GameSS

SOCIAL ENGINEERING

WHO IS THE MATERIAL FOR?

This material will provide introduction into social engineering attacks and countermeasures. It is suitable for a broad range of target groups, such as developers, admins, employees and managers.

WHO MADE THIS MATERIAL?

Oksana Kulyk

Associate Professor at IT University of Copenhagen (ITU)

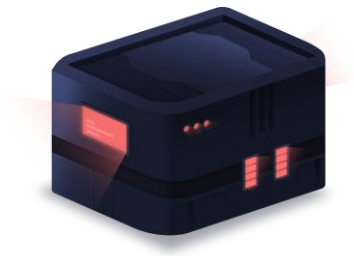
okku@itu.dk

WHAT ARE THE MAIN TAKEAWAYS FOR THIS CONTENT?

- Social engineering attacks are attacks aiming at influencing actions of a person or a group of people. In the context of security, social engineering attacks can take various forms (e.g. phishing or baiting) and involve digital as well as physical vectors.

- Social engineering attacks usually go through steps of choosing a target, contacting a target and exploiting the target. Information gathering, including information from public sources such as social media, is critical for success of the attack. Persuasion tactics such as appeal to authority are commonly used.

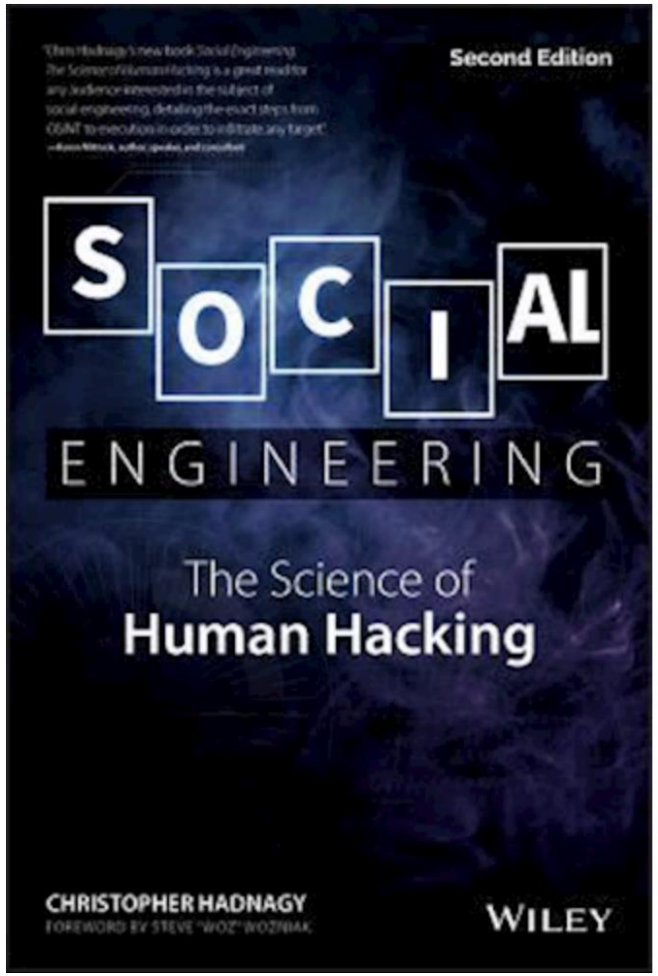
- Protection against social engineering is challenging due to how people make decisions, especially in unknown and/or high-stress situations. Resilience against social engineering can be built via reliable trustworthy infrastructure and well-thought out security policies for the employees, but people should not be treated as the only line of defence.



Disclaimer: the tools and techniques in this learning module are described for educational purposes only, so that you can be aware of them to better protect yourself or your company. Using them in real world on targets that don't give you permission to do so can be highly unethical and lead to legal reprecussions.

WHAT IS SOCIAL ENGINEERING

- Definition: ”Any act that influences a person to take an action that may or may not be in their best interest”
- Not necessarily cybersecurity–related: social engineering tactics can be used in ”traditional” scams
- Not necessarily malicious: social engineering tactics can be used for behavioral change towards a positive individual/societal effect!



