



Funded by the
Erasmus+ Programme
of the European Union

Cyber-Attacks: Social Engineering and Phishing

Social Engineering Modules and Manipulation

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.



Learning Goals



- Explain influencing and manipulative techniques and learn to recognize them
- Explain social engineering and its psychological aspects.
- Review how decision-making is affected by emotions, workload, and our entire environment.
- Explain influencing and manipulative techniques and learn to recognize them

Student Workload



Lecture	4 h
Audio and video material	2 h
Case studies	2 h
Further reading	8 h
Preparation for exam	1 h

Contents

- Human factor
- Social engineering
- Decision making process
- Psychological aspects of Social Engineering
 - Emotions
 - Weapons of Influence
- Reverse Social Engineering
- Tips to Prevent Social Engineering

Human Factor

**\$ 400
BIL**



Estimated cost of cyber attacks on organisations globally

Organizations rarely invest in and plan for the **human component of cybersecurity** until **after** a breach occurred. For major breaches, this can cost the organization **millions of dollars**.

35 %



of data breaches were attributed to human error or negligence

Types of cyber threats and methods of prevention change each day. Instilling a culture of cyber **interest** and **awareness** equips an organisation to **better handle changing cybersecurity threats**.

47 %



Of IT professionals describe collaboration between security risk management & business as poor or nonexistent

Many executives have the **mindset that cybersecurity is the responsibility of IT**; rather it is **everyone's responsibility**. Employee awareness should be the first line for **defense** of an organization's digital assets.

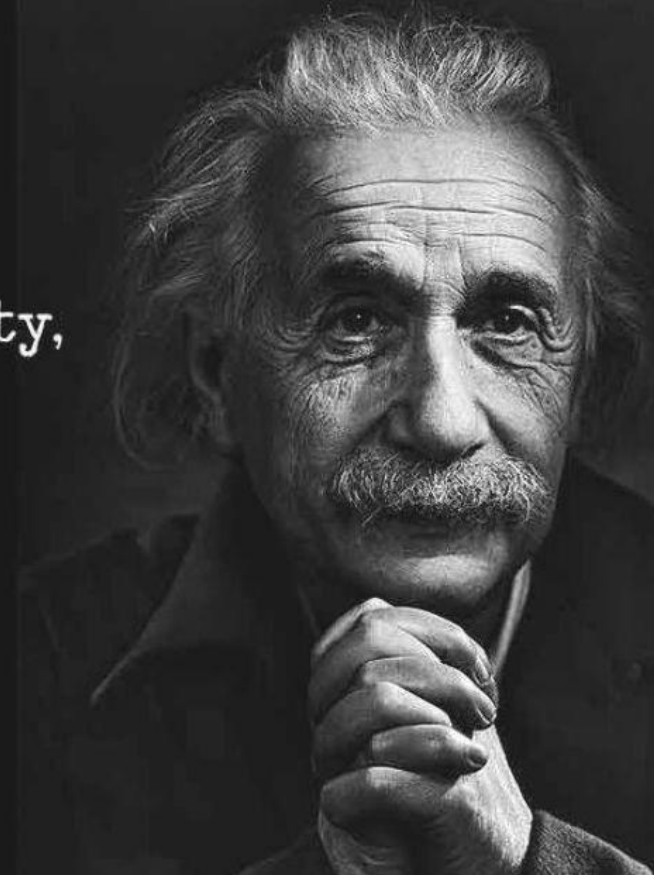
Human Factor

- People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.
- Technical security measures are constantly evolving, but people do not change they remain the weakest link in information security with their weaknesses, stereotypes and attitudes

Human Factor

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

Albert Einstein



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

What is Social Engineering?



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



What is Social Engineering?

- Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to obtain
- Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

Social Engineering: Statistics

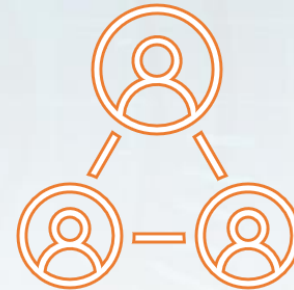


98% of cyber attacks rely on social engineering

/



43% of IT professionals targeted by social engineering last year



21% of current or former employees use social engineering

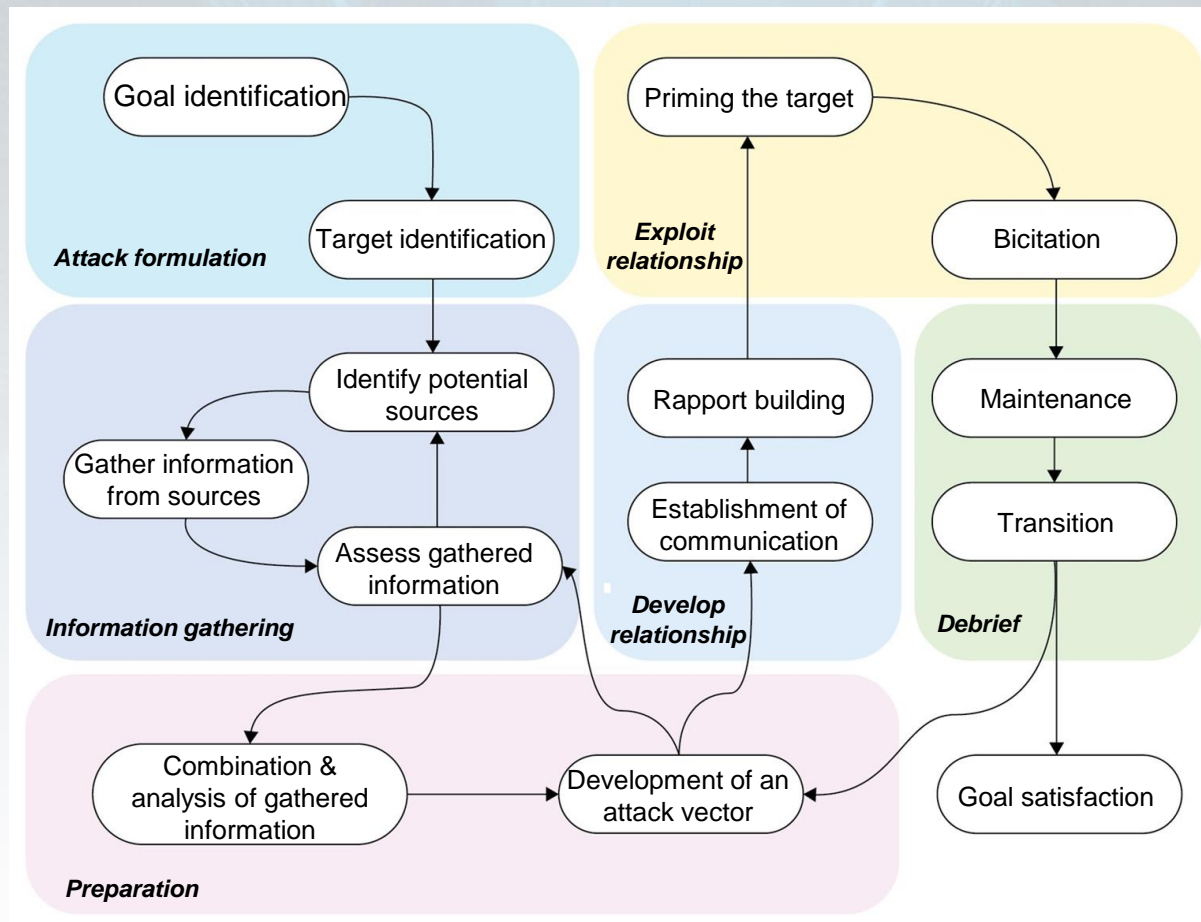


Social engineering attempts increased more than 500% in 2018

The Social Engineering Framework



Social Engineering “Roadmap”



Source: Dr. Erdal Ozkaya “Learn Social Engineering”, 2018

Step 1: Targeting

- Social engineering - target-specific
- Choosing a target based on the final “results” (e.g., information, money, etc.)



