

Introduction to Key Cybersecurity Concepts

Course Incharge: **Yahya Batla**

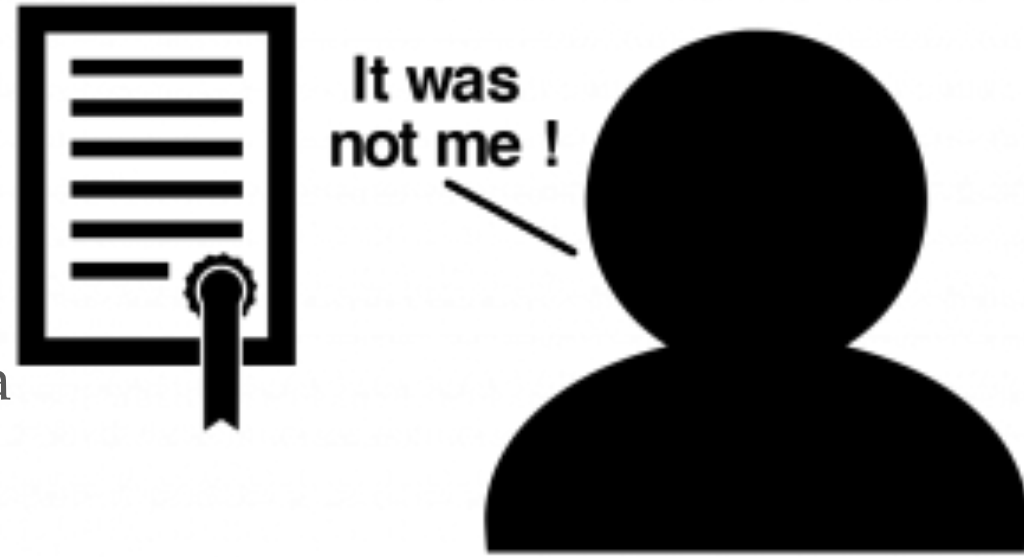


Course Instructor: **Instructor_Name**

Non-Repudiation

Non-repudiation is a concept in information security that means a party cannot deny the authenticity or origin of a message or action.

In simpler terms, it ensures that someone who sends a message or performs a transaction cannot later claim they didn't do it. Non-repudiation is often used in electronic communication and digital transactions to provide proof of the sender's identity and the integrity of the message or transaction, preventing individuals from disowning their actions.



Vulnerability, Threat, Asset, & Risk

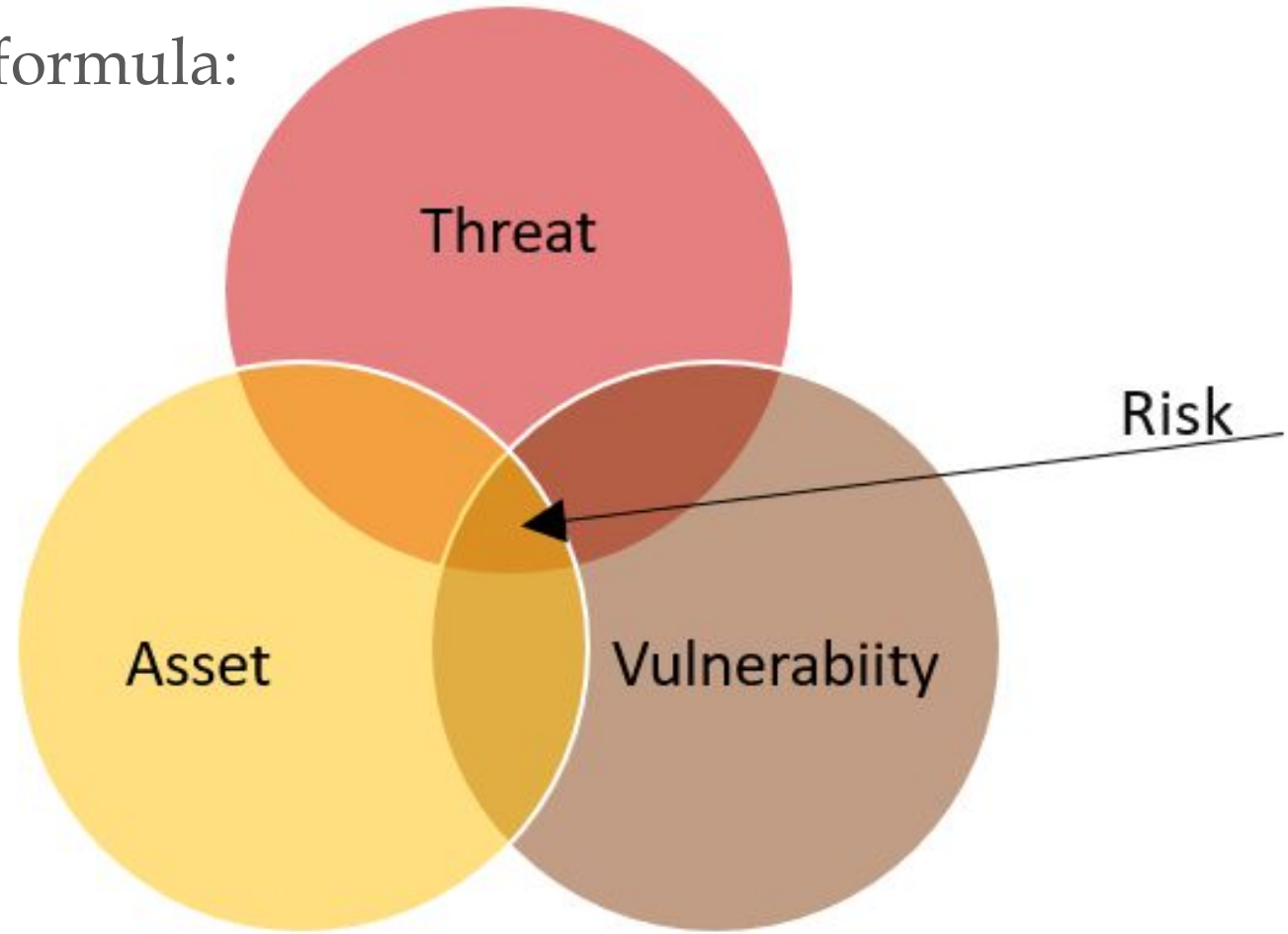
1. A **vulnerability** is a flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by a threat.
2. A **threat** is a potential for a threat agent to exploit a vulnerability.
3. An **asset** is something that needs to be protected
4. A **risk** is the potential for loss when the threat happens.

