Module#3 Accessible Learning

Name_____ Class number: _____
Section: _____ Schedule: _____ Date: _____

Lesson title: Basic of Computing Platform: <u>What is Cybersecurity?</u>
Learning Targets:

1. Why is Cybersecurity is important?.
2. Types of Cybersecurity threats.

A. Introduction

What is Cybersecurity?

Protecting systems, networks, and programs from cyberattacks is the practice of cybersecurity. These hacks typically try to disrupt regular corporate operations, extort money from users through ransomware, or access, alter, or delete important information.

Nowadays, there are more devices than humans, and hackers are getting more creative, making it difficult to implement efficient cybersecurity measures.

B. Main Lesson

1. Why Cybersecurity is important?

   In the connected world of today, cutting-edge cyberdefense programs are beneficial to everyone. A cybersecurity assault can personally lead to anything from identity theft to extortion attempts to the loss of crucial information like family photos. Critical infrastructure, such as power plants, hospitals, and financial service providers, is a necessity

for everyone. To keep our society running smoothly, it is crucial to secure these and other institutions.

Everyone gains from the efforts of cyberthreat researchers who look into new and existing risks as well as cyber assault tactics, such as the 250-person threat research team at Talos. They strengthen open source tools, expose new flaws, and inform others about the value of cybersecurity. Their efforts increase everyone's online safety.

2. Types of Cybersecurity threats

- **Phishing**
  - Phishing is the act of sending phony emails that look like they are coming from reliable sources. The intention is to steal private information, including login credentials and credit card numbers. The most typical kind of cyberattack is this one. Through education or a technological solution that filters harmful emails, you can better protect yourself.

- **Social Engineering**
  - Adversaries may employ social engineering to deceive you into disclosing sensitive information. They can ask for money or try to access your private information. Any of the risks mentioned above can be paired with social engineering to increase your propensity to click on links, download malware, or believe a suspicious source.

- **Ransomware**
  - Malicious software includes ransomware. By preventing access to files or the computer system until the ransom is paid, it is intended to extort money. Even if the ransom is paid, there is no guarantee that the system will be fixed or the files will be restored.

- **Malware**
  - A sort of software called malware is intended to harm a computer or obtain unauthorized access to it.

C. Conclusion:

- Cybersecurity?" has shed light on the critical importance of safeguarding digital systems and data. We've explored why cybersecurity is vital in today's interconnected world, emphasizing its role in protecting sensitive information, maintaining privacy, and ensuring the smooth operation of businesses and institutions. Furthermore, we've delved into the various types of cybersecurity threats, ranging from malware and phishing attacks to data breaches and social engineering. Recognizing these threats is essential for developing effective defense strategies and staying vigilant in the face of evolving cyber risks. As our reliance on technology continues to grow, the knowledge gained from this lesson serves as a foundation for responsible digital citizenship and the protection of personal and organizational assets in an increasingly digital landscape.

Author:

Cisco: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~types-of-threats