

INFORMATION ASSURANCE AND SECURITY 1

Activity 1 (25 pts)

1. Explain why Information Security is Important to us?

As we are now in a data-driven environment where most processes involve data, it is important to protect this information for everyone's safety. In the context of business, information security provides protection for potential users. With guidelines and policies in place, data privacy compliance can be implemented, thus reducing the risk of cyberattacks and data breaches. Through information security, we can explore and establish procedures to secure information from unauthorized access, ensuring the safety of its users and processes.

2. Search for some measure to prevent security threats?

Two-factor authentication (2FA): Enable 2FA whenever possible. This adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone.

Keep software updated: Regularly update your operating system, web browsers, apps, and antivirus software. Updates often include security patches that address known vulnerabilities.

Use firewalls and intrusion detection systems: Firewalls help prevent unauthorized access to your network, while intrusion detection systems monitor network traffic for suspicious activity.

3. Choose three types of threats and explain?

Hackers: Also known as black-hat hackers, they engage in criminal activities like data theft, which involves stealing sensitive information, malware distribution by spreading viruses and malicious software, and service attacks aimed at overwhelming systems with traffic to render them unusable.

Malicious insiders: Individuals who have access to a system but exploit it for financial gain, personal revenge, or to disrupt the organization for social reasons.

Cyber terrorism: The use of computers and the internet to conduct violent acts, typically for economic gain or to disrupt an organization.

4. Search on the internet an article about a company that encountered an attack and explain what happened to that company and how they resolved that security issue?

One of the most prominent cyberattacks in history is the Yahoo incident. Massive data breaches occurred in 2013 and 2014 but were only disclosed in 2016. A total of 3 billion user accounts in 2013 and

200 million accounts in 2014 were affected, resulting in stolen data such as names, email addresses, and phone numbers. In some cases, security questions and answers were left unencrypted.

To resolve the issue, Yahoo conducted an internal investigation and worked with law enforcement to understand the scope and nature of the attacks. They publicly disclosed the breaches and forced password resets for all affected accounts, invalidating unencrypted security questions and answers. Yahoo also implemented enhanced security measures, including improved encryption and detection systems, to prevent future attacks.

https://en.wikipedia.org/wiki/Yahoo_data_breaches#:~:text=The%20User%20Account%20Database%20included,numbers%2C%20dates%20of%20birth%2C%20hashed

<https://digitalcommons.wcl.american.edu/aulr/vol66/iss5/3/#:~:text=The%20information%20stolen%20likely%20included,some%20cases%2C%20encrypted%20or%20unencrypted>

5. As a student, how do you protect your data and secure your devices against possible threats?

Here are some of the ways I protect my data in different scenarios:

- **Using social media:** I avoid clicking on shared links that claim to transfer me to other sources, as most of these links are affiliate links or are associated with sketchy websites.
- **Personal information:** I avoid sharing information about myself or others as it could be used for harmful purposes. I also refrain from being easily persuaded to provide personal information.
- **Browsing the internet:** I use browsers like Brave, which offer some protection against potential risks.
- **Password management:** I do not use a password manager, as I prefer to manually manage my passwords for assurance.

These practices help ensure my data remains safe and my devices are secure.