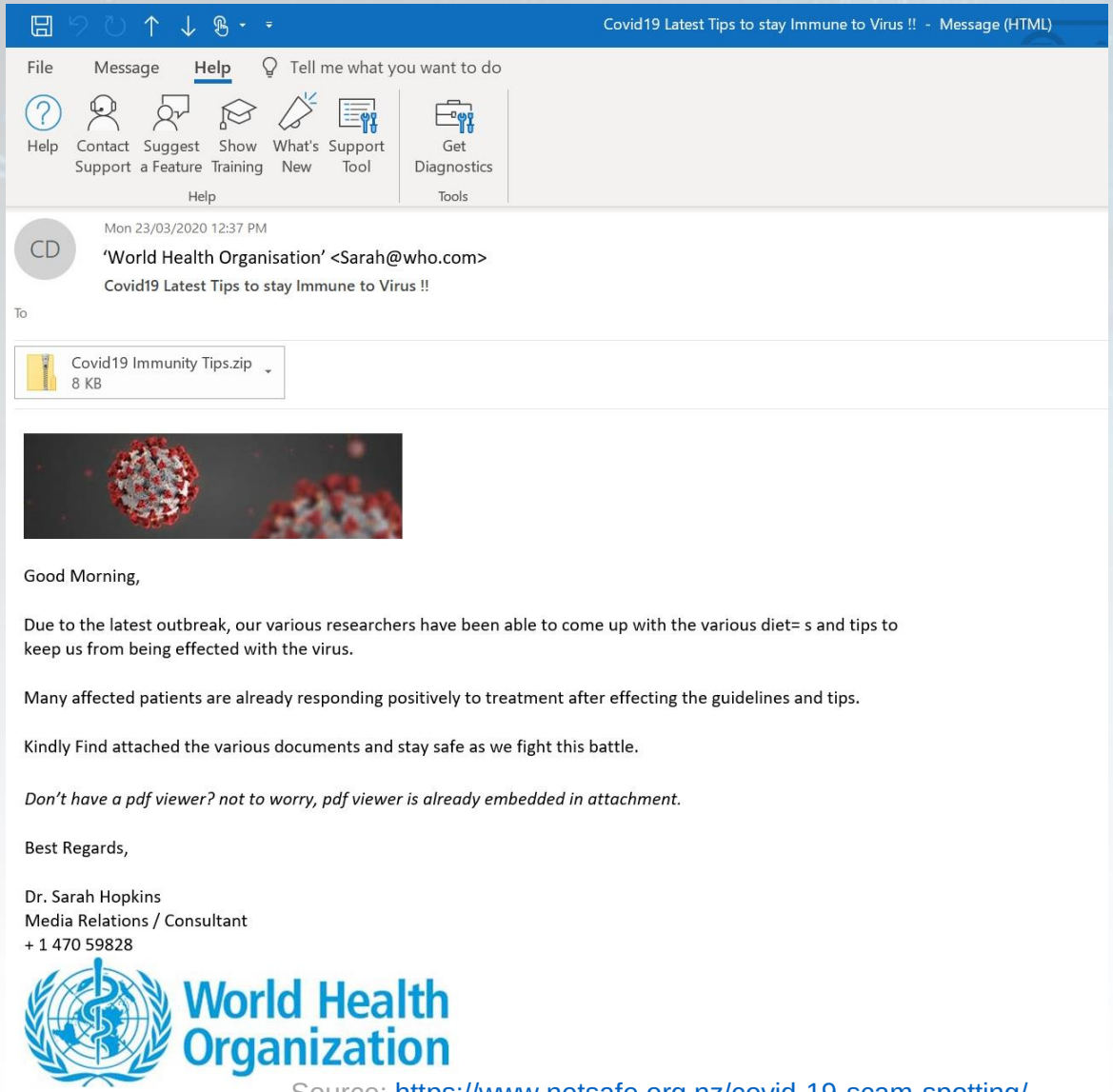
- Pluralistlik teadmatus: iga inimene otsustab, et kuna keegi pole mures, pole midagi valesti



https://psychologenie.com

[Cialdini, 2007]

Consensus
Üksmeel



Covid19 Latest Tips to stay Immune to Virus !! - Message (HTML)

File Message Help Tell me what you want to do

Help | Contact Support | Suggest a Feature | Show Training | What's New | Support Tool | Get Diagnostics

Help Tools

CD

Mon 23/03/2020 12:37 PM

'World Health Organisation' <Sarah@who.com>

Covid19 Latest Tips to stay Immune to Virus !!

