SOCIAL ENGINEERING

Timothy Mah 8750634

txamah001@mymail.sim.edu.sg

CSIT302 Cybersecurity Assignment Q2

Definitions

Cybersecurity: The practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification or destruction.

Hacking: A colloquial term that typically refers to unauthorised access to data within digital systems. In Singapore, it is defined under the Computer Misuse Act

Network: A group of interconnected digital devices and systems that communicate and exchange data. ie. office shared folder, home wifi

Definitions

Access Control: A system that gatekeeps a user or device from accessing a resource. Can be physical or digital. Typically based on identity of user or device

Attack: A malicious process or action to commit cyber offences

Phishing: A cyber attack that typically involves fraudulently impersonating a legitimate source to trick or scam victims

Definitions: Computer Misuse Act (CMA)

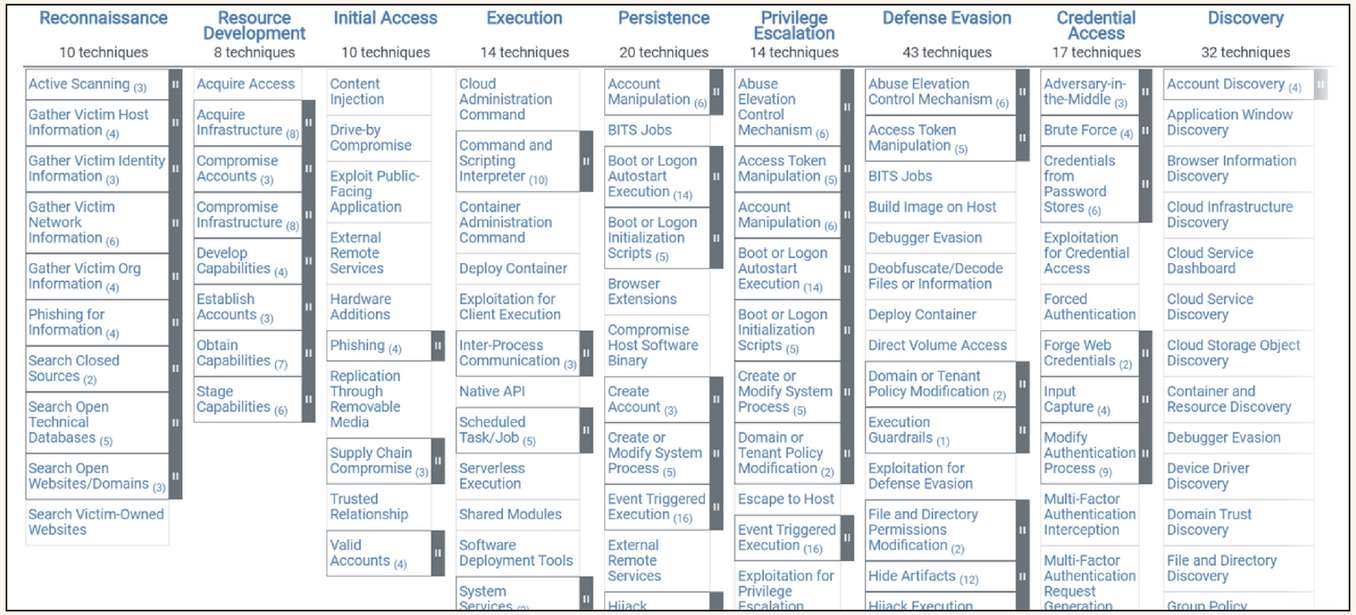
Excerpt of offences outlined in CMA:

1. **Unauthorised Access to Computer Material (Section 3)**
    - ie. using boss computer without permission
2. **Unauthorised Modification of Computer Material (Section 5)**
    - ie. installing malware on boss computer
3. **Unauthorized Obstruction of Use of Computer (Section 7)**
    - ie. maliciously download files on office wifi so that boss network connection slows down
4. **Unauthorized Disclosure of Access Code (Section 8)**
    - ie. giving passwords without permission

