openHPI Course: Digital Identities – Who am I on the Internet?

Identity Theft – Social Engineering Attacks on Users

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

What is Social Engineering?

Exploiting human weaknesses to provoke certain reactions

- Under a false (e.g. stolen) identity, the attacker exploits the human weaknesses (trust, fear, respect, helpfulness) of a victim
- Victim is made to do something that he/she would not do under normal circumstances, e.g.
  - Release of information, such as identity data
  - Granting access to a protected system / location
- Most common social engineering method on the Internet:

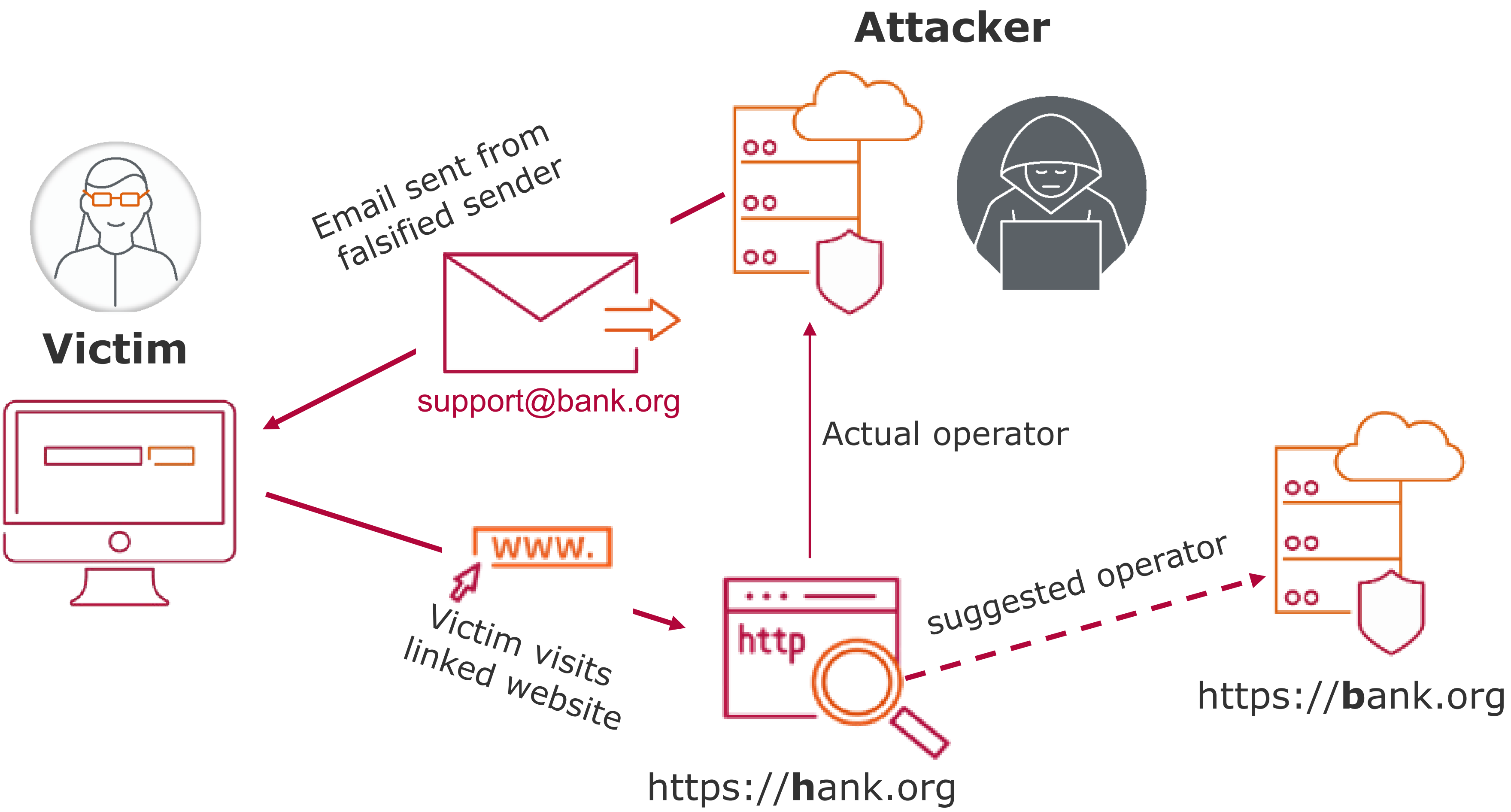
  → **Phishing**

Phishing (1/2)

Attack technique for fraudulent acquisition of sensitive information

- Typical procedure: Sending **fraudulent emails**
  - □ sent with trustworthy sender address, e.g. bank, company, authority, family, ...
    - – sender address (are easy to fake - spoofing) is selected according to the information to be spoofed
  - □ **Exploiting the acquired trust** to initiate desired response, e.g.
    - – release of data
    - – click on link of a dangerous website
    - – installation of malware

Phishing (2/2)



