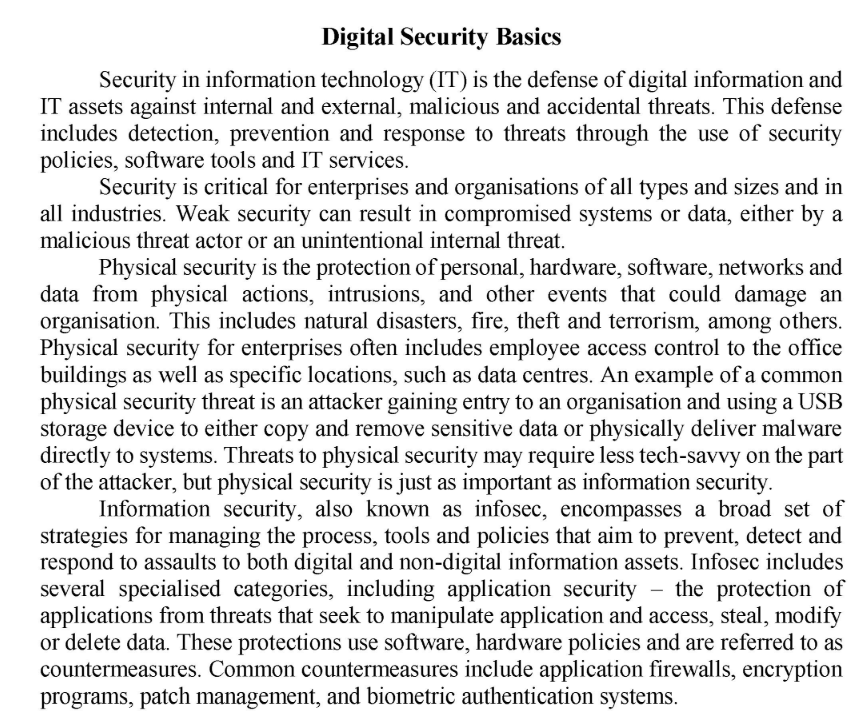
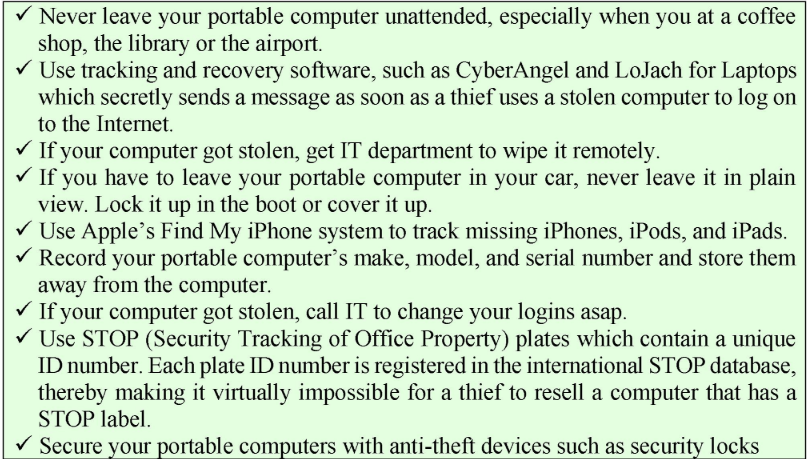
* **Digital security basics**





* **Computer protection and maintenance**

To ensure that your computer stays in good condition, its essential to protect it from power surges. A power surge is a sudden increase in electrical energy affecting the current that flows to energy affecting the current that flows to electrical outlets. Power surges often occur before or after power failures.

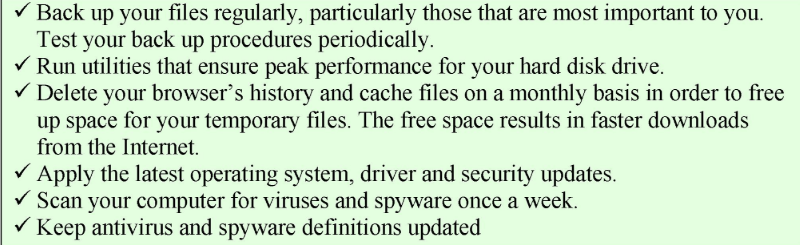
Computer and peripheral devices require stable current and are particular sensitive to sudden bursts of electricity energy. Smaller surges can slowly damage your computers circuit board and other electrical components.