[More sections]

Introduction

- Social engineering is the most powerful hacking technique
- It does not require as much technical knowledge yet has the highest gains
- highest ROI (returns on investment)
- commonly used in conjunction with other attack techniques as part of a larger attack process
- used in early stages of popular cybersecurity attack standard (how an attacker typically performs a cyber attack operation)[MITRE ATT&CK Matrix]



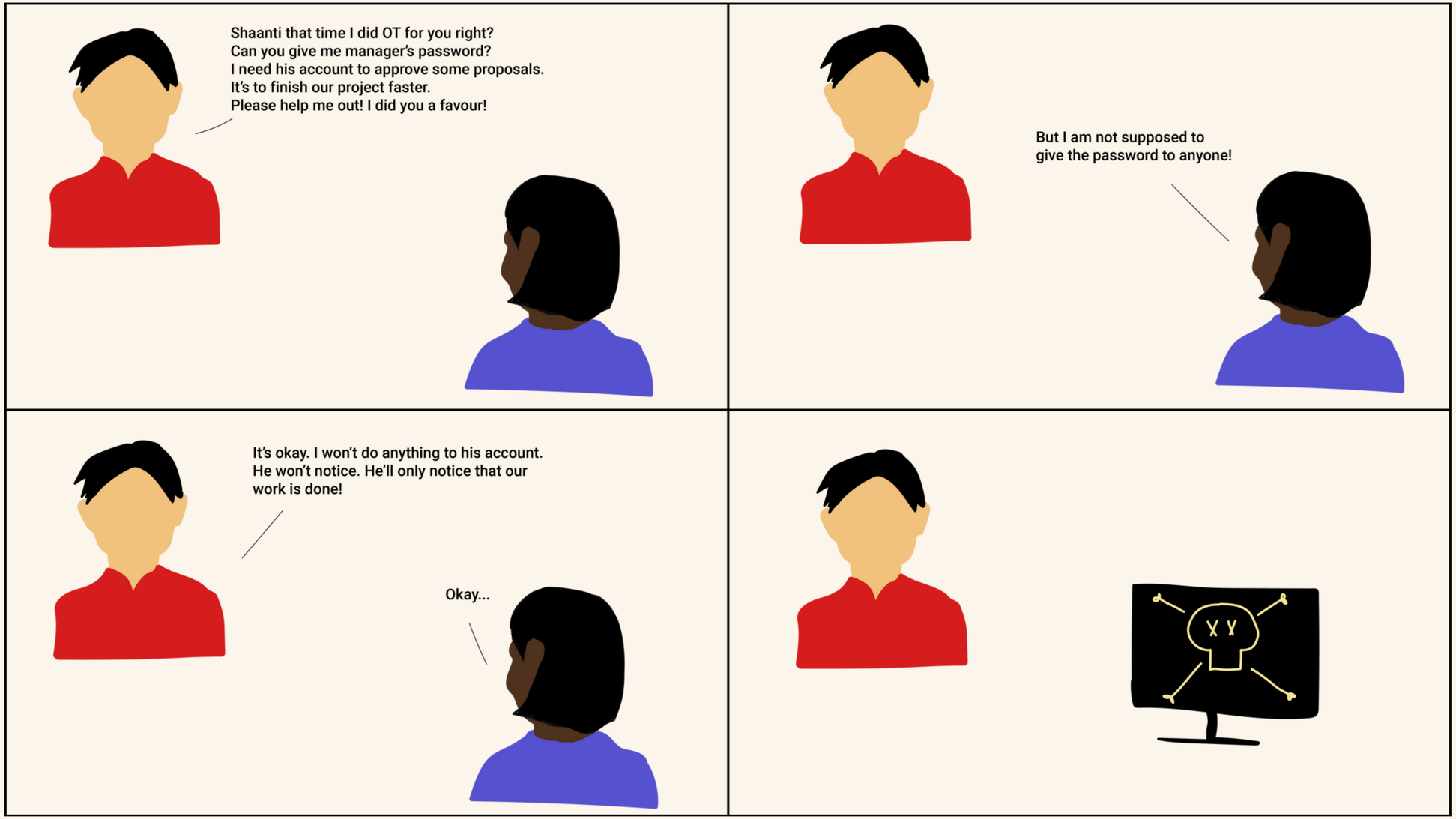
What is Social Engineering?

