



Funded by the
Erasmus+ Programme
of the European Union

Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana

Sociālās inženierijas moduļi un manipulācijas

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.



Apmācību mērķis



- Izskaidrot ietekmēšanas un manipulācijas paņēmienus un iemācieties tos atpazīt
- Izskaidrot sociālo inženieriju un tās psiholoģiskos aspektus.
- Apskatīt, kā lēmumu pieņemšanu ietekmē emocijas, darba slodze un visa mūsu vide.
- Izskaidrot ietekmēšanas un manipulācijas paņēmienus un iemācieties tos atpazīt

Kursantu darba slodze



Lekcija	4 st.
Audio un video materiāli	2 st.
Pētījumi	2 st.
Papildu lasīšana	8 st.
Sagatavošanās eksāmenam	1 st.

Saturs

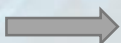
- Cilvēciskais faktors
- Sociālā inženierija
- Lēmumu pieņemšanas process
- Sociālās inženierijas psiholoģiskie aspekti
 - Emocijas
 - Ietekmes ieroči
- Reversā sociālā inženierija
- Padomi sociālās inženierijas novēršanai

Cilvēciskais faktors

**USD 400
mljd.**



Paredzamās izmaksas par
kiberuzbrukumiem
organizācijām visā
pasaulē

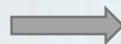


Organizācijas reti ievieš kiberdrošības cilvēcisko komponentu vai plāno to izmantot līdz brīdim, kad noticis uzbrukums. Lielu pārkāpumu gadījumā organizācijai tas var izmaksāt miljoniem dolāru.

35%



no datu pārkāpumiem tika
saistīti ar cilvēka kļūdām
vai nolaidību

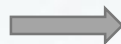


Kiberdraudu veidi un novēršanas metodes mainās katru dienu. Kiberinteresu un izpratnes kultūras iedibināšana nodrošina tādas organizācijas pastāvēšanu, kas spēj labāk tikt galā ar mainīgajiem kiberdrošības apdraudējumiem.

47%



IT speciālisti sadarbību starp
drošības risku pārvaldību un
biznesu raksturo kā vāju vai vispār
neesošu



Daudzi vadītāji domā, ka kiberdrošība ir IT daļas atbildība; drīzāk tā ir katra paša atbildība. Darbinieku informētībai ir jābūt pirmajai organizācijas digitālo līdzekļu un aktīvu aizsardzības fronteī.

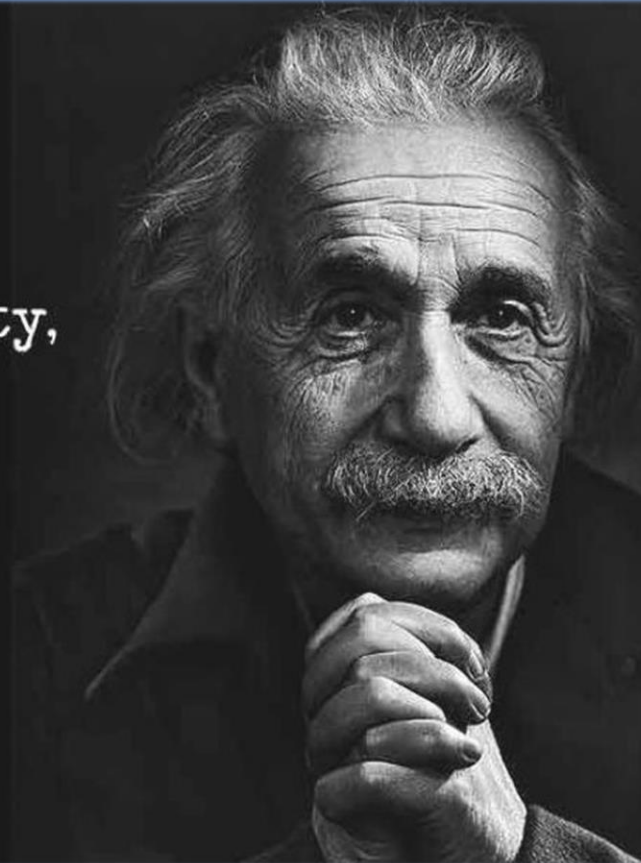
Cilvēciskais faktors

- Cilvēki bieži vien ir vājākais posms drošības ķēdē un ir hroniski atbildīgi par drošības sistēmu kļūmēm.
- Tehniskie drošības pasākumi nemitīgi attīstās, bet cilvēki nemainās, paliekot kā vājākais posms informācijas drošībā ar savām vājībām, stereotipiem un attieksmi

Cilvēciskais faktors

Only two things are infinite,
the universe and human stupidity,
and I'm not sure about
the former.

Albert Einstein



Avots: <https://iheartintelligence.com/>

Kas ir sociālā inženierija?

“

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

”

Kas ir sociālā inženierija?

- Sociālo inženieriju var definēt kā manipulāciju ar cilvēkiem, visbiežāk izmantojot psiholoģisku pārliecināšanu, lai piekļūtu sistēmām, kas satur datus, dokumentus un informāciju, kuras iegūšanas spējai sociālajam inženierim nevajadzētu pastāvēt.
- Sociālā inženierija ir cilvēka psiholoģijas izmantošanas māksla, nevis tehniskas uzlaušanas metodes, lai piekļūtu ēkām, sistēmām vai datiem.

Sociālā inženierija Statistika

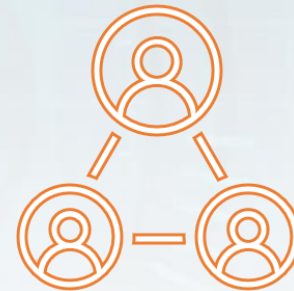


98% kiberuzbrukumu ir
balstīti uz sociālo
inženieriju

/



Pagājušajā gadā no
sociālās inženierijas
mērķauditorijas 43%
bija IT profesionāļi

