COLLEGE OF ENGINERING AND COMPUTER STUDIES

**PERFORMANCE TASK # 2**

Computer Platform Technologies

Reflection paper. IT3-1 Seminar for Cybersecurity

Submitted By

Altea, Gabriel Dominic K.

Course & Section

BSIT 3-1

Date

March 24, 2025

**OUTCOMES OUTLINE**

1. **DESCRIPTION**

The paper must have a minimum of 5 pages, include pictures and discussion of the topic and main points discussed. In your paper provide discussion how security would be an integral part in computer platform and technologies and provide use cases as examples. Use the OE template.

1. **OBJECTIVES**
   1. Discuss the topic that were in the seminar and how security would be an integral part in computer platform and technologies.
   2. Provide use cases as examples.
2. **RESULTS AND DISCUSSION** (screenshots of I/O, essential codes, logic with brief discussions)

A group of people in a room

AI-generated content may be incorrect.

*Figure 1. Before the seminar begins*

This was before the seminar had begun. The IT 3-1 organizes a seminar with the theme of Squid Game: Cyber Edition. The organizers invited all the IT and CS students of different years to participate in the seminar. The main topic that the seminar will discuss is mostly all about cyber security. As you know, cyber attacks are a common threat to individuals as well as to the industry. It can be critical to the victim if their information has been leaked and exposed by the hacker. This is why the IT 3-1 organizers took the advantage to implement the seminar with the topic of cyber security to assure that our audiences gained knowledge and were fully aware of cyber attacks.

A group of people standing in front of a projector screen

AI-generated content may be incorrect.

*Figure 2. Onto the Main Topic*

We invited a speaker that has knowledge regarding the topic of cyber security. The speaker discusses the different types of threats that were common to the public, like malware, viruses, phishing, etc. This type of threat is critical to one system as it can damage, alter, manipulate, and even erase the entire system. Most cases that an individual experiences are the social engineering attacks. I have been hearing cases that someone has been hacked due to giving out their credentials to someone they didn’t know was an attacker. This is the most common threat that an individual experiences, especially when they don’t have knowledge of whether it is real or fake. Examples of this are texts coming from an unknown contact number and unknown emails. There are also some cases that messages might be legit since their messages look real; for example, the contact number has the name of the legitimate company, and the text is in the right format, which is why some might fall for this scam. In the next figure, the speaker discusses some of the things that relate to this kind of topic.

A person pointing at a screen

AI-generated content may be incorrect.

*Figure 3. Identifying the message if it’s real or fake*

In this figure, a participant is called upon to identify what is wrong with the image. This is a case of a phishing attack, where one attacker sends a message that looks legit to the victim. Back to the figure, as you can see, the message looks legit; it has the company's name on it as well as having a message that somehow looks similar to the real ones. However, the speaker discusses some of the most important things that all of us should look into whenever someone has sent a text. The speaker shared all the possible clues that a text might be fake and that it might be a phishing attack. First, we need to ensure that the sender is legit, like checking out its name. If it is an unknown number, it is possible that it might be a scam. Additionally, check if the contact name is good; it might seem real, but it might be off at some point. Next is checking the content of the message. As you can see, it warns you that your points will expire (which is similar to the real company regarding their points) and that it also instructs you to click on a link to redeem your iPhone 15 Pro Max. In my personal opinion, this content is fake, and the reason behind it is that why did it add a new promo or rather give giveaways if the concern of the first part is all about points? Well, it might be good for me that I was able to identify that it was a fake, but what if the attacker sends it to someone who doesn’t know or have knowledge regarding this content? Some might panic since their points will expire, and some might want the iPhone itself, which is why they are prone to this type of scam. Implementing this seminar is good for other places to share knowledge with everyone regarding phishing attacks.



*Figure 4. QR Phishing*

Well, this is the part where I almost got baited. This is also one of the parts that the speaker included in his talk. QR phishing is also the same as the phishing attack from the previous one. This type of attack might be tricky for all of us since this might be implemented in face-to-face conversation or even in some websites. You don’t know if the person who’s giving you the QR code is legitimate, claiming that you can win a reward after filling out the form after scanning the QR code. Like, for example, the speaker shows a slide claiming that everyone, or rather the first 20 persons, can win a mechanical keyboard. Since we were IT and CS students, we were fond of having new mechanical keyboards, especially when they were free, so some of the audiences scanned the QR code, and I almost scanned it too. However, I noticed that it might be fake due to the fact that 20 persons can have mechanical keyboards that are expensive. After that, the QR scanned by the audience says that the link is just a fake and that they were victimized by the speaker. This is a good practice that the speaker gave us since all of us are not aware or rather do not think before scanning the QR code.

Well, these topics are mostly part of what I had listened to in the talk. Although I have heard of some other topics, such as the deepfake scam, I didn’t focus on it at all since I was doing something at that time. This type of talk helps a lot to me, as it helps me gain knowledge about different types of threats, and the practices also help me to become aware of it. This can also relate to the topic that was discussed in the CPT lecture about security. The topics that were discussed would also be helpful in terms of security, such as having MFA, or multi-factor authentication, wherein this type of authentication helps your information to be more secured even when one attacker tries to infiltrate your system using your own credentials. This seminar really helps to enhance our mindset regarding the things that can be a critical part of our future work. It spreads awareness about cyber attacks and helps other people to have a mindset regarding this topic.

1. **LEARNING OUTCOMES**

I have learned a lot from this seminar, like learning about different types of threats and how they can be exposed. This really helps a lot for other people so that they can be aware of these types of scams. As I mentioned earlier, these types of attacks and how they would be solved are discussed earlier by our classmates; to secure our own information and credentials, we must enable multi-factor authentication so that attackers can’t easily get inside our system. I have learned how to prevent this type of attack and was grateful that our speaker provided us with the needs on how.

1. **REFERENCES**

Photos Provided by the IT 3-1 Document Team