Digital Skills Academy

Introduction to Computer Security

Cre8te Opportunities

People • Business • Property

Contents

Introduction: Understanding computer security and privacy 3
1 Natural Threats 3
2 Measures for protection from natural threats 4
2.1 Back up data 4
2.2 Threats from human actions 4
2.3 Theft 5
3 Viruses, worms, and Trojan horses 5
3.1 Spyware 6
3.2 Internet scams and phishing 7
3.3 Online predators 7
4 Accidental deletion of data 7
4.1 Accidental damage to hardware 7
5 Guidelines for Securing your Computer 7
5.1 Best practices for securing online and network transactions 9
5.2 Use spyware and hacking protection 9
5.3 Clear your browsing history periodically 9
5.4 Cookies 10
5.5 Share personal information carefully 10
5.6 Conduct online transactions only on secured sites 10
5.7 Disable active content 11
5.8 Securing a computer 11
6 Exercise 12

Introduction: Understanding computer security and privacy

If you use a computer regularly, you probably have a lot of information stored on it, such as:

- Tax details
- Business correspondence
- Personal letters
- Personal photographs

All information on the computer can be damaged, lost, or viewed without your permission, so protecting your data is very important.

Computers are fragile and can be easily damaged and information stored on them can be stolen. You probably have many important documents on your computer that you want to protect from loss or theft, such as personal or financial information.

No matter how careful you try to be, your computer will need some safeguards for computer security and privacy.

Anything that has the potential to damage your computer or data is a threat. For example, dropping your computer or leaving it vulnerable to an accident can harm it.

Because of an accident or sabotage, your data or important system files could be deleted, causing your computer to malfunction.

Computer security constitutes the measures you can take to avoid threats and damage to your computer from physical harm or tampering.

Keeping your personal files and data secret and secure from unauthorised viewing or tampering is called computer privacy. You should protect your email, personal information and financial information like online banking transactions.

You can never be too careful when it comes to computer security and privacy. Remember to plan for accidents or human error by protecting your computer from threats of physical damage and internal malfunction.

1 Natural Threats

- **Fire** can be devastating to your computer. In addition to direct damage from flames, the heat generated by fire can melt sensitive components in the computer. Smoke can damage the CPU fan, which can also cause overheating.
- **Extreme Temperature** .Generally, computers are designed to function within a moderate temperature range. Excessive heat or cold can cause important components to malfunction or break. In cases of drastic temperature changes, it is best to allow the computer to return to room temperature before using it.

- **Power Surges**. Sometimes a lightning strike creates an electric surge (or spike) that amplifies the voltage to your computer through the power supply. They can also happen following a power cut. This sudden surge of electricity can destroy crucial components of your computer, including your motherboard. This can be mitigated by the use of a UPS (uninterruptable power supply).

2 Measures for protection from natural threats

2.1 Back up data

Backing up data involves creating multiple copies of your data and saving them either to an external hard drive, memory stick or to an online backup site in the cloud. Events like floods and earthquakes can occur without warning. Regularly backing up your data minimises the impact of these threats, because even if your original data is lost, you have copies that you can recover by using any computer. To provide better recoverability, keep a copy of your important data in a location that is physically separate from your computer, such as in a different building.

It is good idea to back up your information regularly so that you always have a current copy of your files and programs in case you need to restore your data. It is best to back up your data to multiple sources, such as to an external hard drive and to a CD. This ensures you have a second backup copy of your data if one source is damaged or is stolen.

2.2 Threats from human actions

Human actions are also threats to your computer. Some of these actions are malicious, such as those carried out by hackers, and others are human errors.

A hacker is a person who intentionally gains access to your computer when you connect it to the Internet with the intent of doing harm to the system or using the system in an unauthorised manner. Hackers can sabotage personal information, such as your finances, and also sabotage your physical computer, other computers, and programs. Hackers can send out personal information to companies.

In addition to malicious activity, human errors, such as accidentally deleting data or physically damaging the computer, are also a threat to your computer.

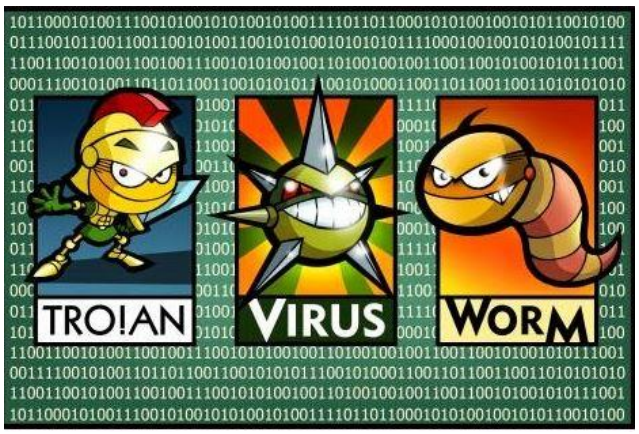
2.3 Theft

Anyone who has access to your computer can steal it or its components. With the popularity of portable computers such as laptops, physical theft of computers has become very common.

