**Security of information systems**

**An introduction to security of information systems**

**Security** – to prevent unauthorized access, alteration, theft or physical damage to information systems security measures, procedures and policies have to be practiced in the business.

**Controls** – methods, procedures and policies ensuring the safety of organizations assets, integrity of its records and adherence to management standards.

**Areas of vulnerability in information systems**

**Malware –** malicious software programs.

**Computer viruses** – software able to attach it self to other software or data files in order to be executed e.g. display message, destroy data, clog computer.

**Worms –** programs that copy itself from one computer to the next over a network with the purpose of destroying data and halting operations.

**Trojan horse –** a computer program often disguised as legitimate software, but when installed opens the gate for malicious code to be installed and executed on the target system.

**Other vulnerabilities in information systems**

* **Internet vulnerability –** hackers can intercept conversations, flood servers with traffic.
* **Wireless security concerns –** radio frequency bands are easy to scan; hackers use tools to discover and monitor unprotected networks.
* **Ransomware –** hackers take control of victims’ computers then request money for users to regain access.
* **Spyware –** a computer program designed to keep minimal surveillance on a victims’ computer, unbeknownst to the user.
* **Keyloggers –** records every keystroke made on a computer to steal passwords, personal information, etc.

**Hackers and computer crime**

A hacker is an individual who gains unauthorized access to a computer system by finding security weakness in the system.

* **Spoofing –** when hackers hide their true identities by using a fake email address or masquerading as someone else.
* **Sniffer –** a computer program that is able to monitor and identify information traveling over a network.
* **Denial-of-service attack (DDOS)** – hacker flood a server with requests in an attempt to crash the network.
* **Phishing** – setting up fake websites or email messages that look legitimate in order to harvest credentials.
* **Evil twins** – wireless networks that pretend to offer trustworthy WIFI connections to the internet, but also monitors the users activity over the network.
* **Cyber warfare –** a state-sponsored exercise that has the purpose of penetrating another states’ computer networks in order to cause as much damage and disruption as possible.

**Information systems controls**

* **General controls –** the overall structure, security and use of computer programs and