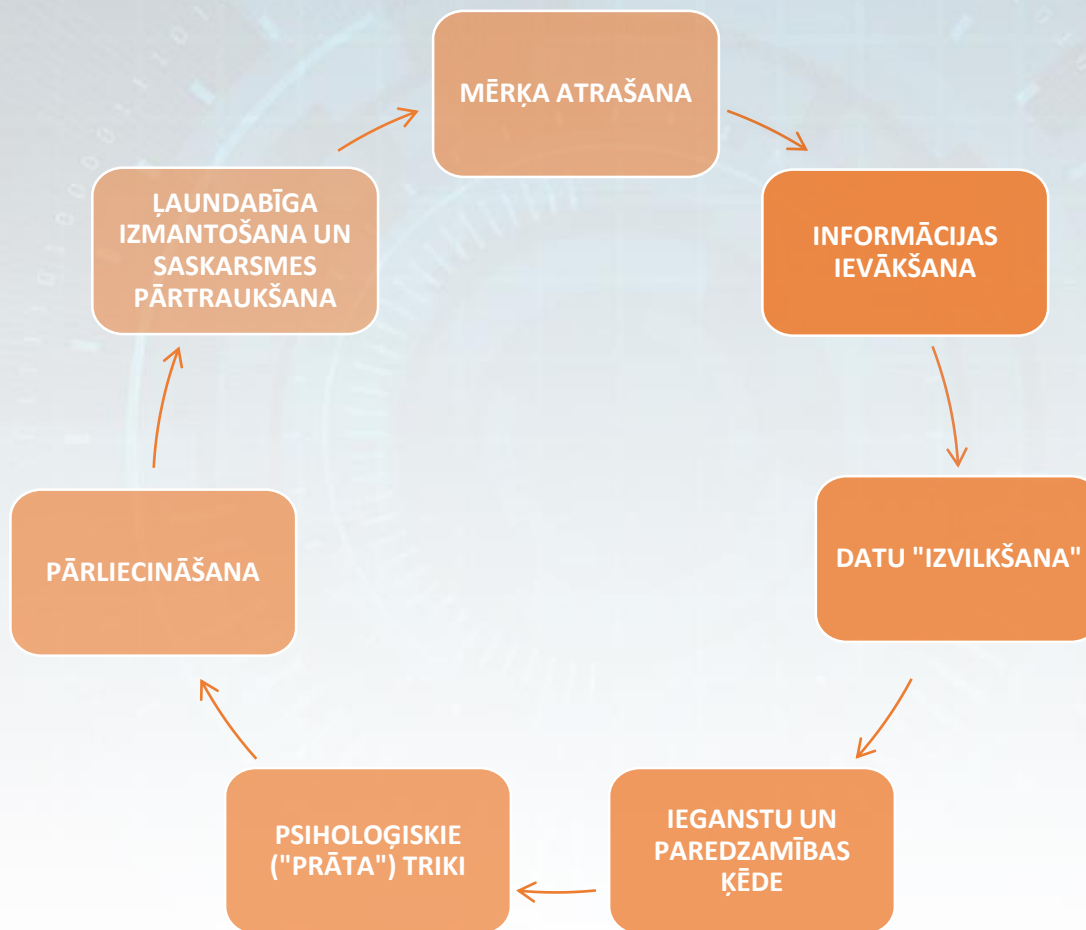


21% pašreizējo vai
bijušo darbinieku
izmanto sociālo
inženieriju

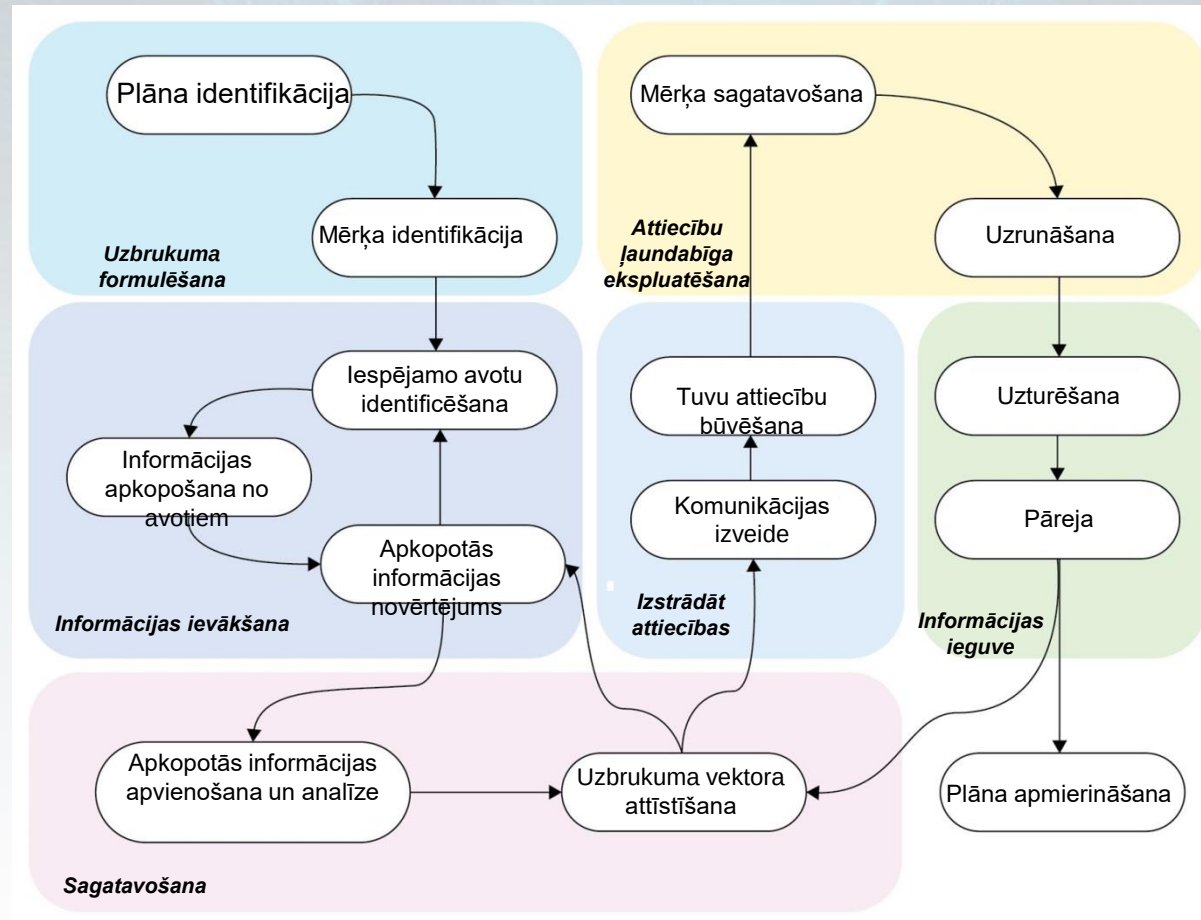


Sociālās inženierijas
mēģinājumi 2018. gadā
pieauga par vairāk nekā
500%.

Sociālās inženierijas ietvars



Sociālās inženierijas “ceļvedis”



Avots: dr. Erdals Ozkaja [Dr. Erdal Ozkaya] "Apgūsim sociālo inženieriju", 2018. gads

1. solis: Mērķa atrašana

- Sociālā inženierija – konkrētam mērķim
- Mērķa izvēle, pamatojoties uz galīgiem “rezultātiem” (piemēram, informācija, naudas līdzekļi utt.)



2. solis: Informācijas ievākšana

- Vislīkumotākais solis visā sociālās inženierijas procesā.
- Var ilgt no dažām stundām līdz dažiem gadiem.
- Informācija reti tiek apkopota visa uzreiz.
- Sociālo mediju platformu izmantošana, specializēta programmatūra, emocionālo prasmju pielietošana
- Divi veidi, kā iegūt datus:
 - *Netehniskās/mehāniskas metodes*
 - *Tehniskās metodes*



3. solis: Datu vai rīcības "izvilkšana"

Izvilkšanu var definēt kā darbību, kurā kaut kas tiek izvilkts vai iegūts, izmantojot loģikas paņēmienus. Tas tiek darīts, stimulējot, lai liktu personai rīkoties noteiktā uzvedības klasē vai kategorijā.

Faktori, kas padara izvilkšanu efektīvu:

- Lielākā daļa cilvēku centīsies būt pieklājīgi, runājot ar svešinieku;
- Profesionāļi, kad tie tiek aptaujāti, vēlēšies izskatīties zinoši;
- Lielākā daļa cilvēku nemelotu kādam, kurš šķiet patiesi noraizējies;
- Visticamāk, ka kāds atbildēs uz labi frāzētiem un uzdotiem jautājumiem par sevi.



4. solis: ieganstu un paredzamības ķēde

Ieganstu un paredzamības ķēde ir obligāta prasme, kas nepieciešama ikvienam sociālajam inženierim, lai veiktu uzbrukumu.

Ieganstu un paredzamības ķēde ieliek cilvēku cita cilvēka ādā.

Vispārējie ieganstu un paredzamības ķēdes principi:

- veikt papildu izmeklēšanu;
- izmantot personīgās intereses;
- praktizēt izteicienus vai dialektus;
- izmantot vienkāršus ieganstus un paredzamības;
- loģiski secinājumi vai kopsavilkums.



5. solis: Psiholoģiskie ("prāta") triki

Prāta triki ir vairāk psiholoģiska lieta, un tos izmanto, lai atbloķētu mērķa personu prātus, pakļaujot tos sociālā inženiera kontrolei.

PRĀTA TRIKU ZINĀTNE≠

Cilvēkā var ļaunprātīgi ekspluatēt trīs dažādus domāšanas veidus:

1. **Vizuālā domāšana;**
2. **Auditoriskā domāšana;**
3. **Kinestētiskā domāšana.**



6. solis: Pārliecināšana

Lai pārliecinātu mērķi, sociālajam inženierim vispirms ir jāapelē pie mērķa interesēm. Pārliecināšanas rezultātā mērķa persona reaģē, domā un dara tieši tā, kā vēlas sociālais inženieris.

5 pamati, ko pārliecināšanā izmanto sociālie inženieri:

1. Skaidri mērķi;
2. Emocionālā saikne;
3. Atrašanās uz viena "viļņa";
4. Fleksibilitāte;
5. Savstarpēja apmainīšanās ar atlīdzību.



7. solis: Eksploatēšana un kontakta izbeigšana

- Upura eksploatēšana, kad ir izveidota uzticēšanās un noskaidrots vājums, lai virzītu uzbrukumu
- Kontakta izbeigšana, kad lietotājs ir veicis vēlamo darbību



Sociālās inženierijas uzbrukuma ontoloģiskais modelis



Sociālās inženierijas uzbrukumi

Vairāki cilvēki zaudēja tūkstošiem dolāru kriptovalūtā pēc tam, kad 2017. gadā tika uzlauzta vietne Ethereum Classic. Izmantojot sociālo inženieriju, hakeri uzdevās par Classic Ether maku īpašniekiem, ieguva piekļuvi domēna reģistram un pēc tam novirzīja domēnu uz savu serveri. Noziedznieki no upuriem izvilka Ethereum kriptovalūtu pēc koda ievadīšanas vietnē, kas ļāva viņiem skatīt privātās atslēgas, kas tiek izmantotas darījumiem.

Sociālās inženierijas uzbrukumi

Shark Tank televīzijas tiesnese Barbara Korkorana [*Barbara Corcoran*] 2020. gadā tika pieviltā gandrīz 400 000 USD vērtā pikšķerēšanas un sociālās inženierijas krāpniecībā. Kibernoziēdznieks uzdevās par palīgu un nosūtīja grāmatvedei e-pastu, pieprasot atjaunošanas maksājumu saistībā ar ieguldījumiem nekustamajā īpašumā. Viņš izmantoja e-pasta adresi, kas ir līdzīga patiesajai. Krāpšana tika atklāta tikai pēc tam, kad grāmatvedis uz asistenta pareizo adresi nosūtīja e-pastu, jautājot par darījumu.

Sociālās inženierijas uzbrukumi

Vienu no lielākajiem sociālās inženierijas uzbrukumiem pret diviem no pasaules lielākajiem uzņēmumiem veica Lietuvas pilsonis Ēvalds Rimašauskis [*Evaldas Rimasauskas*]: uzbrukums bija virzīts pret Google un Facebook.

Rimašauskis un viņa komanda izveidoja viltus uzņēmumu, uzdodoties par datoru ražotāju, kas sadarbojas ar Google un Facebook. Rimšauskis arī izveidoja bankas kontus uz uzņēmuma vārda.

Pēc tam krāpnieki nosūtīja pikšķerēšanas e-pastus konkrētiem Google un Facebook darbiniekiem, izrakstot viņiem rēķinus par precēm un pakalpojumiem, ko ražotājs bija patiesi nodrošinājis – bet liekot viņiem iemaksāt naudu savos krāpnieciskajos kontos. Laikā no 2013. līdz 2015. gadam Rimašauskis un viņa domubiedri izkrāpa abiem tehnoloģiju gigantiem vairāk nekā 100 miljonus ASV dolāru.

Kāpēc sociālā inženierija ir tik efektīva?

- Mēs pēc dabas esam sociālas būtnes;
 - Mums piemīt vēlme atšķirties no pārējiem;
- Citi cilvēki būtiskā apjomā ietekmē mūsu pieņemtos lēmumus;
 - Mums piemīt vēlme būt izpalīdzīgiem;
 - Mums piemīt tendence uzticēties cilvēkiem, ko nepazīstam.

Kāpēc sociālā inženierija ir tik efektīva?