You can become a victim of virtual theft when your computer is connected to the Internet. An example of virtual theft is identity theft. Identity theft happens when someone, usually a hacker, steals your personal information and uses it without your permission to assume your identity. The hacker then uses your identity to gain access to your finances or perform illegal actions. In this way, the hacker can damage your reputation.

Another example of virtual theft is software piracy, which is theft of a computer design or program. Software piracy also refers to the unauthorised distribution and use of a computer program or confidential documents.

3 Viruses, worms, and Trojan horses



Viruses, worms, and Trojan horses are computer programs that can damage the data or software on your computer, or steal the information stored on your computer.

A virus is a malicious program (also called malware) that makes copies of itself and then inserts those copies into other programs or data files on your computer or on your hard drive. Viruses can reach your computer, without your knowledge, through the Internet or storage devices, such as disks and CD- ROMs.

A worm is a stand-alone malicious computer program that replicates itself with the goal of spreading the original code to other computers, usually through computer networks. This can cause harm by consuming bandwidth or possibly deleting files or sent documents.

A Trojan horse is a type of malicious software that appears to be harmless but that contains hidden code designed to exploit or damage your computer. Unlike worms, Trojan horses do not have the ability to replicate, but after they are installed, they infect additional files on your system. They can even send information from your computer to the developer of the malware over the Internet, which allows the developer to control aspects of your system. This can lead to stolen data, installation of more malware, the recording of your keystrokes (called key logging), and other illegal actions.

3.1 Spyware

Spyware is a program that can be installed on your computer without your knowledge. Spyware collects private information such as your browsing habits, downloads, and personal data, for example, your name and address.

There are many different strains of spyware. Some spyware can redirect you to a different site, install additional software that causes your computer performance to

slow down, change your computers' settings, change the home page, or serve you a personal advertisement known as adware.

3.2 Internet scams and phishing

You might come across attractive offers in email messages or through a website or chat room communication. Although these offers appear legitimate, they are often fake and trick you into revealing personal or financial information.

3.3 Online predators

Online predators are individuals who lure people online into inappropriate and unethical relationships and habits. An online predator commonly attacks a victim by manipulating that person so that he or she is unaware of the dangers. Online predators can be found in instant messaging rooms, chat rooms, and social networking sites.

4 Accidental deletion of data

Many times, damage to a computer is a result of unintentional human errors. Accidental deletion of an important file can disrupt the integrity of data or prevent other files or programs from working.

4.1 Accidental damage to hardware

Computer components are extremely delicate, and being delicate makes them vulnerable to carelessness. For example, accidentally dropping your laptop computer might result in damage to the hardware components, such as the motherboard or hard drive, which could cause data loss. Likewise, spilling food and beverages on storage devices can cause physical damage to your computer and thus to the data stored on it.

5 Guidelines for Securing your Computer

An unsecured computer is an invitation to trouble. Let's look at some steps you should take to keep your computer safe from ill intent and harm.

1 **User Accounts.** One way to keep your data safe from others who may have contact with your computer is to create user accounts (see our lesson on User Accounts) authorising only those you choose the privilege of unrestricted access.

You can set up a username and password to add security to your computer. In an office environment each employee would have their own unique username and password.

2 **Lock Screen.** If you need to leave your computer unattended, lock the computer to prevent unwanted access and to hide your screen from prying eyes. Only individuals who have the correct user name and password can unlock it.

3 **Antivirus/spyware Programmes.** You must also protect your computer from dangerous viruses and spyware that can be picked up from the internet. Some of the nastier ones can do considerable harm. To prevent this from happening, install antivirus and antispyware software into your computer that can prevent and remove the viruses. Antivirus and antispyware programs that are present in the computer's memory can alert you to the presence of a virus in your system and prevent viruses from entering. You must regularly update these programs on your system, because the programs are revised when new viruses and spyware are discovered. These updates will further protect your computer. Most programs offer an automatic update feature that automatically installs the updated version of the program.

4 **Email.** Because the source of many viruses, spyware, and Trojan horses are email sources and email software, Microsoft Outlook, amongst others, have features that allow you to block junk email messages; filter messages from viruses, Trojan horses, and spyware; and scan your attachments for malware.

5 **Data Encryption.** Data encryption allows you to make your data unreadable unless you authorise otherwise. It converts readable data into an unreadable code until it is "decrypted". This prevents data from being visible or copied if your computer is stolen or lost.