EXAMPLES: DIGITAL

- Phishing, including vishing (voice phishing), smishing (sms phishing)…
- Baiting, e.g. distributing infected devices
- Waterholing
- WiFi spoofing

Source: military.com

Warning Issued to Troops Receiving Strange Smartwatches in the Mail

Airman wears a smartwatch, Dec. 3, 2020, at Hill Air Force Base, Utah. (U.S. Air Force photo by Cynthia Griggs)

EXAMPLES: PHYSICAL

- Dumpster diving
- Tailgating
- Shoulder surfing

Source: Business Insider

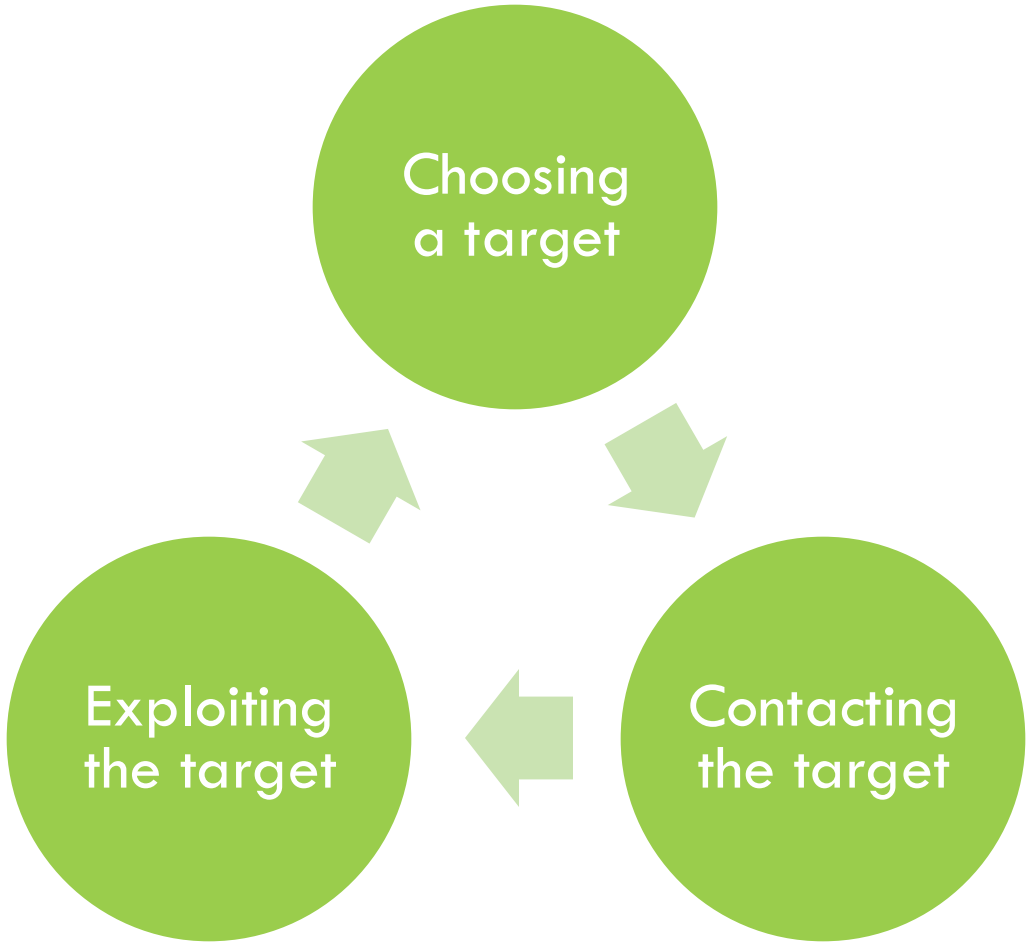
TRANSPORTATION

A British man boarded a flight to NYC without a passport or a boarding pass by tailgating behind unsuspecting passengers, report says

Joshua Zitser Feb 12, 2024, 12:37 PM CET

Share | Save

SOCIAL ENGINEERING STEPS



CHOOSING A TARGET

- General aim: Which people have access to the data/system components the attacker is interested in? → requires information gathering

- Can be also a pivoting point, i.e. using the initial target as a stepping stone for further attacks (example: an employee's account is compromised that is used for internal emails)

- Specificity of the target
  - Explicit → specific people are targeted
  - Opportunistic → mass targeting (e.g. all employees of the company, people frequenting a certain physical location, people visiting a certain website…)
  - Combination of both (e.g. all visitors of a coffee shop the actual intended target is known to frequent)