To

Covid19 Immunity Tips.zip
8 KB

Good Morning,

Due to the latest outbreak, our various researchers have been able to come up with the various diet= s and tips to keep us from being effected with the virus.

Many affected patients are already responding positively to treatment after effecting the guidelines and tips.

Kindly Find attached the various documents and stay safe as we fight this battle.

Don't have a pdf viewer? not to worry, pdf viewer is already embedded in attachment.

Best Regards,

Dr. Sarah Hopkins
Media Relations / Consultant
+ 1 470 59828

World Health Organization

Source: https://www.netsafe.org.nz/covid-19-scam-spotting/

Scarcity - Nappus

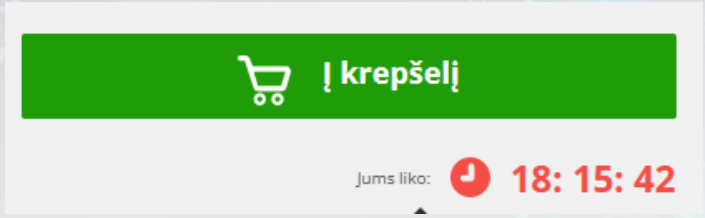
- Võimalused tunduvad meile väärtuslikumad, kui nende kättesaadavus on piiratud.
- Me tahame seda veelgi rohkem, kui oleme selle nimel konkureerinud

[Cialdini, 2007]

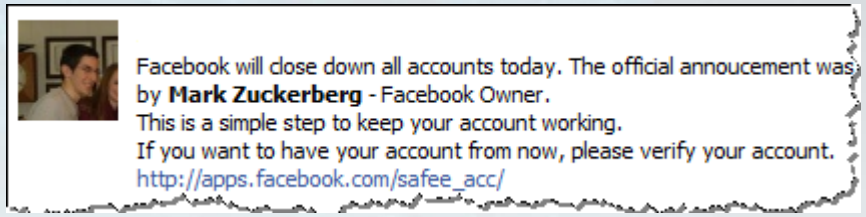
Funded by the Erasmus+ Programme of the European Union