You can protect your computer equipment from power surges by plugging it into a surge suppressor, instead of directly into a wall outlet. For added protection during thunderstorms, shut down your computer, turn off your peripheral devices, and unplug the surge suppressor and all computer-related cables from wall outlets, including thee cable for your modem.

A surge strip (surge suppressor/surge protector) is a device that contains electrical outlets protected by circuitry that blocks surges. Some surge strips also have sockets for modem connections that prevent surges from traveling down telephone or cable lines and into your computer.

A UPS( uninterrupted power supply) is a device that not only provides surge protection, but also furnishes desktop computers and network devices with battery backup power during a power outage.

If your desktop computer is connected to a UPS when a power outage occurs, the battery backup allows you to save what you are doing and properly shut down your computer. A UPS with high-performance battery might give you enough backup power to keep your computer running for several hours.



**Types of password assaults**

* **Password attacks** is a big serious problem nowadays.
* When someone gains unauthorised access to your personal data and uses it illegally, it is called identity theft.
* If a hacker doesn't have physical access to your work area, but your computer is connected to a network, your password can be discovered by hacker using a remote commuter and sottware tools that systematically guess your password, intercept it.
* The **brute force attack** uses passwords cracking software which choose all possible combinations of letters to decrypt a password, a brute force attack can run for days to crack some passwords.
* Sniffing is a process of interception information sent out over computer networks.
* **Sniffing** software is used legitimately by network administrators to record network traffic for monitoring and maintenance purposes. The same software can also be used for illicit activities.
* **Phishing** is when a hacker poses as a legitimate representative of an official organization such as ISO in order to persuade you to disclose highly confidential information.
* **A key logger** is software that secretly records a user’s keystrokes and sends the information to a hacker.
* **Trojan** is a computer program that seem to perform one function while actually doing something else.

## How to prevent attacks

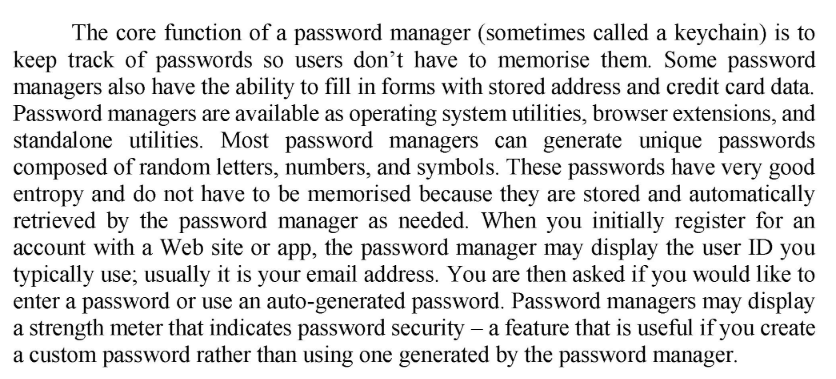
The best way to prevent password attacks is to adopt best practices for password hygiene and management. Easy-to-hack environments that have a weak security posture are much more appealing to opportunistic cybercriminals.

Boosting password security significantly improves the enterprise’s ability to [avoid a data breach](https://www.sailpoint.com/identity-library/prevent-data-breach/). Password best practices include:

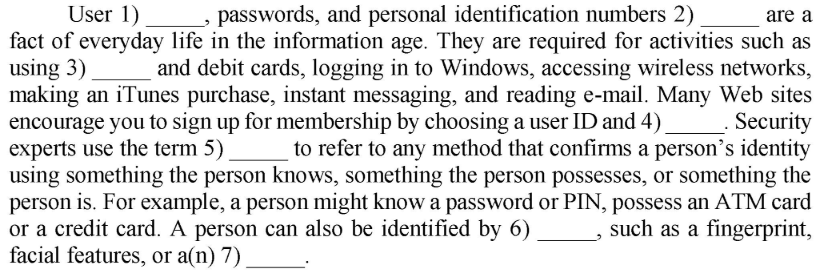
* Requiring long, complex passwords that are unique for each website or account
* Implementing [multi-factor authentication](https://www.sailpoint.com/identity-library/what-is-multi-factor-authentication/) when possible
* Adopting a password manager to simplify password management and ensure secure storage