CONTACTING THE TARGET

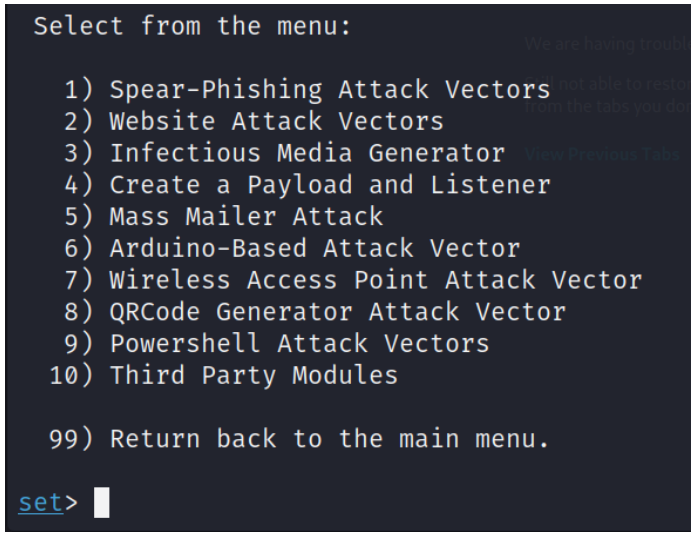
- Channel of contact: email (phishing), phone, social media, physical contact, use of compromised removable media…

→ depends also on goals of the attack (reveal sensitive information, run malware, provide access…)

- Can be one-off contact or long-term relationship/observation

- Can be manual or automated

- A variety of tactics to make contact more successful
  - Personalization via *information gathering*
  - Use of *pretexts* and *persuasion tactics*



Source: Social Engineering Toolkit

WHERE CAN INFORMATION BE FOUND?

- Content indexed by search engines

→ Google (Bing, etc.) searches

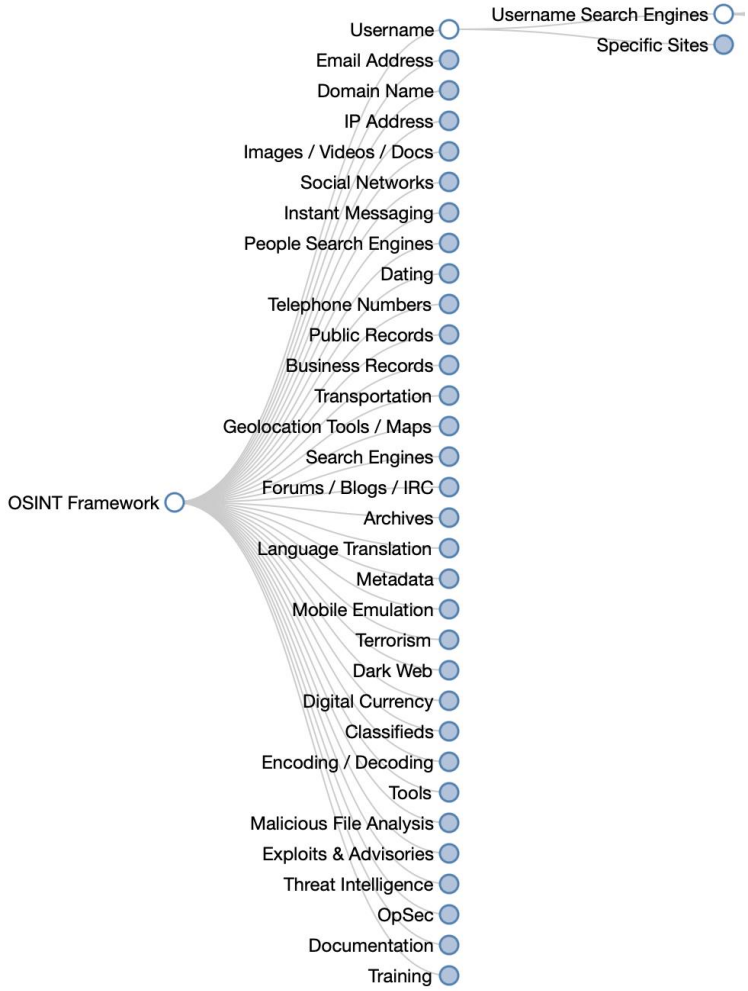
- Content not indexed by search engines, e.g. internal web pages or pages that require a user account to access

→ specialised approaches for searching (might require additional access)

- Content only accessible anonymously via specific software (e.g. Tor browser)