- Instead of exploiting a computer or a system, attacker exploits people
- Six levers of social engineering
  - reciprocation
  - scarcity
  - consistency
  - liking
  - authority
  - validation

- these are the ways an attacker can perform social engineering
- insider threats often use social engineering as they have an existing level of trust within an organisation

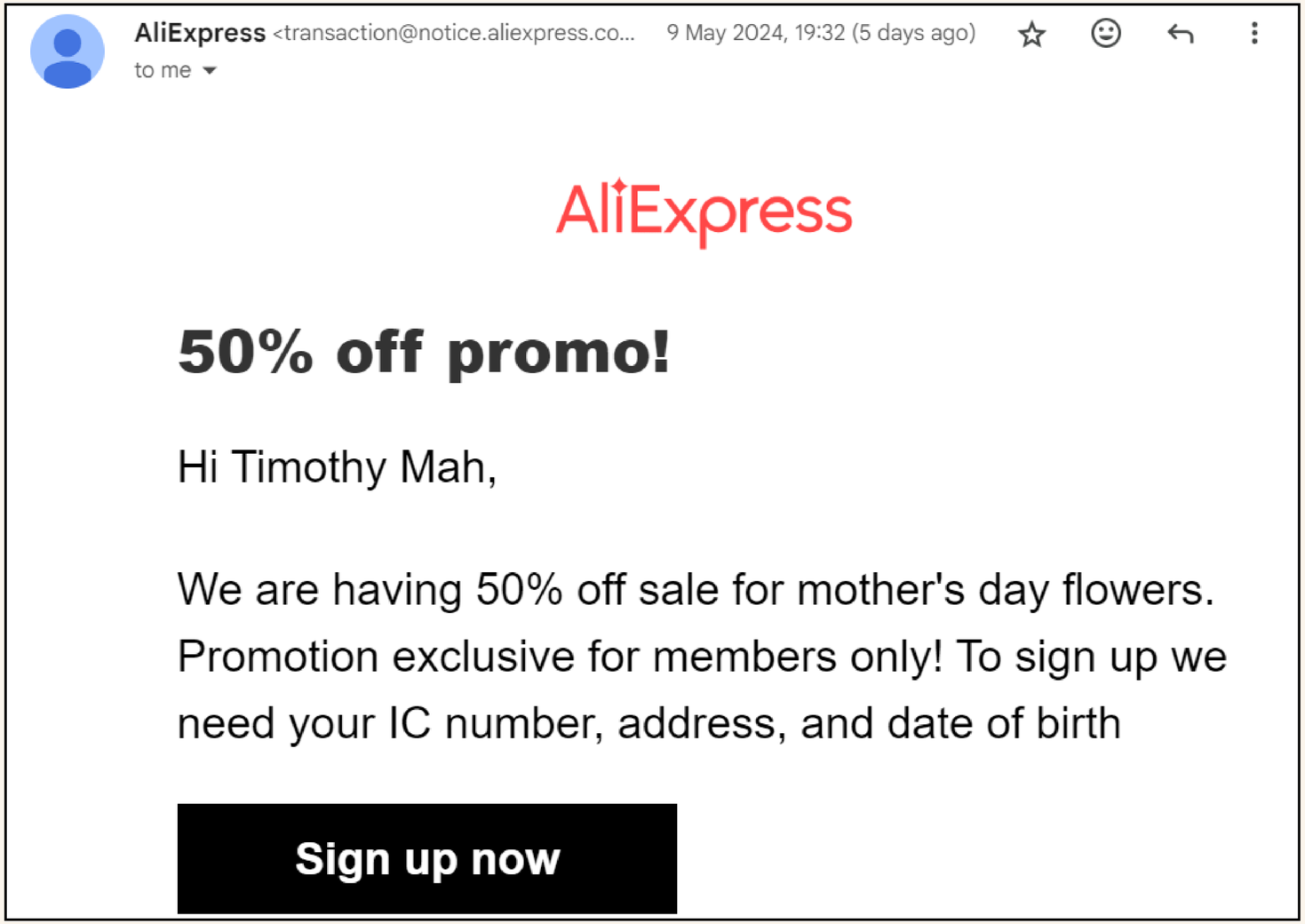
What is Social Engineering? 6 levers - <u>reciprocation</u>