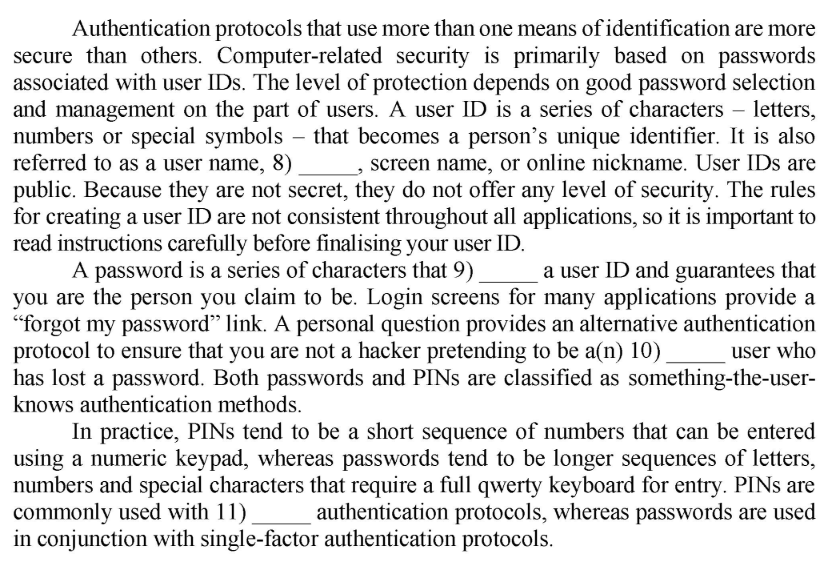
The enterprise’s IT team should also limit access to [privileged accounts](https://www.sailpoint.com/identity-library/8-benefits-of-privileged-access-management/) and add additional security layers for those accounts. Of course, educating all employees and other stakeholders about password security also enables prevention. With security breaches the new norm, employees and [anyone else with access](https://www.sailpoint.com/identity-library/what-is-third-party-risk/) to organizational resources play a key role in maintaining the company’s security posture.

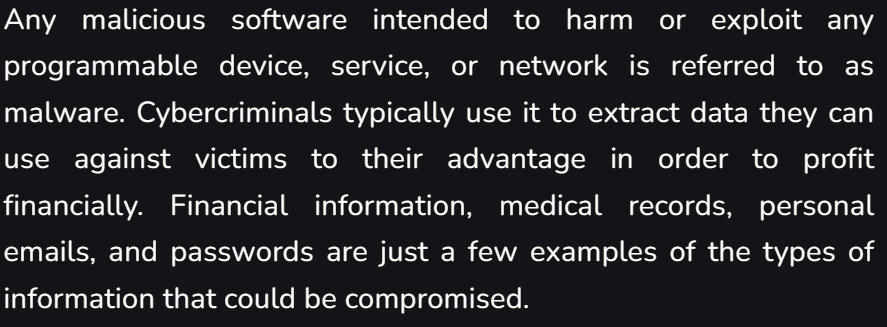
* **Password security, authentification**



1. IDs
2. PINs
3. ATMs
4. Password
5. Authentification protocols
6. Biometrics
7. Retinal pattern
8. Login
9. Verifies
10. Legitimate
11. Two-factor





-**Malware and its types**

Malware is a program designed to gain access to computer systems, generally for the benefit of some third party, without the user’s permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs.

. Types of malware include the following:

* A virus is the most common type of malware that can execute itself and spread by infecting other programs or files.
* A worm can self-replicate without a host program and typically spreads without any interaction from the malware authors.
* A Trojan horse is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.
* Spyware collects information and data on the device and user, as well as observes the user's activity without their knowledge.
* Ransomware infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
* A rootkit obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
* A backdoor virus or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.
* Adware tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. For example, an advertiser might use cookies to track the webpages a user visits to better target advertising.
* Keyloggers, also called system monitors, track nearly everything a user does on their computer This includes emails, opened webpages, programs and keystrokes.

There are several ways spyware, viruses, worms and malware are transmitted. Below are ways your computer can become infected and spread viruses. We've made this list in the order we believe to be most to least common.

One of the most common ways a computer becomes infected is when a user accepts what they see on the screen without reading or understanding the prompt.

When [downloading](https://www.computerhope.com/jargon/d/download.htm) any software (programs, utilities, games, updates, demos, etc.) via the Internet, make sure you're downloading the software from a reliable source.