→ specific tools/search engines for searching

INFORMATION GATHERING: WHAT CAN BE FOUND



From: osintframework.org

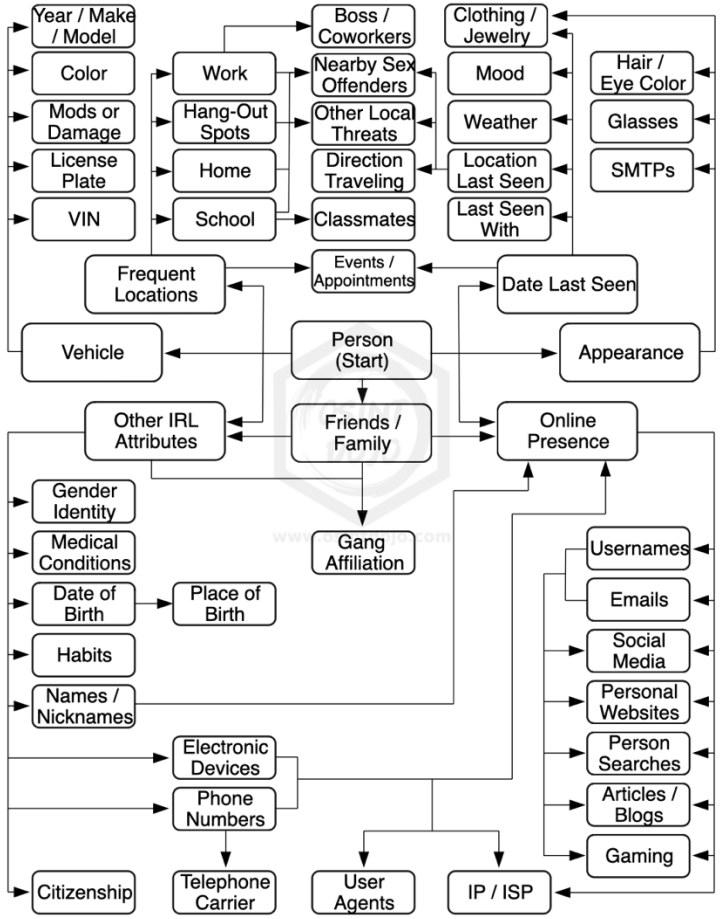
- Public, e.g. governmental records in open access, content publicly shared in social networks…
- Available under conditions (e.g. for pay, upon application, for people from specific groups…)
- Semi-legal, e.g. data breaches

INFORMATION GATHERING: PERSONAL DATA

- Governmental records (e.g. krak.dk)

- Social media, incl. forums, message boards…
  - Basic information: name, employment, relationship status
  - Usernames → can be used to identify other online accounts
  - Interactions with people/services: likes, check-ins, friends…

- Content posted by others
  - Friends/family on social media
  - Company website
  - Media reports
  - …