Scarcity - Nappus

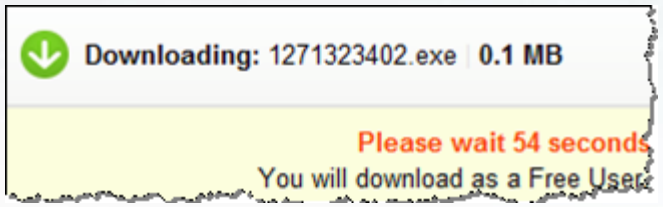
- Ajapiirang



Source: https://pigu.lt/lt/

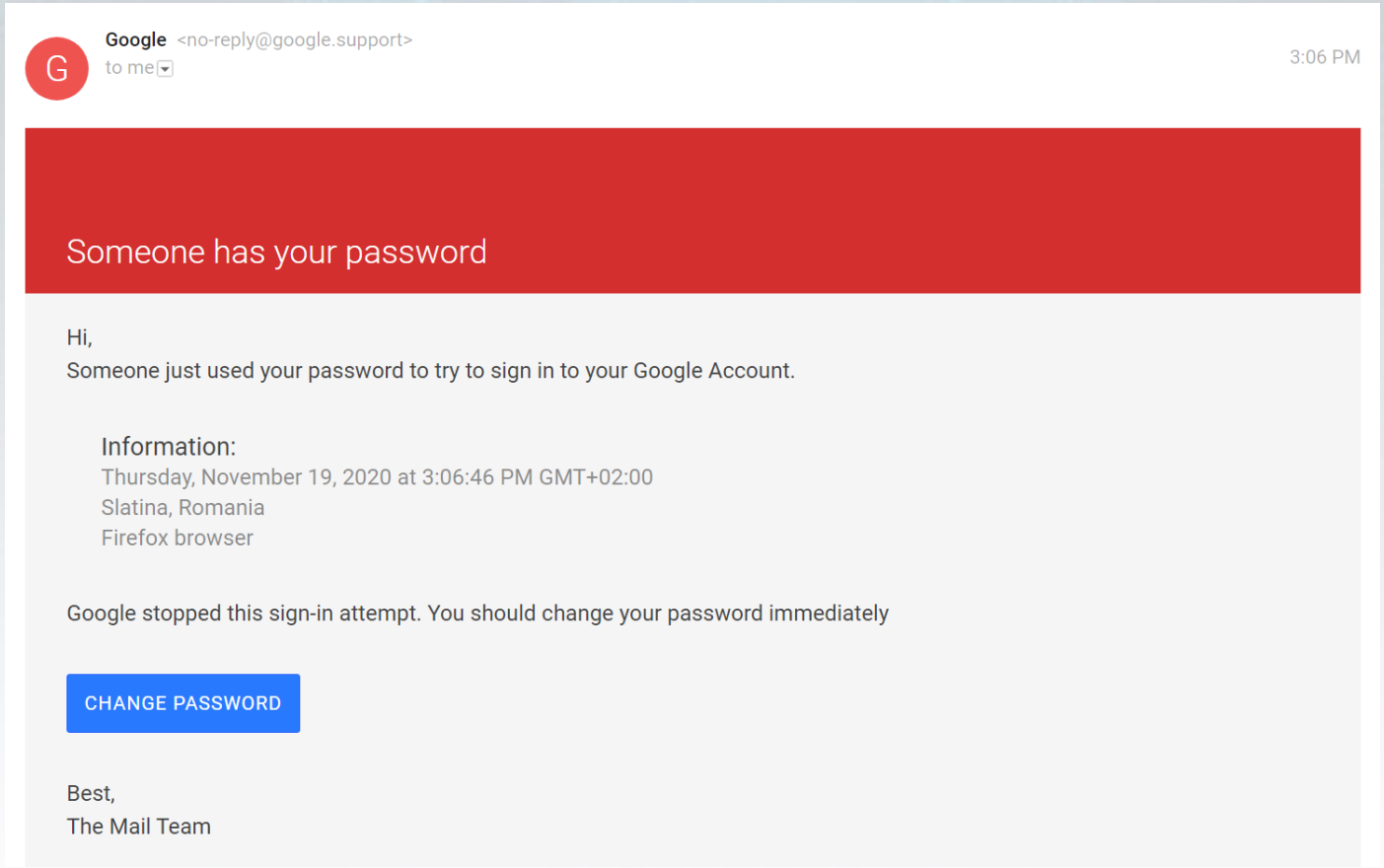


- Takistuste piiramine



Source: https://zeltser.com/how-the-scarcity-principle-is-used-in-online-scams-and/

Scarcity - Nappus



Google <no-reply@google.support>
to me
3:06 PM

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Thursday, November 19, 2020 at 3:06:46 PM GMT+02:00
Slatina, Romania
Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

CHANGE PASSWORD

Best,
The Mail Team

Source: https://au.pcmag.com/

Unity - Ühtsus

- 7. veenmise põhimõte, mille lisas hiljem dr Robert Cialdini
- Lähtudes ideest, et mida rohkem me end teistega samastame, seda tõenäolisemalt oleme neist mõjutatud