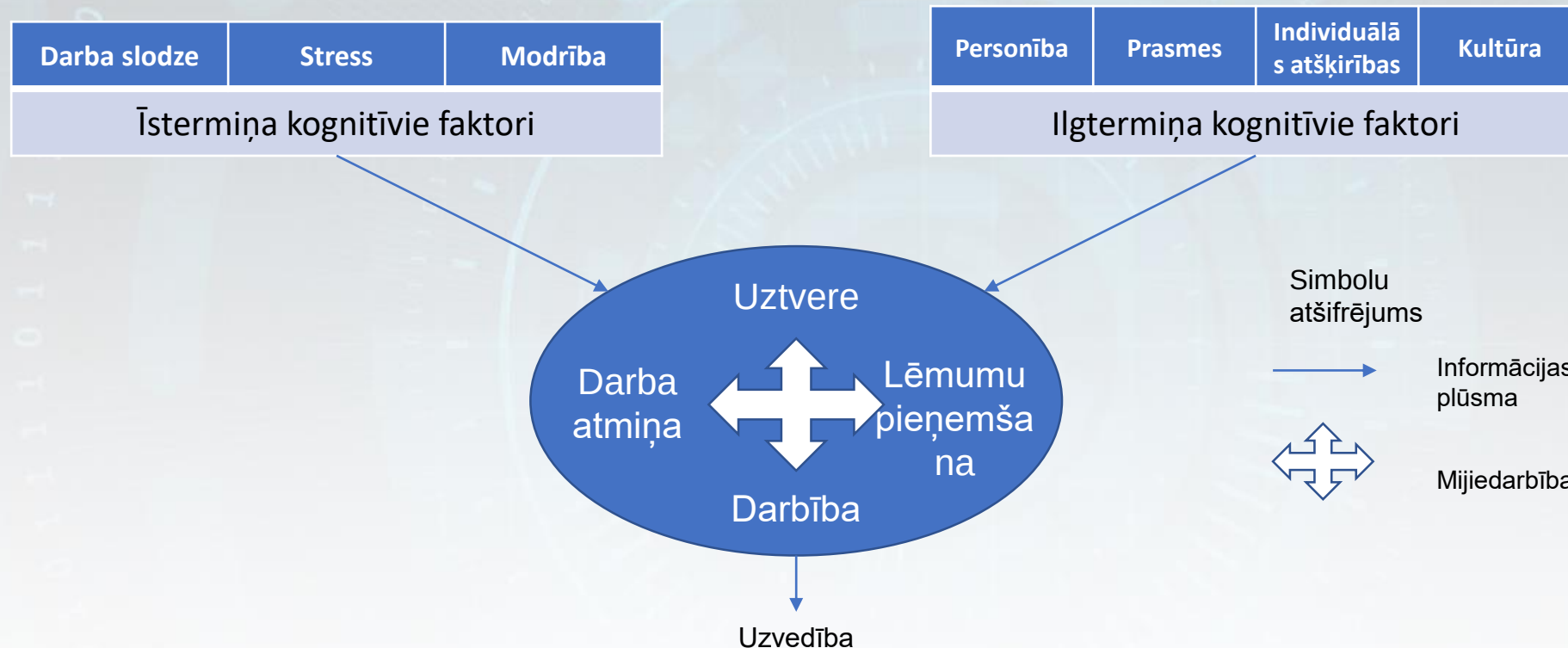
- Mēs tiekam pārslogoti ar informāciju un meklējam īsākos ceļus, lai ietaupītu laiku.
 - Mums piemīt vēlme, lai viss labais notiktu ātri un bez piepūles.
 - Mums piemīt bailes nokļūt nepatikšanās.
- Mums piemīt zināšanu trūkums par drošības apsvērumiem;
- Notiek pārlieta dalīšanās ar personīgo informāciju sociālajos medijos;

Sociālās inženierijas psiholoģiskie aspekti

Daži autori atbalsta sociālās inženierijas kiberuzbrukumu pastāvēšanu kā īpašu psiholoģisku uzbrukumu.



Cilvēka kognitīvās funkcijas



Liela kognitīvā darba slodze, augsts stresa līmenis, zema uzmanības un modrības pakāpe, zināšanu trūkums konkrētajā jomā un/vai iepriekšējās pieredzes trūkums padara cilvēku uzņēmīgāku pret sociālās inženierijas kiberuzbrukumiem.

Tiešsaistes pārliecināšanas psiholoģija

"Pašreizējā interneta patērētāju paaudze dzīvo tūlītēja apmierinājuma un ātru risinājumu pasaulē, kas noved pie pacietības zaudēšanas un padziļinātas domāšanas trūkuma." – Robs Vezerheds [Rob Weatherhead], laikraksts [The Guardian](#)

- Mūsu uzvedību, domas un uzskatus pastāvīgi veido apkārtējā vide, kā arī mūsu pašu dažādās pieredzes.
- Ietekme un pārliecināšanas māksla ir process, ar ko kāds cits panāk, ka upuris *vēlas* darīt, reaģēt, domāt vai ticēt tā, kā nepieciešams.

Sakāpinātas emocijas

Emocionālas manipulācijas sniedz uzbrucējiem virsroku jebkurā mijiedarbībā. Ir daudz lielāka iespēja veikt neracionālas vai riskantas darbības, ja esat paaugstinātā emocionālā stāvoklī.



Sakāpinātas emocijas



Bailes

COVID-19



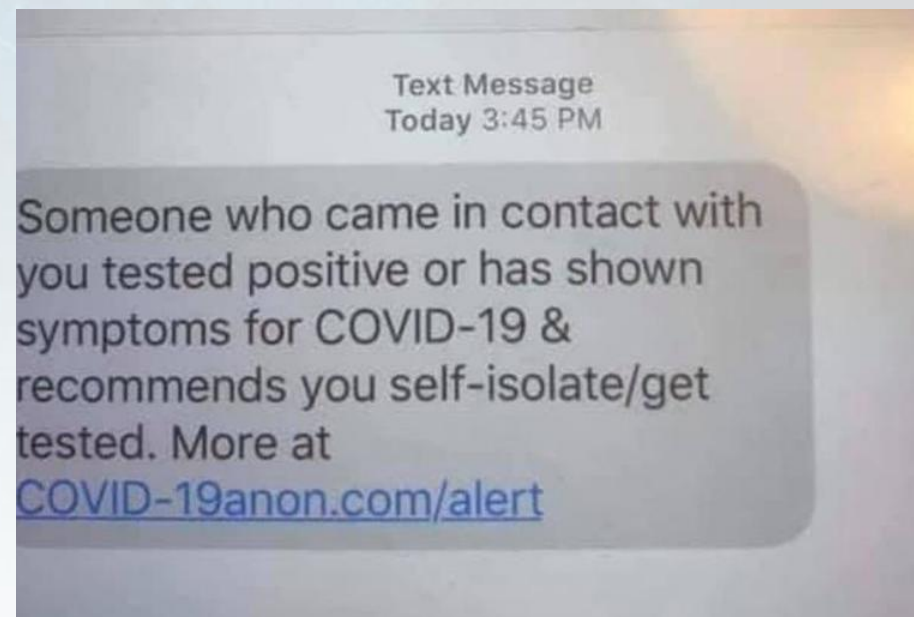
● nicholsschoolorg@alsummers.com <nicholsschoolorg@alsummers.com>

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

Avots: Viļņas Universitātes Kauņas fakultātes iekšējā pikšķerēšanas datubāze

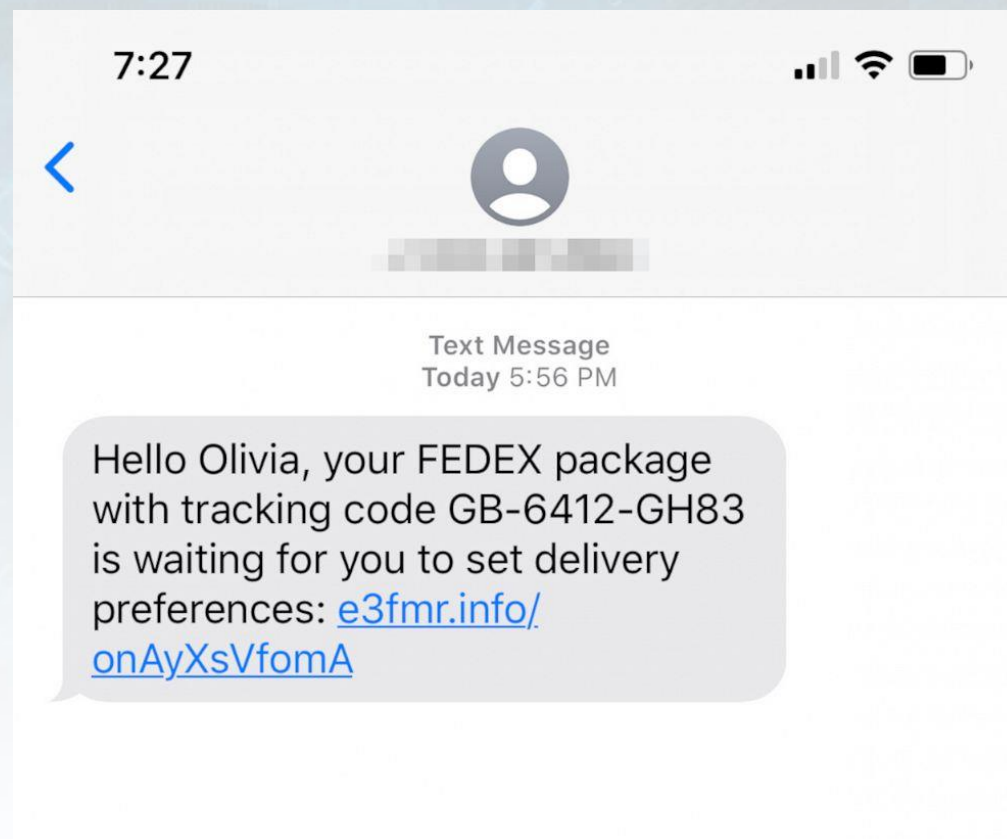


Avots: <https://www.thesun.co.uk/news/11422572/scam-message-hoax-tricks-americans-exposed-to-coronavirus-must-self-isolate/>

Ziņkārība



Avots: <https://soravjain.com/cyber-security-for-women-in-social-media/>



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

Izpalīdzīgums



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.