Source: https://www.osintdojo.com/diagrams/person

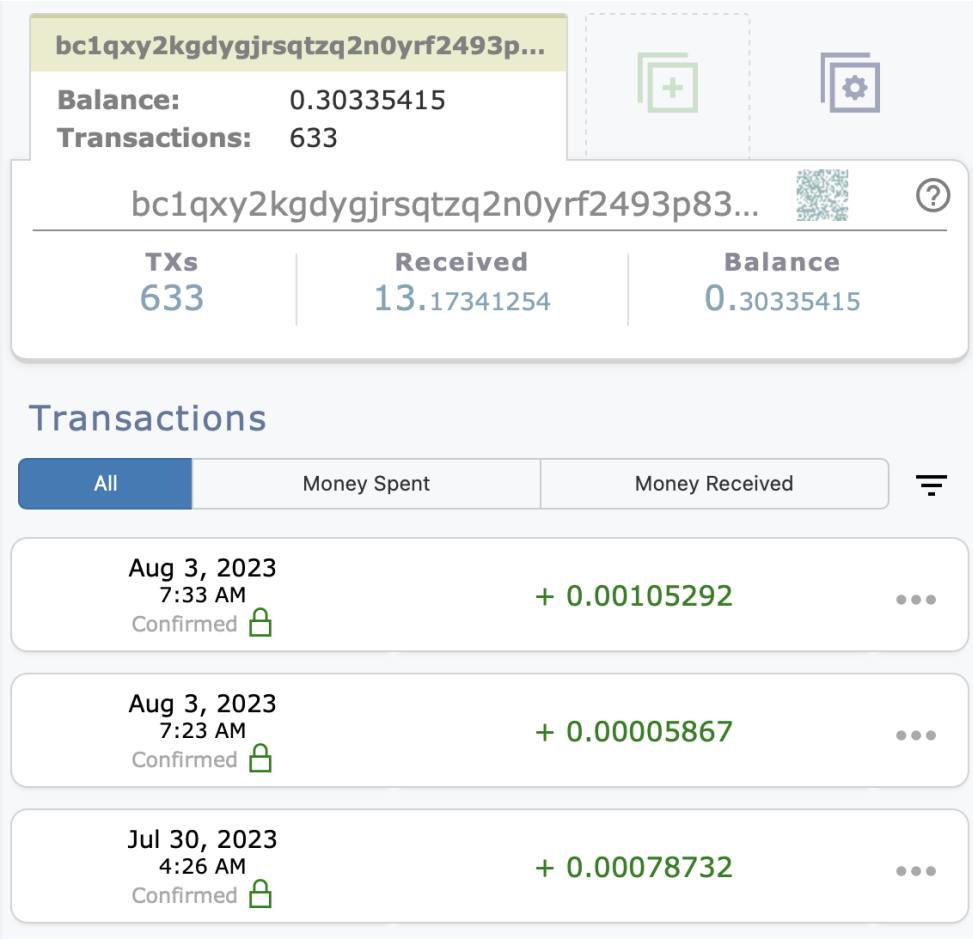
INFORMATION GATHERING: ORGANISATIONS

- Public records, e.g. CVR register, court documents…
- DNS records (see e.g. whois.com)
- Information directly from the company: website, press releases, social media…
- Information from company employees (e.g. social media)

```
Domain:                 gamess.dk
DNS:                    gamess.dk
Registered:             2023-05-08
Expires:                2025-05-07
Registrar:              ONE.COM A/S
Registration period:    1 year
VID:                    no
DNSSEC:                 Signed delegation
Status:                 Active
```

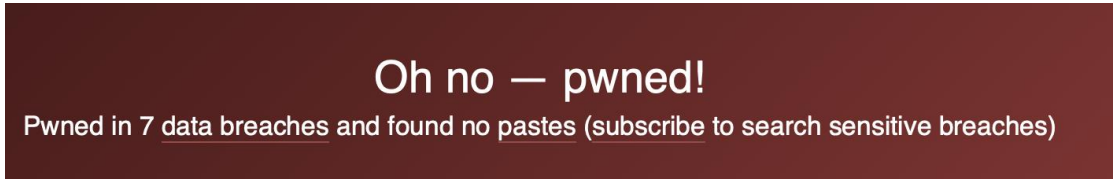
INFORMATION GATHERING: FINANCIAL INFORMATION

- Public information, e.g. tax records
- Leaks, e.g. financial papers, payment service transactions…
- Cryptocurrency
  - Transactions of a certain public key + network analysis → ledgers
  - Identities connected to certain keys → social media, personal/business pages…

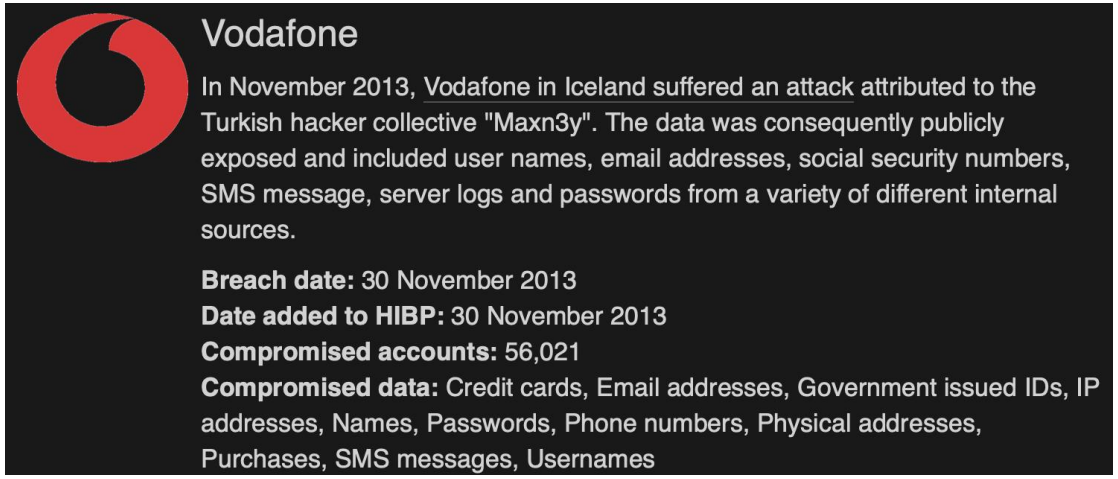


INFORMATION GATHERING: DATA BREACHES

- Information about user accounts
- Passwords/login credentials
- Other personal data (e.g. phone number, address…)
- Other data related to the organisation



Source: haveibeenpwned.com



PRETEXT: WORK

- Impersonate colleagues/supervisors
- Use current events to make communication more convincing

From: Alice <alice-mail@gmail.com>
To: Bob <bob@supertech.com>
Subject: TechInnovation presentation

Hi Bob,

As you know, our research team will present our latest product at the TechInnovation conference next month. As we need contributions from all our team members, we have set up a portal with the most current information about the event here (you would need your company login to access it). Please check that the information about your part of the project is accurate.

