School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Week 9

Social engineering: The *what* and the *how* and *countermeasures*

Learning objectives

- PART 1:
  - What is social engineering?
  - Targets of social engineering
  - The impact of the Internet on the scalability of social engineering
- PART 2: Top threats
- PART 3: Steps to perform social engineering attacks
- PART 4: Countermeasures

PART 1: WHAT IS SOCIAL ENGINEERING?

Activity #1: What is it?

- What is social engineering?
- Have you heard of any social engineering attacks?

Kevin Mitnick

Image courtesy: Mikhail Romanenko

Kevin Mitnick

Imprisoned for breaking into phone systems.

Typical hack: pretend to be company employee, solicit ‘help’ such as the password.

“Social engineering uses **influence and persuasion** to deceive people by convincing them that the social engineer is someone he is not, or by **manipulation**. As a result, the social engineer is able to take advantage of people to **obtain information with or without the use of technology.**”

Kevin Mitnik et. al. from *The Art of Deception: Controlling the Human Element of Security (2002).*

Targets

Effective social engineers can obtain the following information:

- User passwords
- Security badges or keys to the building and even to the computer room
- Intellectual property such as design specifications, source code, or other research and development documentation
- Confidential financial reports
- Private and confidential employee information
- Personally-identifiable information (PII) such as health records and cardholder information
- Customer lists and sales prospects

Targets (cont.)

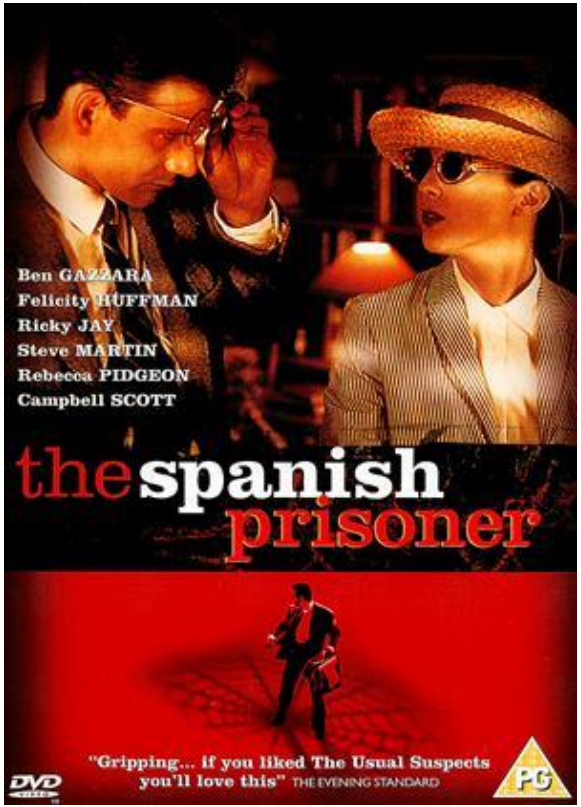
- People are **the weakest link** in any security system.
- *"Only **amateurs** attack machines; **professionals** target people." Bruce Schneier*
- "People hacking".
- *Exploits people's trusting nature.*
- Hardest thing to defend against.

SOCIAL ENGINEERING IS OLD

Spanish Prisoner Scam

- 19th century confidence trick.
  - Gain confidence (trust) of a mark
  - Defraud them
- Spanish prisoner scam
  - Wealthy prisoner
  - False identity
  - Small amount needed to release
  - Monetary and non-monetary reward
  - Unexpected expenses

