AS and A LEVEL
Information Technology
9626

Chapter 5

eSafety

Faisal Chughtai
info.sirfaisal@gmail.com
www.faisalchughtai.com

Personal data

Personal data refers to any information that relates to an identified or identifiable individual. It includes any data that can be used, either alone or in combination with other information, to identify, contact, or locate a specific person. Personal data can be collected, processed, and stored in various formats, such as electronic records, paper documents, photographs, videos, audio recordings, and more.

Examples of personal data include:

1. **Basic identification information:** Name, address, date of birth, social security number, passport number, etc.
2. **Contact information:** Phone number, email address, mailing address, etc.
3. **Financial information:** Bank account details, credit card numbers, financial transactions, etc**.**
4. **Employment details:** Work history, job title, salary, etc.
5. **Health and medical information:** Medical records, diagnoses, prescriptions, etc.
6. **Biometric data:** Fingerprints, facial recognition data, DNA samples, etc.
7. **Online identifiers:** IP address, cookies, device information, user IDs, etc.
8. **Social media and online activity:** Posts, comments, likes, shares, browsing history, etc.
9. **Personal preferences:** Interests, hobbies, preferences, lifestyle choices, etc.

Sometimes the data has been manipulated so that it does not allow an individual to be identified. So, even if personal data has been de-identified, encrypted or pseudonymized, it is still classed as personal data.

De-identification, also known as anonymization or pseudonymization, refers to the process of removing or altering personally identifiable information from data sets in order to protect individual privacy. The goal of de-identification is to prevent the identification of individuals from the data, while still retaining its usefulness for analysis and research purposes.

Pseudonymized data refers to personal data that has undergone a process to replace or remove identifying information, making it more difficult to directly link the data to an individual without additional information. When data is pseudonymized, identifiable information such as names, addresses, or social security numbers is replaced with pseudonyms or codes. The purpose of pseudonymization is to enhance privacy and security while still allowing for data analysis and processing.

If, however, the data has been amended to make it appear anonymous in such a way that it is impossible to recognize the individual, then it is no longer classed as personal data.

Keeping personal data confidential

Computers are used by organizations and companies to store large amounts of personal information. If it were to fall into the wrong hands, the data could be used for identity theft or to withdraw huge sums of money from bank accounts.

Identity theft is when a fraudster pretends to be another individual online by using that individual's personal information. Fraudsters who have accessed an individual's personal data can use their login details to access their bank accounts or commit other types of fraud.

It is essential that personal information should only be seen by those people who are authorized to see it. Keeping data confidential is an essential part of an organization's responsibilities.

Organizations and businesses can take certain measures to ensure the confidentiality of data.

- Have strong passwords set on any account that holds personal data. Stronger passwords include characters, numbers and symbols and are not a recognizable word.
- Encrypt (scramble text so that it cannot be read without a decryption key) nay personal data that you can store on your computer.
- Have a firewall present, scanning incoming and outgoing data from your computer system.
- Regularly scan your computer with preventive software, such as an anti-virus package, that is used to identify a virus on a computer and remove it.
- Make use of any biometric devices (devices that measure a person's biological data, such as thumbprints), that are built into technology.
- Only visit and provide data to websites that are a trusted source.
- Do not open any email attachments from a sender you do not recognize.
- Check the URL attached to any link requesting data to see if it is genuine.
- Be cautious about any pictures or opinions that you post or send to people.
- Remove data about your location that is normally attached to your photos and videos that you may post, such as geotags.
- Do not become friends on social networking sites with people you do not know.
- Set all the privacy controls to the most secure setting that is available on social media accounts.
- Report and block any suspicious user.
- Use a nickname pseudonym when using the internet for entertainment, for example, playing games.
- If it is possible. Use a virtual private network (VPN), an encrypted connection that can be used to send data more securely across a network.

How is personal data collected?