As a general rule, do not open e-mail you were not expecting to receive. Viruses enter the computer when users open [e-mail attachments](https://www.computerhope.com/jargon/a/attachme.htm) that contain malicious [code](https://www.computerhope.com/jargon/c/code.htm).

* Any disk, disc, or thumb drive connected or inserted into your computer can be infected with a virus. As long as something is writable, a virus can move from a computer to that disk, disc, or drive. A common tactic used by hackers to access a network is by leaving out a thumb drive with malicious code on it. Then, when a user puts the thumb drive into their computer, it becomes infected with a virus or trojan horse.
* Visiting unknown links
* Not running the latest updates
* Pirating software, music, or movies
* No antivirus spyware scanner

**-How To Protect From Malware?**

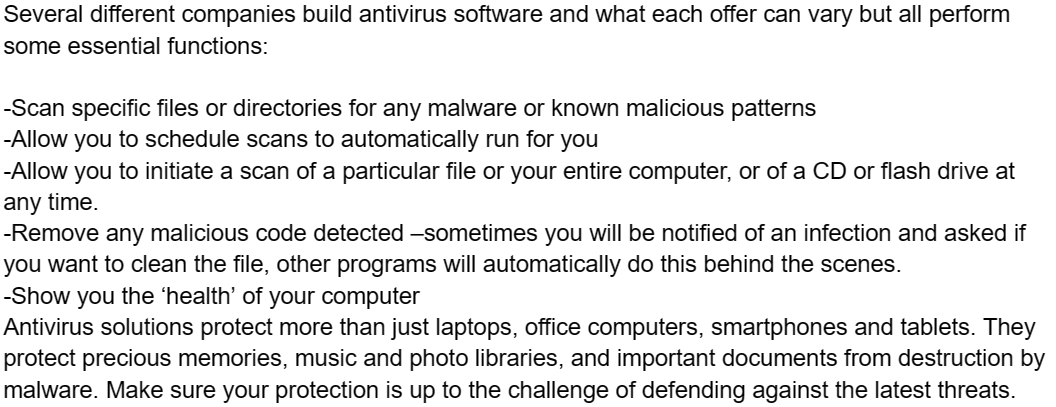
**The good news is that there are just as many ways to protect yourself from malware as there are different types of malware. Look at these top suggestions:**

* Protect your devices.
* Update your operating system and software. Install updates as soon as they become available because cybercriminals search for vulnerabilities in out-of-date or outdated software.
* Never click on a popup’s link. Simply click the “X” in the message’s upper corner to close it and leave the page that generated it.
* Don’t install too many apps on your devices. Install only the apps you believe you will regularly use and need.
* Be cautious when using the internet.
* Do not click on unidentified links. If a link seems suspicious, avoid clicking it whether it comes from an email, social networking site, or text message.
* Choose the websites you visit wisely. Use a safe search plug-in and try to stick to well-known and reputable websites to avoid any that might be malicious without your knowledge.
* Emails requesting personal information should be avoided. Do not click a link in an email that appears to be from your bank and asks you to do so in order to access your account or reset your password. Log in immediately at your online banking website.

**-Antivirus Software**

Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

These antivirus tools are critical for users to have installed and up-to-date because a computer without antivirus software protection will be infected within minutes of connecting to the internet.



**-What is a cyberattack?**

A cyberattack is an attempt to steal, alter, destroy, disrupt, or disable information resources and systems found in computer networks and systems. Cyberattacks can fit into two categories: insider threats or outsider threats. Insider threats stem from individuals with legitimate access to the systems they target, using their access to exploit vulnerabilities intentionally or inadvertently.

### 1. Malware

Cyberattackers use harmful software such as spyware, viruses, ransomware, and worms known as malware to access your system's data. When you click on a malicious attachment or link, the malware can install itself and become active on your device.

### 2. Phishing

Phishing attacks rely on communication methods like email to convince you to open the message and follow the instructions inside. If you follow the attackers’ instructions, they gain access to personal data, such as credit cards, and can install malware on your device.

### 3. Spoofing

Cyber attackers will sometimes imitate people or companies to trick you into giving up personal information. This can happen in different ways. A common spoofing strategy involves using a fake caller ID, where the person receiving the call doesn’t see that the number is falsified. Other spoofing methods include subverting facial recognition systems, using a fake domain name, or creating a fake website.

