Social Engineering

Attack Tactics and Preventive Measures

Group 11

Aisha Guiamadin 201511655

Hala Amin 201508473

Alanoud Alyafei 201300537

Outline

- What is social engineering?
- Social engineering attack phases
- Types of social engineering attacks
- Social engineering taxonomy
- How to prevent social engineering attacks?
- Conclusion

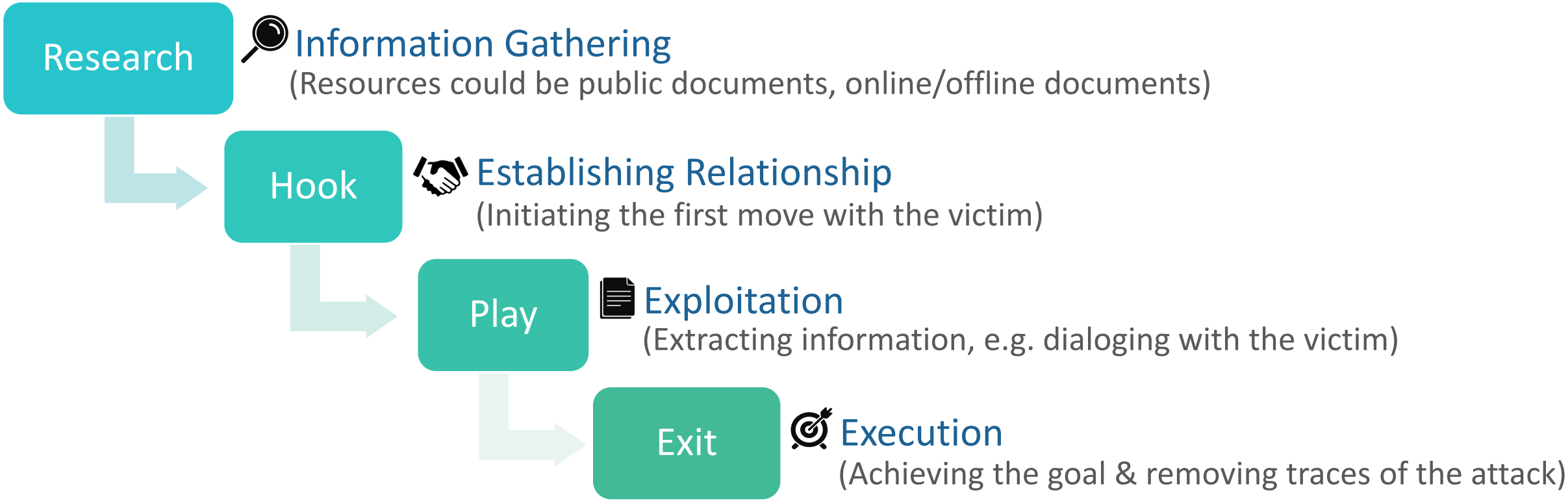
What is social engineering?

- Manipulating human nature weakness in **psychological aspect** rather than technology to gain unauthorized access to confidential and sensitive information.

