# COMPUTER THREATS, SECURITY & ETHICS

## What is system security?

i. It refers to the measures and protocols to protect computer systems, networks, and data from unauthorized access, cyberattacks, and other potential threats.
ii. It includes various practices, technologies, and policies designed to ensure information confidentiality, integrity, and availability.

### Approaches in system security:

There are several approaches to system security, including:

1. Preventive Measures: Implementing measures such as firewalls, antivirus software, intrusion detection systems, and access control mechanisms to prevent unauthorized access and malicious activities.
2. Detective Measures: Using techniques like log monitoring, intrusion detection systems, and security audits to detect and respond to security breaches or suspicious activities in real-time.
3. Corrective Measures: Employing procedures for incident response, data recovery, and system restoration to mitigate the impact of security incidents and restore normal operations.
4. Proactive Measures: Conducting risk assessments, security assessments, and penetration testing to identify vulnerabilities and weaknesses in the system before they can be exploited by attackers.
5. Security Policies and Procedures: Establishing comprehensive security policies, procedures, and guidelines to govern the use of IT resources, define roles and responsibilities, and ensure compliance with security standards and regulations.
6. Security Awareness Training: Educating users and employees about security best practices, safe computing habits, and how to recognize and respond to security threats effectively.
7. Encryption and Authentication: Implementing encryption mechanisms to protect data in transit and at rest, as well as using strong authentication methods such as multi-factor authentication to verify the identity of users and devices.

By combining these approaches and continuously monitoring and updating security measures, organizations can strengthen their overall system security posture and reduce the risk of security breaches and incidents.

## How to conduct system security?

Conducting system security involves several steps:

1. Risk Assessment: Identify potential threats, vulnerabilities, and risks to your system and prioritize them based on their likelihood and potential impact.
2. Security Policy Development: Establish clear security policies and procedures that outline acceptable use, access control, password management, data protection, and incident response protocols.
3. Access Control: Implement access control mechanisms to restrict access to sensitive data and resources only to authorized users and devices. This may include user authentication, role-based access control, and network segmentation.
4. Security Awareness Training: Educate users and employees about security best practices, common threats, and how to recognize and respond to security incidents effectively.
5. Regular Software Updates and Patch Management: Keep all software, operating systems, and firmware up to date with the latest security patches and updates to mitigate known vulnerabilities.
6. Network Security: Implement firewalls, intrusion detection / prevention systems, and encryption to protect network traffic from unauthorized access, interception, and tampering.
7. Data Encryption: Encrypt sensitive data both in transit and at rest to prevent unauthorized access and protect confidentiality.
8. Monitoring and Logging: Implement logging and monitoring systems to track user activity, network traffic, and system events for signs of unauthorized access or suspicious behaviour.
9. Incident Response Plan: Develop and document a comprehensive incident response plan that outlines procedures for detecting, containing, and mitigating security incidents.
10. Regular Security Audits and Testing: Conduct regular security audits, vulnerability assessments, and penetration testing to identify and address weaknesses in your system before they can be exploited by attackers.

11. Backup and Disaster Recovery: Implement regular data backups and disaster recovery plans to ensure data integrity and availability in the event of a security breach or system failure.

By following these steps and continuously monitoring and updating security measures, you can effectively conduct system security to protect your organization's assets and data from cyber threats.

# Computer Security Threats:

It encompasses a wide range of risks and vulnerabilities that can compromise the confidentiality, integrity, and availability of computer systems, networks, and data. Here are some common computer security threats:

1. Malware: Malware is malicious software designed to infiltrate, damage, or disrupt computer systems and networks. Common types of malware include viruses, worms, Trojans, ransomware, spyware, and adware.
2. Phishing Attacks: Phishing attacks involve tricking users into providing sensitive information, such as usernames, passwords, or financial details, by masquerading as legitimate entities through email, social media, or messaging platforms.
3. Ransomware: Ransomware is a type of malware that encrypts files or locks down computer systems and demands a ransom payment from victims in exchange for decryption keys or system access.
4. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: DoS and DDoS attacks aim to disrupt the availability of computer systems, networks, or services by flooding them with excessive traffic or requests, causing them to become slow, unresponsive, or inaccessible.
5. Insider Threats: Insider threats involve individuals within an organization, such as employees, contractors, or partners, who misuse their privileges or access rights to steal sensitive information, sabotage systems, or compromise security controls.
6. Social Engineering: Social engineering attacks manipulate individuals into revealing confidential information or performing actions that compromise security, such as clicking on malicious links, downloading malware, or disclosing passwords.
7. Zero-Day Exploits: Zero-day exploits target previously unknown vulnerabilities in software, operating systems, or hardware components, which have not been patched or mitigated by vendors. Attackers exploit these vulnerabilities to gain unauthorized access or execute malicious code on target systems.
8. Man-in-the-Middle (MitM) Attacks: MitM attacks intercept and eavesdrop on communication between two parties, allowing attackers to intercept sensitive information, alter data, or impersonate legitimate entities without their knowledge.
9. Data Breaches: Data breaches involve unauthorized access to confidential or sensitive information stored on computer systems or networks. Breached data may include personal identifiable information (PII), financial records, intellectual property, or trade secrets.
10. Web Application Vulnerabilities: Web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR), allow attackers to manipulate or exploit weaknesses in web applications to gain unauthorized access or steal sensitive data.
11. IoT Security Risks: Internet of Things (IoT) devices, such as smart home appliances, wearable devices, and industrial sensors, may introduce security risks due to vulnerabilities in firmware, weak authentication, or lack of encryption, making them susceptible to exploitation by attackers.
12. Supply Chain Attacks: Supply chain attacks target third-party vendors, suppliers, or partners to compromise software, hardware, or services used by organizations, allowing attackers to gain unauthorized access, steal sensitive information, or distribute malware to target systems.