Step 2: Information Gathering

- Most tortuous step in the whole social engineering process
- May last anywhere from a few hours to a few years
- Information is rarely gathered all at once
- Use of social media platforms, specialised software, soft skills
- Two ways of gathering data:
 - *Non-technical/ Mechanical methods*
 - *Technical methods*



Step 3: Elicitation

Elicitation can be defined as the act of drawing something out using logic. It is done through stimulation to get one to act in a certain class of behaviours.

Factors making elicitation effective:

- Most humans will try to be polite when talking to a stranger
- Professionals, when questioned, will want to appear knowledgeable
- Most people would not lie to someone who appears genuinely concerned
- It is more likely than not for someone to respond to well-posed questions about themselves



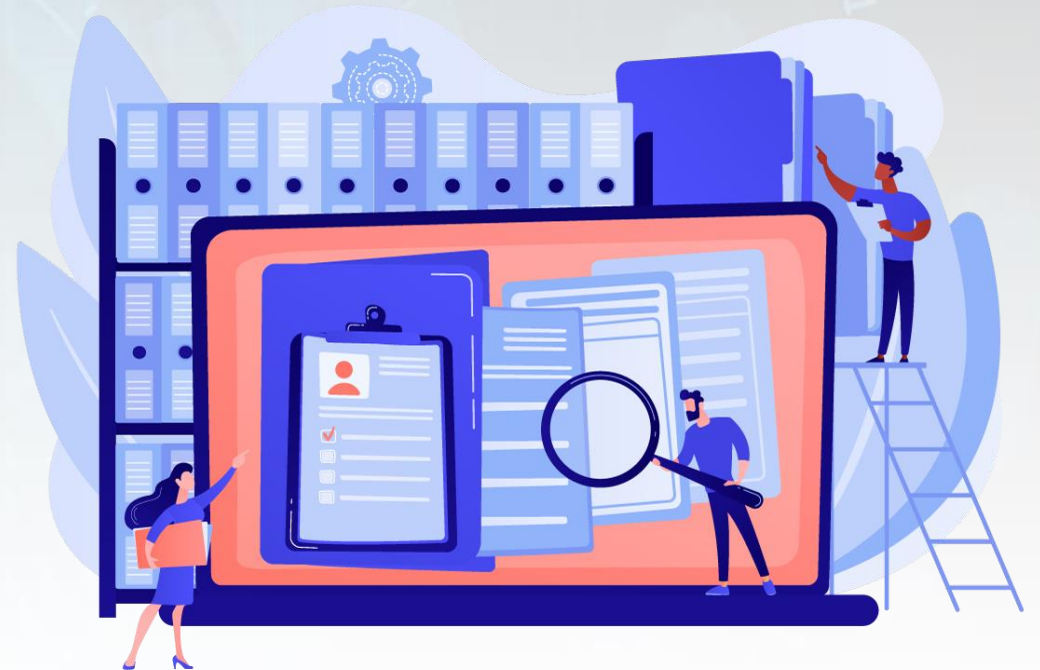
Step 4: Pretexting

Pretexting is an imperative skill that any social engineer needs in order to accomplish an attack.

Pretexting puts a person in the skin of another.

General principles of pretexting:

- Research more
- Use personal interests
- Practice expressions or dialects
- Use simpler pretexts
- Logical conclusions



Step 5: Mind Tricks

Mind tricks are more of a psychological affair, and they are used to unlock the minds of the targets exposing them to the control of the social engineer.

MIND TRICKS \neq SCIENCE

There are three modes of thinking that can be exploited in a human:

1. **Visual thinking**
2. **Auditory thinking**
3. **Kinaesthetic thinking**



Step 6: Persuasion

To persuade a target, a social engineer needs to appeal to the target's interests first. Persuasion gets targets to react, think, and do exactly as the social engineer wants.

5 fundamentals used in persuasion by social engineers:

1. Clear goals
2. Rapport
3. Being in tune
4. Flexibility
5. Reciprocation



Step 7: Exploiting and Disengaging

- Exploiting the victim once trust and a weakness are established to advance the attack
- Disengaging once the user has taken the desired action



An Ontological Model of a Social Engineering Attack



Social Engineering Attacks

Several people lost thousands of dollars in cryptocurrency after the [Ethereum Classic website was hacked](#), in 2017. Using social engineering, hackers impersonated the owner of Classic Ether Wallet, gained access to the domain registry, and then redirected the domain to their own server. Criminals extracted Ethereum cryptocurrency from the victims after entering a code on the website that allowed them to view private keys that are used for transactions.

Social Engineering Attacks

Shark Tank television judge [Barbara Corcoran was tricked](#) in a nearly USD 400,000 phishing and social engineering scam in 2020. A cybercriminal impersonated her assistant and sent an email to the bookkeeper requesting a renewal payment related to real estate investments. He used an email address similar to the legitimate one. The fraud was only discovered after the bookkeeper sent an email to the assistant's correct address asking about the transaction.

Social Engineering Attacks

One of the biggest social engineering attacks was perpetrated by Lithuanian national Evaldas Rimasauskas against two of the world's biggest companies: Google and Facebook.

Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimasauskas also set up bank accounts in the company's name.

The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided - but directing them to deposit money into their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over \$100 million.

Why is Social Engineering so Effective?

- We are social by nature;
 - Our desire to stand out from others
- Other people make a big impact on our decisions;
 - Our desire to be helpful
 - Our tendency to trust people we don't know

Why is Social Engineering so Effective?