There are several ways that an unauthorized person can try and collect your data. These include:

- Phishing
- Pharming
- Smishing
- Vishing

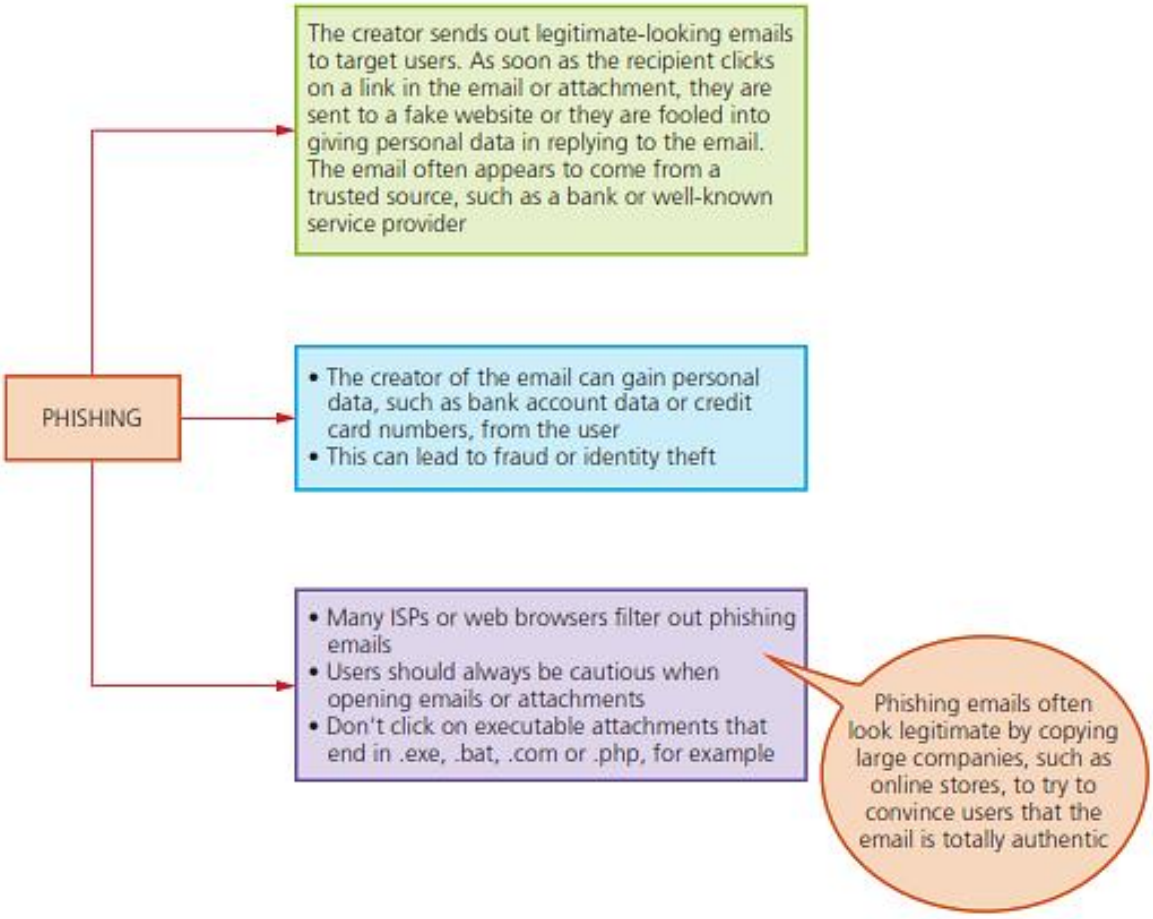
Phishing

Phishing occurs when a cybercriminal sends out legitimate-looking emails to users.

The emails may contain links or attachments that, when initiated, take the user to a fake website or they may trick the user into responding with personal data (for example, bank account details or credit/debit card details).

The email usually appears to be genuine coming from a known bank or service provider.

The key point is that the recipient has to initiate some act before the phishing scam can cause any harm. If suspicious emails are deleted or not opened, then phishing attacks won't cause any problems.