## Impact of system security risks:

System security risks can have significant impacts on individuals, organizations, and society as a whole. These impacts can affect various aspects of operations, finances, reputation, and trust. Here are some common impacts of system security risks:

1. Financial Losses: Security breaches and cyber attacks can result in financial losses due to theft of funds, fraudulent transactions, ransom payments, regulatory fines, legal fees, and costs associated with incident response, recovery, and remediation.
2. Data Breaches: Security breaches can lead to unauthorized access, theft, or exposure of sensitive or confidential data, including personal identifiable information (PII), financial records, intellectual property,

trade secrets, and proprietary information. Data breaches may result in reputational damage, loss of customer trust, and regulatory non-compliance.

3. Operational Disruptions: Security incidents and malware infections can disrupt business operations, interrupting critical services, workflows, and productivity. System downtime, network outages, and service disruptions may lead to revenue losses, customer dissatisfaction, and operational inefficiencies.
4. Reputation Damage: Security breaches and data breaches can damage an organization's reputation, brand image, and credibility among customers, partners, investors, and stakeholders. Negative publicity, media coverage, and public scrutiny may erode trust and confidence in the organization's ability to protect sensitive information and maintain security.
5. Regulatory Compliance: Security risks may result in non-compliance with data protection laws, industry regulations, and privacy standards, exposing organizations to regulatory fines, penalties, and legal liabilities. Failure to protect sensitive data and secure computer systems may result in legal consequences and reputational harm.
6. Intellectual Property Theft: Security breaches can lead to theft or unauthorized access to intellectual property, including trade secrets, proprietary algorithms, software code, and research data. Intellectual property theft may undermine innovation, competitiveness, and market advantage, leading to financial losses and economic harm.
7. Identity Theft and Fraud: Security incidents, such as phishing attacks, malware infections, or data breaches, can result in identity theft, financial fraud, and account takeover. Cybercriminals may use stolen credentials, personal information, or financial data to commit fraud, impersonate individuals, or engage in fraudulent activities.
8. Disruption of Critical Infrastructure: Security risks targeting critical infrastructure, such as energy, transportation, healthcare, and finance, can have severe consequences on public safety, national security, and economic stability. Cyber attacks on critical infrastructure may disrupt essential services, cause physical damage, or pose risks to public health and safety.
9. Supply Chain Disruptions: Security breaches within supply chains and vendor ecosystems can impact the reliability, availability, and integrity of products, services, and operations. Cyber attacks targeting suppliers, partners, or third-party vendors may disrupt supply chains, compromise product quality, and increase operational risks.
10. Social and Psychological Impact: Security incidents and data breaches can have social and psychological impacts on individuals affected by cyber attacks, such as stress, anxiety, loss of privacy, and feelings of insecurity. Victims of cybercrime may experience emotional distress, financial hardship, and trust issues related to their online security and privacy.

Overall, the impacts of system security risks are multi-layered and can have far-reaching consequences on individuals, organizations, and society. By recognizing and addressing these risks proactively, organizations can mitigate their impact and strengthen their resilience to cyber threats and security breaches.

**CAUSES OF LOSS OR DAMAGE OF A COMPUTER OR ITS INFORMATION:**

1. Malware Infections: Downloading and executing malicious software, such as viruses, worms, Trojans, ransomware, or spyware, can compromise the security and integrity of a computer system, leading to data loss, system corruption, or unauthorized access.
2. Phishing Attacks: Falling victim to phishing emails, social engineering tactics, or fraudulent websites can result in users disclosing sensitive information, such as usernames, passwords, or financial details, which can be used for identity theft, fraud, or unauthorized access to computer systems.
3. Hardware Failure: Hardware components, such as hard drives, solid-state drives (SSDs), memory modules, or power supplies, can fail due to mechanical, electrical, or manufacturing defects, resulting in data loss, system crashes, or hardware damage.
4. Software Bugs or Glitches: Software applications or operating systems may contain bugs, vulnerabilities, or coding errors that could lead to system crashes, data corruption, or unexpected behavior, especially if exploited by attackers or malware.