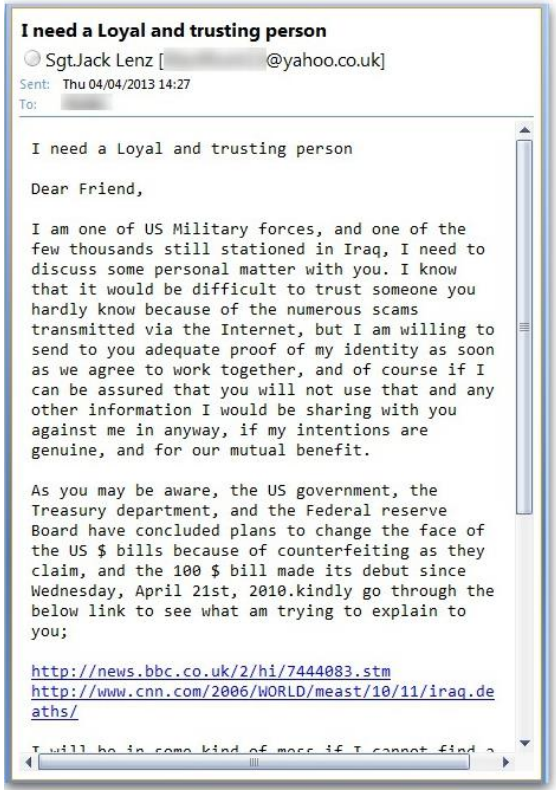
https://en.wikipedia.org/wiki/Spanish_Prisoner



419 Scam

- 419 is a number of a penal code in Nigeria (although most scammers are in the USA).
- Small outlay, get something of much greater value.
- Many variations of central idea:
  - Romance
  - Jobs
  - Pets
- Much greater pool of marks

https://en.wikipedia.org/wiki/Advance-fee_scam



I need a Loyal and trusting person

Sgt.Jack Lenz [@yahoo.co.uk]

Sent: Thu 04/04/2013 14:27

To:

I need a Loyal and trusting person

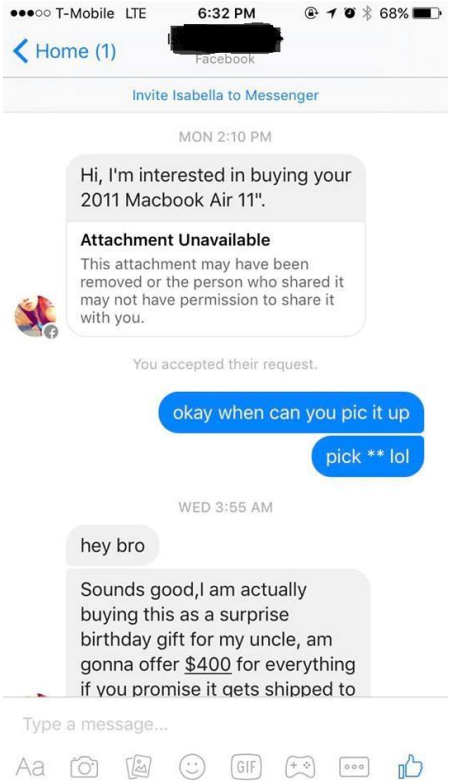
Dear Friend,

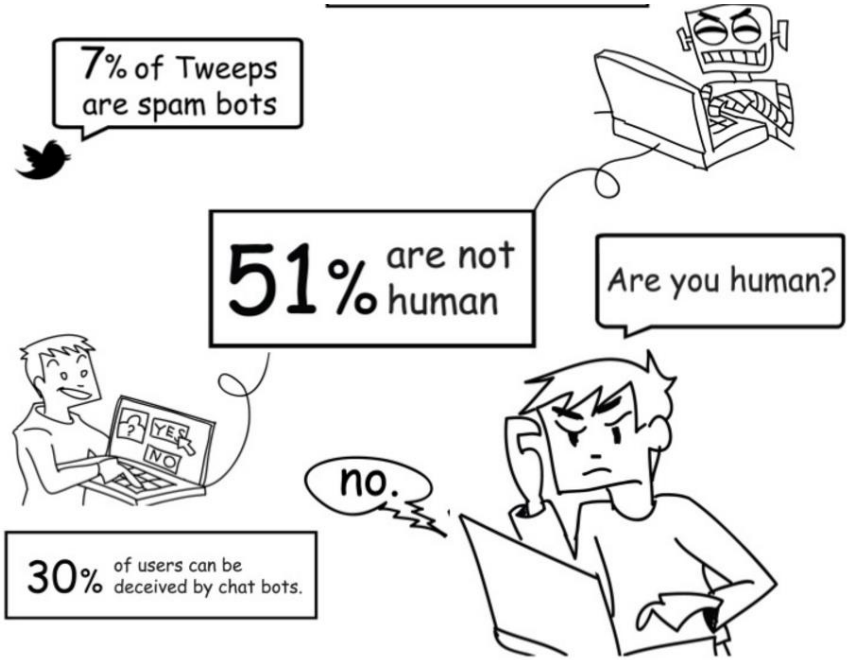
I am one of US Military forces, and one of the few thousands still stationed in Iraq, I need to discuss some personal matter with you. I know that it would be difficult to trust someone you hardly know because of the numerous scams transmitted via the Internet, but I am willing to send to you adequate proof of my identity as soon as we agree to work together, and of course if I can be assured that you will not use that and any other information I would be sharing with you against me in anyway, if my intentions are genuine, and for our mutual benefit.