Best regards,
Alice

PRETEXT: WORK + PERSONAL

- Use personal information to make the approach more believable
- Aid in planning attacks, e.g. identifying targets that are unavailable for direct communication

- Use compromised personal accounts as a pivoting point to work accounts
  - Password reuse → try found passwords on other accounts
  - Mix of personal and professional accounts/devices → use to run malware

From: Alice <alice-mail@gmail.com>
To: Bob <bob@bob.com>
Subject: Access to budget

Hi Bob,

Can you please share with me the document with the budget overview? I am currently traveling, so I don't have access to my work device – but I need to finish my report by the end of the week, and I need the numbers from the budget for it…

Thanks a lot!
Alice

PRETEXT: PERSONAL

- Use as an initial conversation topic
- Establishing further rapport with the target (if long-term communication is the goal)

From: Jane
To: Bob

Hi Bob,

This is Jane Smith, we used to sit next to each other in the Advanced Programming class at the IT University. I saw the photos you posted and decided to reach out ;) How have you been doing?

From: FitnessPlus <info-fitnessplus@gmail.com>
To: Bob <bob@bob.com>
Subject: New offers for your gym membership

Dear Bob,

We have now opened new gym locations and have prepared some exciting new offers, including new classes and personal training sessions, to our members. Please check the attached file for a full overview of our offers.

Best regards,
FitnessPlus team

Activities.pdf

PERSUATION TACTIC: OFFERING OR PROMISING A REWARD

- People respond to being offered rewards

- Social engineering tactics
  - Offer a reward to the target
  - Do a small favor to the target, then ask for another favor in return
  - Ask for a favor, promising to return the favor in the future

PERSUATION TACTIC: LIKING AND SOCIAL PROOF

- People are more likely to do favours for someone they like/members of one's own social group

- Social engineering tactics
  - Pretend to be a member of one's social circle
  - Pretend to be a member of one's group (professional, political, ethnic,…)
  - Pretend to be someone likeable/attractive to the target

HOME > MILITARY & DEFENSE

Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up.

Sophia Ankel Sep 5, 2022, 4:27 PM

Source: Business Insider

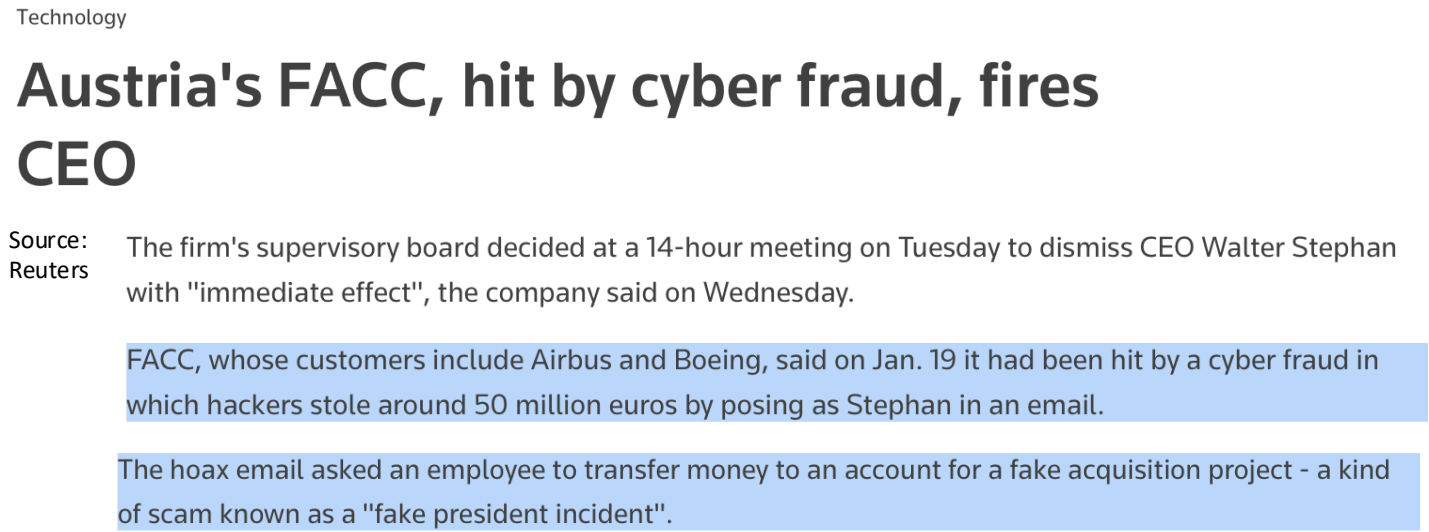
PERSUATION TACTIC: TRUST

- People are likely to find people (companies, websites…) trustworthy e.g. based on their appearance