5. Natural Disasters: Natural disasters, such as floods, earthquakes, hurricanes, tornadoes, fires, or power outages, can damage computer hardware, data storage devices, or network infrastructure, resulting in data loss, system downtime, or physical damage to computers and IT assets.
6. Human Errors: Accidental actions or mistakes by users, administrators, or IT personnel, such as deleting critical files, misconfiguring systems, or mishandling hardware, can cause data loss, system failures, or security breaches.
7. Physical Theft or Loss: Theft or loss of computers, laptops, mobile devices, or storage media containing sensitive data can result in unauthorized access, data breaches, or identity theft, especially if the devices are not properly secured or encrypted.
8. Cyber Attacks: Deliberate cyber attacks, such as distributed denial-of-service (DDoS) attacks, ransomware attacks, data breaches, or insider threats, can disrupt computer systems, compromise data integrity, or steal sensitive information, causing financial losses or reputational damage.
9. Software or Firmware Updates: Installing faulty or incompatible software updates, device drivers, or firmware upgrades can lead to system instability, compatibility issues, or hardware malfunctions, resulting in data loss or damage to computers and peripherals.
10. Unauthorized Access: Unauthorized access to computer systems, networks, or data by hackers, insiders, or malicious actors can result in data breaches, information theft, or system compromise, leading to financial losses, legal liabilities, or regulatory penalties.

To reduce risks of loss or damage to computers and information, individuals and organizations should implement proactive measures, such as regular data backups, security awareness training, software updates, disaster recovery plans, access controls, encryption, and physical security measures. Additionally, adopting cybersecurity best practices and adhering to industry standards can help safeguard computer systems and mitigate the impact of potential threats and vulnerabilities.

## Identify a computer that has been infected with malware

Identifying a computer that has been infected with malware can be challenging, as malware often operates stealthily to avoid detection and removal. However, here are some common signs and symptoms that may indicate a computer is infected with malware:

1. Slow Performance: Malware can consume system resources, such as CPU, memory, or disk space, causing the computer to slow down or become unresponsive, even during normal tasks.
2. Unexpected Pop-ups: Malware may generate intrusive pop-up windows, advertisements, or browser redirects, even when not browsing the internet, indicating the presence of adware or potentially unwanted programs (PUPs).
3. Unexplained Network Activity: Malware may communicate with remote servers or command-and-control (C&C) infrastructure over the network, leading to unusual network traffic, data transfers, or connections, as observed in network monitoring tools or firewalls.
4. Changed Browser Settings: Malware may modify browser settings, such as homepage, search engine, or default tabs, without the user's consent, redirecting web traffic to malicious or phishing websites.
5. Disabled Security Software: Malware may attempt to disable or circumvent antivirus software, firewalls, or security features installed on the computer to evade detection and removal, leaving the system vulnerable to further infections.
6. Unexplained File Changes: Malware may modify, delete, or encrypt files and data stored on the computer, resulting in file corruption, loss of data, or ransomware encryption, as observed in file integrity checks or backup audits.
7. Unexpected System Crashes: Malware-infected computers may experience frequent system crashes, blue screen errors, or application failures due to software conflicts, memory leaks, or system instability caused by malware infections.
8. High CPU or Disk Usage: Malware processes running in the background may consume excessive CPU or disk resources, as observed in task manager or system monitoring utilities, indicating malicious activity or crypto-mining malware.
9. Strange Behavior: Malware may exhibit unusual behavior, such as creating new files or folders, modifying system settings, or executing commands, which can be observed through system logs, process monitoring, or behavior analysis tools.

10. Antivirus Alerts: Antivirus software or security tools may detect and alert users to the presence of malware infections, suspicious files, or malicious activities during real-time scanning, on-demand scans, or system scans.

If you suspect that your computer may be infected with malware, it's important to take immediate action to quarantine, isolate, and remove the malware using reputable antivirus software, malware removal tools, or professional assistance from cybersecurity experts. Additionally, restoring the computer from a clean backup, performing a system restore, or reinstalling the operating system may be necessary to fully remove the malware and restore the integrity of the system.

## Technologies for securing computer systems:

Several technologies can be used to secure computer systems and protect them from various cyber threats and vulnerabilities. They include use of:

