**Class Assignment 1– SPRING 2025**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Course Title: | Applications of ICT | Course Code: | CSC-101 | Credit Hours: | 2,1 |
| Course Instructor/s: | Rabail Asghar | Program Name: | BSCS-A | | |
|  |  | **Maximum Marks:** | | **20** | |

**Question 1: CLO:1 <** **Describe the fundamental concepts of ICT domains>, Taxonomy <Understanding>**

**1. Briefly explain the following major security threats to users, hardware, and data.**

* **Threats to Users:** Identity Theft, Loss of Privacy, Online Spying Tools, Online Theft, Online Fraud, & Other Dot Cons.
* **Threats to Hardware:** Power-Related Threats, Hardware Loss, Hardware Damage, System Failure, Unauthorized Access & Use, Natural Disasters.
* **Threats to Data:** Malware, Viruses & Malicious Programs, Cybercrime, Cyber-Terrorism, and Countermeasures.

**Solution:**

### ****1. Security Threats to Users****

Users face numerous security threats that target their personal information and online activities. These threats include:

* **Identity Theft**: The illegal use of personal information, such as identification or financial details, by criminals for fraudulent activities. **Example**: A cybercriminal steals someone's credit card information and uses it for unauthorized purchases.
* **Loss of Privacy**: Occurs when personal data is accessed, shared, or sold without the user's knowledge or consent, often compromising their confidentiality. **Example**: Social media platforms collecting and selling users' private data without explicit consent.
* **Online Spying Tools**: Refers to malicious software or techniques used to covertly monitor or record users’ online activities. **Example**: Keylogger software capturing users' keystrokes to steal passwords and sensitive information.
* **Online Theft**: The act of stealing digital assets, such as financial credentials, through hacking or other criminal methods. **Example**: Unauthorized access to an individual's cryptocurrency wallet to transfer funds.
* **Online Fraud**: Deceptive practices designed to trick individuals into providing sensitive information or money. **Example**: Phishing scams where fraudulent emails mimic a legitimate bank and request account details.
* **Other Dot Cons**: A broad category encompassing various internet scams designed to exploit or deceive users. **Example**: Fake e-commerce websites tricking users into paying for products that are never delivered.

### ****2. Security Threats to Hardware****

Hardware is vulnerable to both physical and electronic threats that can damage or compromise its functionality. These include:

* **Power-Related Threats**: Electrical issues, such as power surges or outages, can damage hardware components or lead to data loss. **Example**: A sudden power surge damages a computer's internal circuitry, making it inoperable.
* **Hardware Loss**: The physical loss or theft of devices, including laptops and external drives, often results in compromised data security. **Example**: A stolen laptop containing confidential business files leads to data exposure.
* **Hardware Damage**: Physical damage caused by accidents or mishandling can render devices unusable. **Example**: A dropped smartphone suffers internal hardware damage, making it nonfunctional.
* **System Failure**: Malfunctions within hardware components can disrupt device operations and prevent access to stored data. **Example**: A hard drive failure results in the loss of critical files and software.
* **Unauthorized Access and Use**: Occurs when individuals gain physical or remote access to devices without permission, often leading to data theft. **Example**: An intruder accesses an unlocked workstation to copy sensitive documents.
* **Natural Disasters**: Unpredictable events, such as floods, earthquakes, and fires, can severely damage hardware and infrastructure. **Example**: A flood destroys servers in a company’s data center, causing data loss and operational disruptions.

### ****3. Security Threats to Data****

Data faces various security challenges, including cyberattacks and the misuse of technologies. Key threats to data include:

* **Malware**: Refers to malicious software, such as ransomware and spyware, designed to infiltrate, harm, or disrupt systems and steal data. **Example**: Ransomware encrypts user files and demands payment for the decryption key.
* **Viruses and Malicious Programs**: These are self-replicating codes that spread across systems to corrupt files or disrupt operations. **Example**: A computer virus spreads through infected email attachments, corrupting stored documents.
* **Cybercrime**: Criminal activities targeting data, such as hacking, phishing, and data breaches, often for financial gain. **Example**: Hackers breach a company’s database to steal customer information and sell it on the dark web.
* **Cyber-Terrorism**: Politically or ideologically motivated cyberattacks aimed at disrupting services or creating fear. **Example**: Cyber-terrorists hack into a government infrastructure to disable critical utilities.
* **Countermeasures**: Security measures implemented to safeguard data against threats, such as antivirus software, firewalls, and regular updates. **Example**: Deploying advanced antivirus software and enabling encryption to secure sensitive files.