As you may be aware, the US government, the Treasury department, and the Federal reserve Board have concluded plans to change the face of the US $ bills because of counterfeiting as they claim, and the 100 $ bill made its debut since Wednesday, April 21st, 2010.kindly go through the below link to see what am trying to explain to you;

http://news.bbc.co.uk/2/hi/7444083.stm
http://www.cnn.com/2006/WORLD/meast/10/11/iraq.deaths/

Social media and bots





Activity #2: Role of Internet

- How does the Internet make modern scams such as 419 more profitable and **easier** to carry out?

Activity #2: Role of Internet

- How does the Internet make modern scams such as 419 more profitable and easier to carry out?

  - Previously one-to-one interaction, now one-to-many via email or social media platforms
  - Larger number of marks means larger absolute number of marks who fall for the scam
  - People find it hard to make trust judgements **in the absence of body language** and other signals that you get in a one-to-one interaction

PART2: TOP THREATS

Phishing

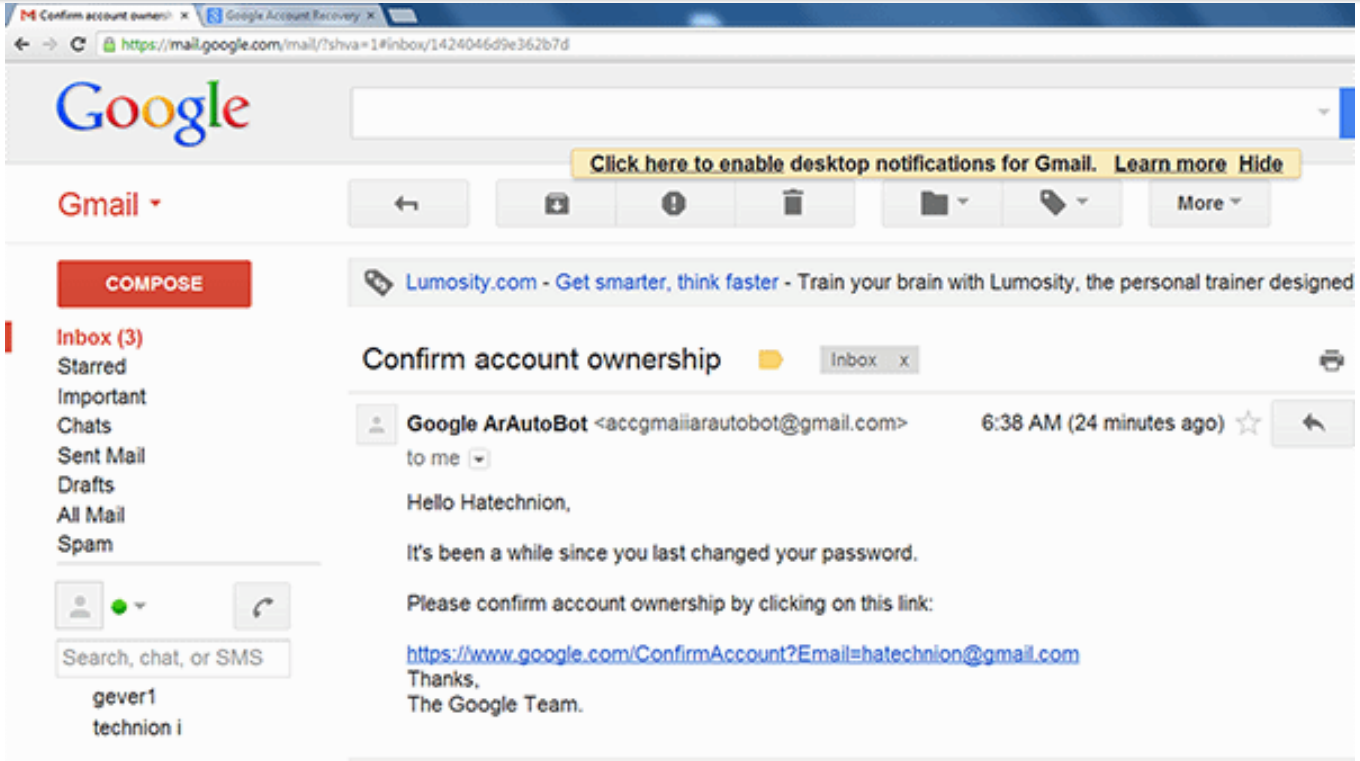
- Attacker sends email, text, messenger, ...