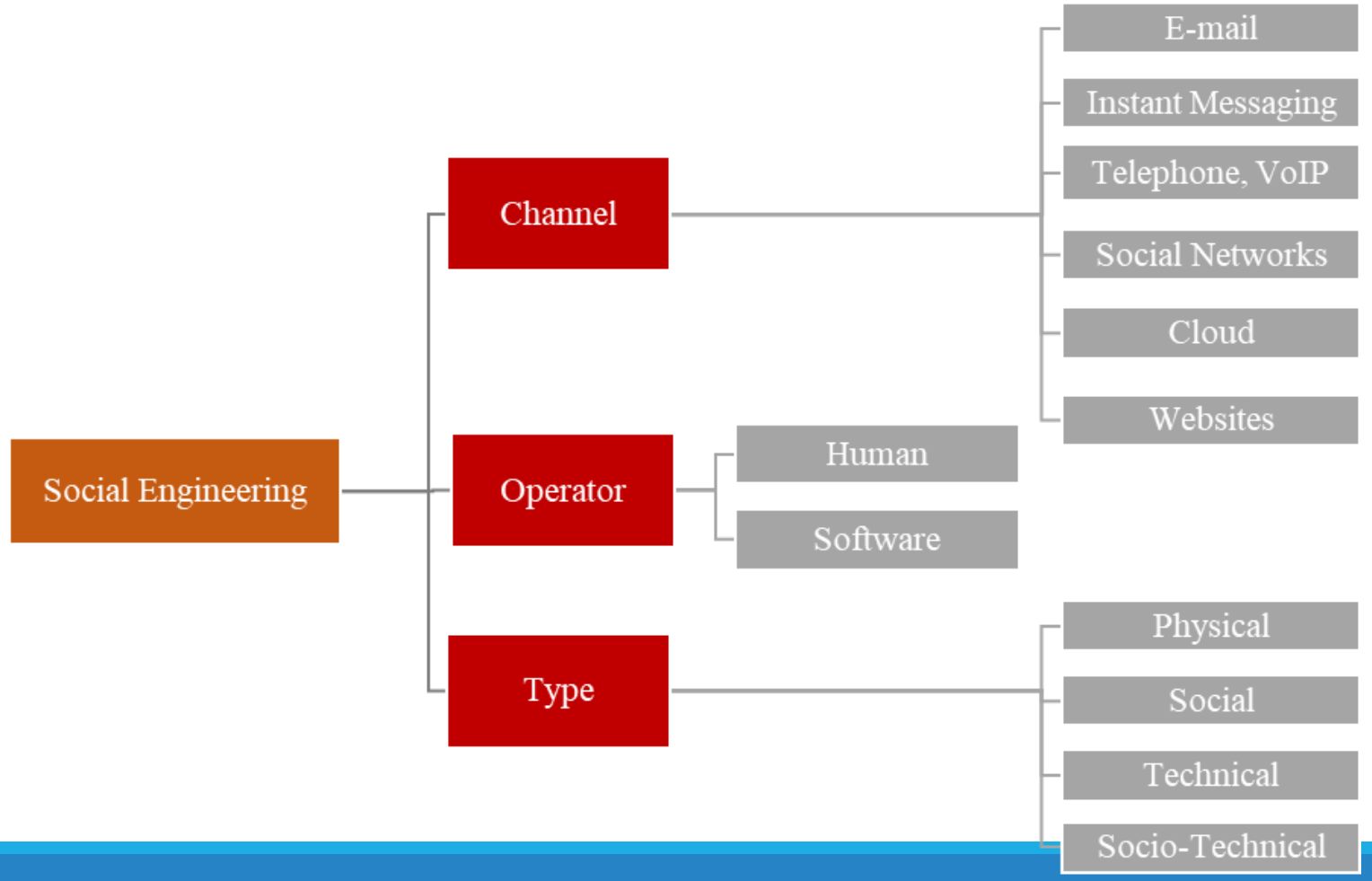
What makes its attacks **effective**?

- It targets the weakest security link: the human!

Social Engineering Attack **Phases**



Social Engineering **Taxonomy**



Phishing

- It is when the adversary disguises as a trustworthy entity
- Done through an electronic communication medium such as e-mails, web-sites, social networks, or cloud services
- Usually targets a large group of people

(If the attack targets specific individuals then it is called **spear-phishing**)

From: "Microsoft Outlook (Account Locked)" <chard@collegesontario.org>
Date: March 29, 2017 at 11:34:48 AM EDT
To: [redacted]
Subject: Final Notice : (One Step Validation Process 03-29-2017)