### 4. Backdoor Trojan

Backdoor Trojan attacks involve malicious programs that can deceptively install malware or data and open up what’s referred to as the “backdoor” to your computer system. When attackers gain access to the backdoor, they can hijack the device without it being known to the user.

### 5. Ransomware

Ransomware is malicious software that cyberattackers can install on your device, allowing them to block your access until you pay the attackers a ransom. However, paying the ransom doesn’t guarantee the removal of the software, so experts often advise individuals not to pay the ransom if possible.

### 6. Password attacks

Password attacks can be as simple as someone correctly guessing your password or other methods such as keylogging, where attackers can monitor the information you type and then identify passwords. An attacker can also use the aforementioned phishing approach to masquerade as a trusted site and try to fool you into revealing your account credentials.

### 7. Internet of Things attack

Communication channels between connected IoT components can be susceptible to cyberattacks and the applications and software found on IoT devices. Since IoT devices are in connection with one another through the internet and may have limited security features, there is a larger attack surface that attackers can target.

### 8. Cryptojacking

Cryptojacking involves gaining unauthorized use of a computer system, usually through malware that allows the attacker to use the computer's resources for mining cryptocurrency. Mining cryptocurrency can come with significant operational costs, so cryptojacking provides attackers with a way to avoid these expenses.

### 9. Drive-by download

Drive-by download attacks occur when you download malicious code to your device through an app, website, or operating system with flawed security systems. This means you could do nothing wrong and still be a victim of a drive-by download since it can occur due to a lack of security measures on a site you believe to be safe.

### 10. Denial-of-service attack

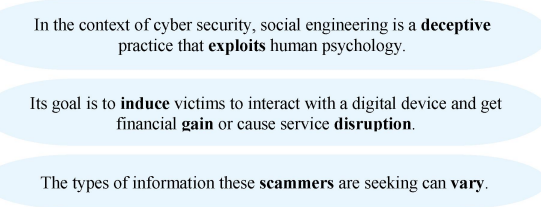
A denial-of-service attack causes an entire device or operating system to shut down by overwhelming it with traffic, causing it to crash. Attackers don’t often use this method to steal information. Instead, it costs the victim time and money to get their systems up and running again. Cybercriminals typically use this method when the target is a trade organization or government entity.

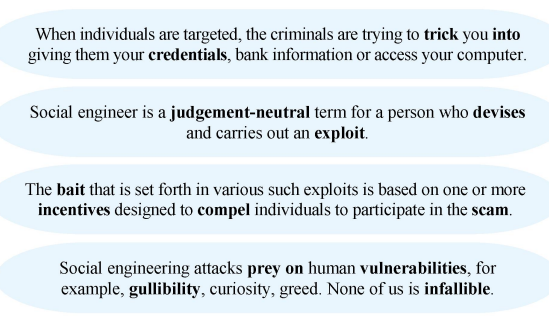
A cyber weapon is a type of malware or software tool that is designed to infiltrate, disrupt, or damage computer systems, networks, or electronic devices. These weapons are used by governments, military organizations, intelligence agencies, and other entities to conduct cyberattacks for various purposes, such as espionage, sabotage, or warfare.

Cyber weapons can take various forms, including viruses, worms, trojans, ransomware, and other types of malicious software. They can be used to steal sensitive information, disrupt critical infrastructure, or disable communication networks.

The development and use of cyber weapons have raised concerns about the potential for cyber warfare and the impact on national security, privacy, and civil liberties. Governments around the world are increasingly investing in cybersecurity measures to defend against cyber threats and protect their critical infrastructure from cyber attacks.









1. **Shouldering (shoulder surfing)**: g) It occurs when someone surreptitiously watches over your shoulder to nab valuable information.
2. **Pharming**: f) It redirects website traffic to fraudulent websites that distribute malware, collect personal data, sell counterfeit products, and perpetrate other scams.
3. **Phishing**: a) This tactic includes deceptive emails to steal information.
4. **Baiting**: c) It’s an online and physical social engineering attack that promises the victim some gain.
5. **Spear Phishing**: b) A spoofed email is used to carry out targeted attacks against individuals or businesses.
6. **Vishing**: h) It is voice solicitation over the phone (voice+phishing).
7. **Tailgating**: e) It relies on human trust to give the criminal physical access to a secure building or area.
8. **Rogue Antivirus**: d) Victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed.