There are numerous ways to help prevent phishing attacks:

- It is important to use anti-phishing software on a computer connected to the internet. This identifies any content which could be interpreted as phishing contained in websites or emails.
- It is a good idea to always have anti-virus and anti-spyware software running on a computer, and to update it at regular intervals.
- Phishing emails often contain grammatical and/or spelling mistakes, so it is important for users to look out for these.
- Users should never trust emails that come from people whose names they do not recognize. If an email looks suspicious, it is best practice to just delete it.

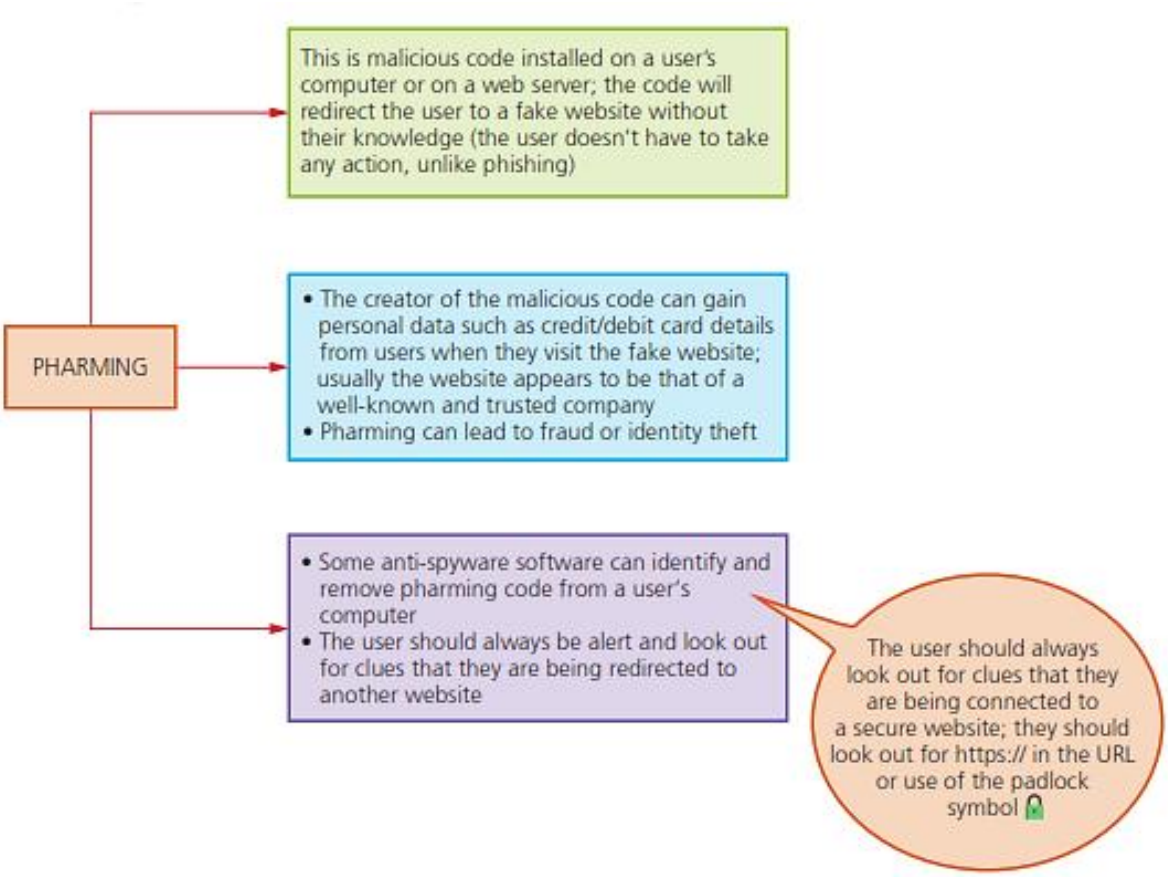
- If an email starts 'Dear customer' rather than using the receiver's name, it should also be treated with caution, as should emails asking the recipient to confirm their personal or financial information. Personal and financial information should never be sent in an email.
- If the email contains a message that the receiver has won a large amount of money or some other reason why they will benefit financially, it is likely to be a fake.
- Links placed within the email that are shorter than normal are used to hide the real URL and the best way of checking this is for the user to place the mouse cursor over the shortened link. This reveals the actual URL and the user can see straight away if it is suspicious.