- We are overloaded with information and look to shortcuts to save time.
 - Our desire for all good things to happen quickly and effortlessly
 - Our fear of getting into trouble
- Lack of security knowledge;
- Oversharing personal information on social media;

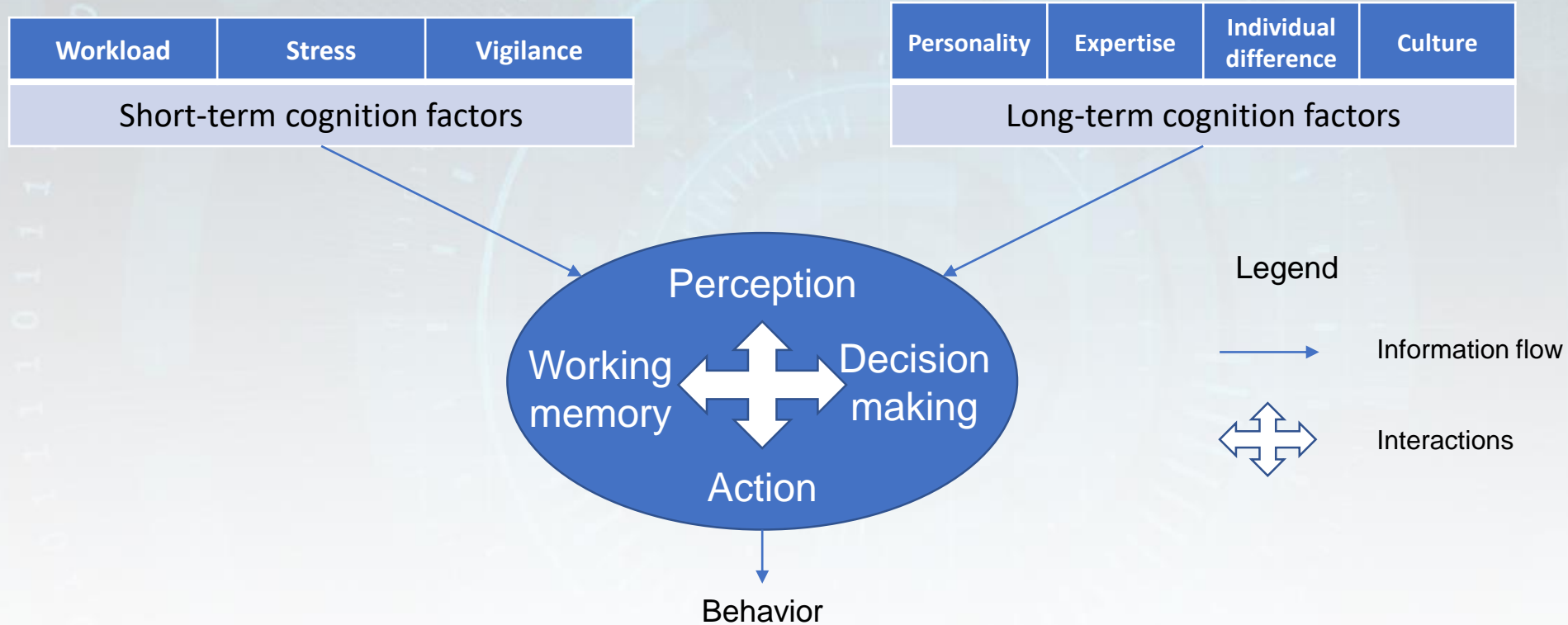
Psychological Aspects of Social Engineering

Some authors advocate treating social engineering cyberattacks as a particular kind of psychological attack.



[Montañez at al. 2020]

Human Cognitive Functions



a high cognitive workload, a high degree of stress, a low degree of attentional vigilance, a lack of domain knowledge, and/or a lack of past experience makes one more susceptible to social engineering cyberattacks

The Psychology of Online Persuasion

*"The current generation of internet consumers live in a world of **instant gratification and quick fixes**, which leads to a **loss of patience and a lack of deep thinking**." - Rob Weatherhead, [The Guardian](#)*

- Our behaviors, thoughts, and beliefs are constantly shaped by the environment around us, as well as by our own experiences
- influence and the art of persuasion is the process of getting someone else to *want* to do, react, think, or believe in the way you want them to.

Heightened Emotions

Emotional manipulation gives attackers the upper hand in any interaction. You are far more likely to take irrational or risky actions when in an enhanced emotional state.



[Montañez at al. 2020]



Funded by the
Erasmus+ Programme
of the European Union

Heightened Emotions



[Montañez at al. 2020]

Fear

COVID-19



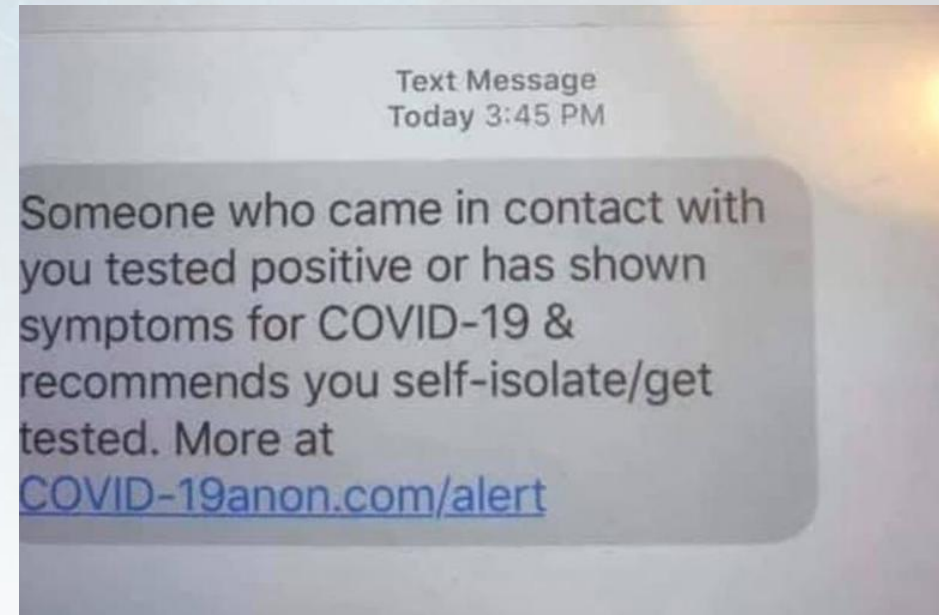
● nicholsschoolorg@alsummers.com <nicholsschoolorg@alsummers.com>

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) 18P3S6DuNUpW2WLozsrW6rRd6xh24Rc7N