Avots: <https://usa.kaspersky.com/blog/fake-charity-scam/18580/>

Steidzamība

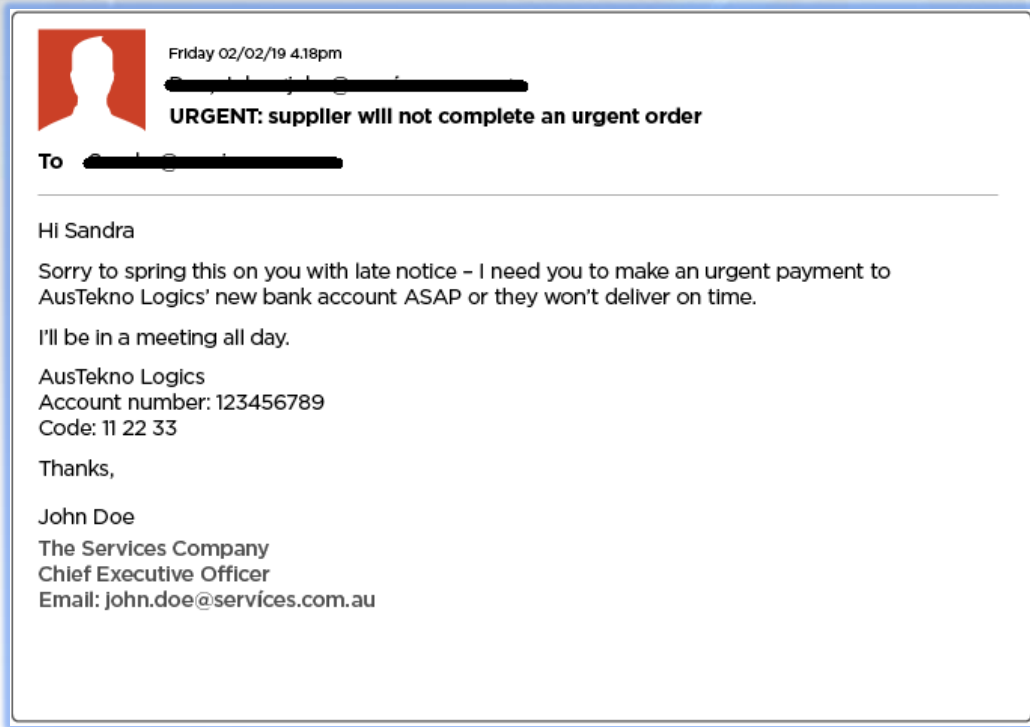
Laika ziņā sensitīvas iespējas vai pieprasījumi ir vēl viens uzticams rīks uzbrucēja arsenālā.

Lietotājs var būt motivēts kompromitēt sevi nopietnas problēmas iedomātā aizsegā, kurai nepieciešama tūlītēja uzmanība.

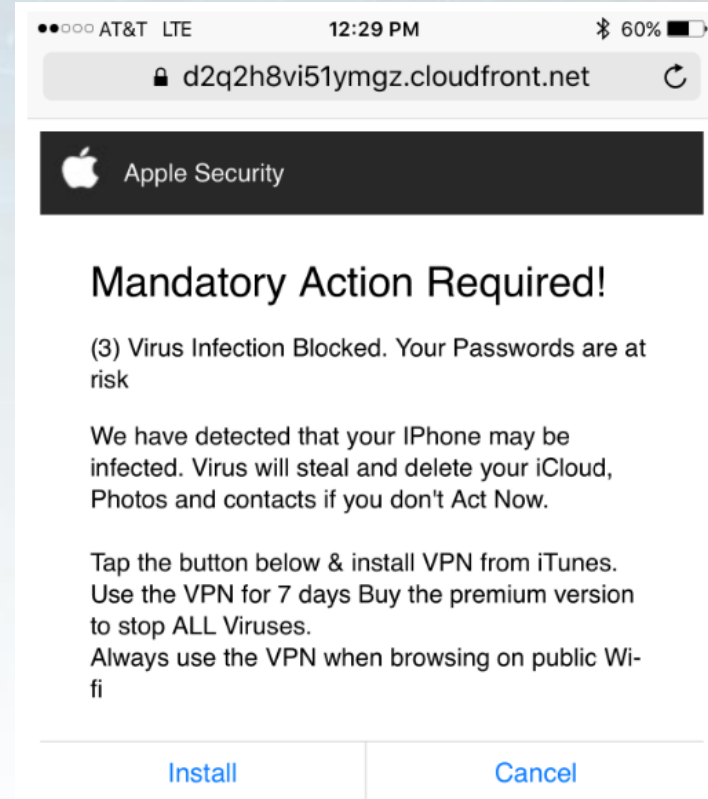
Alternatīvi, lietotājs var tikt pakļauts balvai vai atlīdzībai, kas var pazust, ja netiek veiktas ātras darbības.

Jebkura pieeja pārspēj lietotāja kritiskās domāšanas spējas.

Steidzamība



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



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



Funded by the
Erasmus+ Programme
of the European Union

Dusmas

- Mēs mēdzam izvairīties no dusmīgiem cilvēkiem
- Mēs mēdzam izvairīties no konfliktiem
- Dusmīgs "priekšnieks" zvana darbiniekam, lūdzot paroli



Alkatība

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.

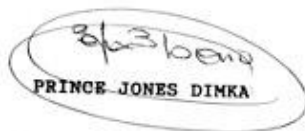
PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME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

- Tie ir daži no vecākajiem krāpniecības gadījumiem – bagātības solīšana no Nigērijas prinčiem vai militārpersonām, kas piedāvā dalīties ar kādu nozagtu dārgumu.
- Dažreiz tā ir bagāta atraitne, kas mirst no vēža, vai britu advokāts, kas sola nodrošināt mērķa personas mantojuma daļu.

Avots: <https://www.businessinsider.com/online-scams-internet-phishing-2019-3>

Invitation to Google Analytics users



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

To **media**

[Reply](#) [Reply All](#) [Forward](#) [...](#)

Thu 5/16/2019 12:56 AM

[i](#) 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](#)

Avots: Viļņas Universitātes Kauņas fakultātes iekšējā pikšķerēšanas datubāze

letekmes ieroči



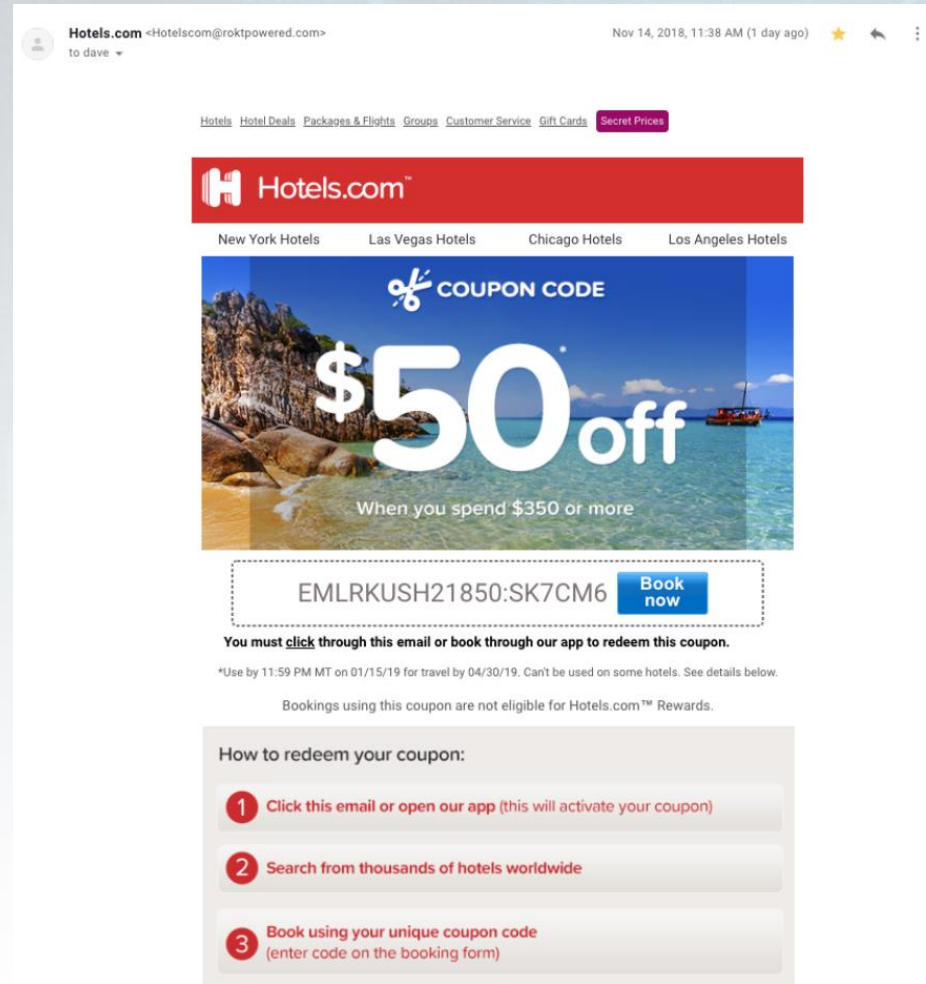
Apmainīšanās ar atlīdzību

- “...mums jācenšas natūrā atmaksāt to, ko mums ir sagādājusi cita persona.”
- 1. metode: Ja kāds piekāpjas, mums ir pienākums atbildēt ar piekāpšanos vai vērtības pametumu. Piekāpšanās rada otrai pusei atbildības sajūtu par rezultātu un lielāku gandarījumu par gūto risinājumu.