1. Firewalls: Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between internal networks and the internet, preventing unauthorized access and filtering out potentially malicious traffic.
2. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): IDS and IPS are security solutions that monitor network or system activities for signs of unauthorized access, intrusions, or malicious behavior. IDS detects suspicious activities and generates alerts, while IPS can actively block or prevent malicious activities in real-time.
3. Antivirus Software: Antivirus software is designed to detect, prevent, and remove malware infections, including viruses, worms, Trojans, ransomware, and spyware. It scans files, emails, and web traffic for known malware signatures or behavioral patterns, quarantining or removing infected files to protect the system.
4. End-point Security Solutions: End-point security solutions, such as end-point protection platforms (EPP) and end-point detection and response (EDR) systems, provide comprehensive security for end-point devices, such as desktops, laptops, smartphones, and servers. They include features like antivirus, firewall, device control, encryption, and threat detection capabilities.
5. Encryption Technologies: Encryption technologies, such as encryption algorithms, cryptographic protocols, and secure communication channels (e.g., SSL / TLS), are used to encrypt sensitive data both at rest and in transit, protecting it from unauthorized access or interception.
6. Access Control Systems: Access control systems manage user authentication and authorization, enforcing least privilege principles to restrict access to sensitive resources based on user roles and permissions. They include technologies like access control lists (ACLs), role-based access control (RBAC), and multi-factor authentication (MFA).
7. Security Information and Event Management (SIEM): SIEM solutions collect, analyze, and correlates security event data from various sources, such as network devices, servers, and applications, to detect security incidents, threats, and compliance violations. They provide real-time monitoring, alerting, and reporting capabilities for security operations and incident response.
8. Patch Management Systems: Patch management systems automate the process of identifying, prioritizing, and deploying security patches and updates for software applications, operating systems, and firmware. They help mitigate known vulnerabilities and reduce the risk of exploitation by attackers.
9. Data Loss Prevention (DLP) Solutions: DLP solutions monitor and control the movement of sensitive data across networks, endpoints, and storage devices, preventing unauthorized access, leakage, or exfiltration of confidential information. They use content inspection, encryption, and policy enforcement to protect data assets.
10. Backup and Disaster Recovery Solutions: Backup and disaster recovery solutions create and maintain copies of critical data and system configurations, allowing organizations to recover quickly from data loss, corruption, or system failures caused by cyber attacks, natural disasters, or human errors.

By deploying a combination of these technologies and implementing security best practices, organizations can strengthen the security posture of their computer systems, protect sensitive information, and mitigate the risks of cyber threats and vulnerabilities.

## Computer security risks and attacks:

Computer security risks and attacks come in various forms, targeting different aspects of computer systems, networks, and data. Here are some common types of computer security risks and attacks:

1. Malware: Malware is malicious software designed to infiltrate, damage, or disrupt computer systems and networks. Common types of malware include viruses, worms, Trojans, ransomware, spyware, and adware.
2. Phishing: Phishing attacks involve tricking users into providing sensitive information, such as usernames, passwords, or financial details, by masquerading as legitimate entities through email, social media, or messaging platforms.
3. Ransomware: Ransomware is a type of malware that encrypts files or locks down computer systems and demands a ransom payment from victims in exchange for decryption keys or system access.
4. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks: DoS and DDoS attacks aim to disrupt the availability of computer systems, networks, or services by flooding them with excessive traffic or requests, causing them to become slow, unresponsive, or inaccessible.
5. Insider Threats: Insider threats involve individuals within an organization, such as employees, contractors, or partners, who misuse their privileges or access rights to steal sensitive information, sabotage systems, or compromise security controls.
6. Social Engineering: Social engineering attacks manipulate individuals into revealing confidential information or performing actions that compromise security, such as clicking on malicious links, downloading malware, or disclosing passwords.
7. Zero-Day Exploits: Zero-day exploits target previously unknown vulnerabilities in software, operating systems, or hardware components, which have not been patched or mitigated by vendors. Attackers exploit these vulnerabilities to gain unauthorized access or execute malicious code on target systems.
8. Man-in-the-Middle (MitM) Attacks: MitM attacks intercept and eavesdrop on communication between two parties, allowing attackers to intercept sensitive information, alter data, or impersonate legitimate entities without their knowledge.
9. Data Breaches: Data breaches involve unauthorized access to confidential or sensitive information stored on computer systems or networks. Breached data may include personal identifiable information (PII), financial records, intellectual property, or trade secrets.
10. Web Application Vulnerabilities: Web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR), allow attackers to manipulate or exploit weaknesses in web applications to gain unauthorized access or steal sensitive data.
11. IoT Security Risks: Internet of Things (IoT) devices, such as smart home appliances, wearable devices, and industrial sensors, may introduce security risks due to vulnerabilities in firmware, weak authentication, or lack of encryption, making them susceptible to exploitation by attackers.
12. Supply Chain Attacks: Supply chain attacks target third-party vendors, suppliers, or partners to compromise software, hardware, or services used by organizations, allowing attackers to gain unauthorized access, steal sensitive information, or distribute malware to target systems.

    These are just some examples of computer security risks and attacks that pose threats to individuals, businesses, and organizations. Understanding these risks and implementing appropriate security measures is essential for mitigating their impact and protecting against cyber threats and vulnerabilities.

# Approaches for securing a computer system:

1. Use of Passwords:
   i. Implement password policies: Establish password policies that mandate regular password changes, password length, complexity requirements, and account lockout thresholds.
   ii. Use multi-factor authentication (MFA): Enhance security by implementing MFA, requiring users to provide additional verification factors, such as biometrics or one-time codes, in addition to passwords.
   iii. Require strong passwords: Enforce the use of complex passwords that include a combination of uppercase and lowercase letters, numbers, and special characters.
2. Use of Biometrics:
   i. Implement biometric authentication: Use biometric authentication methods, such as fingerprint scans, iris scans, or facial recognition, to verify the identity of users and grant access to computer systems.
   ii. Integrate with access control systems: Integrate biometric authentication systems with access control mechanisms to enforce user authentication and authorization based on biometric data.

