cybersecurity centre

GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

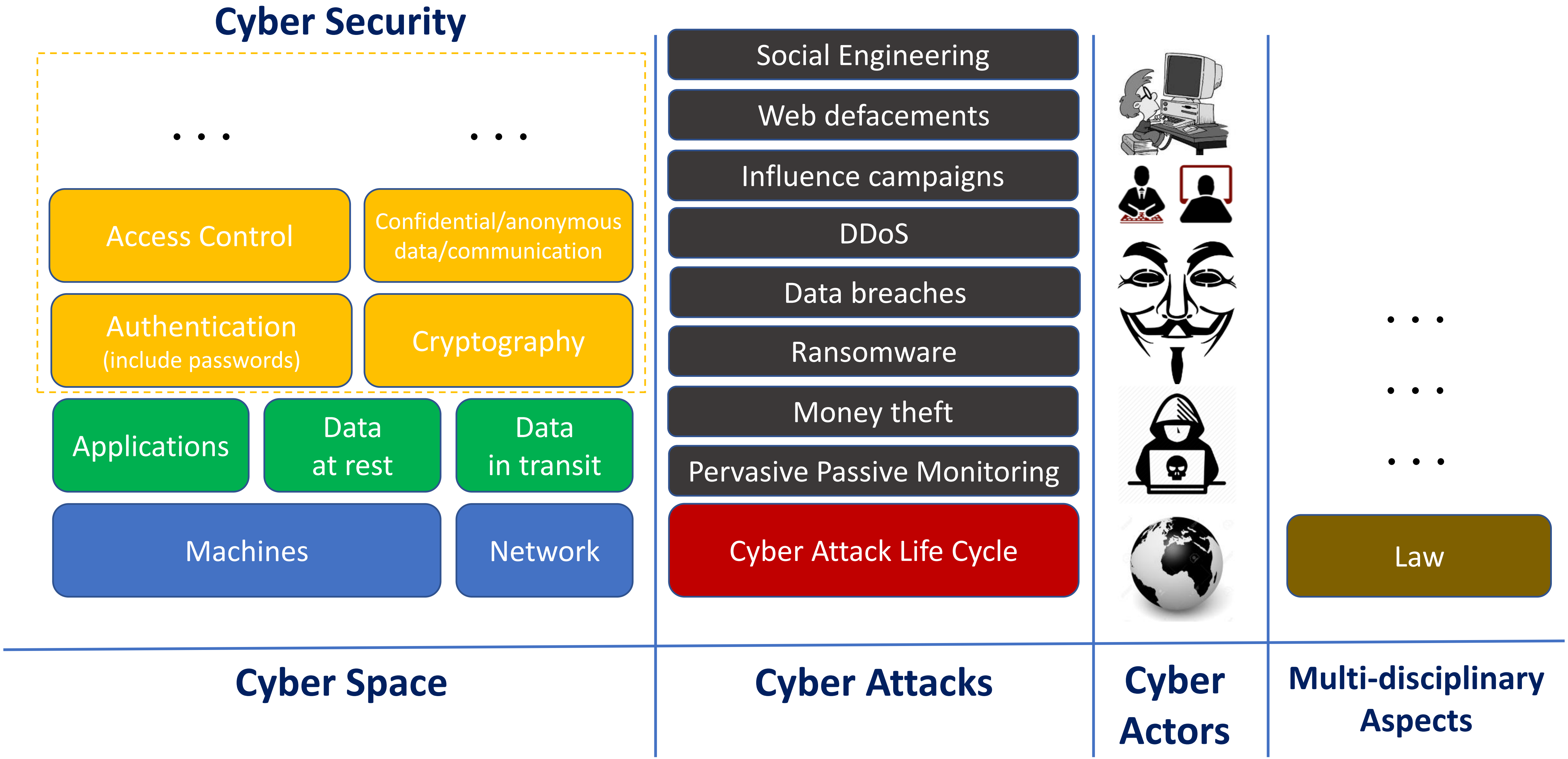
Social Engineering

Week 8 – Tuesday 19th November 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Link with previous lectures



Cyber Security

. . .

. . .

Access Control

Confidential/anonymous data/communication

Authentication (include passwords)

Cryptography

Applications

Data at rest

Data in transit

Machines

Network

Cyber Space

Social Engineering

Web defacements

Influence campaigns

DDoS

Data breaches

Ransomware

Money theft

Pervasive Passive Monitoring

Cyber Attack Life Cycle

Cyber Attacks

Cyber Actors

. . .

. . .

. . .

Law

Multi-disciplinary Aspects

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Describe what social engineering (SE) is
- LO2 Discuss the main SE techniques used in the cyber space
- LO3 Select behaviours that can be effective against SE techniques

Outline

- ➢ **What is Social Engineering?**
- Anatomy of SE attacks
- SE techniques
  - o Information gathering
  - o Interaction with the target
  - o Tailgating
  - o Baiting

What is Social Engineering?

