Foundation in Information Technology (FIT)

FIT 103: ICT Applications
Module 1: Computing for the Society

Topic 6: Safeguarding Hardware, Software and Data

6. Safeguarding Hardware, Software and Data

Today's technology has come up to a level that makes all of the things happen through a single click. However, these achievements could lead to emerging risks and vulnerabilities. Crimes and illegal acts such as financial, monetary and commercial frauds can happen behind these achievements. It emphasises on taking necessary precautions to safeguard hardware, software and data from possible vulnerabilities.

6.1. Laws, Standards and Procedures

The enacting laws, standards and procedures can assist in preventing crimes and illegal acts. It will make people hesitant to attempt in doing crimes and illegal acts. If someone does a crime, then there are legal actions that can be taken against them. The following are some acts that have been developed to prevent crimes and illegal activities related to digital devices' usage.

6.1.1. Gramm – Leach – Bliley Act

Gramm-Leach-Bliley Act is known as the GLB Act, GLBA or Financial Modernization Act of 1999. In the United States, the federal law is that financial institutions should explain how they share and protect customers' data. Companies need to ensure the customers that their information is secured. The companies should also give the customers the right to opt-out if they do not want to share their data with the company and other third-party companies. Through this Act, companies are entitled to protect sensitive private data such as National Identity numbers, credit/debit card numbers etc. These guidelines should be given to the customers in a written format.

The benefit of this Act is that it protects sensitive data related to the customers. The sensitive data can be credit card details, Social Security number, date of birth, address, name, contact numbers etc. Violating the rules of the Act can result in paying penalty charges for each violation and can send to prison for five years.

6.1.2. HIPPA Act

HIPPA stands for "Health Insurance Probability and Accountability". This Act was established in 1996. It maintains the patients' information confidentially and ensures that the information cannot be shared without the patient's approval. The Act provides information on what situations give the authority to disclose information without consent and what penalties are imposed on people or organisations who violate the Act's laws.

This Act protects the sensitive data of the "covered entities". There are three types of covered entities. They are:

- Healthcare providers – the practices that provide a health care facility
- Health plans – organisations that provide health care plans such as insurances

- Healthcare clearinghouse – a third-party organisation that processes transactions related to insurance claims and billing

6.2. Data Protection and Security

The world today is built of the data. The evolution of technology drags on the use of data on a much larger scale emerging new study areas such as "data science". The data comprises of both public and confidential data. When personal data are used, it is essential to maintain their privacy without letting any unauthorised persons access them. Following are some of the methods that can be used to protect the data.

6.2.1. Passwords

Password is a secret code that is used to authenticate access to a digital device or personal account. When creating a password, it is important to use a "Strong Password". A strong password comprises ten or more characters that include upper- and lower-case characters, numbers, and nonalphanumeric characters. Following is an example of a strong password.

P@s$W0rD

A password that is easier to guess or commonly used is called a "Weak Password". Weak passwords can be your name, phone number, pet's name etc. Following are a list of weak passwords.

- 123456
- Qwerty
- Password
- Football
- Monkey

6.2.2. Software Firewall

A software firewall is installed on a computer which is connected to a network. It can filter incoming and outgoing traffic. Software firewalls protect your computer network from malware and hackers. It can protect the computer on which it is installed. For instance, if it is installed on your computer, then it protects your computer.

The software firewall can control data traffic flowing in and out of a network. It can help you block specific applications or websites accessing the computer and prevent sending sensitive and or secured data to the network. Software firewalls can deny access to prohibited IP addresses or suspicious websites. The Windows operating system (Windows 7 and onward) and the Mac operating system have inbuild software firewalls. If you have an Administrator login to your computer, you can change your software firewall settings and allow or block apps communicating through the firewall.

6.2.3. Antivirus Software

Antivirus software is used to protect your digital devices from malware and computer viruses. It scans the computer (disks, memory and programs) to identify any possible threats. If it finds a threat, then it cleans or quarantines the files that are affected by the malware. Malware or malicious software can be a worm, trojan or adware. A worm is a virus that replicates automatically and infects the files. Trojan represents as a legitimate file and trick you. So, you will be misled and downloaded to install it on your computer. It can steal your data or even damage your data. Adware is a scam that shows unwanted ads on your computer. Therefore, to prevent this malware, installing antivirus software is important.

6.2.4. Backups

If your computer is lost or crashes, then you will lose your data. Backups and data recovery methods help in protecting your data. Backup is storing data in different locations, and recovery is restoring the data to its original state. Backups can be made periodically in secondary data storages or cloud.