3. Firewalls:
    i. Deploy network firewalls: Install network firewalls at the perimeter of the network to monitor and control incoming and outgoing traffic, blocking unauthorized access and filtering out malicious content.
    ii. Configure firewall rules: Define firewall rules to allow or deny specific types of traffic based on source and destination IP addresses, ports, protocols, and applications.
    iii. Enable intrusion prevention features: Enable intrusion prevention features in firewalls to detect and block known and emerging threats, such as malware, exploits, and suspicious network activity.
4. Antivirus Software:
    i. Install reputable antivirus software: Deploy antivirus software on computer systems to detect, prevent, and remove malware infections, including viruses, worms, Trojans, ransomware, and spyware.
    ii. Keep antivirus definitions up to date: Ensure antivirus software is regularly updated with the latest virus definitions and security patches to detect and mitigate new and emerging threats.
5. Honey-pots:
    i. Deploy honey-pots: Set up honey-pots, which are decoy systems or network resources designed to attract and deceive attackers, allowing security teams to monitor and analyze their activities.
    ii. Gather threat intelligence: Collect information about attackers' tactics, techniques, and procedures (TTPs) by monitoring honeypots for unauthorized access attempts, malware infections, or reconnaissance activities.
6. Intrusion Detection Programs:
    i. Deploy intrusion detection systems (IDS): Install IDS solutions to monitor network or system activities for signs of unauthorized access, intrusions, or malicious behavior, generating alerts or notifications for security incidents.
    ii. Configure IDS rules: Customize IDS rules to detect specific types of threats, such as known attack signatures, anomalous behaviors, or suspicious network traffic patterns.

By implementing these security approaches and best practices, organizations can strengthen the security posture of their computer systems, protect sensitive data, and mitigate the risks of cyber threats and attacks. Additionally, regular security audits, vulnerability assessments, and penetration testing can help identify and address security weaknesses and gaps in the system's defenses.

## Secure a computer system:

Securing a computer system both on the network and off the network requires a multi-layered approach that addresses various aspects of security, including access control, network security, end-point security, data protection, and user awareness. Here are steps to secure a computer system in both scenarios:

### On the Network:

1. Implement Network Segmentation:
    i. Divide the network into separate segments or VLANs to isolate critical systems and sensitive data from less secure areas.
    ii. Use firewalls and access control lists (ACLs) to control traffic flow between network segments and enforce security policies.
2. Deploy Firewalls and Intrusion Detection / Prevention Systems:
    i. Install network firewalls at the network perimeter and between network segments to monitor and filter incoming and outgoing traffic.
    ii. Deploy intrusion detection and prevention systems (IDS/IPS) to detect and block malicious activities, such as unauthorized access attempts or network attacks.
3. Enable Encryption:
    i. Encrypt network traffic using secure protocols, such as SSL/TLS, to protect data confidentiality and integrity when transmitted over the network.
    ii. Implement Virtual Private Networks (VPNs) for secure remote access to the network, encrypting data between end-points and the corporate network.
4. Enforce Access Controls:
    i. Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to verify the identity of users accessing the network or sensitive resources.

ii. Use network access control (NAC) solutions to enforce security policies and restrict access based on user roles, device health, and compliance status.

5. Regularly Update and Patch Systems:
   I. Keep network devices, servers, and endpoints up to date with the latest security patches and updates to mitigate known vulnerabilities and reduce the risk of exploitation by attackers.

## Off the Network:

1. End-point Security:
   i. Install endpoint protection software, including antivirus, anti-malware, and host-based firewalls, to secure individual devices and prevent malware infections.
   ii. Configure endpoint security solutions to perform regular scans, monitor system activities, and block suspicious behavior or unauthorized access attempts.
2. Implement Data Encryption:
   i. Encrypt data stored on local drives, removable media, and cloud storage to protect sensitive information from unauthorized access or theft.
   ii. Use encryption technologies, such as BitLocker (Windows) or FileVault (macOS), to encrypt disk volumes and folders containing confidential data.
3. Enforce Strong Password Policies:
   i. Implement strong password policies for user accounts, requiring complex passwords, regular password changes, and multi-factor authentication where possible.
   ii. Encourage users to use password managers to generate and securely store complex passwords for different accounts.
4. Secure Remote Access:
   i. Secure remote access to the computer system using VPNs or remote desktop solutions with strong encryption and authentication mechanisms.
   ii. Implement remote access control policies to limit access to authorized users and devices, logging remote access sessions for audit purposes.
5. Regular Backups:
   i. Perform regular backups of critical data and system configurations to external storage devices or cloud-based backup services.
   ii. Test backup and recovery procedures regularly to ensure data integrity and the ability to restore operations in the event of data loss or system failure.
6. User Training and Awareness:
   i. Provide security awareness training to users to educate them about common threats, safe computing practices, and security policies.
   ii. Encourage users to be vigilant against phishing emails, suspicious links, and social engineering tactics that could compromise their security both on and off the network.

By implementing these security measures both on the network and off the network, organizations can enhance the overall security posture of their computer systems, protect against various cyber threats, and minimize the risk of unauthorized access, data breaches, and system compromises.

