**SYSTEM AND DATA SECURITY**

**System security/ cyber security/computer security**

System security refers to the measures and precautions implemented to protect computer systems, networks, and data from unauthorized access, attacks, damage, or disruptions.

System security is the protection of computer systems, data and information from harm, theft and unauthorized access.

**Key aspects in system security (goals of computer security)**

The CIA triad is a fundamental concept that outlines three core principles to achieve the overall security goals within a computing system. The CIA triad stands for:

1. **Confidentiality:**

**Definition:** Confidentiality ensures that information is accessible only to those who are authorized to access it. It involves protecting sensitive data from unauthorized disclosure.

1. **Integrity:**

**Definition:** Integrity ensures the accuracy and reliability of data throughout its lifecycle. It involves protecting data from unauthorized modification, deletion, or tampering.

1. **Availability:**

**Definition:** Availability ensures that information and system resources are accessible and usable by authorized users when needed. It involves preventing and mitigating disruptions to services.

**Computer Security risk**

A computer security risk is any action or event that may cause harm to computer hardware, software, data, or information.

**Categories of computer security risks**

Computer security risks are broadly categorized into;

1. Physical security risks
2. Data / information security risks

**Physical security risks**.

A computer physical security risk refers to a threat or potential danger to the physical components of a computer system, network infrastructure, or related hardware.

Some of the potential physical security risks include;

1. **Hardware Theft:**

* **Description:** this is stealing of computers, servers, or other hardware components.

1. **Hardware Vandalism:**

* **Description:** this is the deliberate destruction of computer equipment either by internal or external individuals.

1. **Environmental Hazards:**

* **Description:** Risks posed by environmental factors, such as floods, earthquakes, or other natural disasters that can damage or destroy computer equipment.

1. **Power Failures or Fluctuations:**

* **Description:** Risks related to power supply issues, including power outages, surges, or fluctuations that can damage hardware components or lead to data loss.

1. **Fire Outbreaks:**

* **Description:** Uncontrolled fires can pose a serious threat to the physical infrastructure of computer systems, including servers, data centers, and other hardware components.

**Prevention of physical security threats/ risks.**

|  |  |
| --- | --- |
| Physical security risk | Prevention measures |
| Hardware theft | Use physical access controls such as locked doors, windows, etc.  Use cables to lock equipment on desk e.g. keyboard locks  Use alarm systems to warn in case of intrusion  Put bulgar proofing in windows  Hiring security guards |
| Hardware vandalism | Monitoring using CCTV cameras  Limit access to equipment |
| Environmental hazards | For cases of lightening, have a lightening conductor  The computer laboratory should be on a raised ground in case of floods. |
| Power failures | Using uninterruptable power supply (UPS) to provide power backup in case of outages.  Using surge protectors to protect computer equipment in cases of electrical spikes  Using power stabilizers in case of voltage fluctuations. |
| Fire outbreaks | Having a fire extinguisher to put out any fires. |

**Data security risks**

A computer data security risk refers to a threat or potential danger to the data and information of a computer system.

Some of the potential data security risks include;

1. **Viruses:**
   * **Description:** Viruses are malicious software programs that disrupt the normal functioning of a computer.
   * **Categories of computer viruses**

**Worm**: A worm is a type of computer virus that reproduces itself continuously until it the computer runs out of memory.

**Trojan horse**: A Trojan horse is a deceptive type of malware that disguises itself as a legitimate or beneficial program but actually contains malicious code.

**Boot sector virus**: A boot sector virus infects the master boot record (MBR) or the boot sector of a computer's hard drive or removable storage.

**Joke**: A joke is a harmless program that displays annoying messages on the screen.

* + **Sources of computer viruses**
* Fake games,
* pirated software,
* freeware from the internet,
* infected storage devices,
* rogue sites,
* infected software installers,
* infected email attachments
  + **Signs and symptoms of computer viruses**
* Flickering of the screen
* Un usual messages on the computer screen
* Programs taking longer to open
* Corrupted files
* Failure to boot
* Reduction in computer memory
* Reduction in computer speed
* Missing computer icons
* Frequent system

crashes

* + **Prevention of computer viruses**
* Install an updated antivirus
* Scan all removeable devices
* Handle email attachments with caution
* Use a firewall
* Make regular data backups
* Avoid visiting rogue sites

1. **Unauthorized Access:**

* **Description:** Unauthorized access refers to individuals gaining access to an organization's data, networks, endpoints, applications or devices, without permission

1. **Hacking:**
   * **Description:** Hacking involves gaining unauthorized access to computer systems or networks with the intent to exploit vulnerabilities, disrupt services, or steal data.
2. **Cracking:**
   * **Description:** Cracking is the process of bypassing software licensing restrictions to gain unauthorized access to software or systems.
3. **Phishing:**
   * **Description:** Phishing is a form of social engineering where attackers use deceptive emails, messages, or websites to trick individuals into providing sensitive information.
4. **Eavesdropping:**
   * **Description:** Eavesdropping involves the unauthorized interception and monitoring of communication, often over networks, to gain access to sensitive information.
5. **Electronic Fraud:**
   * **Description:** Electronic fraud includes various deceptive practices conducted online to trick individuals or organizations into providing money, sensitive information, or access credentials.
6. **Spoofing:**
   * **Description:** Spoofing involves impersonating a trusted entity or manipulating data to deceive individuals or systems.
7. **Denial of Service Attack (DoS):**
   * **Description:** Denial of Service attacks overwhelm a system, network, or service with excessive traffic, rendering it unavailable to legitimate users.
8. **Sabotage:**
   * **Description:** Sabotage involves intentional actions to disrupt, damage, or destroy computer systems, networks, or data.
9. **Backdoor Attacks:**
   * **Description:** Backdoor attacks involve creating secret access points (backdoors) in systems, allowing unauthorized entry at a later time.
10. **Information theft**

* **Description**: Information theft refers to the unauthorized and intentional act of stealing or acquiring sensitive information from individuals, organizations, or systems.