- Action that the attackers wants you to do:
  - install malware
  - direct you to a phishing website
  - pay money

Phishing email

- Embed links to legitmate looking websites owned by attacker.
- Use similar sounding domains (anz.ezpay.nz), link shorteners or HTML links to hide target.
- Email claims to be from a trusted source and usually creates a fake **urgency** to pressure victim.
- Early in the Internet you could pretend to be anyone else and send mail.
- Sender Policy Domain (SPF) controls which computers can send mail.
- *Problem is it isn't implemented everywhere yet*.

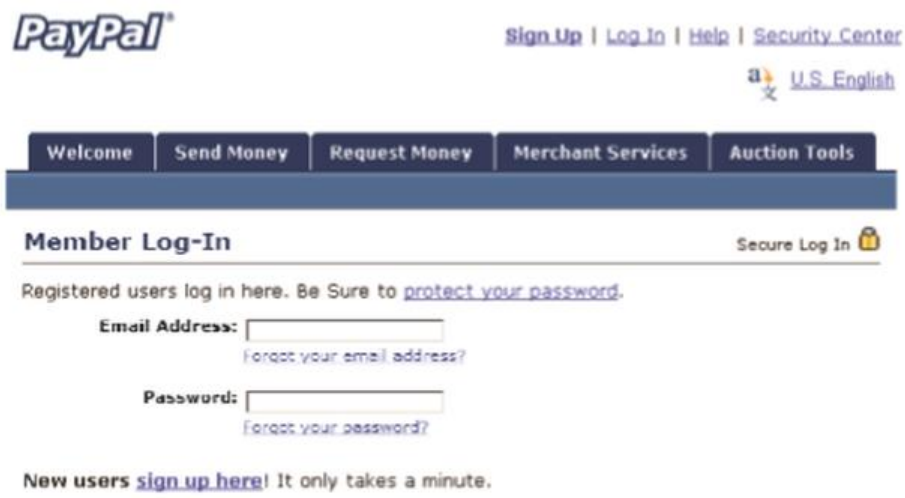
Example: phishing email



Mousing over the link might reveal a different target than you think...

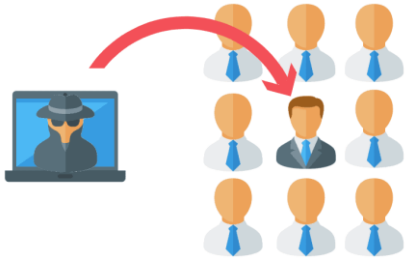
Example: phishing website

- Copying websites is easy!
- Mimic the company that they are **spoofing**.
- Redirect the user to an error page but keep the data.
- Browsers have blacklists of phishing websites.
- Attackers just create new ones - 1.4 million unique websites per month (Zdnet 2017).



More sophisticated phishing

- Spear phishing targets:
  - Organisations
  - Businesses.
  - Indviduals.
- **Whaling** targets:
  - High value individuals.
  - Name, job title, relevant information.
- Email compromise and invoice scam:
  - Take over business email.
  - Send invoices to victims.