- Attacker finds a way to make victim obligated to give sensitive information



What is Social Engineering? 6 levers - scarcity

- attacker convinces victim lacks something and needs it

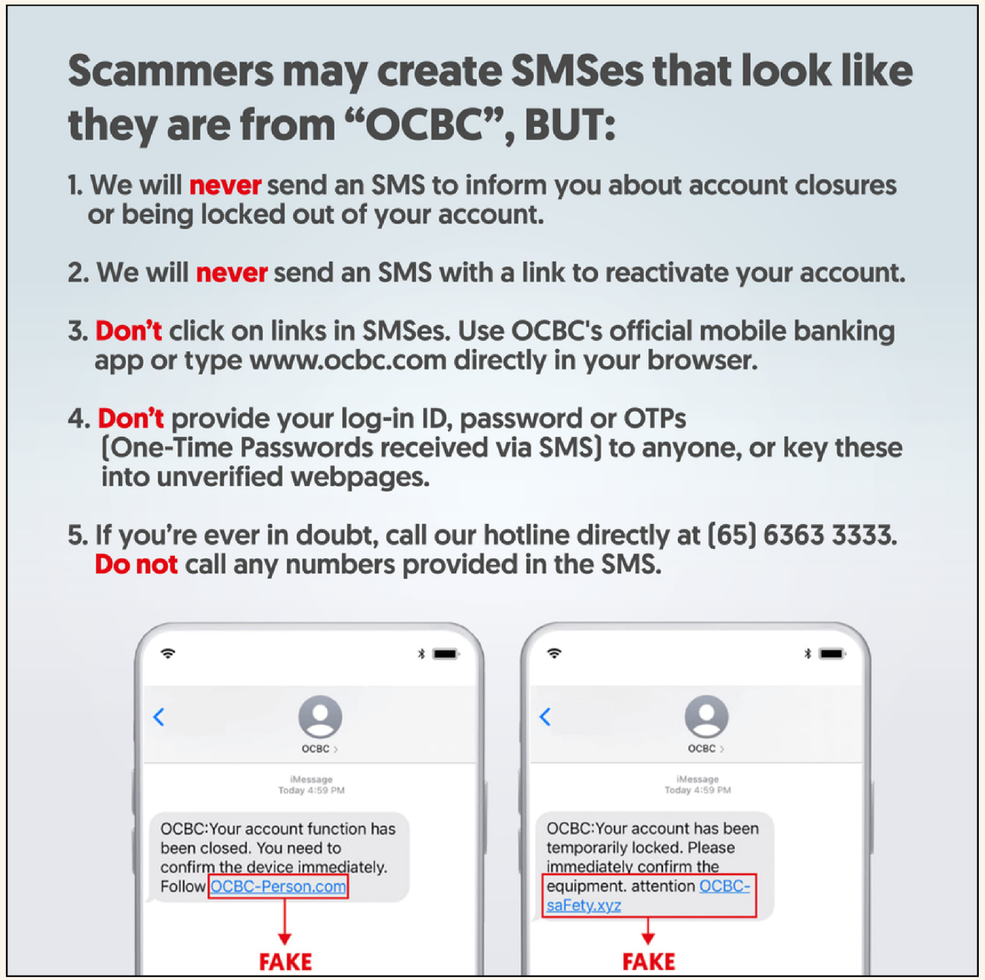


What is Social Engineering? 6 levers - liking

- attacker catches the appeal and attraction of victim to reveal sensitive information

What is Social Engineering? 6 levers - authority

- attacker impersonates legitmate authority typically from government bodies. Highly successful on non tech-savvy conservative victims



What is Social Engineering? 6 levers - validation

- victims tend to comply with behaviour that other groups are performing

How is Social Engineering performed?