Vulnerability, Threat, Asset, & Risk

The relationship can be visualized in a formula:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset}$$

1. Threats exploit vulnerabilities.
2. Vulnerabilities expose assets to threats.
3. Assets have value, and protecting them is the goal.
4. The combination of threats, vulnerabilities, and assets determines the level of risk.





Threat

In cybersecurity, a threat is any potential danger or adverse action that could exploit a vulnerability in your systems, data, people, or other assets, and potentially affect the confidentiality, integrity, or availability of those assets.



Vulnerability

A vulnerability is a weakness, flaw, or shortcoming in a system, infrastructure, database, software, process, or set of controls that can be exploited by a threat actor.



Risk

Risk is the likelihood and potential impact of a negative event occurring. The risk faced by an organization can change over time due to internal and external factors. Cyber risk is the probability of loss in terms of both frequency and magnitude.

THREAT VERSUS VULNERABILITY



Threat is a person or thing likely to cause damage or danger

Danger posed by someone else

Can be identified, but cannot be controlled

Vulnerability refers to being open to attack or damage

Flaw or weakness in us

Can be identified and corrected

Pediaa.com



Types of Attacks

1. Malware
2. Denial-of-Service (DoS) Attacks
3. Phishing
4. Spoofing
5. Code Injection Attacks
6. Supply Chain Attacks
7. Insider Threats
8. IoT-Based Attacks

Types of Attacks

Malware — or malicious software — is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, cryptojacking, and any other type of malware attack that leverages software in a malicious way.

A **Denial-of-Service (DoS)** attack is a malicious, targeted attack that floods a network with false requests in order to disrupt business operations. In a DoS attack, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

Types of Attacks

Phishing is a type of cyber attack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.

Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.

A **supply chain attack** is a type of cyber attack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Software supply chain attacks inject malicious code into an application in order to infect all users of an app. Software supply chains are particularly vulnerable because modern software is not written from scratch: rather, it involves many off-the-shelf components, such as third-party APIs, open source code and proprietary code from software vendors.

Types of Attacks

Code injection attacks consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action. There are different types of such attacks including SQL injection. A SQL Injection attack leverages system vulnerabilities to inject malicious SQL statements into a data-driven application, which then allows the hacker to extract information from a database. Hackers use SQL Injection techniques to alter, steal or erase application's database data.

IoT (Internet of Things) based cyber attacks refer to malicious activities that target devices connected to the Internet of Things. IoT devices are everyday objects embedded with sensors, software, and other technologies to collect and exchange data over the internet. These devices can include smart thermostats, security cameras, fitness trackers, home appliances, industrial machines, and more.