Apmainīšanās ar atlīdzību

- 2. metode: Noraidīšana un pēc tam atkāpšanās: pārspīlēts pieprasījums tiek noraidīts, vēlmais mazākais pieprasījums tiek pievienots sekojoši
- 3. metode: Kontrasta princips: vispirms pārdot dārgāko preci; vai vispirms uzrādīt nevēlamo iespēju

Apmaiņšanās ar atlīdzību



Avots: <https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email>

Konsekvence

- Mums ir "gandrīz obsesīva vēlme būt (un izskatīties) atbilstošiem un saskaņā ar to, ko jau esam paveikuši".
- Kad esam izdarījuši izvēli vai ieņēmuši nostāju, mēs saskaramies ar personisku un starppersonu spiedienu rīkoties atbilstoši šīm saistībām.

Konsekvence

- Kājas durvīs metode: piekrišana nelielam pieprasījumam palielina iespējamību, ka piekritīsiet otram, lielākam pieprasījumam.
- Durvju sejā tehnika: liela pieprasījuma noraidīšana palielina iespējamību, ka upuris piekritīs otram, mazākam pieprasījumam.

Konsekvence

- Zemākā piedāvājuma paņēmiens: pārliecinātājs liek personai apņemties izpildīt zemāko piedāvājumu, kuru viņam nav nodoma ievērot; un tad cena pēkšņi tiek paaugstināta. Tā kā cilvēks jau ir apņēmies, tad jaunajam augstākas cenas pieprasījumam ir grūti pateikt nē.

Konsekvence

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

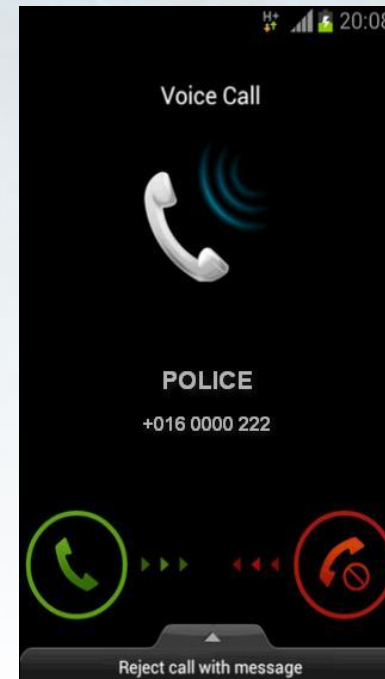
Avots: <https://www.forbes.com/sites/barrycollins/2021/07/07/is-this-amazon-email-fake-how-to-spot-the-scams/?sh=605d881d119a>

Autoritāte

- Informācija no atzītas iestādes var sniegt mums vērtīgu īsāku un vieglāku ceļu, lai izlemtu, kā rīkoties konkrētajā situācijā.
- Arvien vairāk mūsu cieši saistītajā pasaulē "patiesā" autoritāte ir indivīds, zīmols, organizācija vai sasniedzamais mērķis ar vislielāko auditoriju.

Autoritāte

- Amatu nosaukumi
- Uniformas
- Drēbes
- Zīmoli



Avots: <https://apkpure.com/nl/call-from-police/com.opik.fakegv.fyuukfq>



Autoritāte

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? There's pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me because 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 in case 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.

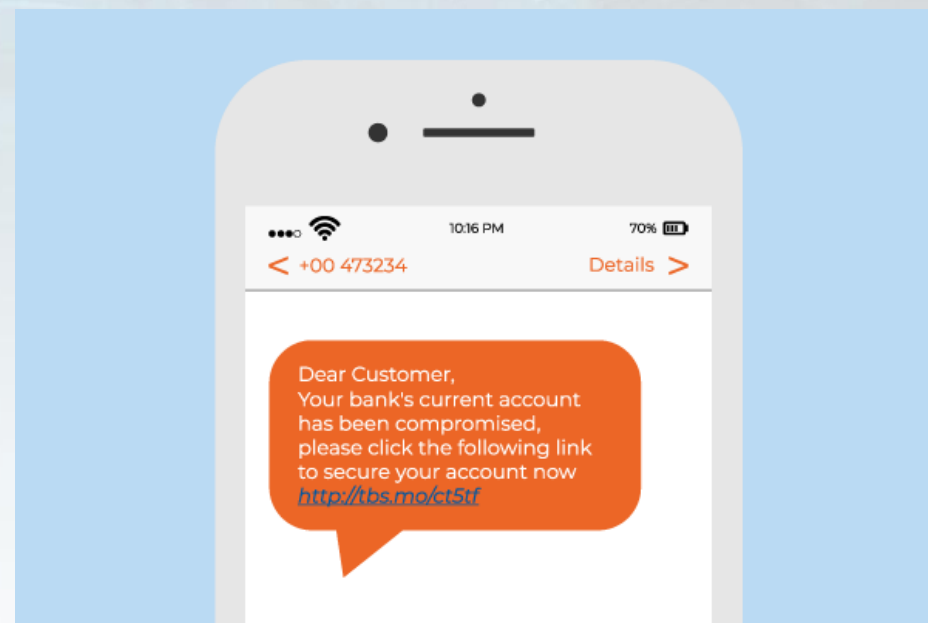
Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

Autoritāte



Avots: <https://www.twitter.com>



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

Patikšana

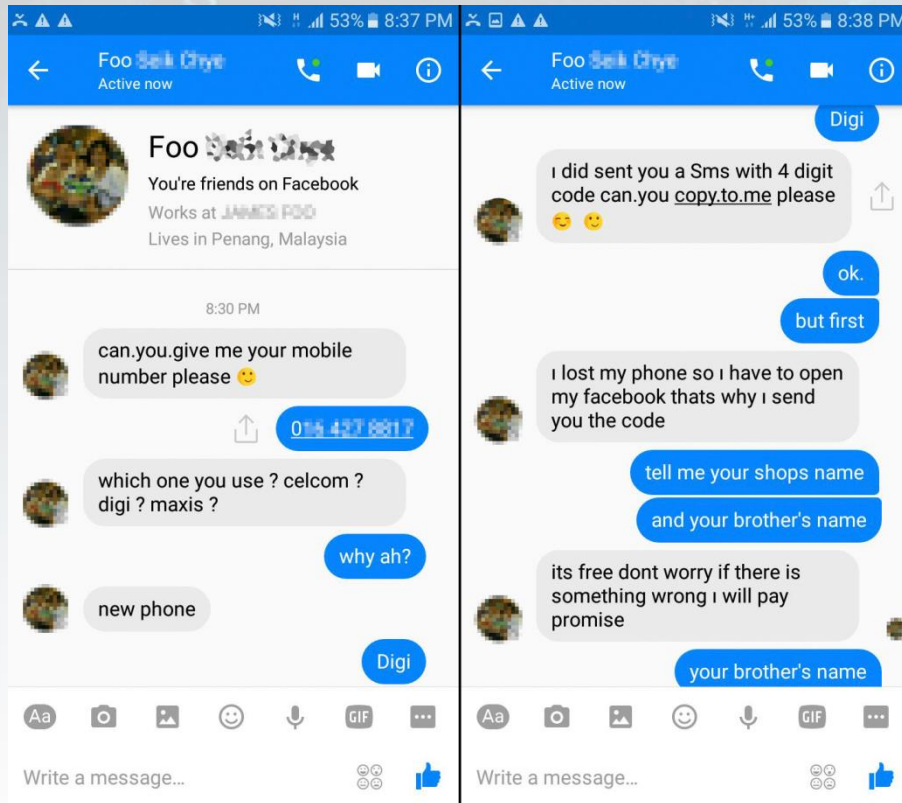
- Cilvēkiem patīk tie, kuriem viņi patīk, un viņus vairāk ietekmē tie, kas viņiem patīk
- Mēs esam priecīgi izpildīt pieprasījumus no cilvēkiem, kas mums patīk