In the cyber security context, social engineering concerns techniques to psychologically manipulate people into performing some action or divulging specific information

What is Social Engineering?

80% OF HACKERS SAY
humans are the most responsible for security breaches
thycotic
thycotic.com/BlackHatReport2017

What is Social Engineering?

- Attack vector through the person
  - People are vulnerable to psychological manipulation
  - People usually is the “weakest link in the chain” of security
  - People can’t be easily “patched”

Why cracking a password when you can simply ask for it?

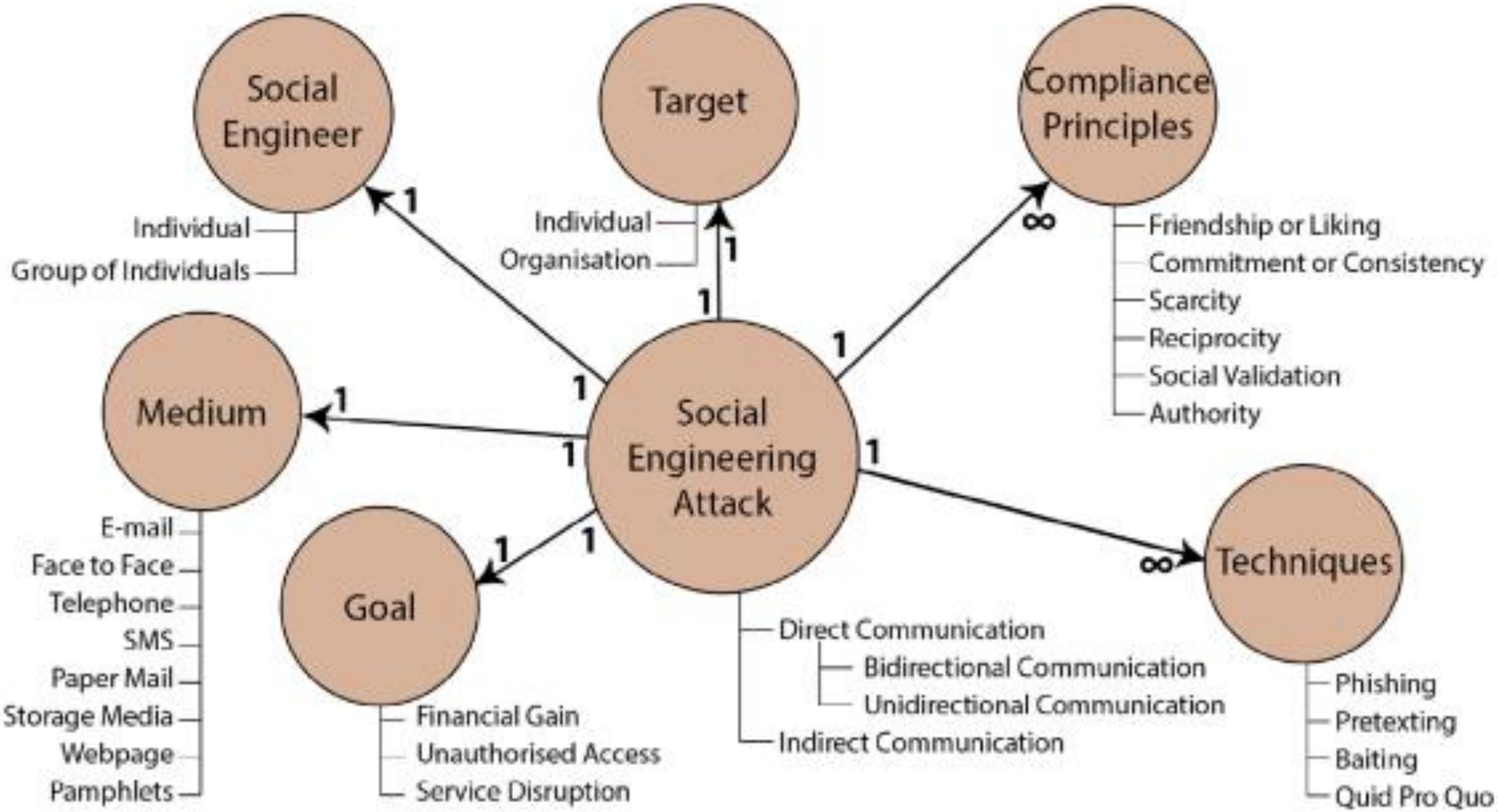
Outline

- What is Social Engineering?