Pretexting

- Pretext = fabricated scenario used to steal the victim's information.
- Unlike phishing emails, which use **fear** and **urgency** to their advantage, **pretexting** attacks rely on building a **false sense of trust** with the victim.
- Strength is in the believability of the story.
- Use a completely fake identity.
- Target is usually an organisation whereas **phishing** targets an individual.
- Examples:
  - "Hello Victoria University payroll, I am from the Inland Revenue Department. I need Harith's home number and address in order to contact him."
    New Zealand Inland Revenue
  - http://video.link/w/qH6d

Baiting

- Promise of item or good that is desirable to the victim.
- Secure Network Technologies (2006).
- 20 USB sticks left in parking lost.

- Each contained an image and trojan horse malware.
- All 15 found were plugged into their (organisation's) computer.

Quid Pro Quo

- Benefit in exchange for information.
- Benefit could be service or be an item.
- Study in 2003, 90% of office workers at Waterloo Station in the UK gave away their computer password for a cheap pen (**men were worse than women by difference of 5%**).
- Similar studies involving chocolate bars.

Tailgating

- Can’t get into a building?
- No problem, just wait until someone with access enters the building and follow after them.
- Strike up conversations with employees (become a smoker) to increase trust.
- Also known as “**piggy backing**”.
- See this all the time at the Victoria gym.

PART 3: HOW TO DO IT (*PLEASE DON'T*)

How to do social engineering?

1. Define your goal.
2. Seek information about victim.
3. Build trust.
4. Exploit the relationship.
5. Use the information gathered for malicious purposes.

#1 Seek information

- Find out as much as possible about the victim.
- Google the victim, their company, their friends.
- Social networking sites – facebook, Instagram, linkedin, oldfriends …
- Search for newspaper stories or blogs about the target.
- Dig through the rubbish thrown out at home or at the office.
- Send phishing emails or use pre-texting.
- Use the company's website, phone directory.

#2 Build trust

- **Be nice**. Be courteous but don't be creepy.
- Reflect their likes and dislikes.
- Identify common interests.
- Infiltrate social groups (for example, become a facebook friend of a friend or join a group or attend meetups).

- **Believability**. Important if impersonating others.
- Pose as new employees victim hasn't met.
- Post as vendors.
- Do something nice to create sense of obligation.

#3 Exploit the relationship

- Coax more information out of them.

- Don’t be careless, overly anxious or a bragger.
- Use reverse social engineering…
  - offer to help with a specific problem
  - The problem occurs (thanks to them)
  - save the day
  - ask for a favour

#4 Go in for the kill

- Apply one of the techniques we have seen so far to achieve your goal.

PART 4: COUNTERMEASURES

#1 Policies

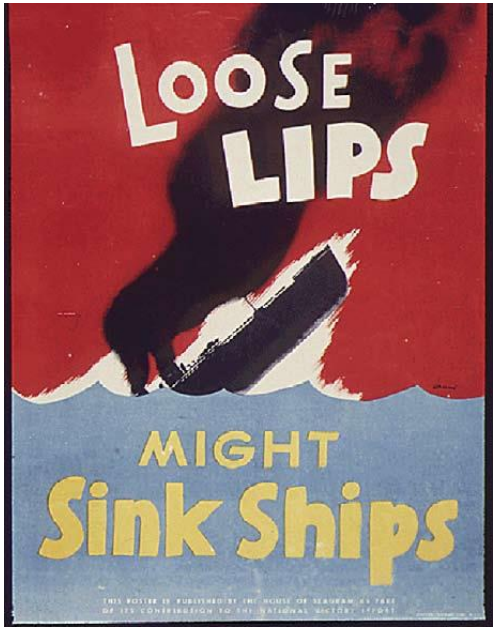
Define organisational policies to minimise risk.

- Classifying information so that users don't have access to certain levels of information they don't need
- Establishing acceptable computer usage that employees agree to in writing
- Removing user IDs for employees, contractors, and consultants who no longer work for the organisation
- Setting and resetting strong passphrases
- **Responding quickly** to security incidents, such as suspicious behaviour and known malware infections
- **Properly handling** proprietary and confidential information
- Escorting guests around your building(s)
- ***No fault policy if you are the victim of social engineering.***

#2 User awareness and education

- Get someone external to train you and staff.
  - Sometime external person carries more weight.
  - Run internal phishing attacks to increase awareness.
  - Teach general rules that aim to keep people safe.
  - Use non-technical language.