# Moral Principles (code of conduct) while using ICT tools

Establishing a code of conduct to regulate the use of Information and Communication Technologies (ICTs) within a community involves defining moral principles and ethical guidelines to govern the responsible and ethical use of technology. They include:

1. Respect for Privacy:
   i. Respect the privacy rights of individuals by not accessing or sharing their personal information without their consent.
   ii. Safeguard sensitive data and confidential communications from unauthorized access or disclosure.
2. Integrity and Honesty:
   i. Conduct oneself with integrity and honesty in all digital interactions, communications, and transactions.
   ii. Avoid spreading misinformation, false rumors, or deceptive content online.
3. Responsible Use of Resources:

i. Use ICT resources, such as network bandwidth, storage, and computing resources, responsibly and efficiently.
ii. Avoid excessive or unnecessary consumption of resources that may impact system performance or availability for others.

4. Respect for Intellectual Property:
   i. Respect intellectual property rights, copyrights, and licenses when creating, sharing, or using digital content, software, or information.
   ii. Avoid unauthorized copying, distribution, or modification of copyrighted materials without permission.
5. Cybersecurity and Safety:
   i. Protect computer systems, networks, and data from cyber threats and vulnerabilities by implementing security measures and best practices.
   ii. Report security incidents, suspicious activities, or cyber threats promptly to relevant authorities or IT support personnel.
6. Digital Citizenship:
   i. Practice responsible digital citizenship by promoting positive and constructive online behavior, respecting diverse viewpoints, and fostering a culture of mutual respect and civility.
   ii. Avoid engaging in cyberbullying, harassment, or online abuse that may harm others or violate their rights.
7. Accessibility and Inclusivity:
   i. Ensure that ICT resources, services, and digital content are accessible to all individuals, including those with disabilities or special needs.
   ii. Design and develop ICT solutions with accessibility features and usability enhancements to accommodate diverse users and ensure inclusivity.
8. Environmental Sustainability:
   i. Consider the environmental impact of ICT usage and adopt sustainable practices, such as energy-efficient computing, electronic waste recycling, and eco-friendly technology solutions.
   ii. Minimize the carbon footprint and environmental impact of ICT infrastructure and operations.
9. Professionalism and Ethical Conduct:
   i. Uphold professional standards, ethics, and codes of conduct in the use of ICTs, especially in professional or organizational contexts.
   ii. Avoid conflicts of interest, unethical behavior, or misuse of technology resources for personal gain or unethical purposes.
10. Continuous Learning and Improvement:
    i. Stay informed about emerging technologies, digital trends, and best practices in ICT usage through ongoing education, training, and professional development.
    ii. Foster a culture of continuous learning, collaboration, and innovation to adapt to evolving ICT environments and challenges.

By adhering to these moral principles and ethical guidelines, members of the community can promote responsible, ethical, and respectful use of ICTs, fostering a positive digital culture and contributing to the well-being and prosperity of society.

# Computer Viruses

Computer viruses are malicious programs designed to replicate themselves and infect other computer systems.

## Symptoms of computers with computer viruses:

Computers infected with viruses can exhibit a range of symptoms, depending on the type of virus and its intended purpose. Some common symptoms include:

1. Sluggish performance: The infected computer may run noticeably slower than usual, taking longer to boot up, launch programs, or perform tasks.
2. Frequent crashes or freezes: Virus-infected systems may experience more frequent crashes or freezes, as the virus interferes with system processes and stability.
3. Unexplained changes to files or settings: Viruses may modify or delete files, change system settings, or create new files without the user's knowledge.
4. Pop-up windows: Infected computers may display an increased number of pop-up windows, often containing advertisements or warnings about fake security threats.

5. Strange behavior: Users may notice strange behavior such as programs launching or closing unexpectedly, mouse movements without user input, or the cursor moving erratically.
6. Unusual network activity: Some viruses spread through networks and may cause increased network activity on infected computers, such as excessive data usage or attempts to connect to unfamiliar servers.
7. Missing files or disk space: Viruses may delete or hide files, resulting in missing data or a sudden decrease in available disk space.
8. Security warnings: Antivirus software or the operating system may display warnings about the presence of malware or security threats on the system.
9. If you suspect your computer may be infected with a virus, it's important to run a thorough antivirus scan and take appropriate measures to remove the malware and mitigate any damage it may have caused.

## How Computer viruses can be transmitted?

1. Through Email attachments: Viruses can spread through infected email attachments. When a user opens an attachment containing a virus, the virus can execute and infect the user's computer.
2. Through downloaded files: Viruses can be embedded in files downloaded from the internet. This includes software downloads, documents, images, or any other type of file. When the infected file is opened or executed, the virus can infect the user's computer.
3. Through infected removable media: Viruses can spread through USB flash drives, external hard drives, CDs, and other removable media. When an infected device is connected to a computer, the virus can spread to the computer and potentially to other connected devices.
4. Through malicious websites: Visiting malicious websites or clicking on malicious links can lead to virus infections. Some websites may automatically download and execute malware onto the visitor's computer without their knowledge.
5. Through networks: Viruses can spread through local area networks (LANs) or the internet. They can exploit vulnerabilities in network protocols or use social engineering tactics to trick users into downloading and executing malware.
6. Through file sharing: Viruses can spread through peer-to-peer (P2P) file-sharing networks or file-sharing services. Infected files shared through these networks can infect other users who download and open them.
7. Exploiting software vulnerabilities: Viruses can exploit vulnerabilities in operating systems, applications, or software plugins to infect computers. This can occur through methods such as drive-by downloads or exploiting unpatched security flaws.