Flash drives or USB drives are commonly used to backup data mainly because it is smaller and portable. However, these two benefits can make it problematic, as well, because such a small device can easily get lost. Also, to make backups in a USB drive, you have to manually copy each file, and remember to do this often. During this process, you might delete or alter the files. Therefore, letting your computer to back up the files automatically is the best option. Also, you can use cloud services to back up your files. There are three types of backups. They are:

- Full Backup – whenever you backup your files it copies everything in your computer
- Incremental backup – in the next time when you want to copy the files, it checks for changes made for the files compared to the previous backup. Then it only copies the files that were changed after completing the last backup.
- Differential backup – copies new files and update the files which have been modified after the last full backup

6.2.5. Input Controls

Input controls are used to block any illegitimate applications accessing your data. It maintains the privacy and confidentiality of your data when they are being transferred between different applications. There are three types of input controls. They are:

- Input authorisation – Before data is entered to the computer **authorise, record, and monitor** the data sources.

- Data conversion – Transcribe the input data accurately during computer transactions.
- Data editing – Verify data inputs and edit if any errors occurred during the entering.

6.2.6. Software Upgrades

A software upgrade is done to get the newest version of the software. The new versions come with updated features than the older version. Not only to get the latest features but also to improve the security of the software, upgrades are done. For example, you can upgrade the antivirus guard periodically. The companies update the antivirus guards to protect your data from new viruses that appear from time to time.

6.2.7. Disposal Policies and Procedures

Data disposal policy is implemented to ensure that the data of computers or other digital devices that are not in use are permanently (retired) deleted. It can also be defined as discarding the digital devices by deleting their data securely so that no one can retrieve them. This approach guarantees data privacy and confidentiality. Not only digital devices (computers, laptops and mobile phones) but also storage devices (CDs, USBs, HDDs, etc.) can be destroyed under disposal policies.

6.2.8. General Data Protection Regulations and Principles (GDPR)

GDPR sets guidelines on collecting and processing personal information of people living in the European Union (EU). It was established in April 2016 by the European Parliament to protect the personal data of EU residents. To maintain data privacy, companies should get consent from individuals to process their data. Also, they need to anonymise the data. There are seven principles covered under GDPR. They are:

- Data of the individuals should be processed "lawfully, fairly and transparently".
- Data should be processed according to the agreed conditions and purposes.
- Personal data of an individual should only be processed for its intended purpose.
- Keep accurate and up to date personal data.
- Personal data can be stored until its purpose is achieved.
- Both integrity and confidentiality should be maintained when processing personal data.
- The data controller is accountable for maintaining the above six principles.

6.3. Intellectual Property Rights

Intellectual Property is inventions of inventors. Intellectual Property Rights are developed to give complete right for the creator to use their inventions. It allows protecting the knowledge related to developing the invention. Intellectual Property Right types are copyrights, trademarks and patents.

- Copyrights – It protects tangible creations of an inventor. They can be music, software codes or artwork. The copyright owner has the right to sell or reproduce them.
- Trademarks – It is a unique sign that can be used to differentiate a product or service. E.g. KFC
- Patents – It gives the right to the owner to commercialise their patent. Therefore, no one can sell or create an invention without the patent owner's permission.

6.3.1. Copyright

Copyright gives the owner of the work to protect their work without being duplicated by another. The original creator of the work gets the ownership to that work automatically. If another party wants to duplicate it, then they need to get permission from the owner.

Movies, dramas, music, artwork, books, software, and video games are examples of work that can be copyrighted. Copyright gives credit to the owner, and they can charge when allowing others to use their work. This approach encourages people to develop new things as it gives credit to their effort and ability. When you want to state that your work is copyrighted, then you need to state that "no copyrighted infringement is intended".

Copyrights give the owner exclusive rights to reproduce the work, develop new work based on the initial work, share the work by selling, leasing or transferring the ownership to another party.

6.3.2. Patents

Patent grants exclusive rights for inventions. Each invention contains technical information. When you apply for a patent, you need to make it public regarding your invention's technical information. You disclose this information in a patent application. There are three types of patents.

- Utility patent – given for machinery items and processes
- Design patent – given for the design of the product
- Plant patent – given for exploration on new and distinctive plants

6.3.3. Confidential Information

Confidential information is information that cannot be disclosed due to privacy and secrecy of the data. Confidential agreements are non-disclosure agreements (NDAs) where the parties involved in the agreement are bound to protect the data's confidentiality. Companies can sign NDAs with the employees to ensure that the company data are not disclosed to outside. There are two types of confidential information. They are:

- Personal information – sensitive data of an individual (date of birth, health history etc.)

- Competitive advantage information – companies protect their business-related information from their competitors

6.4. Safeguarding Hardware

Safeguarding hardware is that protecting your hardware from damage and stealing. To protect the hardware from damages, you can take safety measures such as storing and managing them with care. To protect the hardware from stealing imposing security measures is important.