Source: Vilnius University Kaunas faculty internal phishing database

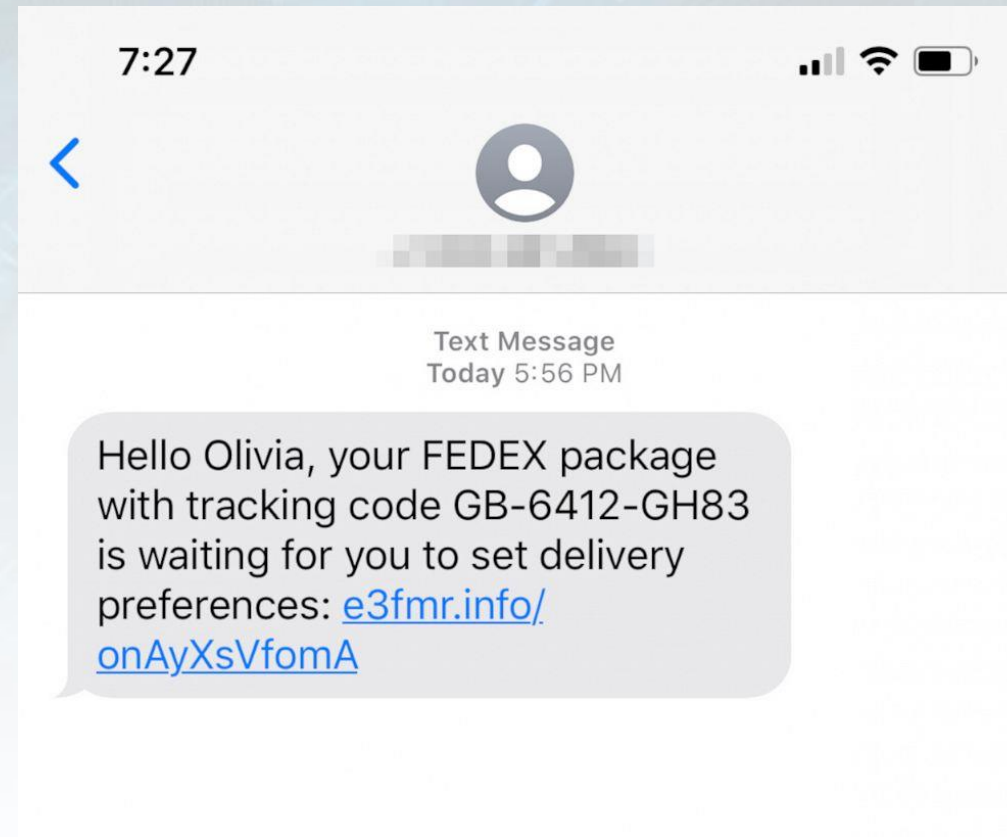


Source: <https://www.thesun.co.uk/news/11422572/scam-message-hoax-tricks-americans-exposed-to-coronavirus-must-self-isolate/>

Curiosity



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>

Helpfulness



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/>

Urgency

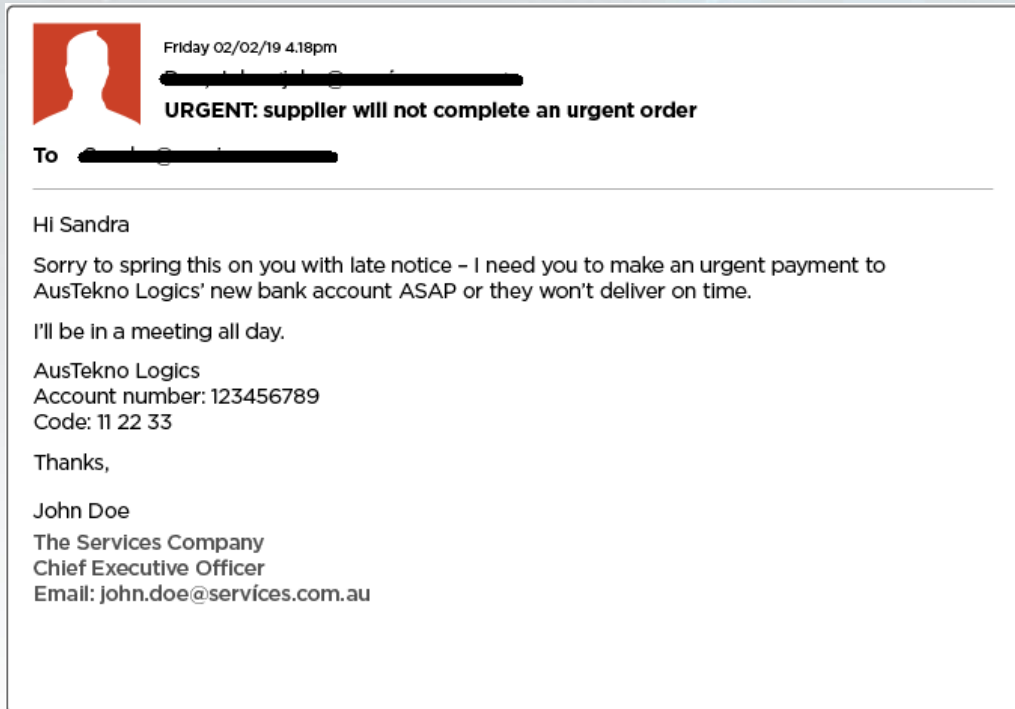
Time-sensitive opportunities or requests are another reliable tool in an attacker's arsenal.

You may be motivated to compromise yourself under the guise of a serious problem that needs immediate attention.

Alternatively, you may be exposed to a prize or reward that may disappear if you do not act quickly.

Either approach overrides your critical thinking ability.

Urgency



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/

Anger

- We avoid angry people
- We avoid conflicts
- Angry “boss” calls employee asking for password



Greed

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 ASSISTANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

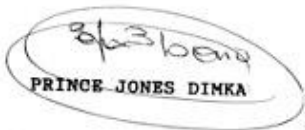
PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME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

- These are some of the oldest scams—promising wealth from Nigerian princes or military personnel offering to share some stolen treasure.
- Sometimes it's a wealthy widow dying of cancer, or a British solicitor delivering your share of an estate.


Source: <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

 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

Weapons of Influence



[Cialdini, 2007]

Reciprocity

- “...we should try to repay, in kind, what another person has provided us.”
- Technique 1: If someone makes a concession, we are obligated to respond with a concession
Making a concession gives the other party a feeling of responsibility for the outcome and greater satisfaction with resolution

Reciprocity

- Technique 2: Rejection then retreat: exaggerated request rejected, desired lesser request acceded to
- Technique 3: Contrast principle: sell the costly item first; or present the undesirable option first

Reciprocity


Hotels.com <Hotelscom@roktpowered.com>
to dave ▾

Nov 14, 2018, 11:38 AM (1 day ago) ★ ↶ ⋮

[Hotels](#) [Hotel Deals](#) [Packages & Flights](#) [Groups](#) [Customer Service](#) [Gift Cards](#) [Secret Prices](#)

H Hotels.com™

[New York Hotels](#) [Las Vegas Hotels](#) [Chicago Hotels](#) [Los Angeles Hotels](#)

 **COUPON CODE**
\$50 off
When you spend \$350 or more

EMLRKUSH21850:SK7CM6 [Book now](#)

You must click through this email or book through our app to redeem this coupon.

*Use by 11:59 PM MT on 01/15/19 for travel by 04/30/19. Can't be used on some hotels. See details below.

Bookings using this coupon are not eligible for Hotels.com™ Rewards.

How to redeem your coupon:

- 1 Click this email or open our app (this will activate your coupon)**
- 2 Search from thousands of hotels worldwide**
- 3 Book using your unique coupon code (enter code on the booking form)**

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

Consistency

- We have a “nearly obsessive desire to be (and to appear) consistent with what we have already done”
- Once we have made a choice or taken a stand, we will encounter personal and interpersonal pressures to behave consistently with that commitment.

Consistency

- The Foot in the Door Technique: agreeing to a small request increases the likelihood of agreeing to a second, larger request.
- The Door in the Face Technique: refusing a large request increases the likelihood of agreeing to a second, smaller request.

Consistency

- The Low-Ball Technique: the persuader gets a person to commit to a low-ball offer they have no intention of keeping; then the price is suddenly increased. Since a person has already committed, it is hard to say no to the new higher price demand.