Pharming

Pharming is malicious code installed on a user's computer or on an infected website. The code redirects the user's browser to a fake website without the user's knowledge.

Unlike phishing, the user doesn't actually need to take any action for it to be initiated. The creator of the malicious code can gain personal data, such as bank details, from the user.

Often the website appears to come from a trusted source and can lead to fraud and identity theft.



There are several ways to help prevent pharming attacks:

- Using up-to-date anti-virus software is one way to prevent the downloading of software which changes the hosts file. Users need to make sure they install the latest software updates.
- An up-to-date browser can cause an alert to be raised that a fake website has been loaded. It is sensible to use a trusted, legitimate internet service provider (ISP).
- Digital certificates can be checked to make sure that the site is legitimate.
- Any site that requires the entry of personal data should begin with HTTPS. If it does not, it may well be a fake site, particularly if it has not got a coloured padlock icon next to it.
- It may be useful to check that the URL is indeed correct for that site.
- The actual fake website may have tell-tale signs such as poor grammar or spelling and this should alert a user that it may be a fake site.

Smishing

Smishing is short for 'SMS phishing'. It uses the SMS system of mobile phones to send out fake text messages. It is very similar to phishing.

These scams often contain a URL or telephone number embedded in the text message.

The recipient will be asked to log on to the website or make a telephone call.

If they do, they will be asked to supply personal details such as credit/debit card numbers or passwords.

As with phishing attacks, the text message will appear to come from a legitimate source and will make a claim, for example, that they have won a prize or that they need to contact their bank urgently.

Methods used to prevent smishing attacks:

- Many digital security companies produce mobile protection software which users should have running in their smartphone.
- Users should also look out for all the same signs as in a phishing attempt, that is, spelling and grammatical errors, messages requiring immediate action or offering financial rewards, 'sign up now'.
- Good practice is to open the sender's website itself rather than replying to a text with personal information included in it.
- A sensible action is to check the sender's phone number against the phone number of the company they claim to represent.
- Users should never type in personal or banking information, other than when using an organization's official website.
- Receivers of a text should not click on links from senders they do not recognize.
- They should not click on any links in a text message since it is far safer to type the URL into a browser.

Vishing

Vishing (voicemail phishing) is another variation of phishing.

This uses a voicemail message to trick the user into calling the telephone number contained in the message.

As with all phishing attacks, the user will be asked to supply personal data thinking they are talking to somebody who works for a legitimate company.

An automated voice could speak to the user and advise them that an issue has occurred, such as there has been a suspicious activity regarding their bank account.

The automated system could be replaced by a real person who will try to convince the user that there has been an issue with an account they have and to provide the log-in details.

To avoid being a victim of vishing:

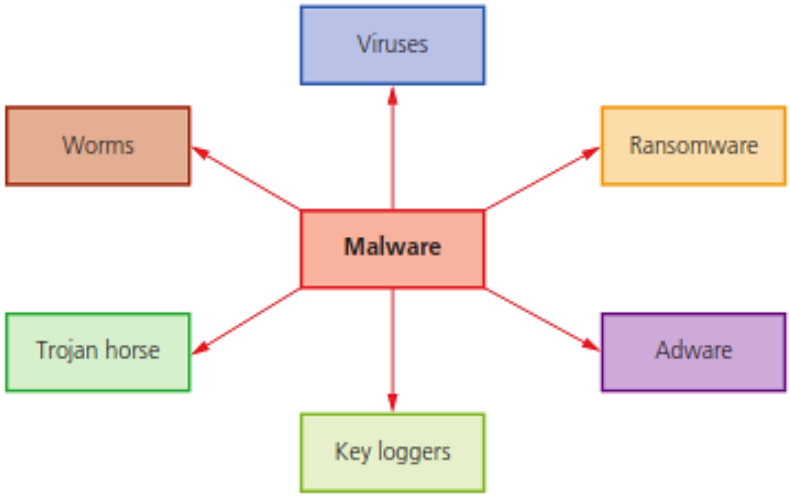
- It is good practice to use another phone to call the bank and ask to speak with the person who has just made the call.
- The main thing is not to give out login information over the phone, as a legitimate bank would never ask for it. The same goes for account information.
- There are also a variety of apps available which go beyond merely blocking the calls and keep a file containing the blocked numbers for all phone owners using the app.
- One software solution is employed by large organizations whereby the software can filter numbers according to the likelihood that scams are being attempted.

Malware

Malware is short for malicious software. It is the general term for computer programs which have been created with the deliberate intention of causing damage or disruption, or gaining access to a computer without the owner's permission.

The term malware covers all the different types of threats to computer security. These include:

- Virus
- Trojan horse
- Worm
- Spyware (key loggers)
- Adware
- Rootkit
- Malicious bots
- Ransomware



Virus

Viruses are programs or program code that replicates (copies itself) with the intention of deleting or corrupting files and causing the computer to malfunction (for example, by deleting .exe files, filling up the hard drive with useless data, and so on).

Viruses need an active host program on the target computer or an operating system that has already been infected, before they can actually run and cause harm (that is, they need to be executed by some trigger to start causing any damage).

Viruses are often sent as email attachments, and reside on infected websites or on infected software downloaded to the user's computer.

Minimizing the risk of a virus

- Install a reputable antivirus program on your computer and keep it updated. This software will help detect and remove viruses, as well as provide real-time protection against malware.
- Regularly update your operating system (e.g., Windows, macOS, Linux) to ensure you have the latest security patches. Enable automatic updates whenever possible to streamline the process.
- Keep all your software, including web browsers, office suites, media players, and plugins, up to date. Software updates often include security patches that address vulnerabilities that could be exploited by viruses.
- Be wary of email attachments, especially if they come from unknown or suspicious sources. Do not open attachments unless you are confident about their legitimacy. Scan attachments with an antivirus program before opening them.
- Download software, files, and media from trusted sources only. Avoid downloading from unverified websites or clicking on random pop-up ads, as they may contain infected files.
- Activate the firewall on your computer to create a barrier between your system and potential threats. Firewalls monitor network traffic and block unauthorized access.
- Be cautious when visiting websites, especially those of questionable nature. Avoid clicking on suspicious links or downloading files from unfamiliar sources.
- Create backups of your important files and data on a separate storage device or cloud service. In case of a virus infection or system failure, having backups ensures you can recover your valuable information.

Trojan horse

A Trojan horse is a malicious program which is often disguised as some legitimate software, but contains malicious instructions embedded within it.

A Trojan horse replaces all or part of the legitimate software with the intent of carrying out some harm to the user's computer system.

They need to be executed by the end-user and therefore usually arrive as an email attachment or are downloaded from an infected website. For example, they could be

transmitted via a fake anti-virus program that pops up on the user's screen claiming their computer is infected and action needs to be taken.

The user will be invited to run fake anti-virus as part of a free trial. Once the user does this, the damage is done.

Once installed on the user's computer, the Trojan horse will give cyber criminals access to personal information on your computers, such as IP addresses, passwords and other personal data.

Minimizing the risk of a trojan

- Install reputable antivirus and anti-malware software on your computer. Keep it up to date and enable automatic scans and real-time protection. Such software can detect and remove Trojan horses and other malicious programs.
- Keep all your operating system, applications, and plugins up to date. Developers frequently release security patches and updates to fix vulnerabilities that can be exploited by Trojans. Enable automatic updates whenever possible.
- Do not open email attachments or download files from untrusted or suspicious sources. Even if the email appears to be from someone you know, exercise caution. Scan attachments with antivirus software before opening them.
- Download files only from reputable sources. Be cautious with free software and avoid downloading files, as they are often used to distribute malware.