6 **Back Up.** Not all loss of data comes from outsiders. User error can also create problems if you do not back up your data. This simply means saving your data on various storage devices such as USB flash drives or other data storage options.

5.1 Best practices for securing online and network transactions

Use a strong password

A strong password is one that is complex enough to not be guessed or accidentally discovered. A strong password combines different password elements such as both uppercase and lowercase letters, numbers, and symbols such as the exclamation point (!) or number sign (#). The best passwords are not complete words and cannot be guessed by someone who knows you or by a stranger.

A strong password is crucial to protecting your data on websites, but you can also use a strong password to limit access to networks, sites with personal or sensitive information on file, and even data on your own computer.

5.2 Use spyware and hacking protection

Spyware programs can be downloaded from the Internet without your knowledge and transmit personal information about you to a hacker. This illegal attack on your computer could come from anywhere in the world, regardless of where you are. Hackers try to put spyware on your computer so that they can steal your confidential data.

You should use all the protection you can get, including Windows built-in antispyware and online security support from your Internet service provider (ISP). Often this support is in the form of anti-spyware software recommendations, firewall protections, and email screening and spam protection.

5.3 Clear your browsing history periodically

For your convenience, websites you visit on the Internet while browsing are saved and can be easily found again in your browser history. Your computer uses temporary memory, called cache memory, to store your Internet browsing history. Some of this temporarily stored data is personal information you have given to a site, such as credit card information when purchasing an item. Hackers can attempt to recover this information, but you can limit this risk by regularly deleting your browser history and cache memory.

5.4 Cookies

A cookie is another type of file created to make Internet browsing and shopping easier. Cookies are used to save preferences and other frequently used information you need on sites you visit often. For example, cookies allow your name and password to be remembered by sites.

But cookies can also become a threat to your computer privacy because hackers can steal this personal data. Just like deleting your browser history, make deleting cookies a regular practice.

5.5 Share personal information carefully

Before you give a website any personal information, make sure you are dealing with a reputable company and that the information requested is appropriate for the services offered. Making online purchases often requires credit card information and leaves you vulnerable to hackers and fraud. To minimise your risks, be sure any Internet commerce is conducted on a secured website and carefully read about how your information will be shared with others. Best practice is to avoid giving any personal information on the Internet unless you know exactly who you are giving it to and how it will be used.

5.6 Conduct online transactions only on secured sites

Eventually you will need to use the Internet to make a purchase, and you will need to provide your credit card number or some other personal data. Before you conduct a transaction, make sure the website is a secure website. A secure website is identified by the prefix **https** in its address. This prefix tells you the website implements the Secure Sockets Layer (SSL) protocol and uses encrypted communications, and it certifies that the website is legitimate.

Also, always check the security certificate of any website before offering your personal information or performing an online transaction.

5.7 Disable active content

Active content are small programs that install into your computer to enhance your browsing experience on the Internet. Often the content provides toolbars or video to make interacting on the Internet easier or more immersive. In some case, however, these programs are used by malicious persons to attack your computer and steal your data without your knowledge. You can disable active content on your computer by using your browser settings.

5.8 Securing a computer

When you are on the Internet, the biggest security risk to your computer comes from viruses and hackers. Often, threats such as these can be greatly reduced simply by making sure your computer security settings are correct and that your security software is up to date.

1 **Firewall settings** are used to restrict unauthorised access to your computer while online. A firewall prevents unauthorised access to a private network that is connected to the Internet. It forms a barrier between trusted and untrusted websites.

A firewall does not protect you from all viruses, so it is necessary to also install an antivirus or antimalware app.

2 **Settings** allow your computer to automatically download and install security updates to protect against the latest viruses.

- Privacy and security settings you can set on individual Internet sites that you visit.

- Malware protection settings to detect and eliminate dangerous software that could harm your computer.

- Maintenance tools that can perform tasks such as troubleshooting Windows and offering the latest updates.

3 Updates. Even on a brand new computer, software can be outdated. It is important to keep your computer current by installing the latest security and system updates.

Updates are made available by Microsoft on the second Tuesday of each month. It can be good practice to leave your PC/Laptop on overnight to allow the updates to install so they do not interrupt work the next morning.

You will be prompted to restart your computer when it is time to install an update. Restarting automatically initiates installation of the update.

It is always recommended that you install all official updates for Windows 7, 8, 8.1 and 10 to keep your computer running as fast and efficiently as possible.

Updates are necessary to keep your computer running well and virus-free.

6 Exercise

What is a cookie?

What is identity theft?

Keeping your personal files and data secret and secure from unauthorised viewing or tampering is called what?

Name three types of Malware, and for a bonus point, describe them.

What are some of the steps that can be taken to secure your computer?