Consistency

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,

Amazon.com

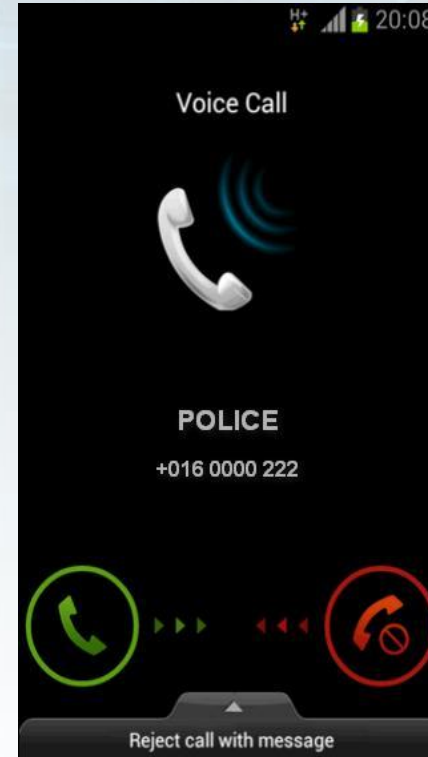
Source: <https://www.forbes.com/sites/barrycollins/2021/07/07/is-this-amazon-email-fake-how-to-spot-the-scams/?sh=605d881d119a>

Authority

- Information from a recognized authority can provide us a valuable shortcut for deciding how to act in a situation.
- Increasingly, the right authority is frequently the individual, brand, organization, or cause with the biggest audience.

Authority

- Titles
- Uniforms
- Clothes
- Brands



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

Authority

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 a 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.

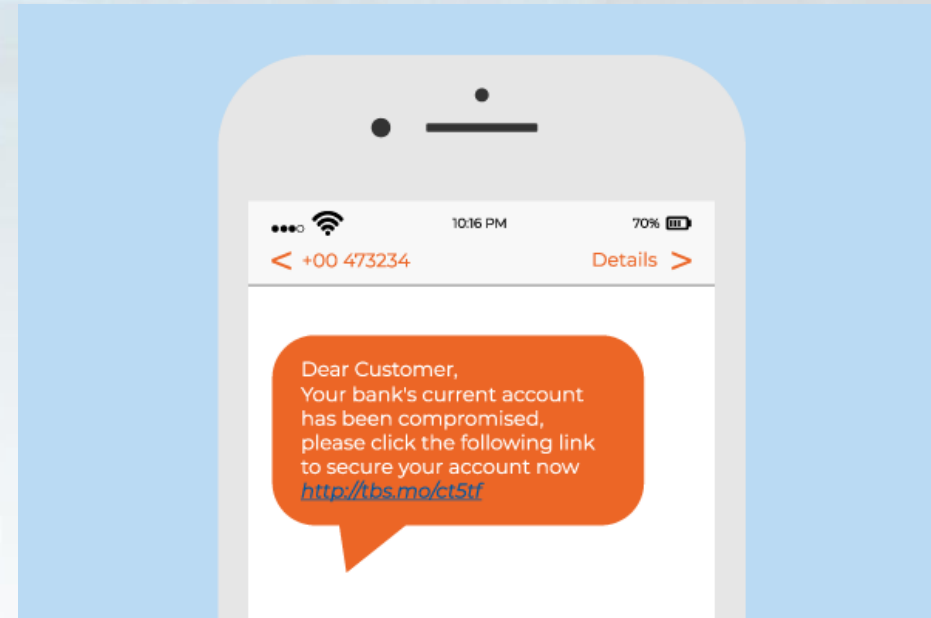
Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

Authority



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



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

Liking

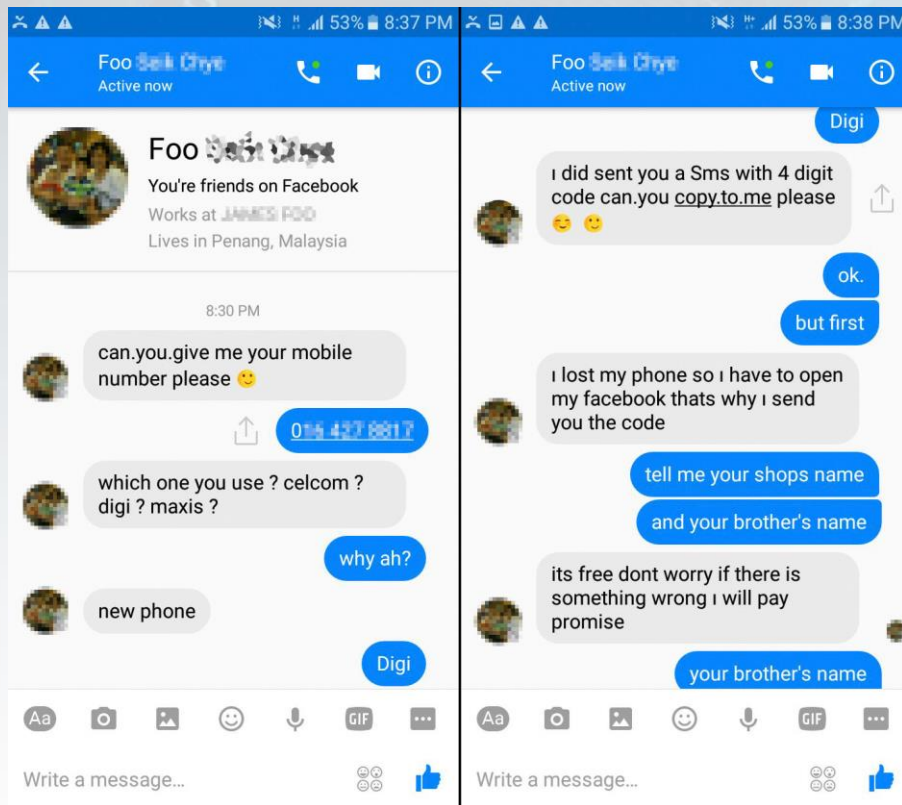
- People like those who like them, and are more influenced by those they like
- We are happy to fulfill requests from people we like