1. **Software piracy**

* **Description**: This is illegal duplication of copyrighted software.

**Prevention of data security risks**.

1. **Passwords:**
   * **Description:** Passwords are a fundamental authentication method where users must provide a unique combination of characters to access a system or data. Strong, complex passwords enhance security by making unauthorized access more difficult.
   * **Characteristics of a good password** 
     1. It should have a minimum of 8 characters
     2. It should a mixture of different characters
     3. It should expire (Always change your password)
     4. It should easy to remember
     5. It should be about your personal information

**Note**: A **username** is a unique public identifier chosen by an individual to represent their identity when accessing a system while A **password** is a private string of characters (letters, numbers, and/or symbols) chosen by a user to prove their identity when logging into an account or system.

1. **Firewalls:**
   * **Description:** Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a secure internal network and untrusted external networks, preventing unauthorized access and protecting against cyber threats.
2. **Biometrics:**
   * **Description:** Biometrics involves using unique physical or behavioral characteristics for user authentication. Common biometric methods include fingerprint scans, retina or iris scans, and facial recognition. Biometrics adds an extra layer of security by relying on individual biological traits.
3. **Antivirus:**
   * **Description:** Antivirus software is designed to detect, prevent, and remove malicious software (malware) such as viruses, worms, Trojans, and ransomware. It regularly scans systems for potential threats and takes action to neutralize or quarantine them.
4. **Data Backups:**
   * **Description:** Data backups involve creating duplicate copies of important information to ensure its availability in the event of data loss, corruption, or system failures. Regular backups provide a means of restoring data to a previous state.
5. **Access Rights:**
   * **Description:** Access rights, also known as permissions, define the level of access and actions users or systems are allowed to perform on data or within a system. Properly managing access rights helps prevent unauthorized access and misuse of information.
6. **Audit Logs:**
   * **Description:** Audit logs record and store information about system activities, user actions, and security events. Regularly reviewing audit logs helps detect suspicious or unauthorized activities, aiding in the identification and mitigation of security incidents.
7. **Honey Pots:**
   * **Description:** Honey pots are decoy systems or networks designed to attract and detect unauthorized access or cyber-attacks. By diverting attackers to these intentionally vulnerable systems, organizations can gather information about potential threats without exposing critical infrastructure.
8. **Intrusion Detection Systems (IDS):**
   * **Description:** IDS monitors network or system activities for signs of malicious behavior or security policy violations. It detects and alerts administrators about potential threats, enabling a swift response to prevent or mitigate security incidents.
9. **Data Encryption:**
   * **Description:** Data encryption involves converting data into a coded form to protect it from unauthorized access during transmission or storage. Encryption algorithms use keys to encode and decode information, ensuring that only authorized parties can decipher the encrypted data.

**Cyber Crimes**

Cybercrime, or computer crime, refers to criminal activities that are carried out using computers, networks, and the internet.

Examples of common cybercrimes include;

* Hacking
* Phishing
* Electronic fraud
* Cyber bullying
* Cyber Espionage
* Cyber extortion

**Intellectual property (IP)**

**Intellectual property** (IP) refers to creations of the mind—ideas, inventions, artistic works, designs, symbols, names, and images.

**Intellectual Property Rights** (IPR) are legal rights granted to individuals or entities to protect their intellectual creations or inventions.

**Protection of intellectual properties.**

1. **Patents:**
   * Patent rights provide inventors with exclusive rights to their inventions, preventing others from making, using, selling, or importing the patented invention without permission. Patents are typically granted for a limited period, often 20 years.
2. **Copyrights:**
   * Copyright grants creators’ exclusive rights to their original works of authorship, including literary, artistic, musical, and dramatic works. Copyright protection allows creators to control the reproduction, distribution, public performance, and display of their works.
3. **Trademarks:**
   * Trademark rights protect distinctive signs, symbols, names, and logos used to identify and distinguish goods or services. Trademark owners have the exclusive right to use these marks in commerce, preventing others from using similar marks that may cause confusion.

**ICT ETHICS**

Ict ethics are moral guidelines that govern the use of computers.

Computer ethics involves the use of computers in a morally acceptable way.

Some of the most common computer ethics include;

* Contribute to society and human well being
* Always avoid harm of others
* Always be honest and trustworthy
* Always exercise fairness and don’t be discriminative
* Honor intellectual property rights
* Respect other individual’s privacy
* Honor confidentiality

**Code of conduct**

A code of conduct is a written guideline that determines whether a particular action is ethical or unethical.

Sample code of conduct includes;

1. Computers shall not be used to harm other people
2. Users shall not interfere with another person’s work
3. Computers shall not be used to steal
4. Computers shall not be used to bear false witness
5. Users shall not copy software illegally
6. Users shall not use another individual’s computer without permission
7. A user shall consider the social impact of the programs they design
8. Users should use computers in a way that demonstrates consideration and respect to other people.