Topic 2

Understanding Cyber Threats

Slides developed by

What you will learn in these slides...

- Common cyber threats
- Importance of phishing awareness
- Mitigating cyber threats

Recap on Topic 1

- A **threat** is any potential danger, hazard or malicious actor that seeks to exploit vulnerabilities and cause harm to assets
  - In this topic, we will learn various examples of these kinds of threats in the cybersecurity landscape!

Common cyber threats

- Malware
- Phishing
- SQL Injection / Cross-site Scripting
- DoS / DDoS Attack
- Insider Threats
- Zero-day Exploit

Malware

- Short for ‘Malicious Software’
- Intrusive software with intent to disrupt, damage, steal or gain unauthorized data to a computer system
- Each type of malware has unique characteristics

Common types of Malware

- Ransomware
- Virus
- Worm
- Trojan
- Adware
- Spyware
- Rootkit

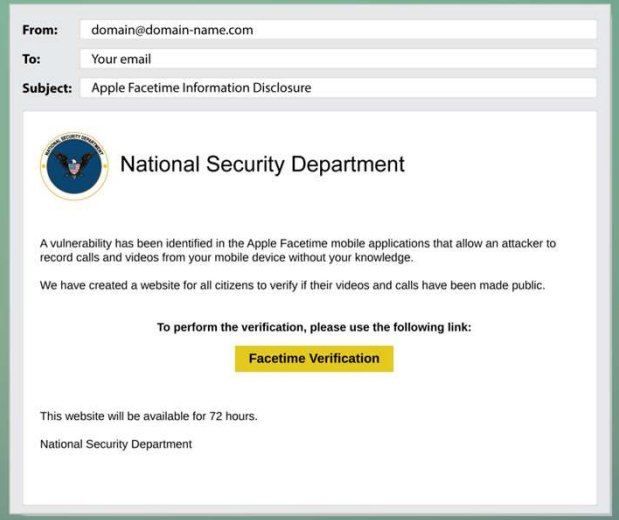
We will go more in-depth on these malware types in Topic 4!

Phishing

- A form of social engineering
  - Convincing someone to reveal sensitive/personal information by talking to them
- Attackers impersonate legitimate entities (CEO/Boss etc.) to deceive users into revealing confidential data by clicking malicious links
- May come in the form of:
  - Emails, Websites, Text messages etc.
- Common types of phishing include:
  - Smishing, Vishing, Deepfake

Email Phishing

- A common form of phishing where attackers send fraudulent emails to victims
- They appear to come from reputable sources (bank, government agency, ISP etc.)
- Often include messages like ‘Your password has expired.’ or ‘Your account has been compromised.’ with a link or button



From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

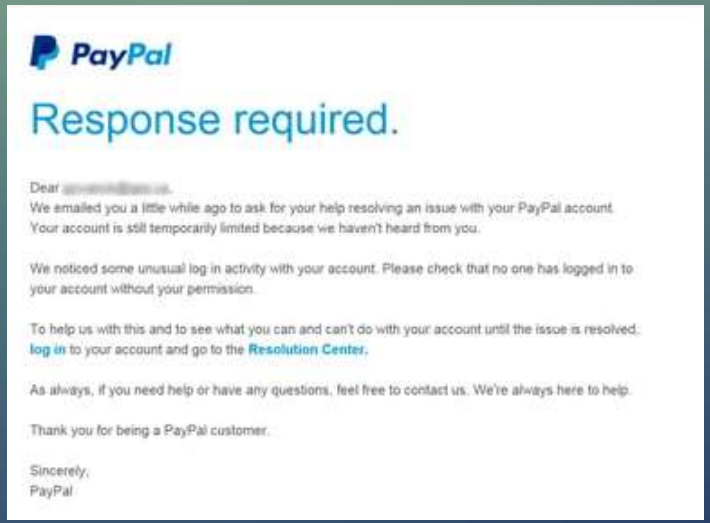
We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department



PayPal

Response required.