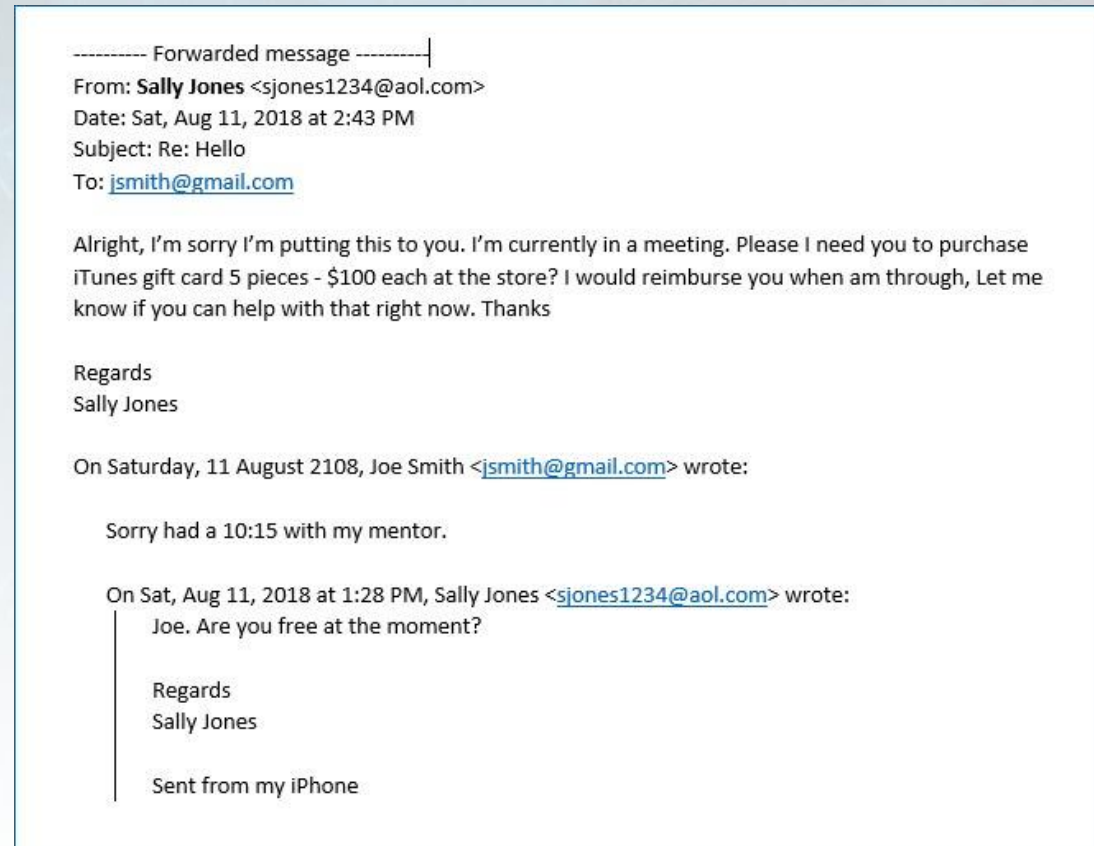
Patikšana

- Cilvēkiem ir tendence veidot uzticēšanos tiem, kas viņus piesaista gan fiziski, gan emocionāli:
 - Mums patīk cilvēki, kas ir līdzīgi mums
 - Mums patīk cilvēki, kuri izsaka mums komplimentus
 - Mums patīk cilvēki, kas ar mums sadarbojas, lai sasniegtu kopīgus mērķus

Patikšana



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



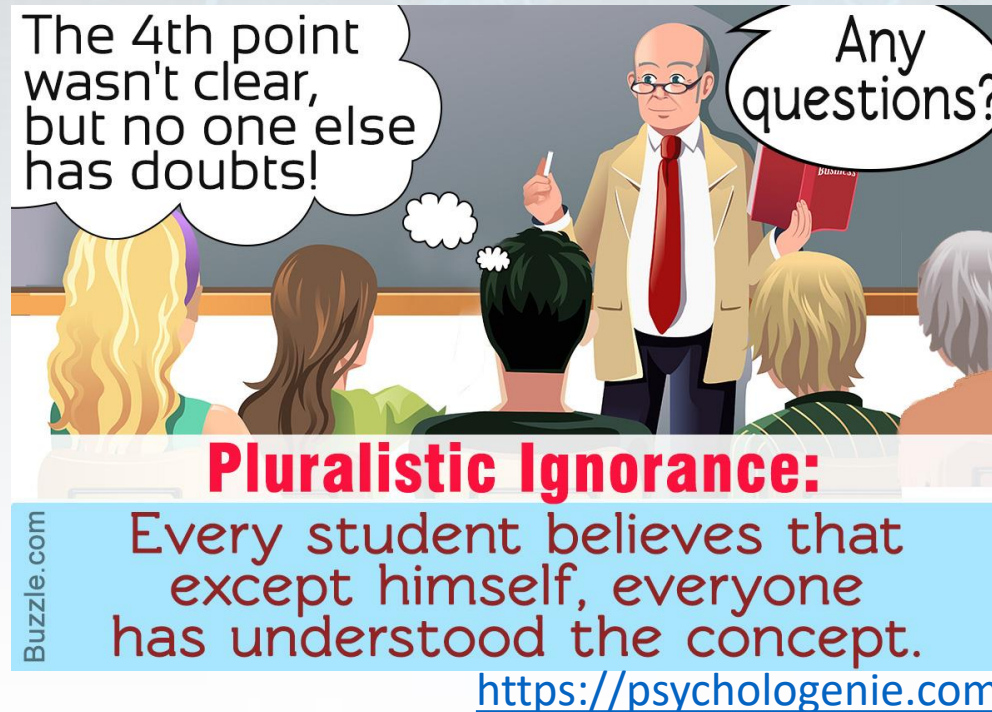
Avots: <https://www.apa.org/about/division/digest/leader-resources/convention-email-scams/>

Vienprātība

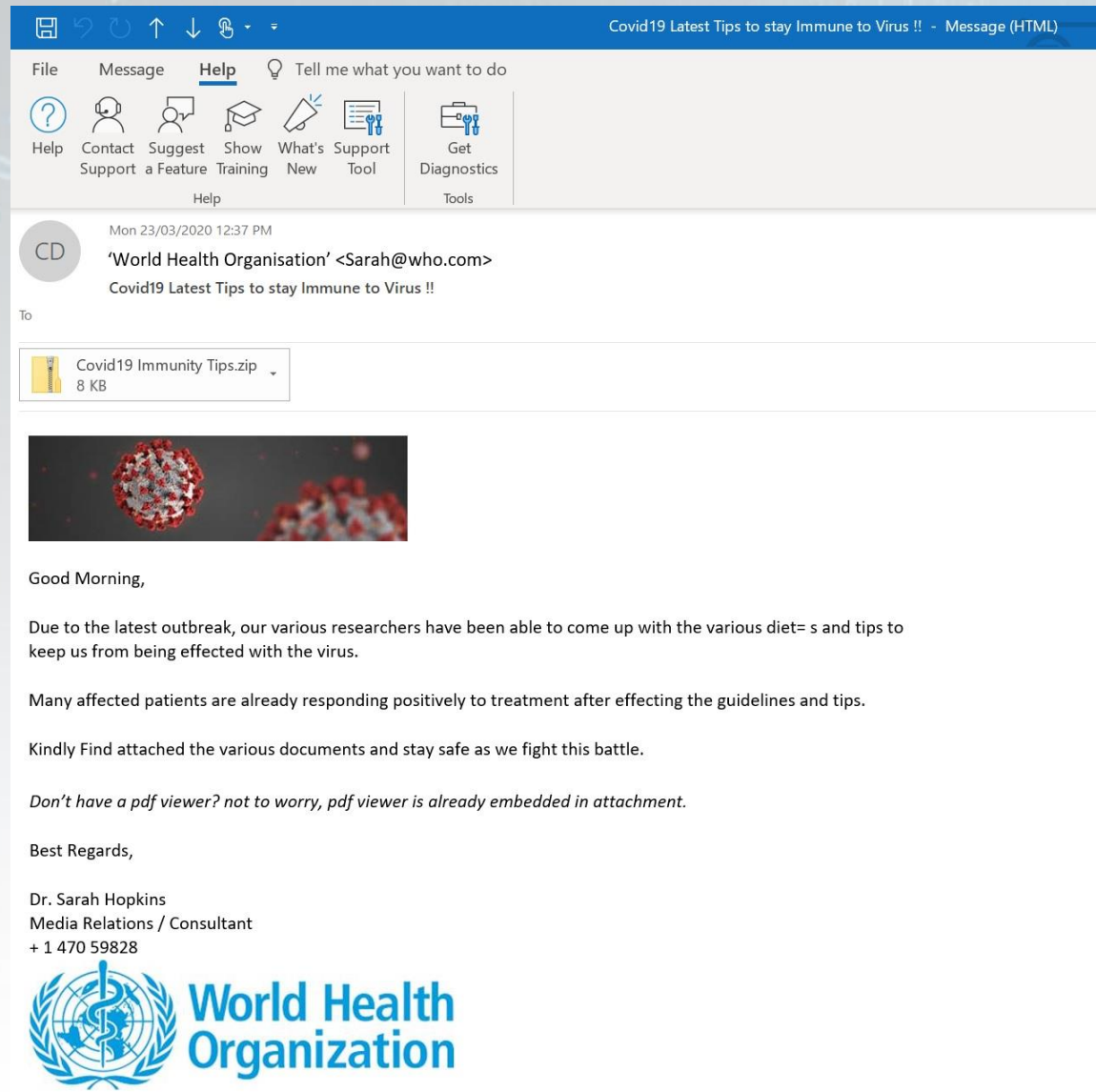
- Viens no rīkiem, ko izmantojam, lai noteiktu, kas ir pareizi, ir noskaidrot, ko citi cilvēki uzskata par pareizu.
- Jo lielāks skaits cilvēku uzskata, ka ideja ir pareiza, jo vairāk ideja būs pareiza.

Vienprātība

- Plurālistiskā nezināšana: katrs cilvēks nolemj, ka, tā kā neviens neuztraucas, viss ir kārtībā



Vienprātība

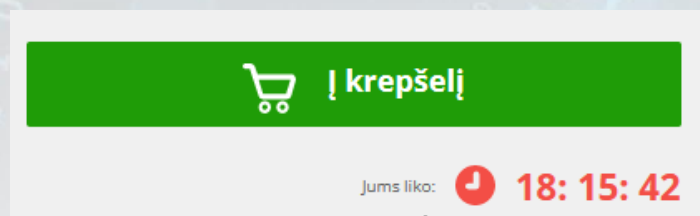


Trūkums

- Iespējas mums šķiet vērtīgākas, ja to pieejamība ir ierobežota.
- Mēs vēl vairāk vēlamies to, par ko pastāv konkurence.

