

Technological Institute of the Philippines

Manila



College of Computer Studies

Bachelor of Science in Information Technology

CITE 008-IT41S2 - Social Issues and Professional Practice

Peer Activity

Submitted by:

Reyes, Zein Benedict C.

Reateran, Iara I.

Submitted to:

Mr. PRAX ANZEL DONOR

Peer Activity | Discussion Question

Members:

- Reateran, Iara I.
- Reyes, Zein Benedict C.

Objective:

To engage students in critical thinking and collaborative discussion about computer network security, its challenges, and the ethical responsibilities of IT professionals in ensuring secure systems.

Instruction Details: Find a peer and select two questions to discuss. Ensure that you submit your work individually in a PDF file format and include the name of your partner in your submission.

Question 1: What are the most significant challenges faced by organizations in maintaining computer network security, and how can these challenges be addressed effectively?

- In our discussion, we talked about how organizations face many challenges in keeping their computer networks secure. One major problem is the constant rise of new cyber threats like hacking, phishing, and ransomware. Many companies also have outdated systems or employees who are not fully aware of security practices. To handle these challenges, we agreed that regular software updates, strong passwords, and employee training are very important. Having a good security policy and response plan can also help organizations stay prepared when attacks happen.

Question 2: How do human factors, such as employee behavior or user awareness, impact the effectiveness of network security measures? What strategies can organizations use to mitigate these risks?

- We realized that human behavior plays a big role in keeping networks safe. Even if a company uses strong security systems, one careless click on a phishing email can cause serious damage. People often make mistakes like sharing passwords or ignoring security warnings. To reduce these risks, organizations should teach employees about safe online habits, how to recognize scams, and why following rules is important. Regular training and reminders can make workers more careful and aware of threats.

Reflection

Zein

- From this activity, I learned that computer network security is not only about technologies and systems but also about people, both individuals and in an organization. Even with the best systems, one action can lead to a big problem if a person is not careful with

what they do online. Our discussion made me understand that everyone in an organization should take part in protecting the network. Training, awareness, and teamwork can make a big difference in preventing attacks. This knowledge is useful in real life because, as a future IT professional, I can help build a secure environment by guiding others and promoting safe practices in the workplace.

Iara

- From our discussion, I learned that maintaining network security requires teamwork and awareness from everyone in an organization or company. Technology alone cannot stop cyber threats if people are not careful with how they use the technologies or systems. I realized that even small actions, like clicking suspicious links or using weak passwords, can cause security problems. Through this activity, I understood the importance of proper training and consistent reminders for employees. In real-life situations, this knowledge can help me contribute to a safer work environment by practicing good security habits and reminding others to do the same. Staying alert and informed is one of the best ways to protect any organization from cyber risks.