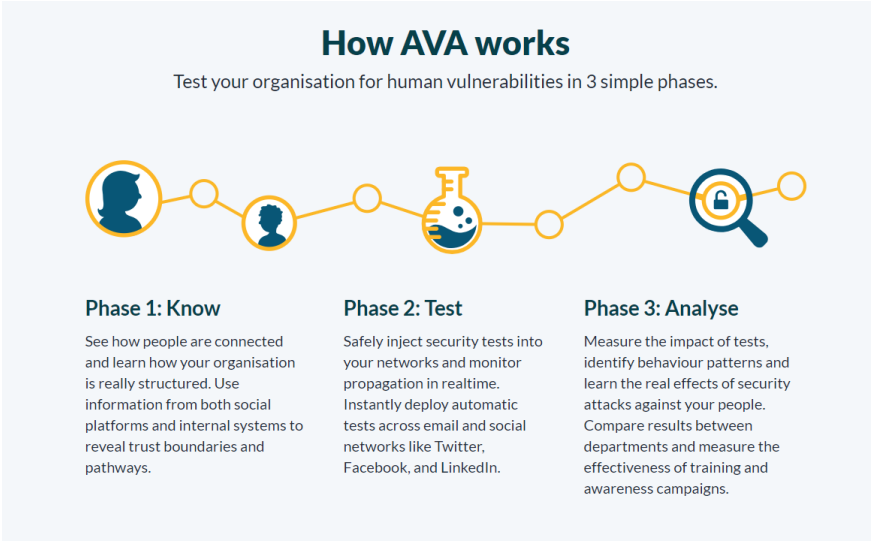
- Example rules.
  - Never give information to someone unless you can validate who they are and they need it.
  - Validate shortened links (bit.ly, go.gl) before clicking.
  - Escort all guests within the building.



UK use education during WW2

Note: Phishing campaigns

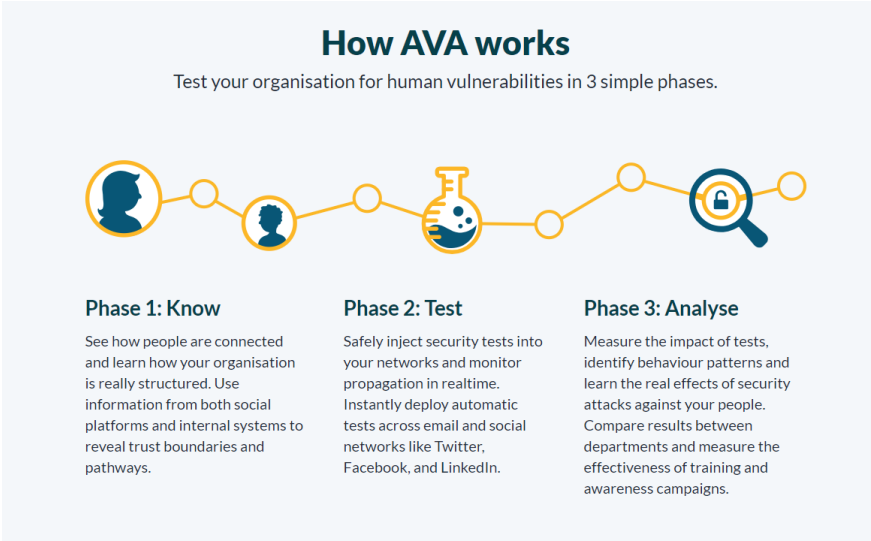
- Phish your own staff.
- Hire someone to do it or use software.
- Laura Bell from Safestack in NZ developed AVA (advanced vulnerability scanner).



Note: Phishing campaigns

Be careful though ...

- Consider how you will debrief staff who fell for it.
- Consider what happens if secrets are revealed.
- Don’t just run it and hope for the best.



WHAT WE COVERED

Content

- **TODAY**
- What is social engineering.
- What are common social engineering threats.
- How do you do it? (methods).
- Countermeasures.

- **NEXT SESSION**
- Social engineering: The *whys*