Practice:

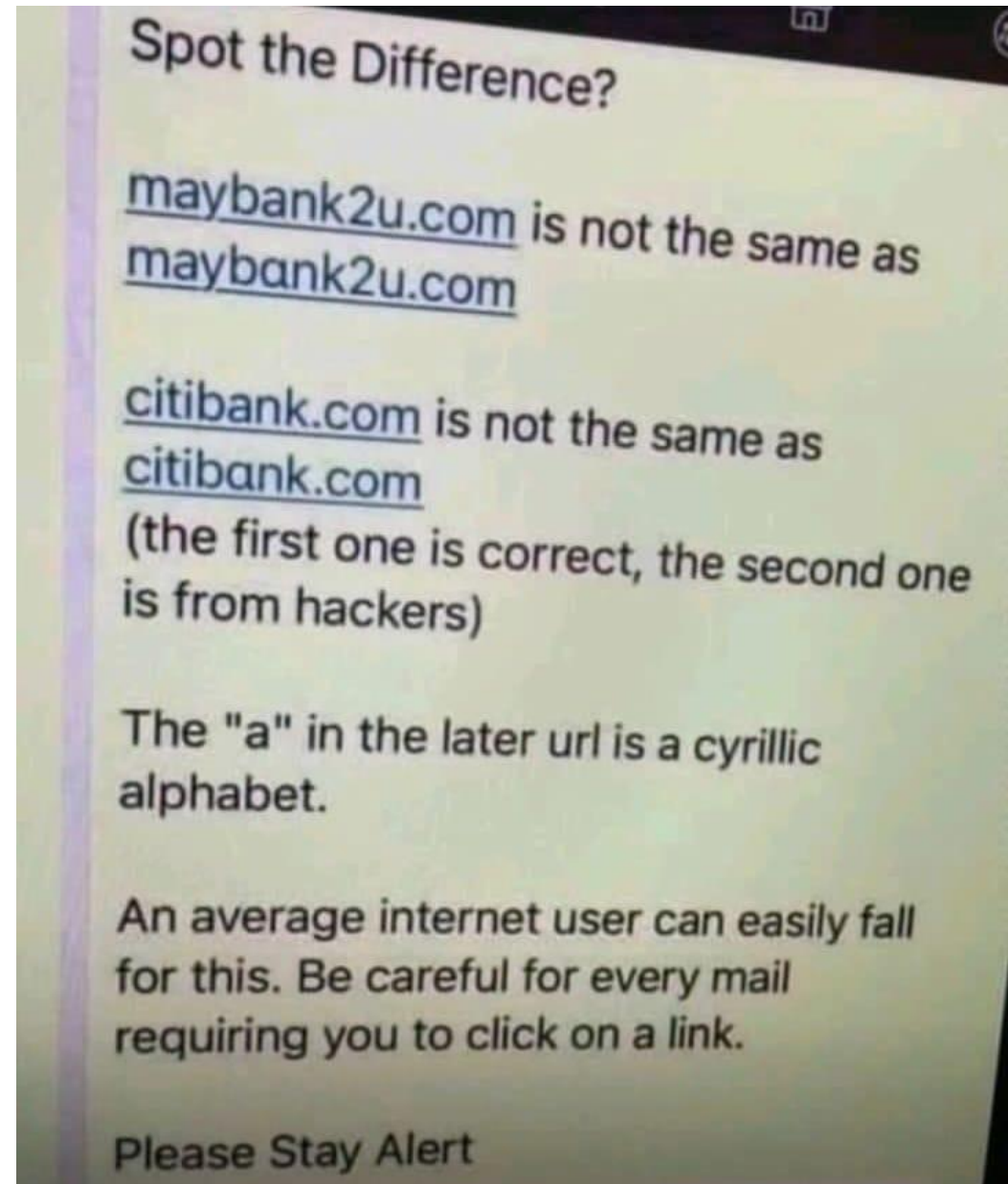
<https://tryhackme.com/room/communicationsattacks>

Students are supposed to complete this entire room.

Social Engineering

Social Engineering attacks manipulate people into sharing information they shouldn't share, downloading software they shouldn't download, visiting websites they shouldn't visit, sending money to criminals, or making other mistakes that compromise their personal or organizational security.

In other words it uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.




Phishing

Phishing attacks are fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal data (e.g., Social Security and credit card numbers, bank account numbers, login credentials), or taking other actions that expose themselves or their organizations to cybercrime.

The attacker typically masquerades as a person or organization the victim trusts e.g., a coworker, a boss, a company the victim or the victim's employer does business with, and creates a sense of urgency that drives the victim to act rashly. Hackers and fraudsters use these tactics because it's easier and less expensive to trick people than it is to hack into a computer or network.

FAKE

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!



Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.