Outlook

Dear User,

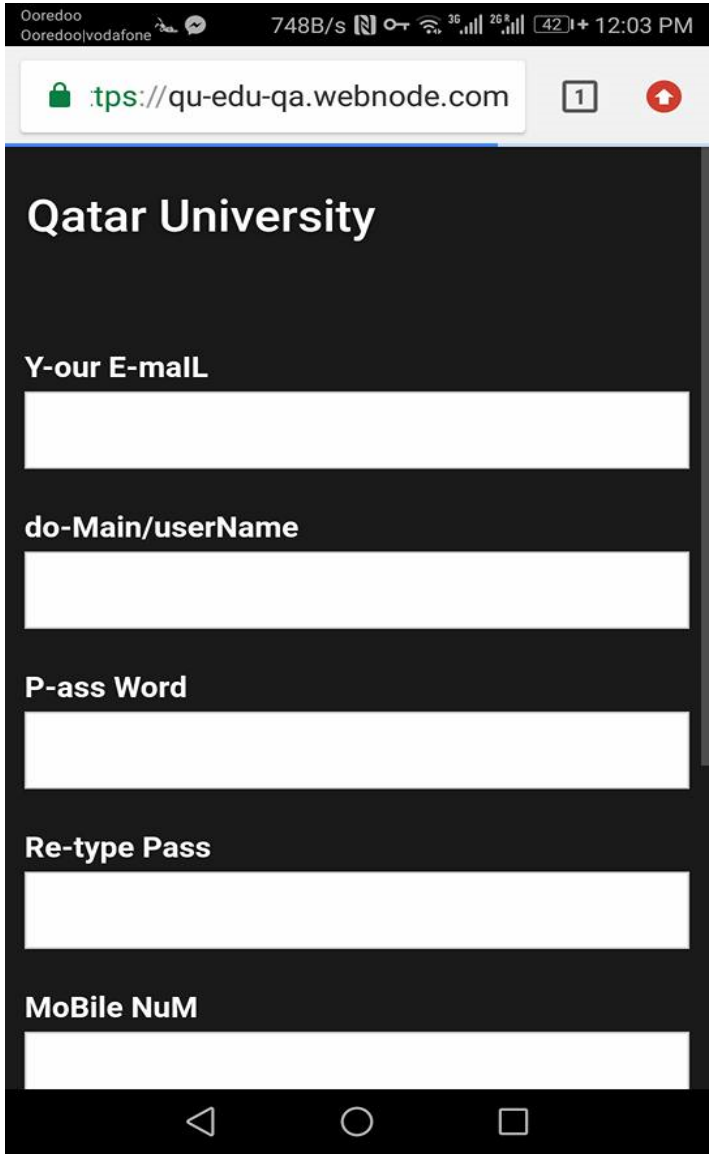
Your Microsoft Outlook Account Requires an Urgent Validation to ensure it would not be deactivated within 24 hours

Proceed to Microsoft Outlook Validation page by clicking on the icon below.

Get Started

Thank you for using Microsoft Outlook.

To stop separating items that are identified as clutter, go to options. To stop receiving notifications about clutter, go to Options and turn them off, This System notification isn't an email message and you cant reply to it.



Dumpster Diving

- Some targeted individuals/companies do not discard their sensitive information completely. This is where dumpster diving takes place
- It is when the attacker searches through the trash of on organization or a company to find confidential information
- The gained information could be used to gain access to a system of the company or an individual's account

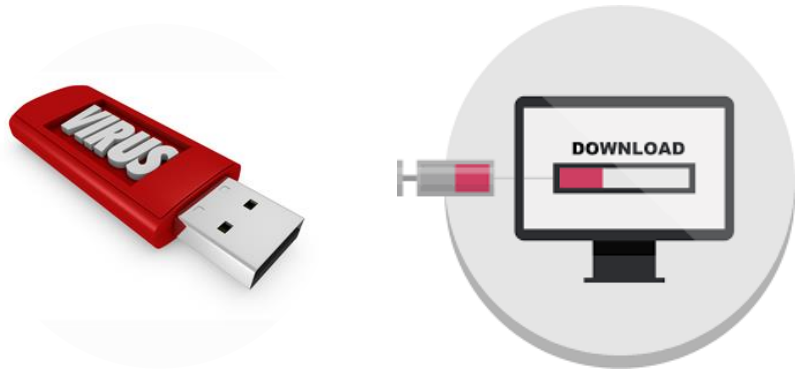
Baiting

- Baiting can take place in websites and online adverts

→ Attacker makes the website user download malware file / click a pop-up with a fake message