Dear [redacted]

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

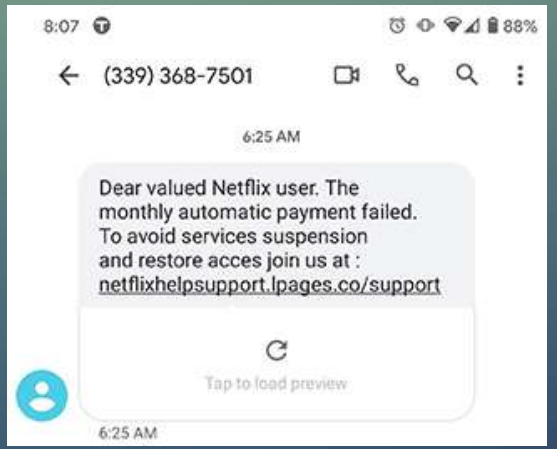
As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Smishing (SMS Phishing)

- Phishing done via SMS text messages
- Usually sent from unknown phone numbers
- Often include messages like ‘Your parcel could not be delivered.’ or ‘Win a prize by doing a survey!’ with a link

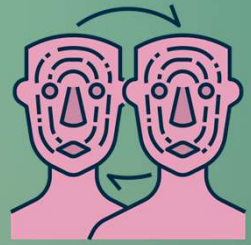


Vishing (Voice Phishing)

- Phishing done via phone calls or audio tapes
- Attackers often impersonate reputable sources (tech support, boss, big organizations)
- Is getting more dangerous due to AI which can alter voices to match a familiar voice

YouTube Link: https://www.youtube.com/watch?v=Hc01oZPvByg

Deepfake



- Synthetic media where a person's likeness (voice, face, or body) is replaced with someone else's using artificial intelligence (AI)
- Uses machine learning (ML) techniques to create highly realistic digital forgeries
- Though not exactly considered phishing, deepfakes can be used in phishing attacks
  - For example, a deepfake can simulate a CEO in their office telling an employee to transfer money to a fraudulent account

An example of a deepfake on famous actor Tom Cruise

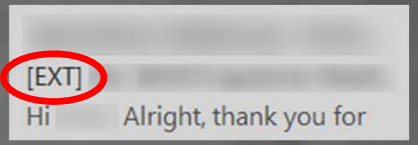
YouTube Link: https://www.youtube.com/watch?v=iyiOVUbsPcM

Wait!!!

Before discussing the next cyber threat…

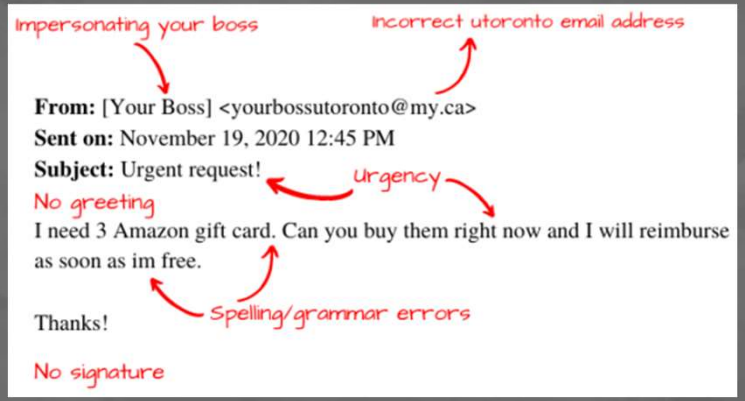
It is **important** to inculcate phishing awareness!