Worm

Worms are a type of stand-alone virus that can self-replicate.

Their intention is to spread to other computers and corrupt whole networks.

Unlike viruses, they do not need an active host program to be opened in order to do any damage, they remain inside applications, which allows them to move throughout networks.

In fact, worms replicate without targeting and infecting specific files on a computer, they rely on security failures within networks to permit them to spread unhindered.

Worms frequently arrive as message attachments and only one user opening a worm-infested email could end up infecting the whole network.

Minimizing the risk of a worm

- Regularly apply security patches and updates to your operating system, applications, and security software. This helps address vulnerabilities that worms may exploit.
- Install and maintain a reliable antivirus and anti-malware solution on all your devices. Keep the software up to date and enable automatic scanning and real-time protection features.
- Avoid opening email attachments or downloading files from untrusted or unknown sources. Worms often spread through email attachments or infected downloads. Scan files with antivirus software before opening or executing them.

- Divide your network into separate segments, with restricted access between them. This helps contain the spread of a worm if one part of the network gets infected.

Spyware

Spyware is software that gathers information by monitoring a user's activities carried out on their computer.

The gathered information is sent back to the cybercriminal who originally sent the spyware.

They are primarily designed to monitor and capture web browsing and other activities and capture personal data (for example, bank account numbers, passwords and credit/debit card details).

Key logging software (or key loggers) is a form of spyware. It gathers information by monitoring a user's keyboard activities carried out on their computer.

The software stores keystrokes in a small file which is automatically emailed to the cybercriminal responsible for the software.

Minimizing the risk of a spyware

- Only download files and software from trusted sources. Avoid downloading from unfamiliar websites or clicking on suspicious email attachments or links, as they can contain spyware.
- Do not click on any links or offers in pop-up adverts, no matter how exciting they may seem.
- Always read the small print when consenting to any user agreement. Commercial companies can sometimes list in the small print that you are consenting to allowing spyware to be downloaded to track information such as your browsing habits. Look for clauses about sharing your data with third parties.
- Cookies are a type of software that you may consent to be used to track your internet surfing habits. You should always check what you are allowing companies to do with the cookies.
- Anti-malware software can be used to scan your computer to see if any key logging software is present.

Adware

Adware is a type of malware. At its least dangerous, it will attempt to flood an end-user with unwanted advertising. For example, it could redirect a user's browser to a fake website that contains promotional advertising.

They can be in the form of pop-ups, or appear in the browser's toolbar thus redirecting the search request.

Although not necessarily harmful, adware can:

- Highlight weaknesses in a user's security defences.
- Be hard to remove. They defeat most anti-malware software because it can be difficult to determine whether or not they are harmful.
- Hijack a browser and create its own default search requests.

Minimizing the risk of adware

- When installing software, carefully read the terms and conditions and the installation prompts. Opt-out of any additional software or toolbars that may be bundled with the program. These extra items are often sources of adware.
- Free software can sometimes come bundled with adware. Be cautious when downloading and installing freeware or shareware. Read user reviews and research the software to ensure it is legitimate and adware-free.
- Adware can be spread through malicious advertisements or deceptive links. Avoid clicking on suspicious ads, pop-ups, or links on websites, especially those offering questionable downloads or promising unrealistic deals.
- Configure your web browser to block pop-up windows. Most modern browsers have built-in pop-up blockers, which can help prevent adware from displaying intrusive ads.

Rootkit

Rootkit is a type of malicious software that is designed to install a set of tools in a computer which allows the attacker to have remote access to that computer continuously.

It gives the attacker continuous privileged access to a computer and hides its presence deep within the operating system, the user is completely unaware that their computer has been infected.

