**NARRATIVE REPORT**

**Name:** John Edward B. Ronda

**Year and Course:**  BSIT 4-F1

**Topic:**

* Awareness Seminar on Cybersecurity and PNPKI

**Speaker:**

Mr. Fidel Kyle M. Subeldia

**Date and Time:**September 13, 2024 | 8:00 am – 11:00 am

**Venue:** Zoom Webinar

**I. Introduction**

The webinar entitled “Awareness Seminar on Cybersecurity and PNPKI” was hosted by DOST Quezon with the goal of raising awareness about Public Key Infrastructure (PKI) and its crucial role in strengthening cybersecurity protocols. The session focused on the Philippine National Public Key Infrastructure (PNPKI), which uses the concepts of cryptography and digital certificates to provide a security mechanism for protecting data in transit (ex. online communications) and even at rest (ex. data in storage). This technology is becoming more relevant as more organizations store their data online. Therefore, making it essential to safeguard these data.

The webinar was conducted by Mr. Fidel Kyle M. Subeldia, who has deep knowledge and experience in cybersecurity and in digital authentication technologies. In fact, he is a Cybersecurity/PNPKI Officer at DICT Quezon. The webinar was attended by students, professionals, and individuals interested in learning about cybersecurity practices and encryption techniques.

**II. Narration of Events**

The event began with a brief opening remarks from the Provincial S&T Director. Ms. Maria Esperanza E. Jawili. The host welcomed the attendees and introduced Mr. Fidel Kyle M. Subeldia, the speaker of the webinar. The speaker started the presentation by discussing the increasing number of cyber threats and the importance of strong cybersecurity. This led to the main topic: Public Key Infrastructure (PKI). PKI is a system that helps keep digital communications safe. It makes sure that people can trust who they're talking to online and that their information is protected. The speaker also explored the key components of a typical PKI system, including Certificate Authorities (CAs), Registration Authorities (RAs), and digital certificates. The speaker provided a detailed explanation of how these components interact to create a secure environment for data exchange. Videos and diagrams were used to illustrate how digital certificates work, showing the process of certificate issuance and management.

Next, the speaker moved on to the main topic which is Cybersecurity 101. The speaker displayed an infographic that shows that the Philippines has a high rate of digital penetration, with nearly all the population using mobile phones and a large portion having internet access, with an average daily internet usage of 9 hours and 14 minutes. Additionally, it shows that the Philippine National Computer Emergency Response Team (PHCERT) monitored 57,400 cybersecurity threats and handled 3,470 incidents from 2021 to February 2023, with the majority of attacks targeting government and emergency services. The speaker then gave a shocking fact and said that a cyberattack happens every 39 seconds. This shows how common they are and why it’s important to protect ourselves online. The speaker then discussed the three key elements of cybersecurity: People, Policy, and Technology. He emphasized that these elements must work together to create a strong defense against cyber threats.

The speaker highlighted the three primary cyber threats facing individuals and organizations: malware attacks, social engineering, and influence operations. Malware attacks involve malicious software designed to harm computer systems. Social engineering tactics manipulate people into revealing sensitive information or performing actions that can compromise their security. Influence operations aim to manipulate public opinion or influence the behavior of individuals or groups through false or misleading information. Furthermore, the speaker presented highlights the importance of basic cybersecurity practices. He emphasized the need for regular backups, secure and private browsing habits, the use of anti-virus software and firewalls, and caution when connecting to public Wi-Fi networks. These practices can help protect individuals and organizations from common cyber threats.

**III. Knowledge/ Learning Acquired**

I learned about the core components of PKI, such as digital certificates, certificate authorities, and registration authorities. These elements work together to provide encryption, digital signatures, and secure authentication. The session showed how digital signatures are used to verify the authenticity of electronic documents. This makes them legally binding and trustworthy.

I learned that cyber threats are a serious problem. There are different kinds of attacks, like malware and social engineering. It's important to be careful online and take steps to protect ourselves. I also learned that basic cybersecurity practices are essential. Things like strong passwords and being cautious with public Wi-Fi can help keep us safe. Understanding the three elements of cybersecurity – People, Policy, and Technology – is important for building a strong defense. Overall, this webinar has helped me understand the importance of cybersecurity and how to protect myself online.

**IV. Observation**

The webinar was well-organized and easy to follow. The speaker was clear and used visuals to help explain complicated ideas. The presentation was well-structured, starting with the basics and then moving on to more advanced topics. There were a few minor technical problems such as no audio and video, but they didn't affect the overall experience. Many people participated in the webinar by asking questions and sharing their thoughts. The speaker answered all the questions carefully to make sure that everyone understood the topic. Overall, it was a successful webinar that helped people learn about PKI and cybersecurity.

**V. Recommendations/ Suggestions**

The webinar was helpful, but there are a few things that could be improved for future events. First, it would be helpful to have a live demonstration of using PNPKI software. This would help the attendees learn how to use the software in real life. Second, it would be good to share more resources, like the slides of the presentation or videos, so people can learn more about the topics covered in the webinar. Finally, it would be helpful to have more workshops or training sessions on cybersecurity. This would help people stay up-to-date with the latest information and protect their organizations from cyberattacks.

**VI. Certificate**

**VII. Screenshots**