Look out for these common signs that may indicate phishing attempts:



Suspicious and/or external email addresses

- Email address that are misspelled (e.g., google.com VS goog1e.com / googlle.com)
- An [EXT] or [EXTERNAL] tag can identify an email from an outside source
  - Do note: NOT all external emails are phishing emails, some can be from a client/contractor outside the organization



Typos and grammatical errors in email

- Some emails are poorly phrased with various errors that differ from legitimate emails

Words that indicate urgency

- Such emails/messages indicate ‘urgent’ phrases such as ‘Immediate Action Required’ or ‘Must do ASAP’

Hover over email links

- Some links may look real, but hovering over them may reveal it redirects to another website

SQL Injection (SQLi)

- SQL (Structured Query Language) is a language for creating and/or accessing databases via specific queries
- SQL Injection uses malicious queries to access hidden data in databases

Cross-site Scripting (XSS)

- Malicious scripts are injected into search bars
- Altered links may redirect victims to malicious websites
  - Users may click a link displaying facebook.com but it redirects to another page
- Links in phishing emails can be considered XSS

SQL Injection VS Cross-site Scripting

SQL Injection (SQLi)	Cross-site Scripting (XSS)
• Is a **server-side** vulnerability • Targets the backend (database) • Alters data in the database by adding, modifying or deleting data • Extracts hidden and confidential data that is not known publicly	• Is a **client-side** vulnerability • Targets the security of users and the frontend (web pages) • Exploits vulnerabilities in the website such as lack of proper input sanitization

Denial of Service (DoS)

- Disrupts the availability of a website or server by flooding malicious requests or queries
- Legitimate requests and queries are unable to be processed and the website/server often hangs or crashes

Distributed Denial of Service (DDoS)

- Involves multiple compromised devices sending requests to a website (as compared to one device for DoS)
- Harder to mitigate due to the large number of devices

Insider Threat

- Posed by individuals within an organization
- Often involves disgruntled employees misusing access privileges
  - Unhappy with their job/boss
- Can also involve partners or third-parties such as contractors
  - Anybody with access to an organization’s resources can became an insider threat

Zero-day Exploit

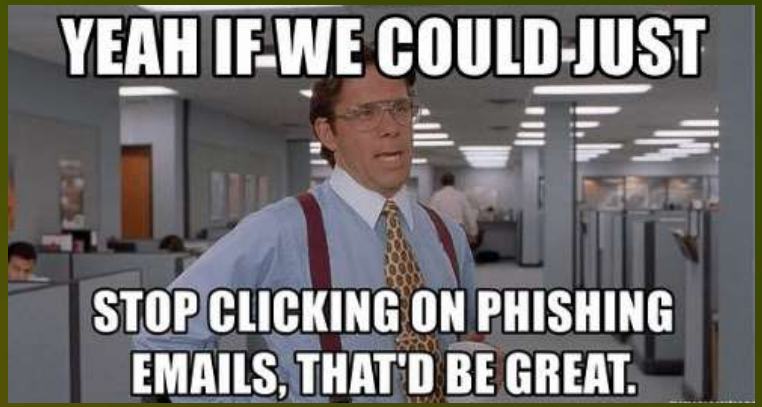
- Exploits vulnerabilities that are not known or discovered yet
- These vulnerabilities are exploited before software developers or vendors can patch them
- ‘Zero-day’ refers to how the vulnerability has 0 days to be fixed as attackers have already exploited it

Mitigations for each threat

SQL Injection	• Implement proper input validation and sanitization before processing • Use parameterized queries • Implement proper error handling to avoid database errors being revealed (to prevent attackers from gaining insights to the database structure)
Cross-site Scripting	• Implement proper input validation and sanitization before processing • Encode data before outputting (use context-specific encoding such as HTML or JavaScript) • Use a Content Security Policy (CSP)
Denial of Service	• Implement rate limiting to set the maximum number of requests your webpage can handle at a time • Use a Web Application Firewall (WAF) to monitor traffic (covered in Topic 7)
Insider Threat	• Use the principle of Least Privilege • Monitor and log user activities • Conduct security awareness training for employees
Zero-day Exploit	• Update software regularly by implementing patch management policies and processes • Whitelist trusted applications • Implement behavioural analysis tools (this is to identify vulnerabilities based on behaviour rather than known signatures)

Topic 2 Summary

- Common cyber threats
- Phishing awareness
- Mitigating cyber threats



In the next topic...

Password Security and Authentication

- Best practices for creating strong passwords
- Multi/Two-factor Authentication