Attacker

Victim

Email sent from falsified sender

support@bank.org

Actual operator

Victim visits linked website

suggested operator

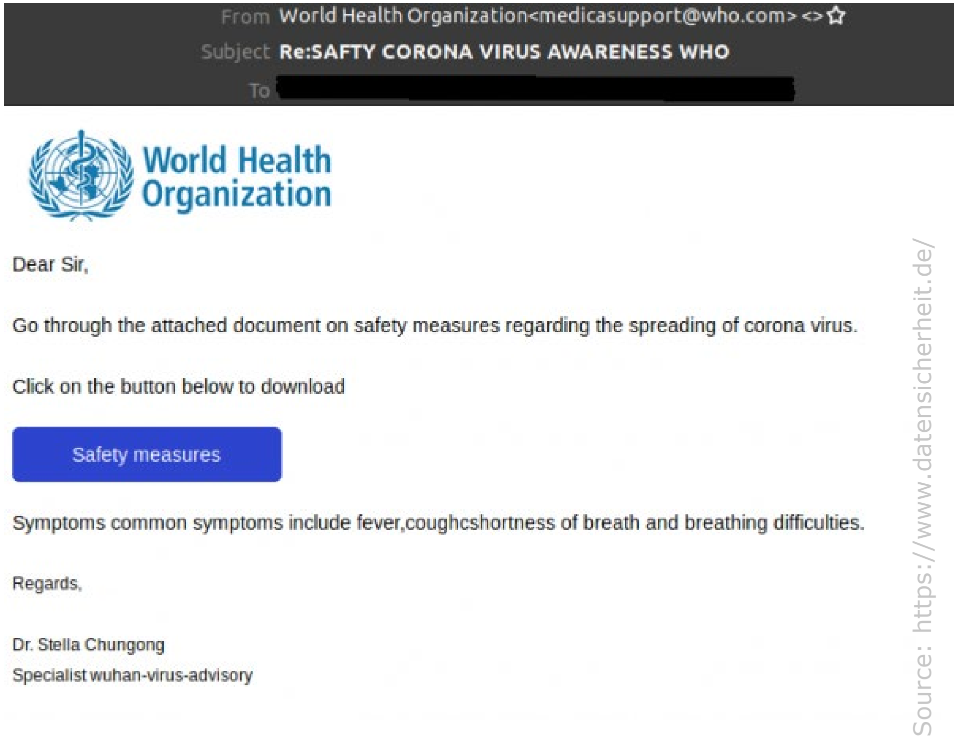
https://**h**ank.org

https://**b**ank.org

Phishing – Example

Goal: Get recipients to reveal sensitive information

- Sending an email with a fake sender
- Message allegedly originates from the **World Health Organization**
- Phishing often visible by linguistic or grammar mistakes or lack of personal contact (“Dear Sir")



From World Health Organization<medicasupport@who.com> <> ☆
Subject **Re:SAFTY CORONA VIRUS AWARENESS WHO**
To [redacted]

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Source: https://www.datensicherheit.de/

Widely Scattered Phishing Attacks

Traditional phishing attacks are relatively **easy to detect**

- Therefore, phishing emails are very widely distributed and undirected – with many millions of potential victims, even a very low conversion rate is sufficient to achieve significant success

Problems for attackers

- Internet users are well sensitised to common phishing scams through the media
- Phishing mails reach many recipients to whom the content does not apply at all and are therefore easy to identify as phishing, e.g.
  - □ sender is a bank where the victim does not have an account

Personalized Phishing (1/2)

Attackers are increasingly turning to personalized phishing, **spear phishing**, as they can no longer achieve their goals with "normal" phishing

- Obtaining sensitive (identity) information
  - in a preliminary phase, very detailed, often private information about the victim is collected
  - helpful for feigned trustworthiness, e.g. using the identity of a person the victim knows and trusts
- Phishing mail is then sent from a fake sender. Victim trusts the fake sender because message contains information that only this sender knows ...
- Chances of success with this scam are very high, but the effort for attackers is significantly higher

Personalized Phishing (2/2)

- Many attacks on the Internet are based on previous personalized phishing attacks
- Personalized phishing is therefore **very dangerous** and is specifically aimed at
  - □ high-ranked target persons, e.g. heads of companies, politicians, high-ranking officials, celebrities, ...
  - □ sensitive objectives, e.g. military, business, politics, financial industry...
  - □ professional attackers, e.g. states, activists, organized crime

Other Social Engineering Techniques

- **Baiting**
  - □ Exploiting the curiosity/curiosity of victims
  - □ Distribution of gifts with malicious secondary functions, e.g.
    - – USB sticks with malware, apps, ...
- **Pretexting**
  - □ Faking stories or lies in order to persuade victims to disclose information or to react in a certain way
  - □ Telling a story while pretending to be an authority or an initiate
- **Reverse Social Engineering**
  - □ Attacker contacts victim seeking help to gain trust

Attacks through Social Engineering - **Protective Measures** (1/2)

- **Awareness raising** of users
  - □ through education, e.g. through our openHPI course
  - □ also through occasional tests with phishing emails
- **Verification of the identity** of the alleged counterpart
  - □ in case of doubt, it is better to distrust and ask for proof of identity
- Use of **secure authentication**, e.g.
  - □ about trustworthy certificates
- **Responsible handling** of personal information
  - □ What is given to the outside world? What is posted on the Internet?

Attacks through Social Engineering - **Protective Measures** (2/2)

- Thorough check of the sender address – not the displayed name in the email software
- When sensitive information is requested, confirm request with the service provider
- Before following a link, check the address in the browser address bar
  - common browsers often warn against phishing websites

Social Engineering Attacks
Summary

Attack Tactics

- Attackers manipulate, exploit human weaknesses, and build trust with victims to initiate certain behaviors, e.g.
  - □ publishing sensitive information or installing malicious software
- Common procedures: Sending fraudulent emails or sneaky phone calls

Special form: **Spear Phishing** (personalized phishing)

- Attacker focuses on a specific person and collects detailed information about the victim
- More complex in preparation, but more effective than "normal" phishing