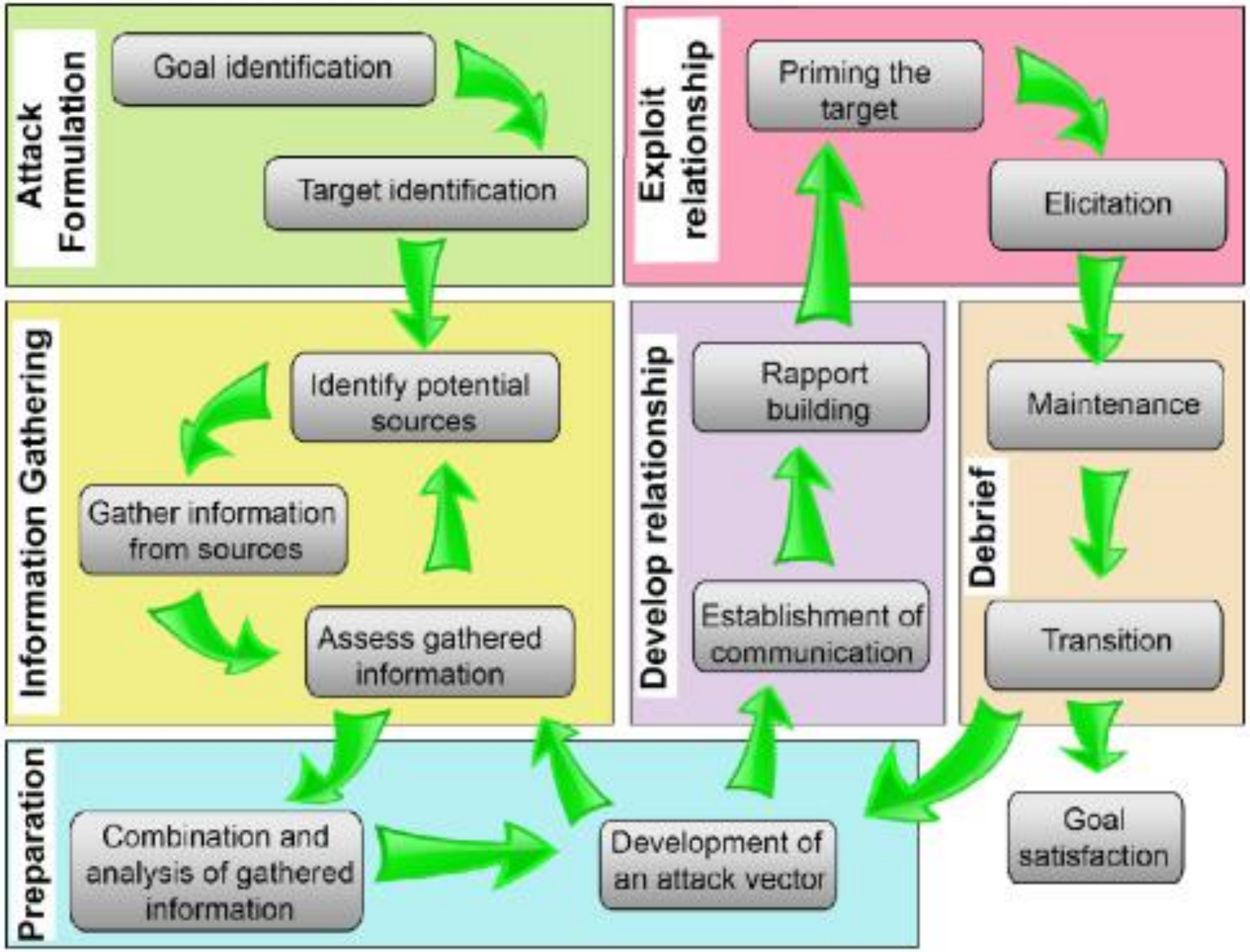
➢**Anatomy of SE attacks**

- SE techniques
  - Information gathering
  - Interaction with the target
  - Tailgating
  - Baiting

Anatomy of SE attacks



Anatomy of SE attacks



Outline

- What is Social Engineering?
- Anatomy of SE attacks

➢ **SE techniques**

  - ○ Information gathering
  - ○ Interaction with the target
  - ○ Tailgating
  - ○ Baiting

Information Gathering

- On the web
  - Company website
    - Background
    - Executives and employees
    - Email addresses
    - Company addresses and telephone numbers
    - Open job positions
  - Social networks
    - Facebook/Instagram
    - LinkedIn
    - Social network mining

Information Gathering

- Dumpster diving
  - Employees commonly use their office thrash rather than a shredder
  - What the attacker may find
    - Account information, e.g. credentials
    - Personally Identifiable Information
      - Email addresses
      - Telephone numbers
      - Calendars with schedules
      - Resumes
    - Sensitive company information, e.g. intellectual property