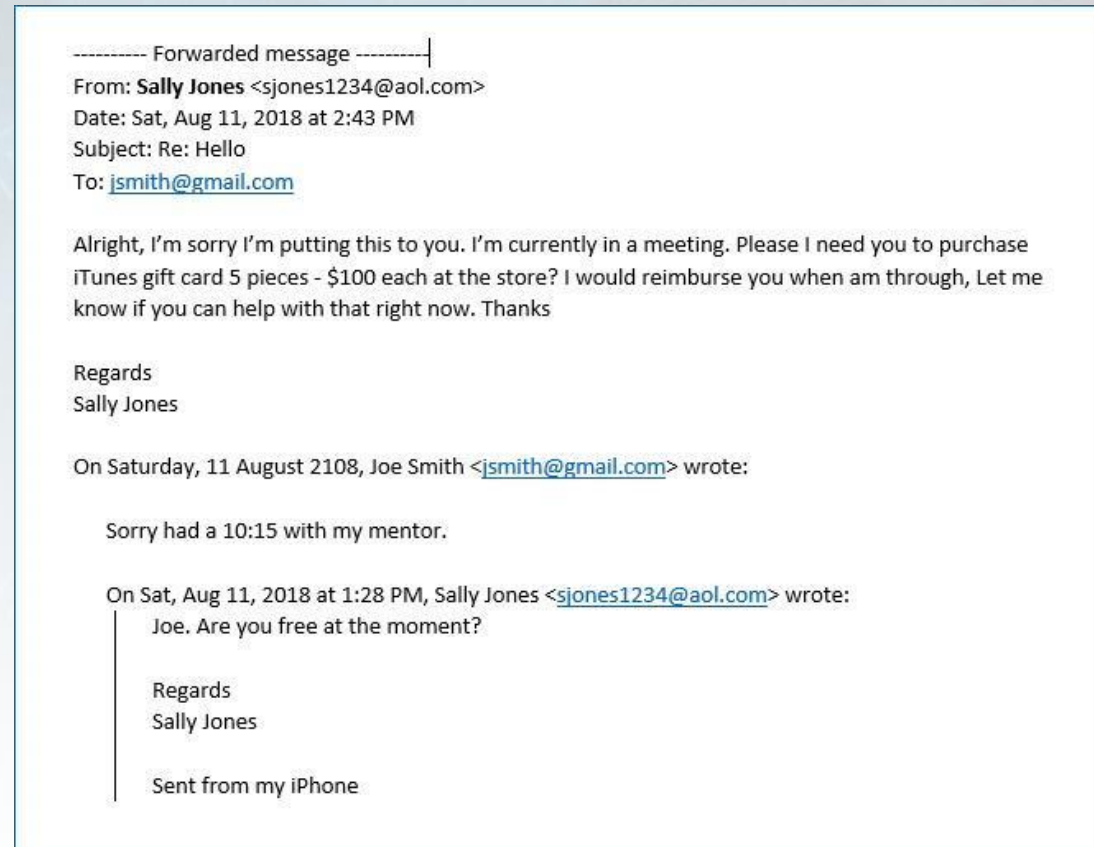
Liking

- People tend to form trust with those they're attracted to, both physically and emotionally:
 - We like people who are similar to us
 - We like people who pay us compliments
 - We like people who cooperate with us towards mutual goals

Liking



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



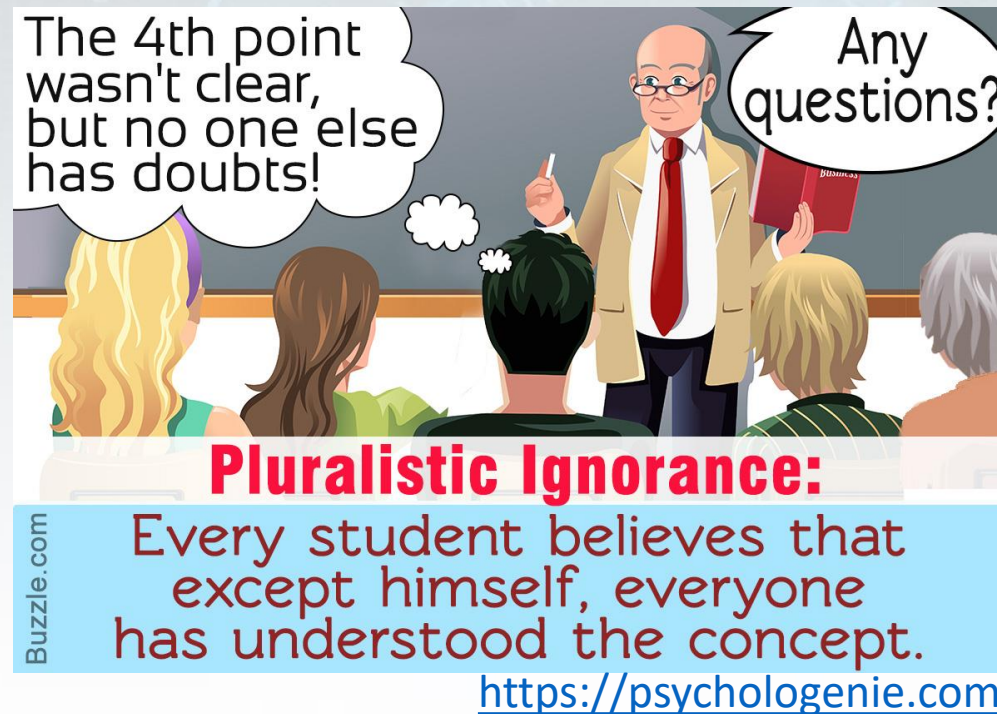
Source: <https://www.apa.org/about/division/digest/leader-resources/convention-email-scams/>

Consensus

- One of the tools we use to determine what is right is to find out what other people think is right.
- The greater number of people who find an idea correct, the more the idea will be correct.

Consensus

- Pluralistic ignorance: each person decides that since nobody is concerned, nothing is wrong



[Cialdini, 2007]


Consensus

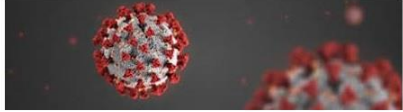
File Message **Help** Tell me what you want to do

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

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**

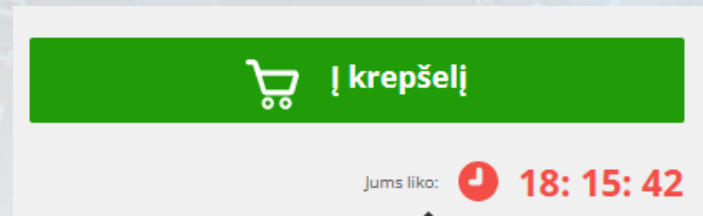
Source: <https://www.netsafe.org.nz/covid-19-scam-spotting/>

Scarcity

- Opportunities seem more valuable to us when their availability is limited.
- We want it even more when we are in competition for it