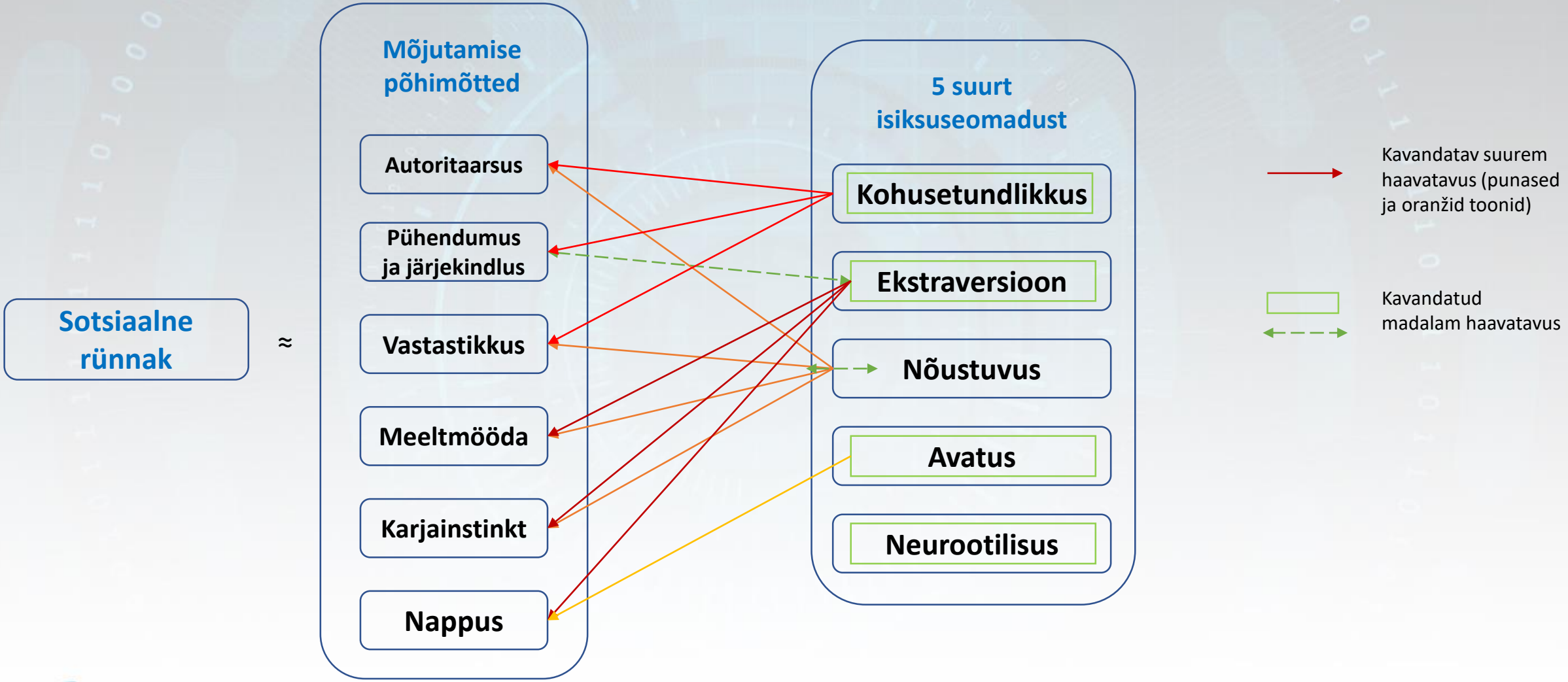
Funded by the Erasmus+ Programme of the European Union

Sotsiaalse rünnaku isiksuse raamistik (SEPF)

Avatus	Kohusetundlikkus	Ekstraversioon	Nõustuvus	Neurootilisus
Fantaasia Esteetika Tunded Tegevused Ideed Väärtused	Pädevus Tellimus Kohusetundlikkus Saavutus Püüdlemine Enesedistsipliin Arutlemine	Soojus Kogudus Eenesekehtestamine Tegevus Põnevuse otsimine Positiivne emotsioon	Usalda Otsekohesus Altruism Vastavus Tagasihoidlikkus Hellameelsus	Ärevus Vaenulikkus Depressioon Eneseteadvus Impulsiivsus Haavatavus stressi suhtes

Source: Susanne Quiel "The Social Engineering Personality Framework"

Sotsiaalse rünnaku isiksuse raamistik(SEPF)



Source: Susanne Quiel "The Social Engineering Personality Framework"

Pööratud suhtlusrünnak

- Sotsiaalne ründaja ei algata ohvriga kontakti
- Rünnak on korraldatud nii, et ohver ise pöördus abi saamiseks ründaja poole
- Kõrge usaldusega suhe luuakse siis, kui selle algatab ohver.

Funded by the Erasmus+ Programme of the European Union

Pööratud suhtlusrünnak

- Tavaliselt realiseeritakse see kolmes etapis:
  - Luuakse sööt või ettekääne, mis ärgitab ohvri huvi või uudishimu (sihtmärgi varustus on saboteeritud või kahjustatud)
  - Tagatakse, et sihtmärk teab, et ründaja on autoriteetne isik ja tal on varustuse parandamiseks vajalikud oskused
  - Abistatakse probleemi lahendamisel, usaldusliku suhte loomisel ja juurdepääsul sihtinformatsioonile või muudele ressurssidele.