- Social engineering tactics
  - Impersonate a trusted person
  - Refer to a trusted institution (e.g. by using logos in phishing emails)
  - Overall create a professional look (paying attention to texts of a phishing email/website design, wearing a suit/uniform,…)

PERSUATION TACTIC: APPEAL TO AUTHORITY

- People are likely to follow authority
- Social engineering tactics
  - Impersonate someone in a position of power (e.g. law enforcement)
  - Refer to organizational hierarchy (e.g. claiming to have a request from one's supervisor)



Technology

Austria's FACC, hit by cyber fraud, fires CEO

Source: Reuters

The firm's supervisory board decided at a 14-hour meeting on Tuesday to dismiss CEO Walter Stephan with "immediate effect", the company said on Wednesday.

FACC, whose customers include Airbus and Boeing, said on Jan. 19 it had been hit by a cyber fraud in which hackers stole around 50 million euros by posing as Stephan in an email.

The hoax email asked an employee to transfer money to an account for a fake acquisition project - a kind of scam known as a "fake president incident".

PERSUATION TACTIC: APPEAL TO URGENCY/SCARCITY

- People are likely to be less rational under pressure
- Social engineering tactics
  - Create a sense of urgency (e.g. claiming that one's account will be blocked unless the target acts immediately)
  - Create a sense of scarcity (e.g. offering a limited offer)

Sony hackers used fake Apple ID emails to steal passwords, says researcher

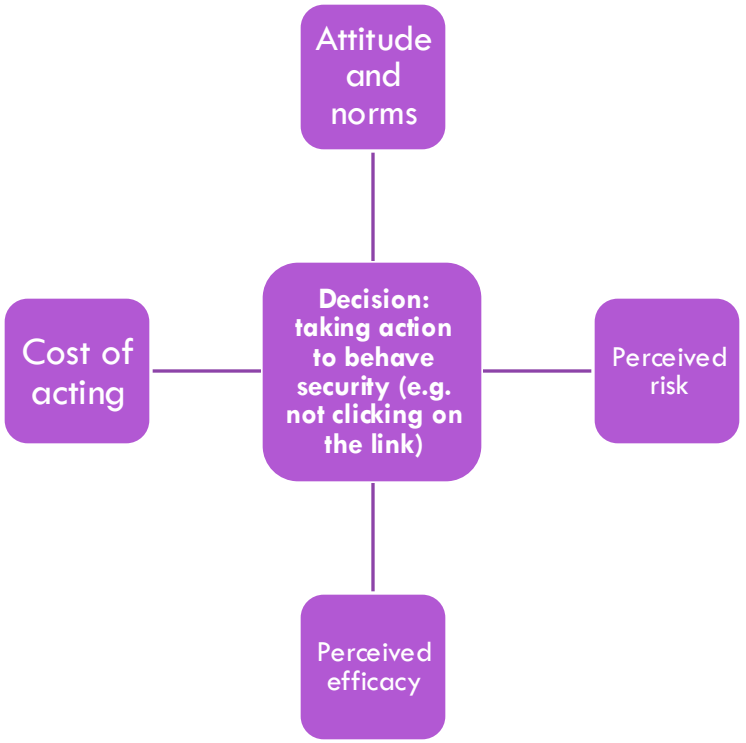
BY COLLEN KRIEL

According to McClure, the fake emails were near identical to official AppleCare emails instructing users to verify their Apple IDs. Users had to take action within 48 hours, stated the emails, or face being locked out of their Apple accounts.

HOW PEOPLE MAKE DECISIONS

- Most of the decisions are automatic
  - Security-related tasks are secondary tasks → for most of the people, these tasks are perceived as distraction/annoyance and as a barrier to the tasks they actually need to do
  - Consequences: advice such as carefully checking the links in emails, making sure that no one follows you when you enter the building, etc. will be very hard to comply with

- Non-automatic decisions rely on a number of factors that are context-dependent and often hard to predict



SOCIAL ENGINEERING PENETRATION TESTING

- Idea: let someone (e.g. external team of experts) try to attack the organisation using SE methods
  - → Similar principle to ”classical” penetration testing

- Issues to consider
  - How much information can one get about a person/company? Are illegal/“gray area” sources (e.g. content of leaked data breaches) ok to use? Is active social engineering (e.g. directly getting in contact with the target or their social circles) ok?
  - Which pretexts and persuation tactics are ethical to use?
  - How are the results reported; should specific people be named? Should information about them found via information gathering be shared with their employees?