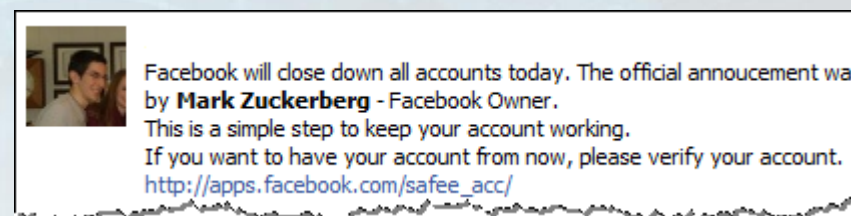
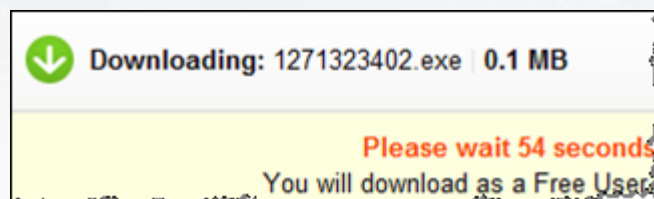
Trūkums

- Laika ierobežojums



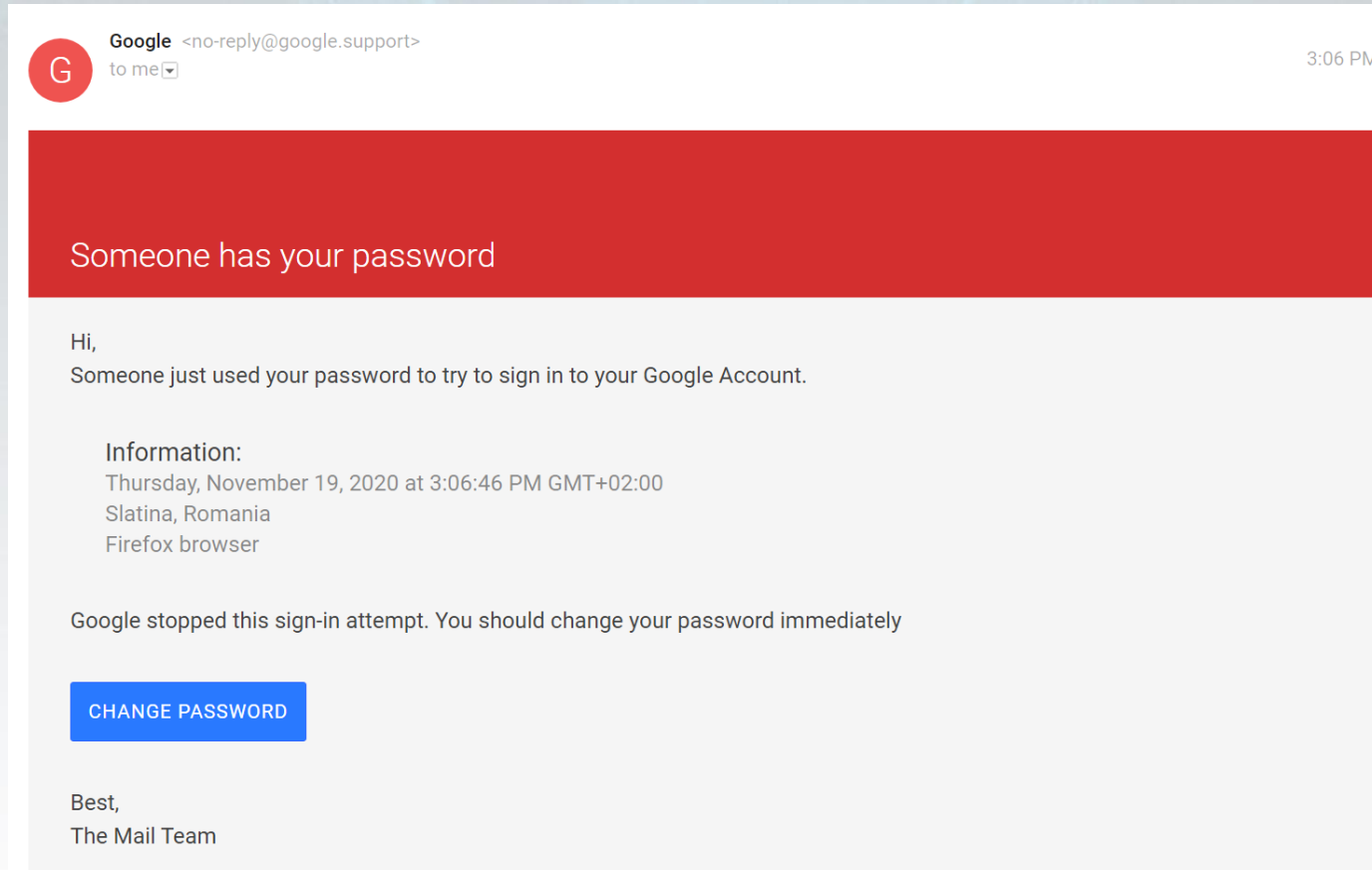
Avots: <https://pigu.lt/lt/>

- Šķēršļu ierobežojumi



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

Trūkums



Avots: <https://au.pcmag.com/>

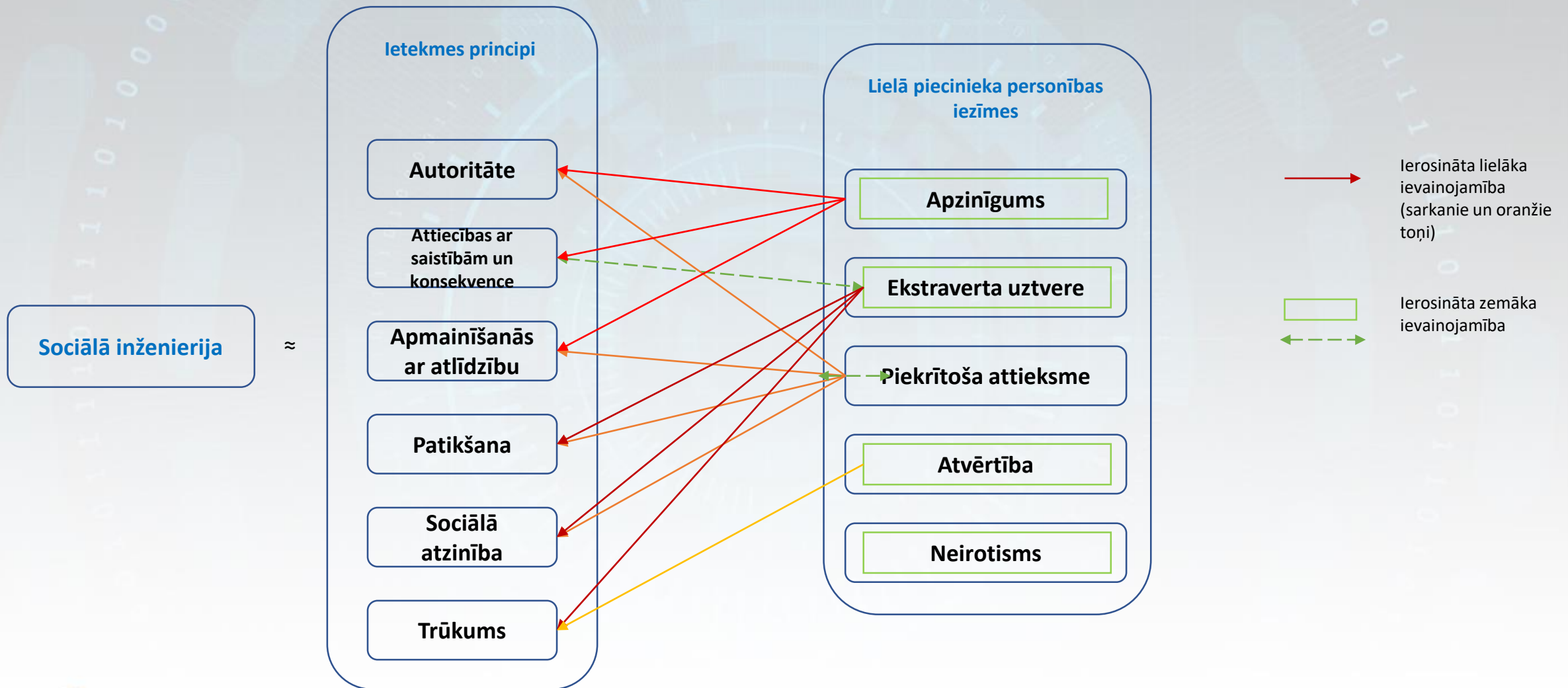
Vienotība

- Septītais pārliecināšanas princips, ko vēlāk pievieno dr. Roberts Čaldini [*Dr Robert Cialdini*]
- Pamatojoties uz domu, ka jo vairāk mēs sevi identificējam ar citiem, jo lielāka iespēja, ka mūs tie ietekmēs.

Sociālās inženierijas personības ietvars (SEPF)

Atvērtība	Apzinīgums	Ekstraverta uztvere	Piekrītoša attieksme	Neirotisms
Fantāzija Estētika Sajūtas Darbības Idejas Vērtības	Kompetence Kārtība Pienākums Sasniegumi Centieni Pašdisciplīna Noteiktība	Sirsnīgums Draudzīgums Pārlicība Aktivitāte Lūkošanās pēc aizrautības Pozitīvas emocijas	Uzticēšanās Tiešums Altruisms Atbilstība noteikumiem Pieticība Smalkjūtīgums	Nemiers Naidīgums Depresija Pašapziņa Impulsivitāte Ievainojamība pret stresu

Sociālās inženierijas personības ietvars (SEPF)



Reversā sociālā inženierija

- Sociālais inženieris neuzsāk kontaktu ar cietušo
- Uzbrukums organizēts tā, ka pats cietušais vēršas pēc palīdzības pie uzbrucēja
- Augstas uzticības attiecības tiek veidotas, jo tās iniciē upuris.