Funded by the Erasmus+ Programme of the European Union

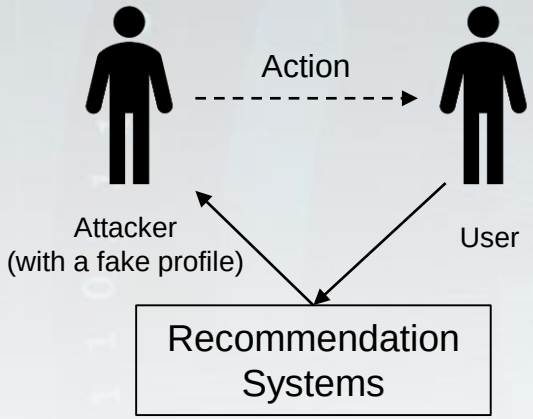
Pööratud suhtlusrünnak

- Sihitud/Sihitu
  Sihitud rünnaku korral keskendub ründaja konkreetsele kasutajale. Seevastu sihitu rünnaku korral on ründaja huvitatud ainult võimalikult paljude kasutajateni jõudmisest
- Otsene/vahendatud
  Otsese rünnaku korral on ründaja peibutustegevus sihitud kasutajatele nähtav. Vahendatud rünnakud seevastu järgivad kaheastmelist lähenemisviisi, mille käigus kogub sööda kokku vaheagent, kes seejärel vastutab selle levitamise eest (sageli erineval kujul) sihtkasutajatele.

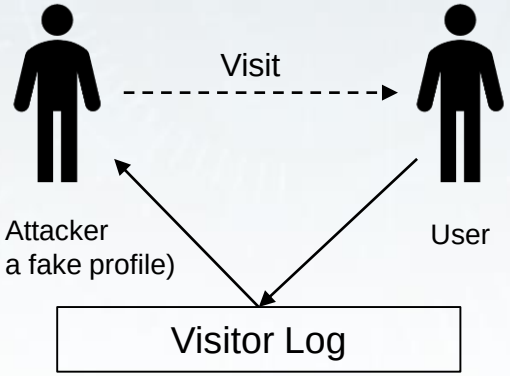
[Irani at al. 2011]

Funded by the Erasmus+ Programme of the European Union

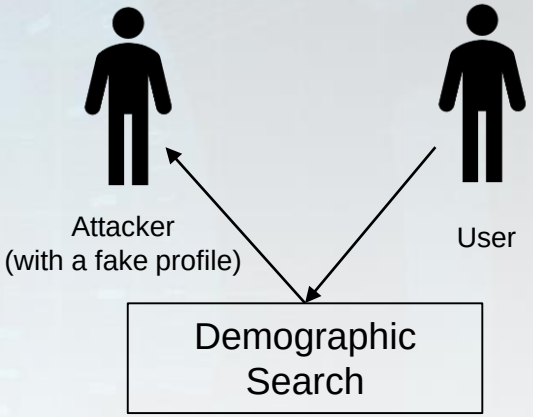
Erinevad pööratud suhtlusrünnakud



(a) Recommendation Systems



(c) Visitor Tracking



(b) Demographic Search

[Irani at al. 2011]

Soovituses suhtlusrünnaku vältimiseks

- Treenige oma teadlikkust veenmise ja manipuleerimise äratundmiseks
  - Kas mu emotsioonid on kõrgendatud?
  - Kas see sõnum tuli seaduslikult saatjalt?
  - Kas mu sõber saatis mulle selle sõnumi?
  - Kas see pakkumine kõlab liiga hästi, et tõsi olla?
  - Kas manused või lingid on kahtlased?
  - Kas see inimene suudab oma isikut tõendada?

Funded by the
Erasmus+ Programme
of the European Union

Soovituses suhtlusrünnaku vältimiseks

- Hallake oma isikuandmeid
  - Tea, millised teie isikuandmed on Internetis saadaval.
- Kaitske ennast
  - Hallake kontosid ja paroole.
  - Kasutage mitmefaktorilist autentimist
  - Hoidke tarkvara ajakohasena
  - Luba rämpspostifilter
  - Kaitske oma seadmeid

Funded by the Erasmus+ Programme of the European Union

Suhtlusründe arengusuunad

1. Nõusoleku andmepüügi suurenemine
2. Ettevõtte e-posti kompromiteerimine muutub kulukamaks
3. Deepvõltsingud tekitavad sügavamaid väljakutseid
4. Rahvusriikide ründajad, kelle arsenalis on suhtlusrünnak
5. Andmepüügi kui teenuse turu laienemine