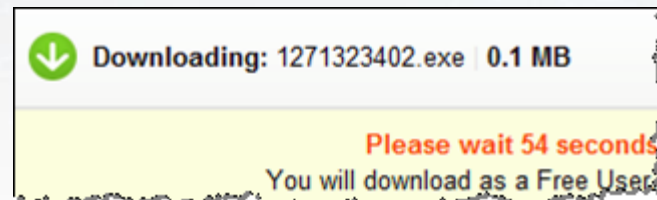
Scarcity

- Time Limitation



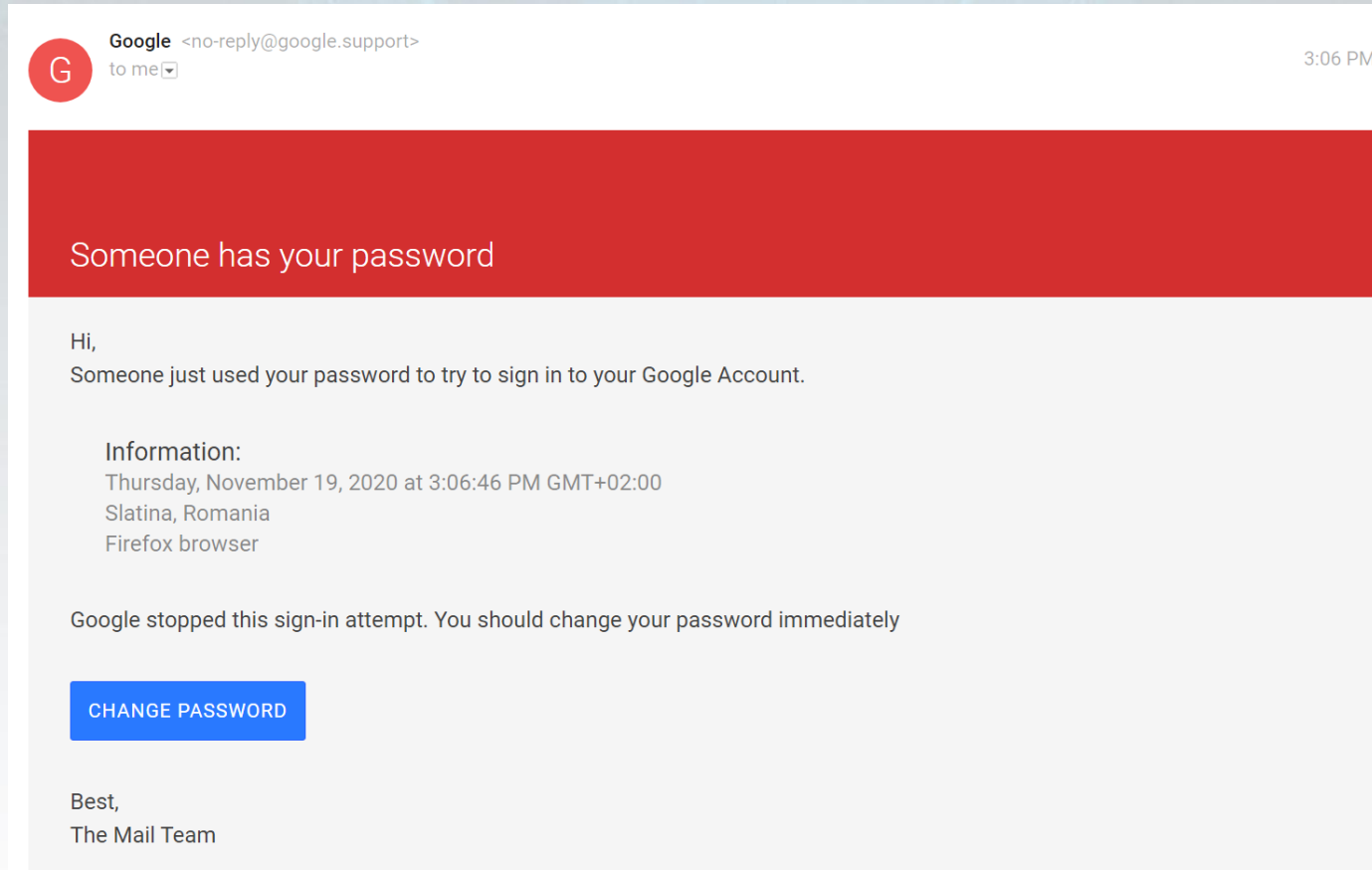
Source: <https://pigu.lt/>

- Obstacle Restriction



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

Scarcity



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

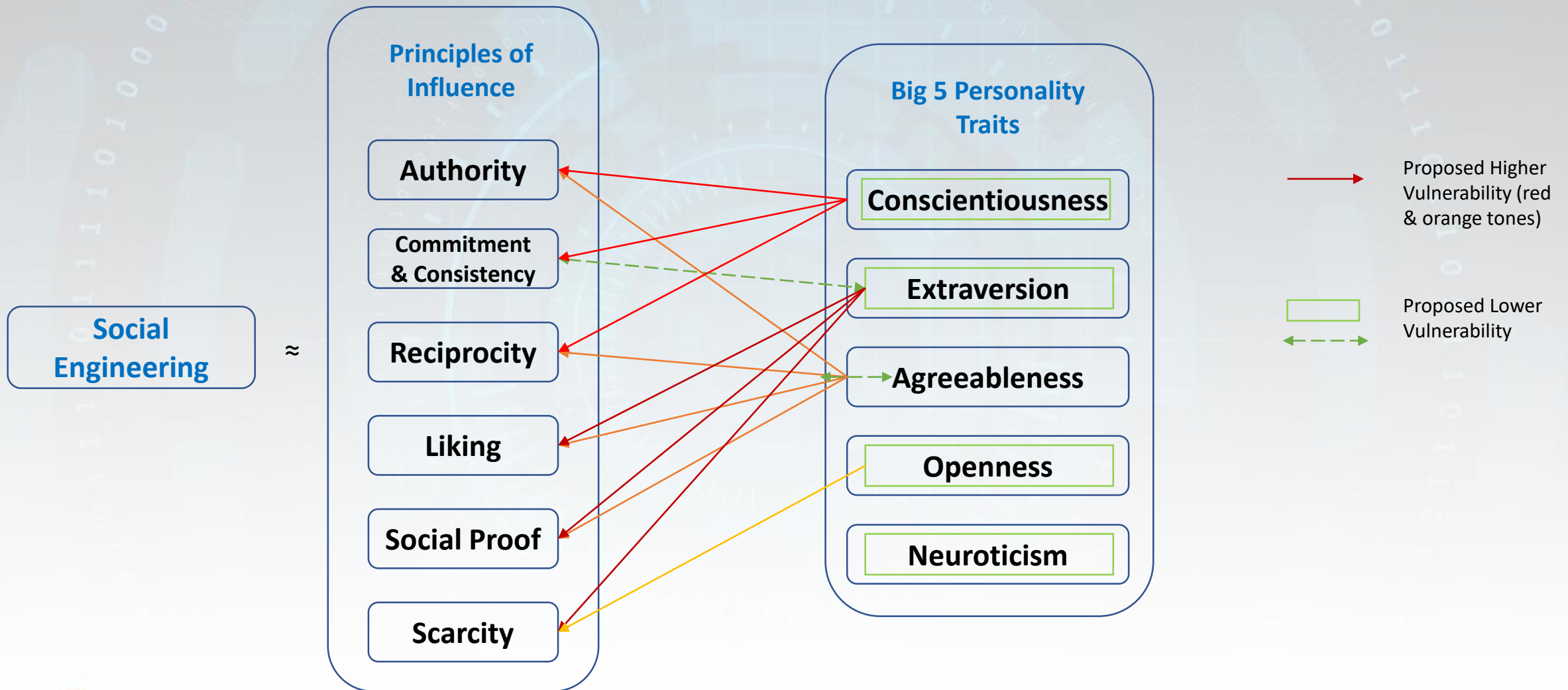
Unity

- 7th principle of persuasion later added by Dr Robert Cialdini
- Based on the idea that the more we identify ourselves with others, the more likely we are influenced by them

The Social Engineering Personality Framework (SEPF)

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Fantasy Aesthetics Feelings Actions Ideas Values	Competence Order Dutifulness Achievement Striving Self-Discipline Deliberation	Warmth Gregariousness Assertiveness Activity Excitement Seeking Positive Emotion	Trust Straightforwardness Altruism Compliance Modesty Tender-mindedness	Anxiety Hostility Depression Self-Consciousness Impulsiveness Vulnerability to Stress

The Social Engineering Personality Framework (SEPF)



Reverse Social Engineering

- The social engineer does not initiate contact with the victim
- The attack is organized in such a way that the victim himself turned to the attacker for help
- A relationship of high trust is created as it is initiated by the victim.