Information Gathering

- Shoulder surfing
  - Simply look over the target’s shoulder when she is at her computer
  - Whatever is shown on screen or typed on keyboard can be obtained
    - Usernames and passwords
    - Confidential data
  - Can be done anywhere, also outside the office
    - Coffee shops
    - Airports

Interaction with the target

- Phishing
  - Practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information
    - Spear Phishing
    - Whaling
  - URL and Email Manipulation (http://www.company.com/ vs http://www.cornpany.com/)
  - Common vectors
    - Current Events and Charities
    - Tech Support
    - Financial
    - Government

SE techniques

Interaction with the target

- Vishing and Smishing
  - Social engineering using
    - The telephone system (voice calls)
    - Text messages (SMS)
  - Tools
    - Caller ID spoofer
  - Notable example: attacker poses as your bank and ask you to enter your authentication data for verification purposes
- Physical Impersonation
  - The attacker shows up in person posing as someone not suspicious
    - Maintenance
    - Check alarms / smoke detectors
    - Deliver a package / food

SE techniques – Group Activity

- Scenario
  - Consider an organisation targeted with SE techniques
  - How should employees behave to minimise the likelihood that SE techniques are successful?
- Activity
  - Split into groups of 4/5 students
  - For each SE technique, discuss with your group (5 minutes in total)
    - What behaviour can prevent it from succeeding?
    - Why?
  - Open discussion (5/10 minutes)

SE Techniques

Information Gathering

- On the web
- Dumpster Diving
- Shoulder Surfing

Interaction with target

- Phishing
- Vishing & Smishing
- Physical Impersonation

SE techniques – Group Activity

- **Information Gathering on the web**
  - Be aware of her own social presence, in terms of available information, and how these information can be used to derive confidential/secret information
  - Revise online personal information
- **Dumpster Diving**
  - Use shredder to get rid off of any potentially sensitive paper document
  - Do not leave written notes or post-it in the office
- **Shoulder Surfing**
  - Keep an eye on who is around you
  - Never leave your laptop unattended
  - Shield your laptop with your body
- **Vishing & Smishing & Physical impersonation**
  - Check for spelling/pronunciation/visual mistakes
  - Don't give up personal information
  - Be wary of demanding language
  - Don't believe everything you read/hear/see

- **Phishing**
  - Take a look at the sender's email address – If it looks suspicious, don't open the email.
  - Look before you click - Hover your mouse over any hyperlinks found in the email and if the address looks weird, don't click on it.
  - Check for spelling mistakes - Legitimate messages usually do not have major spelling mistakes or poor grammar.
  - Who is the email addressed to - Is the email addressed to a vague customer or is it addressed to you personally. Legitimate businesses generally give personal greetings.
  - Don't give up personal information – Legitimate companies will never ask for personal information via email.
  - Be wary of demanding language - Invoking a sense of urgency or fear is a common phishing tactic.
  - Look at the email signature – If there is a lack of contact details in an email signature, it could be a phishing email
  - Don't click on attachments - Including malicious attachments that contain viruses and malware is a common phishing tactic. Don't open any email attachments you weren't expecting.
  - Don't believe everything you see – If it's too good to be true, it probably is not true!

SE techniques

Baiting

- Like real-world Trojan horse
- Examples
  - Infected removable media left where people can find them
    - Car park
    - Bathroom
    - Meeting room
    - Elevator
  - A gift with a wiretap inside: a photo album, a USB hub

SE techniques

Tailgating

- Accessing a secured building/area without any smart-card/biometric, by simply walking closely behind an authorised employee
- General strategy
  - Wait for authorised personnel to enter and quickly join them
  - They are likely to hold the door open and let the attacker in
    - Politeness
    - Attacker wearing a fake badge/card
    - …or simply showing to be searching for it…

Social Engineering – Recap

- What is Social Engineering?
  - Techniques to psychologically manipulate people into performing some action or divulging specific information
- Anatomy of SE attacks
  - SE attack model: core entities and relationships
  - Life cycle of SE attacks
- SE techniques
  - Information gathering
  - Interaction with the target
  - Tailgating
  - Baiting
  - How to prevent them from succeeding?

Social Engineering - References

- 2017 Black Hat Hacker Survey
  - https://thycotic.com/resources/black-hat-2017-survey/
- Anatomy of Social Engineering attacks
  - Mouton, F., Leenen, L., Malan, M.M. and Venter, H.S., 2014, July. Towards an ontological model defining the social engineering domain. In IFIP International Conference on Human Choice and Computers (pp. 266-279). Springer, Berlin, Heidelberg.
  - Mouton, F., Leenen, L. and Venter, H.S., 2016. Social engineering attack examples, templates and scenarios. Computers & Security, 59, pp.186-209.
- Social Engineering Techniques
  - https://www.social-engineer.org/