- Baiting can also use physical media and exploit human curiosity

→ Attacker leaves an infected USB flash drive in an obvious location and can be easily found by the victim. Or can be presented as gifts to employees

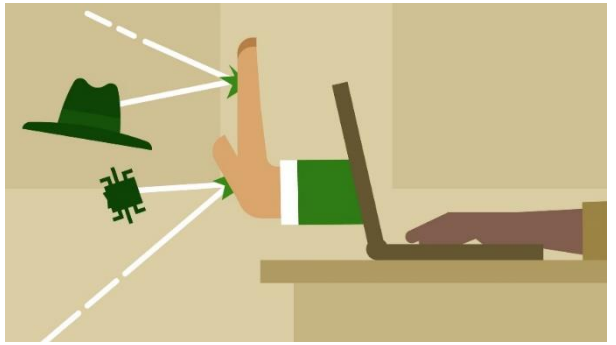


How to **prevent** social engineering attacks?

- **Educate yourself** about social engineering and its attacks
- Create a **strong password** and **different** ones for your accounts
- **Do not share too much** to reduce the chance of exposure to attack
- Some organizations call you for legitimate reasons to perceive some information (e.g. credit card company, mobile service provider,…). Try to get **caller information** such as caller name and extension number
- Use multifactor authentication to protect your credentials

→ **Two-factor authentication (2FA)** is widely used and many applications are made for such purposes

- **Keep your software up-to-date** and use antivirus/antimalware software to scan for any possible infections in your system



Summary

- Social engineering attacks strongly exploit the human nature to gain confidential information

→ Having a background on social engineering attack vectors and classifying them based on the taxonomy is important to understand where and when each attack could happen

→ Using multifactor authentication such as 2FA is a powerful way to protect the user's credentials

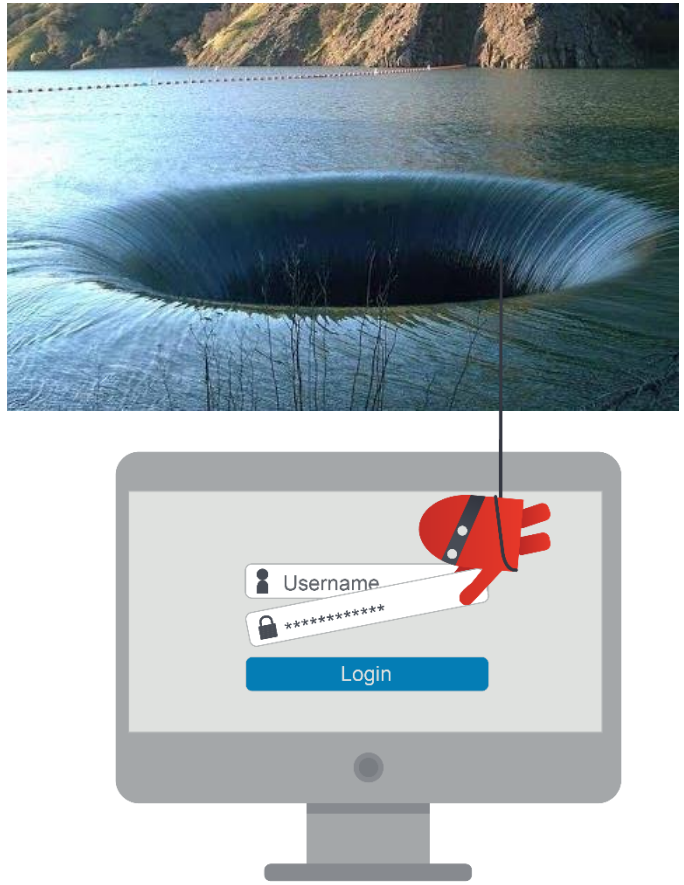
- Organizations need to have awareness sessions for the employees about social engineering attacks and run random test attacks at least once a month