6.4.1. Handling Storage Media

Storage media holds data such as files and documents. These files can hold confidential and important data. Therefore, it is important to protect the storage media. Following are some techniques that can be used to protect the storage media.

- Store devices at room temperature
- Do not place the storage media on top of other electronic devices
- Eject the devices safely before just removing them from the computer
- Do not keep the devices near water or direct sunlight

6.4.2. Storing Computer Equipment

Computer equipment needs to be stored safely without damaging it by moisture and temperature changes. Following are some of the methods that can be taken to store computer equipment correctly.

- Remove batteries and ink cartridges and detach cables and peripherals
- Choose the right container to store items
- Add a desiccant and seal the container
- Store in anti-static bags to protect from electrostatic discharge
- Add a layer of bubble wrap for fragile items
- Separate parts and pieces and give the parts a thorough clean

6.4.3. Access Control Systems

Access controls define who can access the data and resources of a company. They can be classified as physical and logical. While physical access controls can restrict access to rooms or buildings, logical access controls can limit access to data or computer networks. With the use of access, controls unauthorised access to physical and logical resources can be restricted. User credentials to log to the systems, biometrics and access cards to enter a building or a room are examples of access controls.

6.4.4. Recovery of Stolen Property

Use of security mentioned above measures will not help in mitigating theft. Following are some of the approaches that can be taken to recover any stolen property.

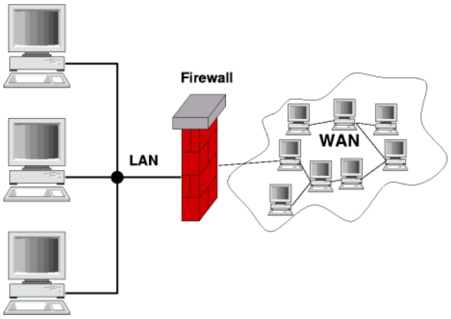
- Keeps the serial numbers of the devices
- Use digital trackers in the devices
- Put locks to the devices
- Use a locator app to find a stolen laptop
- Use surveillance cameras and file a police report
- Wipeout data if you can remotely log to the device

6.4.5. Uninterrupted Power Supply (UPS)

When the main power fails, UPS provides backup power supply to provide an uninterrupted power supply at least until you save your work. If the power goes off, you lose any unsaved data as the in Random Access Memory deletes. Therefore, having a UPS will indicate that the power has gone off so that you need to save it to secondary storage (Hard Disk, USB, CD).

6.4.6. Hardware Firewall

Hardware firewall stands between Local Area Network (LAN) and Wide Area Network (WAN) to filter any unnecessary traffic or possible intruder attacks. For example, the firewall prevents unauthorised persons on the internet or outside your network (WAN) accessing your network (LAN). Hardware firewall protects the entire network using one device. A hardware firewall is physically installed on the network, and you have to protect it by placing it in a secure location. Using a hardware firewall is a cheaper option as it does not require an annual fee. It is fast and does not affect the performance of the network.



6.4.7. Controlled access through locked doors

Controlled access allows preventing any unauthorised person accessing a secured building or a room. You can use locks, biometrics, cameras, alarms and CCTV to control the accesses.

Securing the building or room using a lock is the easiest mechanism to control the access. Then you can use cameras, alarms and CCTV to monitor premises for any illegal actions or people. You can also use biometrics to give authorised people access to enter the secured building or room. Biometrics are unique to each person. For example, you can use the thumbprint, fingerprints or retina scan as the biometrics.

6.4.8. Surge Protector

A surge protector is used to protect the electrical devices from high voltages. If the voltage is high, it can damage the electrical devices. For example: when lightning struck, it could cause a voltage spike and burn the devices' components.

6.4.9. Environmental Factors

Users need to know how to safeguard the hardware from different environmental factors that might harm their performance. The following are some of such conditions.

- Temperature - Temperature is the most significant environmental concern. All hardware should be kept under room temperature to get the best performance and free of damage.
- Humidity - Humidity can cause issues at cable connections. Particularly humid environments may require pre-wired special hardware to prevent the devices from catching humidity.

- Corrosive substances - Corrosive substances might start and increase the corrosion of hardware made of metals. Therefore, it is important to make sure that devices are not near corrosive substances.
- Magnetic fields - With the electronic process going on inside the hardware, they are being kept near magnetic fields can damage the performance of them
- Shock and vibration - Electronics that are well-suited to use in a laboratory might not be suitable to use in the field where there is a lot of shock and vibration. Hence, it is essential to use special hardware in such environments.