****

**Protection against phishing:** a) Be cautious about all communications you receive. If it appears to be a suspicious one, do not respond. Delete it. d) Don’t enter personal information in a pop-up screen. Legitimate companies and organisations don’t ask for personal information via pop-up screens. e) Do not click on any links listed in the email message, and do not open any attachments contained in a suspicious email. f) Install a special spam filter on your email application and your web browser. These filters will not keep out all fraudulent messages, but they will reduce their number.

**Protection against vishing:** b) Don’t pick up the phone, simply let it go to voicemail. Caller IDs can be faked, which means you might not know who’s calling. Later decide whether to call back. c) Don’t press buttons or respond to prompts. Scammers often use these tricks to identify potential targets for more robocalls. And the record of your voice can be used to navigate voice-automated phone menus. g) Hang up. The moment you suspect it’s a fraudulent phone call, don’t feel obliged to carry on a polite conversation. Simply hang up and block the number. h) Verify the caller’s identity. If the person provides a call-back number, it may be part of the scam, so don’t use it.

**Protection against smishing**

1. **Be cautious of unsolicited text messages**: Just like with email phishing, be wary of any unsolicited text messages you receive. Scammers often use this method to reach out to potential victims.
2. **Don’t click on links in text messages**: If a text message includes a link, it’s best not to click on it unless you are sure it’s legitimate. Scammers often use these links to trick you into providing personal information.
3. **Verify the sender**: If you receive a text message from a number you don’t recognize, don’t respond. Instead, look up the number independently to see if it’s associated with a legitimate company.
4. **Install security software on your phone**: Just as you protect your computer with antivirus software, consider doing the same for your phone. There are many security apps available that can help protect against smishing.
5. **Report suspicious text messages**: If you receive a suspicious text message, report it to your mobile carrier and to the FTC in the US or the appropriate authority in your country.
6. **Don’t share personal information via text**: Legitimate companies will never ask for personal information such as your social security number, bank account details, or passwords via text message.

****

Encryption helps protect your online privacy by turning personal information into "for your eyes only" messages intended only for the parties that need them and no one else. You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.

Cybercrime is a global business, often run by multinational outfits. Many of the large-scale data breaches that you may have heard about in the news demonstrate that cybercriminals are often out to steal personal information for financial gain.

Encryption is designed to protect your data, but it can also be used against you. Targeted ransomware is a cybercrime that can impact organisations of all sizes, including government offices. Ransomware can also target individual computer users. Attackers deploy ransomware to encrypt the various devices, including computers and servers, of victims. The attackers often demand a ransom before they will provide a key to decrypt the encrypted data. The goal is to persuade victims to pay out as a way to recover access to their important files, data, video and images. Ransomware attacks against government agencies can shut down services, making it hard to get a permit, obtain a marriage licence, or pay a tax bill, for instance.

But ransomware attacks can also happen to you. Here are some tips to help protect your devices from ransomware attacks and the risk of having your data inaccessible.

Install and use trusted security software on all your devices, including your mobile phone. Keep your security software up to date. It can help protect your devices from cyberattacks. Update your operating system and other software. This can patch security vulnerabilities. Avoid reflexively opening email attachments. Why? Email is one of the principal methods for delivering ransomware. Be wary of any email attachment that advises you to enable macros to view its content. If you enable macros, macro malware can infect multiple files. Back up your data to an external hard drive. If you're the victim of a ransomware attack, you'll likely be able to restore your files once the malware has been cleaned up. Consider using cloud services. This can help mitigate a ransomware infection, since many cloud services retain previous versions of files, allowing you to "roll back" to the unencrypted form. Don't pay the ransom. You could pay a ransom in hopes of getting your files back, but you might not get them back. There's no guarantee the cybercriminal will release your data.

Encryption is essential to help protect your sensitive personal information. But in the case of ransomware attacks, it can be used against you.

When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other 1) **plain text** messages. The simplest method uses the 2) **symmetric** or **public key** system. Here, data is 3) **encrypted** using a secret key, and then both the encoded message and secret key are sent to the 4) **receiver** for decryption. But, if the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the 5) **asymmetric** or 6) **public key** system. In this case, every user has two keys: one public and one private. Senders 7) **use** the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient’s 8) **private key** will decode it.