Demo
using SEToolkit

Water-holing

- The practice of compromising a website that the victim is interested to and will likely enter that website
- In other words, the attacker sets up a fake website (waterhole) and waits for his victim at the waterhole
- Focuses on legitimate popular websites
- Technical knowledge might be needed for the attack to be successful

→ e.g. the attacker searches for the vulnerabilities in the website and injects malicious code in JavaScript/HTML which redirects the victim to a separate site that hosts the malware



Reverse Social Engineering

- The attacker establishes a position of authority and have his victim come to him
- To do that, the attacker will simply initiate a situation that makes the victim needs help
- Once the attacker does that, the attacker will start to show himself up as someone the victim can accept his offer and consider him the one who will resolve his problem

→ Attacker might damage the target's equipment e.g. laptop. Then he disguises himself as a trustworthy entity to be the one who solves the problem

Classification table of the 5 attack vectors according to the Taxonomy

		Phishing	Dumpster Diving	Baiting	Water-holing	Reverse Social Engineering
Channel	E-mail	✔				✔
	Instant Messaging	✔				✔
	Telephone, VoIP	✔				✔
	Social Network	✔				✔
	Cloud	✔				
	Website	✔			✔	
Operator	Human	✔	✔	✔		✔
	Software	✔			✔	✔
Type	Physical		✔	✔		
	Social					✔
	Technical				✔	
	Socio-Technical	✔		✔	✔	✔

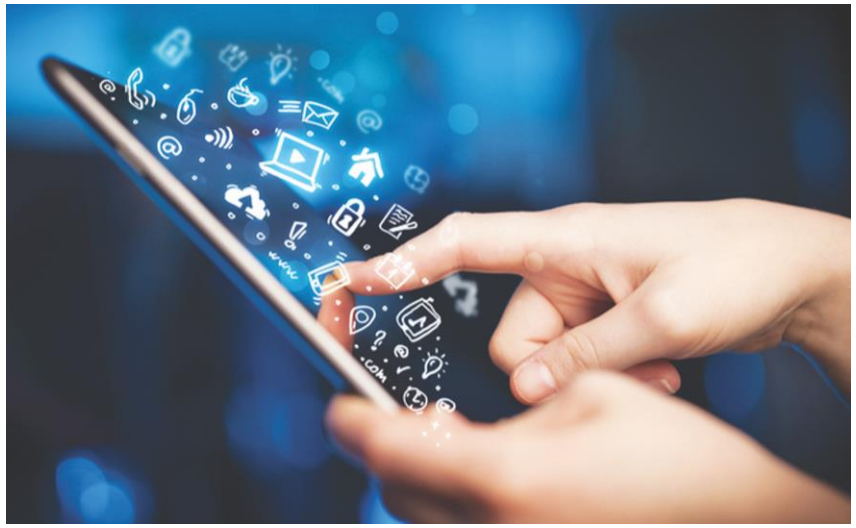
Online Social Networks (OSNs)

OSNs enable automated social engineering (ASE) attacks, because information harvested from OSNs is easy to process. E.g. collecting employee's information of a targeted company.

OSNs could be misused for:

Social phishing: luring victims into entering sensitive information into a faked website that is controlled by the attacker. Where social information specific to the victim is used.

Fake profiles could be used to infiltrate into social networks. Since a huge number of OSNs users accept fake friendship requests. For example “socialbot” to generate fake profiles and send requests.



Mobile Applications

- vulnerabilities can be exploited to hijack user accounts or leak sensitive information.
- Two **scenarios** of attack serve as a starting point for mobile applications attacks:
  1. Some smartphone applications request permissions to access sensitive data on the user's device.

     → If an attacker were to create such an application, he would obtain the information about the users.
  2. Sender ID spoofing can be done on popular mobile messaging applications such as “WhatsApp”.

     → A social engineer can use this to send a message to a victim while pretending to be one of his friends.