- previous slides have displayed the multiple mediums of social engineering
  - SMS
  - email
  - watering-hole (fake website)
  - baiting
  - tailgaiting
- all rely on impersonation, spoofing, and exploiting lack of verification
- greater success on systems with poor physical security
  - USB port protection
  - physical access controls such as keycards to restricted zones
  - gates, automatic barriers, gantries
- network and system security equally as important

Who is involved in Social Engineering?

- attackers
  - insider threats
  - external sources impersonating legitimate sources
  - state sponsored attackers
  - hacktivists (activists that perform hacking for their cause)
- victims
  - targeted spear phished victims are usually high profile with high value or well connected
  - staff within a larger organisation
  - low hanging fruits - individuals with poor cyber literacy

When has Social Engineering occured?

- There were around 8,500 phishing attempts reported to the Singapore Cyber Emergency Response Team (SingCERT) in 2022, more than double the 3,100 cases handled in 2021 [source]
- OCBC SMS scams in 2022. Attackkers exploited a vulnerability within SMS protocol and spoofed legitimate messages from OCBC. [source]
- Before Windows 7, Windows “Autoruns” allowed programs and scripts to be run from a plugged in USB drive. Attackers could run their malware very easily on any computer. Subsequent Windows versions all have much stricter policies on Autorun
- Attackers could have performed social engineering to bypass physical security and exploit Autoruns

Why does Social Engineering occur?

- Social Engineering based attacks, and cybersecurity attacks in general, occur because of push and pull factors
  - push
    - hacktivism
    - financial gain
    - state sponsored
    - vandalism
    - personal gain
  - pull
    - poor physical security
    - poor network security
    - improper training of individuals and staff

Where does Social Engineering occur?

- Social Engineering could come from geologically remote locations. Scam calls and phishing emails are the most prominent
- Social Engineering could also come interally within an organisation, typically from disgruntled staff, or even state sponsored spies
- Social Engineering could stem from anywhere thus security frameworks such as Zero Trust have been developed to mitigate lack of verification

DAMAGE

monetary loss from stolen bank credentials, business downtime, system repair, cost of cybersecurity services, extortion, fraud

breach of privacy from stolen personal information, organisational secrets

defamation from cyber incident itself, from sensitive information being leaked

Prevention

How can individuals or organisations defend against Social Engineering attacks?

- group and/or individual cybersecurity training
- improve physical and digital access controls
- improve physical and digital monitoring
- imrpove physical and digital response (incident response plan)
- backup data
- security audits
- review policies and agreements with cloud services (SLA)
- review source (URL, emaill address, mobile number) when receiving messages
- avoid plugging in unauthorised external devices into personal device or office computer

Conclusion

Social Engineering attacks are real and effective. There are still reports of cybersecurity incidents based on Social Engineering

Social Engineering is typically part of a larger attack process thus other cyber defences are required on top of Social Engineering mitigation

Quiz!

Qn1: What is phishing?

a) email from hr-dept@xyz.com congratulating you for job promotion with bitcoin incentive

b) stranger enter office and leaves USB drive on desk

Qn1: What is phishing? - Answers

a) email from hr-dept@xyz.com congratulating you for job promotion with bitcoin incentive

~~b) stranger enter office and leaves USB drive on desk~~

Qn2: Which is a lever of Social Engineering?

a) reciprocation

b) brute-force

Qn2: Which is a lever of Social Engineering? - Answers

a) reciprocation

~~b) brute-force~~

Thank you!