The different tools enable the attacker to discover the user's passwords and credit card details.

It can be downloaded in a similar way to phishing by clicking on a link within an email, or a hacker could gain administrator privileges and install it remotely.

The rootkit can change any security software such as an anti-virus to convince it that it is not there. It is also capable of removing the anti-virus software.

Minimizing the risk of a rootkit

- Use strong and unique passwords for all your accounts, including your operating system, applications, and online services.
- Only download software and files from trusted sources. Avoid downloading from unverified websites or clicking on suspicious links in emails or other messages.
- Install and maintain reliable antivirus and anti-malware software on your system. Keep it updated to detect and remove known rootkits.

- Regularly update your operating system, software, and applications with the latest patches and security updates. This helps fix vulnerabilities that could be exploited by rootkits.

Malicious bots

Bot is short for internet robot and it performs tasks that are normally undertaken by a human.

Without them, the smooth running of search engines, for example, would not be as efficient.

Unfortunately, there are many malicious bots. Like a worm, a malicious bot can replicate itself and is designed to feed back to a server, this is called a botnet, because it is in control of a network of infected computers.

The botnet can then gather email addresses and from them generate spam to those and other addresses.

They are capable of gathering information from different websites, such as date of birth from one site, health insurance details from another site, and address from another. They are extremely difficult to detect on a computer.

Minimizing the risk of bots

- Bots are often embedded into links or software downloads and are often spread in the same way that phishing is carried out. Avoid clicking on any links without knowing who they are from and that they will link you to a trusted and reputable source.
- As bots can often be used in a chat situation, you should not give out any personal data when chatting online.
- If you suspect that you have downloaded a bot, anti-malware software can be used to detect and remove it.
- A firewall can also be used to detect the activity of a bot as it may recognize suspicious traffic created by the bot.

Ransomware

Essentially, ransomware are programs that encrypt data on a user's computer and 'hold the data hostage'.

The cybercriminal just waits until the ransom money is paid and, sometimes, the decryption key is then sent to the user. It has caused considerable damage to some companies and individuals.

The malware restricts access to the computer and encrypts all the data until a ransom is paid.

It may be installed on a user's computer by way of a Trojan horse or through social engineering.

When ransomware is executed, it either encrypts files straightaway or it waits for a while to determine how much of a ransom the victim can afford.

Minimizing the risk of ransomware

- Install reputable antivirus and anti-malware software on your computer. Keep it up to date and enable automatic scans and real-time protection. Such software can detect and remove ransomware and other malicious programs.
- Keep all your operating system, applications, and plugins up to date. Developers frequently release security patches and updates to fix vulnerabilities that can be exploited by ransomware. Enable automatic updates whenever possible.
- Download files only from reputable sources. Be cautious with free software and avoid downloading files, as they are often used to distribute malware.
- Regularly back up your important files and data to an external storage device or cloud-based backup service.

Summary of types of malware

Viruses	Programs or program code that can replicate/copy itself with the intention of deleting or corrupting files, or cause the computer to malfunction; they need an active host program on the target computer or an operating system that has already been infected before they can run
Worms	This is a type of stand-alone virus that can replicate itself with the intention of spreading to other computers; often uses networks to search out computers with weak security which are prone to such attacks
Trojan horses	These are malicious programs often disguised as legitimate software; they replace all or part of the legitimate software with the intent of carrying out some harm to the user's computer system
Spyware	Software that gathers information by monitoring, for example, all the activity on a user's computer; the gathered information is then sent back to the person who sent the software (sometimes they monitor key presses, which is referred to as key logging software)
Adware	Software that floods a user's computer with unwanted advertising; usually in the form of pop-ups, but can frequently appear in the browser address window redirecting the browser to a fake website which contains the promotional adverts
Ransomware	Programs that encrypt the data on a user's computer; a decryption key is sent back to the user once they pay a sum of money (a ransom); they are often sent via a Trojan horse or by social engineering