To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.liive.com/ResetPassword.aspx>

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity



Microsoft Account

Verify your account

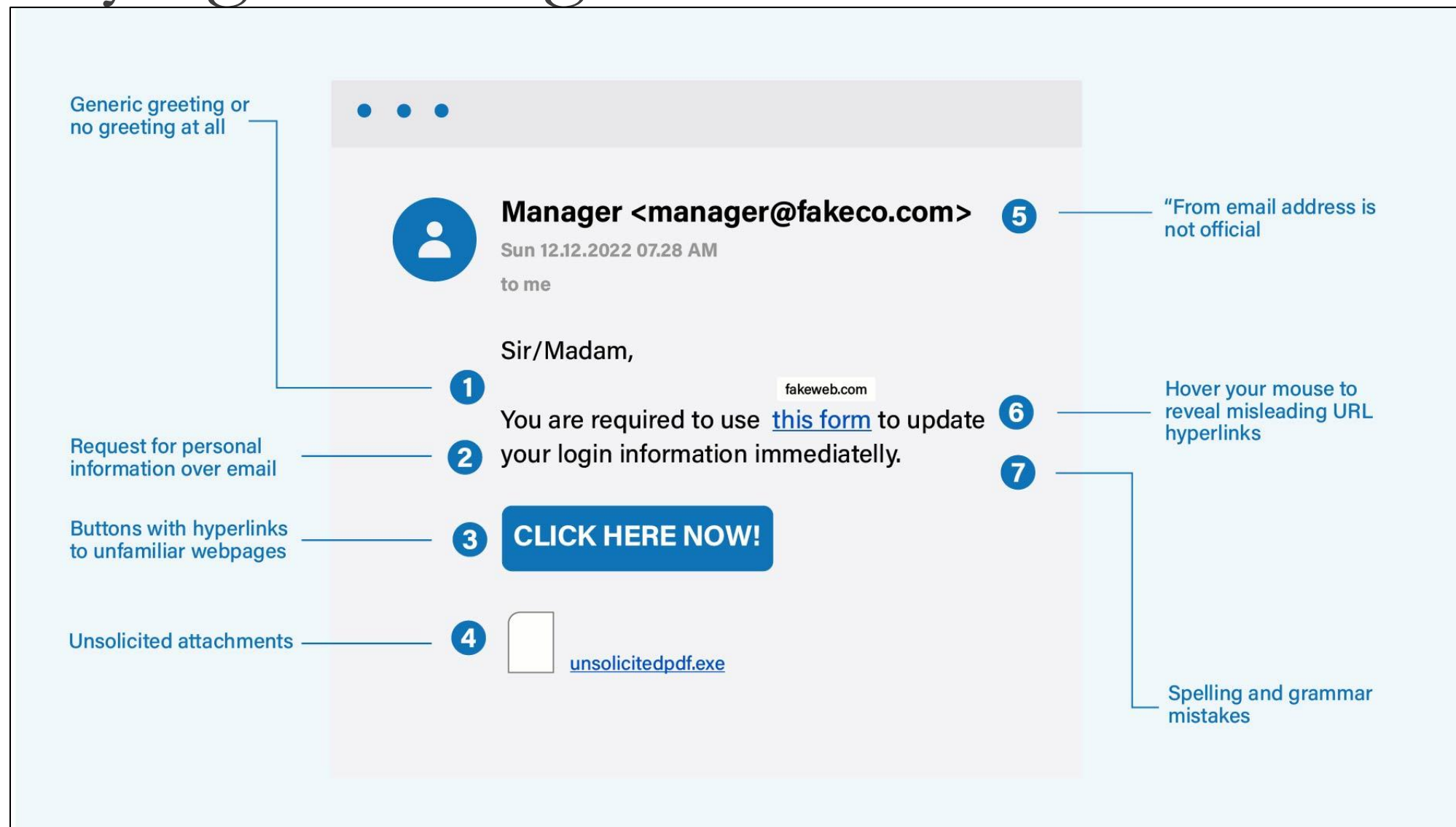
We detected some unusual activity about a recent sign in for your Microsoft account bo*****@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

[Review recent activity](#)

Thanks,
The Microsoft Team

Identifying Phishing Email



Types of Malware

Trojan: A trojan is malware that appears to be legitimate software disguised as native operating system programs or harmless files like free downloads. Trojans are installed through social engineering techniques such as phishing or bait websites.

Adware: Adware is a type of spyware that watches a user's online activity in order to determine which ads to show them. While adware is not inherently malicious, it has an impact on the performance of a user's device and degrades the user experience.

Spyware: Spyware is a type of unwanted, malicious software that infects a computer or other device and collects information about a user's web activity without their knowledge or consent.

Keylogger: Keyloggers are tools that record what a person types on a device. While there are legitimate and legal uses for keyloggers, many uses are malicious. In a keylogger attack, the keylogger software records every keystroke on the victim's device and sends it to the attacker.



THANK YOU