   To minimize the risk of virus transmission, users should exercise caution when opening email attachments, downloading files from the internet, connecting removable media to their computers, visiting websites, and sharing files over networks. Additionally, keeping antivirus software up-to-date and regularly scanning for malware can help detect and prevent virus infections.

# Dangers of computer viruses

Computer viruses pose various dangers to both individuals and organizations. Some of the key dangers include:

1. May lead to data Loss or Corruption: Viruses can delete, modify, or corrupt files and data stored on infected computers. This can result in permanent loss of valuable information, including personal documents, photos, videos, or important business data.
2. May lead to identity Theft: Certain viruses, such as keyloggers or spyware, are designed to steal sensitive information such as usernames, passwords, credit card numbers, and other personal or financial data. This information can be used for identity theft, fraud, or other malicious purposes.
3. May lead to financial Loss: Viruses can lead to financial losses for individuals and businesses. They may cause disruptions to business operations, resulting in downtime, lost productivity, and revenue loss. Additionally, some viruses may initiate unauthorized transactions or redirect users to fraudulent websites, leading to financial losses.
4. May lead to privacy Invasion: Viruses that collect personal information or grant remote access to attackers can invade users' privacy. This can lead to surveillance, monitoring of online activities, or unauthorized access to personal or sensitive information.

5. May lead to system Instability: Viruses can compromise the stability and performance of infected computers, leading to system crashes, freezes, and other technical issues. This can disrupt normal operations and hinder users from completing tasks effectively.
6. May lead to propagation: Viruses are designed to spread and infect other computers, networks, or devices. This can lead to widespread outbreaks, affecting a large number of users and organizations. Additionally, infected devices may serve as vectors for spreading the virus to other connected systems.
7. May lead to legal Consequences: In some cases, virus infections may result in legal consequences, especially if they lead to data breaches, privacy violations, or financial losses. Organizations may face regulatory fines, lawsuits, or other legal actions for failing to adequately protect against viruses and malware.

   To mitigate these dangers, it's essential for users and organizations to implement robust cybersecurity measures, including using reputable antivirus software, regularly updating software and operating systems, practicing safe browsing habits, and educating users about the risks of viruses and malware. Additionally, implementing strong access controls, data encryption, and security best practices can help minimize the impact of virus infections.

## Controlling against computer viruses

Controlling against computer viruses requires a multi-layered approach that combines preventive measures, proactive monitoring, and reactive response strategies. Here's a comprehensive guide to help control against computer viruses:

1. By installing Antivirus Software: Use reputable antivirus software with real-time scanning capabilities to detect and remove viruses before they can cause harm. Ensure the antivirus software is regularly updated to protect against the latest threats.
2. By Keeping Software Updated: Regularly update your operating system, applications, web browsers, and plugins to patch known security vulnerabilities. Enable automatic updates whenever possible to ensure timely protection against emerging threats.
3. By Using Firewalls: Enable firewalls on your computer and network devices to monitor and control incoming and outgoing network traffic. Firewalls help block unauthorized access and prevent malicious software from communicating with remote servers.
4. By Exercising Caution Online: Be cautious when downloading files, opening email attachments, or clicking on links from unknown or suspicious sources. Avoid visiting untrusted websites or clicking on pop-up advertisements, as they may contain malicious code.
5. By Enabling Email Filtering: Use email filtering and spam detection mechanisms to block phishing emails, malicious attachments, and suspicious links. Educate users about the dangers of phishing scams and encourage them to verify the legitimacy of emails before taking action.
6. By Implementing User Education: Educate users about safe computing practices, such as avoiding downloading pirated software, using strong and unique passwords, and recognizing common signs of malware infections. Provide regular training and awareness programs to reinforce security best practices.
7. Through Securing Network Access: Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to control access to sensitive systems and data. Use virtual private networks (VPNs) to encrypt network traffic and secure remote connections.
8. By Backing up Data Regularly: Implement regular data backup procedures to create copies of critical files and data. Store backups in secure locations, both onsite and offsite, to ensure data can be restored in the event of a virus infection or data loss incident.
9. By Monitoring System Activity: Monitor network and system activity for signs of unusual behavior, such as unauthorized access attempts, unusual file modifications, or spikes in network traffic. Use intrusion detection systems (IDS) and security information and event management (SIEM) tools to detect and respond to security incidents in real-time.
10. By Developing Incident Response Plans: Develop and maintain incident response plans to outline procedures for responding to virus infections and other security incidents. Define roles and responsibilities, establish communication channels, and conduct regular drills to test the effectiveness of the response procedures.

By implementing these preventive, detective, and responsive measures, you can effectively control against computer viruses and minimize the risk of security breaches and data loss. Remember that cybersecurity is an ongoing process, and it requires continuous vigilance and adaptation to address evolving threats.