6. Kasutajate teadlikkus pole enam kohustuslik – see on hädavajalik!

Funded by the Erasmus+ Programme of the European Union

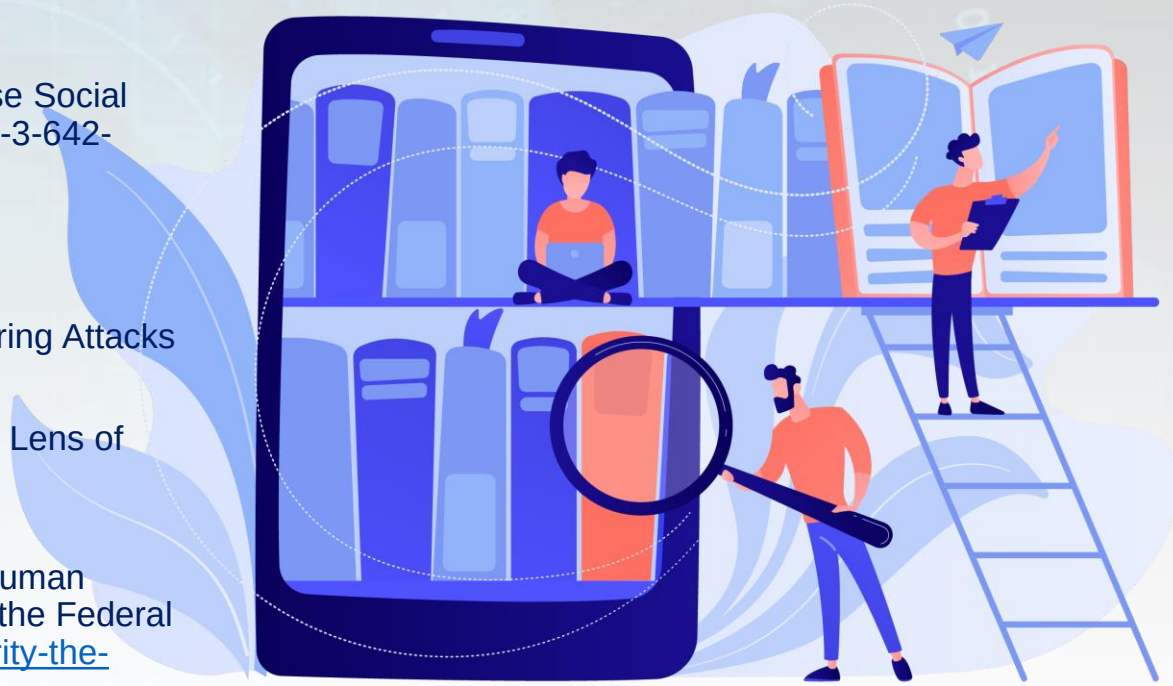
Ülesanded

- Arutage koroonaviiruse pettuste rünnakute sagenemise põhjuseid
- Arutlege Basecapi rakendatava mõju põhimõtte üle
- Arutage, milliseid veenmisrünnakuid olete kohanud

Lisalugemist

Material used in preparation of this lecture

- **Cialdini, R. B.** (2007) Influence: the psychology of persuasion. Rev. ed. ; 1st Collins business essentials ed. New York: Collins.
- **Hadnagy, C.** (2018) *Social engineering: The art of human hacking*. Indianapolis:John Wiley & Sons.
- **Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., Pu, C**. (2011). Reverse Social Engineering Attacks in Online Social Networks. 55-74. doi:10.1007/978-3-642-22424-9_4.
- **McLeod, S. A.** (2014). Techniques of compliance. Retrieved from https://www.simplypsychology.org/compliance.htm
- **Merwe, J. Mouton, F.** (2017). Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle. HAISA.
- **Montañez, R., Golob, E., Xu, S.** (2020) Human Cognition Through the Lens of Social Engineering Cyberattacks. *Front. Psychol.* 11:1755. doi: 10.3389/fpsyg.2020.01755
- **Walker, E. Witkowski, D. Benczik, S. Jarrin, P.** Cybersecurity – the Human Factor. Prioritizing People Solutions to improve the cyber resiliency of the Federal workforce. Retrieved from https://documents.pub/document/cybersecurity-the-human-factor-nist-computer-the-human-factor-prioritizing.html
- **Washo, A.** (2021) An interdisciplinary view of social engineering: A call to action for research. Computers in Human Behavior Reports. Vol. 4. 2021. 100126.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Lühivideod

- Science Of Persuasion
  https://youtu.be/cFdCzN7RYbw
- Hacking challenge at DEFCON
  https://www.youtube.com/watch?v=fHhNWAKw0bY
- Breaking into company under 2 min

  https://www.youtube.com/watch?v=PWVN3Rq4gzw

Tänan kuulamast