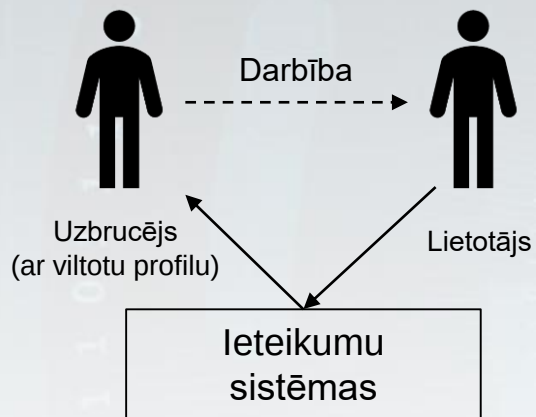
Reversā sociālā inženierija

- Parasti tas tiek realizēts trīs posmos:
 - Tiek izveidota ēsma vai iegansts, kas veicina upura interesi vai zinātkāri (mērķa aprīkojums tiek sabotēts vai bojāts)
 - Tiek nodrošināts, ka mērķa persona zina, ka uzbrucējs ir autoritatīva persona, un viņam ir iekārtas remontam nepieciešamās prasmes.
 - Tiek sniegta palīdzība problēmas risināšanā, uzticības attiecību veidošanā un piekļuvei mērķa personas informācijai vai citiem resursiem.

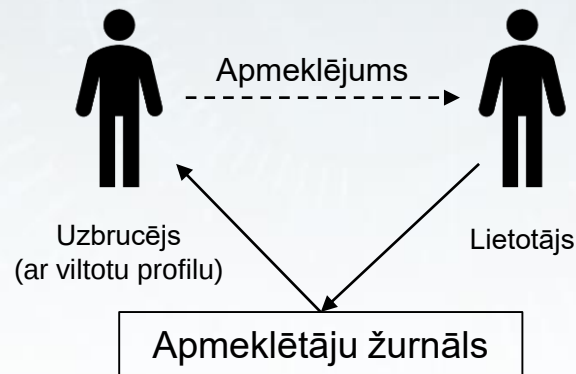
Reversās sociālās inženierijas uzbrukumi

- Speciāli mērķēti/nemērķēti
Mērķtiecīgā uzbrukumā uzbrucējs koncentrējas uz konkrētu lietotāju. Turpretim nemērķtiecīgā uzbrukumā uzbrucējs ir tikai ieinteresēts sasniegt pēc iespējas vairāk lietotāju
- Tiešs/ar starpniecību
Tiešā uzbrukumā uzbrucēja ēsmas darbība ir redzama mērķa lietotājiem. Savukārt starpniecības uzbrukumos tiek izmantota divpakāpju pieeja, kurā ēsmu savāc starpposma aģents, kas pēc tam ir atbildīgs par tās izplatīšanu (bieži vien citā formā) mērķa lietotājiem.

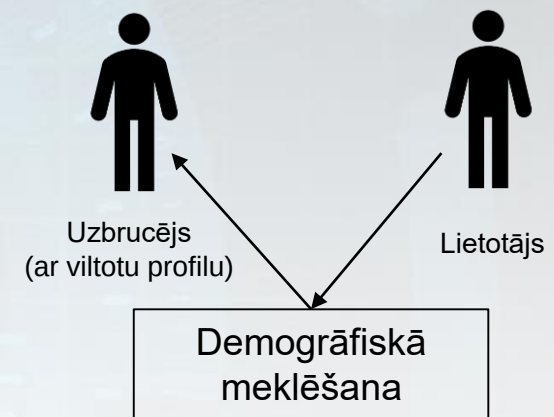
Dažādi reversās sociālās inženierijas uzbrukumi



(a) Ieteikumu sistēmas



(c) Apmeklētāju izsekošana



(b) Demogrāfiskā meklēšana

Padomi sociālās inženierijas novēršanai

- Trenējiet savu apziņu, lai atpazītu pārliecināšanas un manipulāciju mēģinājumus
 - Vai manas emocijas ir sakāpinātas?
 - Vai šis ziņojums iegūts no likumīga sūtītāja?
 - Vai mans draugs tiešām man nosūtīja šo ziņojumu?
 - Vai šis piedāvājums neizklausās pārāk labi, lai tā būtu patiesība?
 - Vai pielikumi vai saites ir aizdomīgas?
 - Vai šī persona var pierādīt savu identitāti?

Padomi sociālās inženierijas novēršanai

- Pārvaldiet savu personīgo informāciju
 - Uzziniet, kāda jūsu personiskā informācija ir pieejama tiešsaistē
- Pasargājiet sevi
 - Pārvaldiet savus kontus un paroles.
 - Izmantojiet daudzfaktoru autentifikāciju
 - Atjauniniet programmatūru
 - Iespējojiet mēstuļu filtru
 - Nodrošiniet visas ierīces

Sociālā inženierija: Tendences

1. Piekrišanas izmānīšanas apjomi pieaug
2. Biznesa e-pasta bojājumi kļūst dārgāki
3. Dziļā atdarināšana (*angl. deepfake*) rada dziļākus izaicinājumus
4. Nāciju valstu uzbrucēji ar sociālo inženieriju savā arsenālā
5. Pikšķerēšanas kā sniegta pakalpojuma tirgus paplašināšana

! Lietotāju informētība vairs nav izvēle – tā ir obligāta!

Uzdevumi

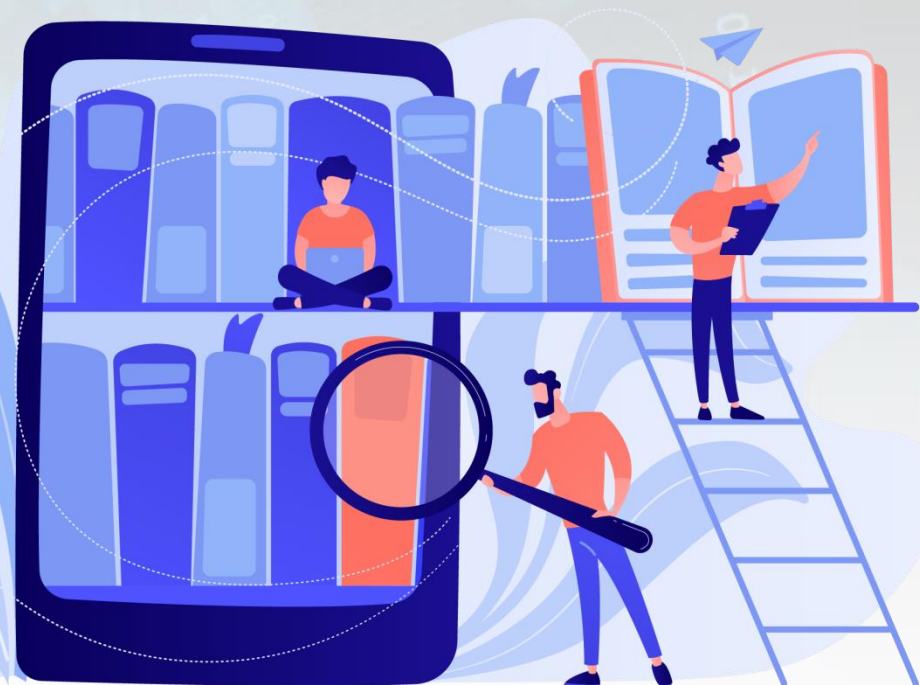


- Apspriediet koronavīrusa krāpšanas uzbrukumu pieauguma iemeslus
- Apspriediet Basecamp izmantoto ietekmes principu
- Pārrunāji, ar kādiem pārliecināšanas uzbrukumiem esat saskārušies

Šīs lekcijas sagatavošanā izmantotie materiāli

- **Čaldini, R. B.** [Cialdini, R. B.] (2007. gads) Ietekme: pārliecināšanas psiholoģija. Rev. izd.; "1st Collins business essentials", red. Ņujorka: Collins.
- **Hednagijs C.** [Hahnagy C.] (2018. gads) *Sociālā inženierija: Cilvēku hakerisma māksla*. Indianapolis: Džons Vailijs [John Wiley] un dēli.
- **Irani D.** [Irani, D.], **Balduči M.** [Balduzzi, M.], **Balcaroti D.** [Balzarotti, D.], **Kirda E.** [Kirda, E.], **Pū C.** [Pu, C.]. (2011. gads). Reversie sociālās inženierijas uzbrukumi tiešsaistes sociālajos tīklos. 55-74. doi:10.1007/978-3-642-22424-9_4.
- **Makleods S. A.** [McLeod, S. A.] (2014. gads). Atbilstības gūšanas metodes. Izgūts no <https://www.simplypsychology.org/compliance.htm>
- **Merve J.** [Merwe J.] un **Mutons F.** [Mouton F.], (2017. gads). Sociālās inženierijas uzbrukumu anatomijas kartēšana sistēmu inženierijas dzīves ciklam. HAISA.
- **Montañezs R.** [Montañez, R.], **Golobs E.** [Golob, E.], **Ksjū S.** [Xu, S.] (2020) Cilvēka izziņa, izmantojot sociālās inženierijas kiberuzbrukumus. *Front. Psychol.* 11:1755. digitālais objekta identifikators: 10.3389/fpsyg.2020.01755
- **Volkers E.** [Walker, E.]; **Vitkovskis D.** [Witkowski, D.] **Benšiks S.** [Benczik, S.] **Džarens P.** [Jarrin, P.] Kiberdrošība – cilvēciskais faktors. Prioritātes noteikšana cilvēkiem Risinājumi, lai uzlabotu federālā darbaspēka kiberneturību un pretestību. Materiāls izgūts no <https://documents.pub/document/cybersecurity-the-human-factor-nist-computer-the-human-factor-prioritizing.html>
- **Vašo A.** [Washo, A.] (2021. gads) Starpdisciplinārs skatījums uz sociālo inženieriju: Aicinājums veikt pētījumus. Datori cilvēku uzvedības pārskatos. 4. sējums, 2021. gads. 100126.

Papildu lasīšana



Īsi video

- Pārliciecināšanas zinātne
<https://youtu.be/cFdCzN7RYbw>
- DEFCON hakerisma un uzlaušanas izaicinājums
<https://www.youtube.com/watch?v=fHhNWAKw0bY>
- Ielaušanās kompānijā mazāk nekā 2 minūtēs
<https://www.youtube.com/watch?v=PWVN3Rq4gzw>



Pateicamies!