If you suspect that your computer is infected with a virus, it's important to run a thorough antivirus scan as soon as possible to identify and remove the malicious software.
Additionally, consider disconnecting from the internet to prevent further spread of the virus and seek assistance from IT professionals if needed.

## Examples of computer viruses

1. Email Attachment Viruses:
- ILOVEYOU: This virus spread via email as an attachment with the message "ILOVEYOU". Opening the attachment executed the virus, which then spread to the user's contacts.
2. Macro Viruses:
   Melissa: Melissa was a macro virus that infected Microsoft Word documents. When an infected document was opened, the virus replicated itself and sent copies to the user's contacts.
3. File Infectors:
- CIH/Chernobyl: Also known as the Chernobyl virus, CIH infected executable files on Windows systems. When an infected file was executed, CIH could overwrite the system BIOS, rendering the computer inoperable.
4. Boot Sector Viruses:
   Stoned: Stoned was one of the earliest boot sector viruses, infecting the master boot record (MBR) of floppy disks and hard drives. When an infected disk was booted, the virus loaded into memory and could infect other disks.
5. Network Worms:
- CodeRed: CodeRed was a worm that exploited a vulnerability in Microsoft IIS servers. It spreads by scanning for vulnerable servers on the internet and infecting them.
6. USB Worms:
   Conficker: Conficker was a worm that spread through removable drives and network shares. It exploited vulnerabilities in Windows to infect computers and create a botnet.
7. Fileless Viruses:
- Poweliks: Poweliks was a fileless malware that resided in the Windows registry. It did not create files on disk, making it difficult to detect and remove.
8. Polymorphic Viruses:
   Storm Worm: Storm Worm was a polymorphic virus that constantly changed its code to evade detection. It spreads via email as a malicious attachment or link.
9. Multipartite Viruses:
- Tequila: Tequila was a multipartite virus that could infect both boot sectors and executable files. It spread through infected floppy disks and email attachments.

These examples illustrate the diverse methods that viruses employ to infect computer systems and propagate through networks. Each type of virus presents unique challenges for detection and removal, requiring proactive security measures to mitigate the risk of infection.

## Other forms of malware

Malware, short for malicious software, encompasses various types of malicious programs designed to disrupt, damage, or gain unauthorized access to computer systems and data. In addition to computer viruses, here are some other common forms of malware:

1. Trojans: Trojans disguise themselves as legitimate software to trick users into downloading and installing them. Once installed, they can perform various malicious actions, such as stealing sensitive information, creating backdoors for remote access, or downloading additional malware.
2. Ransomware: Ransomware encrypts files or locks users out of their systems, demanding a ransom payment in exchange for restoring access. It can spread through email attachments, malicious links, or exploit kits, and can cause significant financial losses and data breaches.
3. Spyware: Spyware secretly monitors users' activities and collects sensitive information, such as keystrokes, browsing habits, login credentials, and personal data. It can be used for identity theft, espionage, or targeted advertising.

4. Adware: Adware displays unwanted advertisements, pop-ups, or redirects to users' screens, often generating revenue for the malware authors through pay-per-click advertising. While not inherently malicious, adware can degrade system performance and compromise user privacy.
5. Worms: Worms are self-replicating malware that spread across networks by exploiting security vulnerabilities or leveraging social engineering tactics. They can infect multiple computers and devices, causing network congestion, data loss, and disruption of services.
6. Botnets: Botnets are networks of compromised computers, or "bots," controlled by a central command-and-control server. Botnets can be used for various malicious activities, such as launching distributed denial-of-service (DDoS) attacks, sending spam emails, or mining cryptocurrencies.
7. Rootkits: Rootkits are stealthy malware designed to conceal their presence and gain privileged access to system resources. They often exploit vulnerabilities in the operating system kernel or firmware to evade detection by antivirus software and security mechanisms.
8. Keyloggers: Keyloggers record users' keystrokes, mouse movements, and screen activity to capture sensitive information, such as passwords, credit card numbers, and personal messages. They can be deployed as standalone programs or as part of other malware payloads.
9. Remote Access Trojans (RATs): RATs provide attackers with remote access and control over infected systems, allowing them to execute commands, steal data, or surveil users' activities covertly. RATs are commonly used for espionage, data theft, or cyber-espionage operations.
10. Fileless Malware: Fileless malware operates directly in memory, without leaving traces on disk, making it harder to detect and remove. It leverages legitimate system tools and processes to execute malicious code, evade detection, and persist on infected systems.

These are just a few examples of the diverse range of malware threats that users and organizations face today. To defend against malware attacks, it's essential to implement comprehensive cybersecurity measures, including robust antivirus software, regular software updates, user education, network segmentation, and proactive threat hunting.

**Scenario:**

**You are a cybersecurity consultant invited to give a presentation to a group of new employees at a financial institution. The management is concerned about the increasing cases of cyber threats, unethical use of company systems, and poor security practices among staff.**

**Task**

**Write a presentation on Computer Threats, Security, and Ethics to educate the employees.**