- See also ”Phishing” lecture on simulated phishing campaigns

USER EDUCATION AND POLICIES

- Can be a helpful way to teach employees to react to social engineering

- What can be useful to communicate
  - Common types of attacks
  - Policies for sharing data/credentials/access, e.g. ”verify the sender of every email that requests you to send sensitive documents”, ” never share your password with anyone”…
  - Other restrictions on behavior, e.g. ”always lock your portable devices”, ”don’t run executable files in email attachments”, ”don’t use the same accounts for personal and work communication”…
  - Guidelines on how to behave in unusual/suspicious situations, including ways to report possible attacks

POLICIES ARE NOT ENOUGH

- Social engineering attacks hard to address with policies only

- Policies will not be followed if
  - They are not integrated into automated decision making
  - Their perceived cost is too high (e.g. using 2FA locks one out of important services or takes too much time out of one's work day)
  - The perceived costs of non-compliance is too low (e.g. "everyone is doing that")

- Policies do not necessarily cover unexpected situations

EXAMPLE 1

- John is a security guard tasked with protecting the physical premises of the company from unauthorized access. A visibly pregnant woman approaches him: she is not feeling well and her phone is not working, so she needs to be let inside the building to use one of their phones for calling for help and to use a bathroom.

- What should John do?
  - Ignore the request → The woman might have serious health issues
  - Let her in → The woman might use the access to the building to e.g. plant eavesdropping devices or removable media with malware

→ Can be addressed e.g. by having a second security guard who stays at the entrance while John helps out the woman while making sure she does not do anything suspicious

EXAMPLE 2

- Alice is on a business trip. She needs to log in to the company web portal to download the sensitive documents she needs for her work during the trip. She sees a free WiFi hotspot in her hotel but is reluctant to connect because she is not sure whether the communications with her company portal will be secured.

- What should Alice do?
  - Do not connect to WiFi → Might be unable to do her work if there are no alternative connections
  - Connect to WiFi → If the company portal does not have sufficient protection and the hotspot is controlled by an attacker, Alice's credentials and the documents she downloads will be leaked

→ Can be addressed by technical means, ensuring that the portal implements encrypted communications (i.e. ensuring that the connection to the website is secured via https and/or offering VPN services for employees that connect to the website while traveling)

EXAMPLE 3

- Bob receives an email from his coworker, Alice, asking him to share a sensitive document with her. She is on vacation, so she does not have access to her work device. She mentions an important deadline for submitting a report for which she requires the document. She is anxious that she will not be able to meet this deadline unless she works on the report already before she comes back to the office.

- What should Bob do?
  - Ignore the request → Alice (and possibly others who depend on the report being submitted on time) might get in trouble
  - Send the document → ”Alice” might be an impersonator

EXAMPLE 3: POSSIBLE SOLUTIONS

- Check the sender's email → "Alice" says that she is writing from her private email account, so the sender's address is different from the email she usually uses

- Contact the sender via alternative channels to confirm the request → since Alice is on vacation, Bob does not have any other way to contact her

- Check whether the attacker can be expected to know the information provided in the email
  - Alice being on vacation
  - Alice having a deadline for the report
  - Alice requiring the document she requests for the report

  → Can work, but requires effort to find out

→ No obvious solution for either Bob or the company!

HOW TO APPROACH SOCIAL ENGINEERING

- Swiss cheese model: do not rely on people as ”the only line of defense”

- Identify potential weak spots
  - Company policies (e.g. use of personal devices, including working from home) that might lead to higher suspectability towards SE attacks
  - Amount of information available from open sources that can be used in SE attacks

  → These are not always possible to 100% mitigate, but useful to know about for monitoring

- Harden company infrastructure, e.g. using 2FA and additional controls (e.g. requiring access only from physical organisation premises) for access to important accounts/assets

- Provide easy and transparent ways to report suspicious incidents

SUMMARY

- Social engineering attacks are variable and rely on factors that are hard to mitigate
  - Availability of information allowing the attacker to select targets personalise their attack
  - Availability of access to the target – sometimes physical access is required, but digital communication works as well
  - Human psychology and being influenced via persuasion tactics

- Holistic approach is needed to protect against social engineering

FIND OUT MORE

https://gamess.dk/

GameSS

WHO IS BEHIND GameSS

Partners behind the project

SDU

DTU

IT UNIVERSITY OF CPH

AALBORG UNIVERSITET

Happy 42

Collaborators

ERHVERVSAKADEMI AARHUS

kea KØBENHAVNS ERHVERVSAKADEMI

Dania ERHVERVSAKADEMI

UCN

UCL Erhvervsakademi og Professionshøjskole

Supported by

Uddannelses- og Forskningsministeriet

Ministry of Higher Education and Science Denmark