Reverse Social Engineering

- It is usually realized in three steps:
 - A bait or pretext is created that stimulates the victim's interest or curiosity (Target equipment is sabotaged or damaged)
 - It is ensured that the target knows that the attacker is an authoritative person and has the skills needed to repair the equipment
 - Assistance is provided in solving the problem, building a relationship of trust and access to target information or other resources.

Reverse Social Engineering attacks

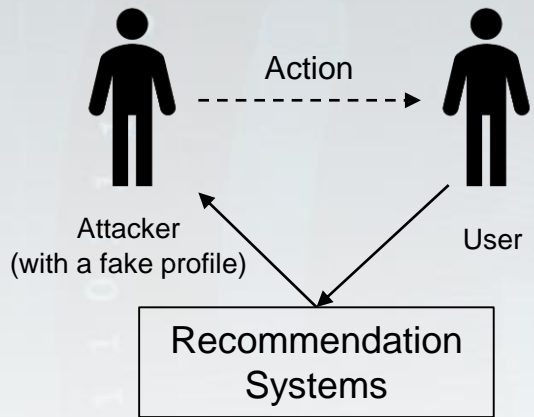
- Targeted/Untargeted

In a targeted attack, the attacker focuses on a particular user. In contrast, in an un-targeted attack, the attacker is solely interested in reaching as many users as possible

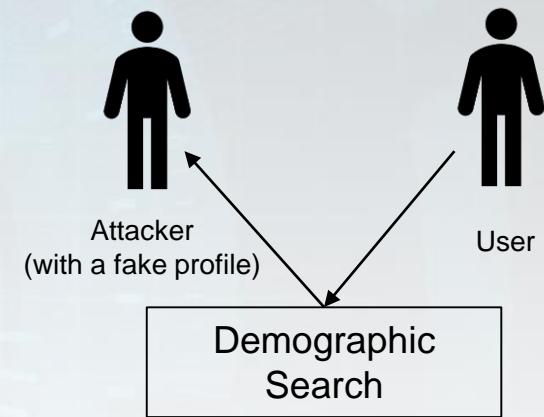
- Direct/Mediated

In a direct attack, the baiting action of the attacker is visible to the targeted users. Mediated attacks, in contrast, follow a two-step approach in which the baiting is collected by an intermediate agent that is then responsible for propagating it (often in a different form) to the targeted users.

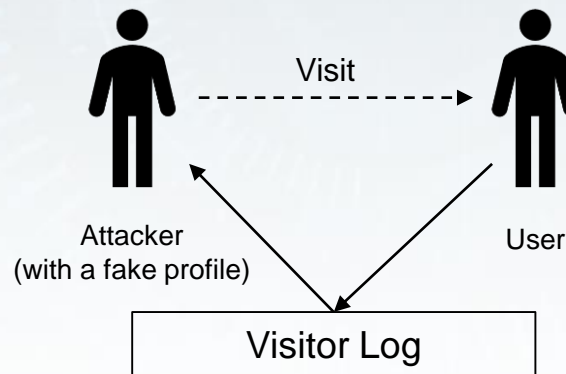
Different attacks of Reverse Social Engineering



(a) Recommendation Systems



(b) Demographic Search



(c) Visitor Tracking

Tips to Prevent Social Engineering

- Train your awareness to recognize persuasion and manipulation
 - Are my emotions heightened?
 - Did this message come from a legitimate sender?
 - Did my friend actually send this message to me?
 - Does this offer sound too good to be true?
 - Attachments or links suspicious?
 - Can this person prove their identity?

Tips to Prevent Social Engineering

- Manage your personal information
 - Know what your personal information is available online
- Protect Yourself
 - Manage accounts and passwords.
 - Use multifactor authentication
 - Keep software up to date
 - Enable spam filter
 - Secure your devices

Social engineering: Trends

1. Consent phishing on the rise
2. Business Email Compromise gets costlier
3. Deepfakes create deeper challenges
4. Nation-state attackers with social engineering in their arsenal
5. Expanding Phishing-as-a-Service market

! User awareness is no longer optional – it's essential !

Assignments

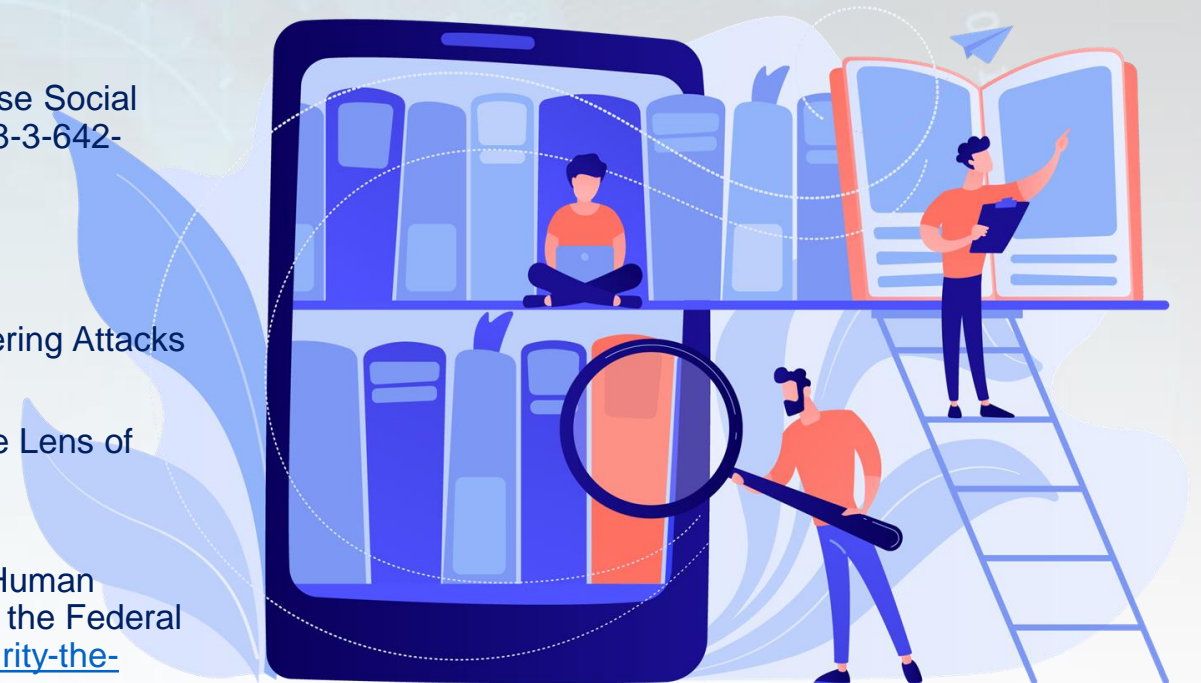


- Discuss the reasons of the increase in coronavirus fraud attacks
- Discuss the principle of influence applied by [Basecamp](#)
- Discuss what persuasion attacks you have encountered

Further Reading

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., Kirida, 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.



Short Videos

- 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>



Thank you!

