# Syllabus
## Subject: - Cyber Security
## BBA /B.Com I Year

| UNIT No. | TOPICS |
|---|---|
| 1 | Introduction to Cyber security:<br>Definition, scope and importance of cyber security<br>Common cyber threats: phishing, malware, ransomware, social engineering<br>History and evolution of cyber threats<br>Cyber security in daily life (online shopping, banking, social media) |
| 2 | Digital Hygiene Practices:<br>Good practices for device and data protection<br>Strong password management and multi-factor authentication<br>Safe browsing habits and software updates<br>Avoiding harmful downloads and unauthorized links |
| 3 | Legal and Ethical Aspects of Cybersecurity:<br>Overview of Indian IT Act and relevant laws<br>Cybercrime reporting in India<br>Digital rights and responsibilities<br>Ethical use of digital content and resources. |
| 4 | Cybersecurity Tools and Software Awareness:<br>Introduction to antivirus, firewalls, anti-malware tools<br>Browser extensions for safety (ad blockers, HTTPS Everywhere)<br>Safe use of public Wi-Fi and VPNS<br>Simple threat detection mechanisms |
| 5 | Indian Knowledge System (IKS) and Digital Ethics:<br>Ethical responsibility in digital behavior based on Indian philosophical traditions<br>Niti and Dharma in online conduct<br>Ancient Indian communication ethics and their relevance today<br>Data integrity and responsibility from Indian Knowledge Lens |

# Introduction to Cyber security

## Unit – 1 : Definition, scope and importance of cyber security

### Definition

At its core, cyber security can be defined as the combination of methods, technologies, and practices designed to protect computer systems, networks, programs, and data from digital attacks. It is a multi-layered defense strategy that can be broken down into three critical aspects:

- **Confidentiality:** Preventing the disclosure of information to unauthorized individuals.
- **Integrity:** Ensuring that information remains accurate and is not tampered with by unauthorized parties.
- **Availability:** Making sure that authorized users can access the information and systems when needed.

### Scope

The scope of cyber security extends across multiple fields, from individual devices to large-scale global networks. Key areas include:

- **Network Security:** Safeguarding the computer network and its infrastructure from unauthorized access, misuse, or theft. This involves using firewalls, intrusion detection systems, and encryption.
- **Application Security:** Protecting software and devices from vulnerabilities that hackers could exploit. This involves secure coding practices and regular updates.
- **Cloud Security:** Protecting data and applications hosted in the cloud. This is a crucial area as more businesses shift their data storage and operations to cloud services.
- **Endpoint Security:** Securing end-user devices such as desktops, laptops, smartphones, and tablets, which often serve as entry points for cybercriminals.
- **Information Security (InfoSec):** A broader category that focuses on the protection of information assets, including data at rest and in transit, and involves tools like encryption and access controls.

- **Operational Technology (OT) Security:** Protecting physical processes controlled by technology, including critical infrastructure like energy grids, manufacturing systems, and water purification facilities.
- **Mobile and Internet of Things (IoT) Security:** A growing area that addresses the security vulnerabilities of the expanding network of smart and connected devices.
- **Disaster Recovery and Business Continuity:** Developing plans and procedures for an organization to restore operations and data quickly after a cyber incident.

## Importance

Cyber security is more important than ever due to our increased reliance on technology and the rise in the sophistication of cyber threats.

- **Protects sensitive information:** Both individuals and businesses store and transmit vast amounts of sensitive data, including financial records, personal details, and intellectual property. A robust cyber security strategy is essential to prevent data breaches that can lead to identity theft and financial fraud.
- **Ensures business continuity:** Cyberattacks can cause significant operational disruption and downtime, which can lead to major financial losses and damage a company's reputation. Cyber security measures help minimize the impact of these incidents, ensuring services and operations remain dependable.
- **Prevents financial losses:** Cybercrime, which includes fraud, intellectual property theft, and ransomware attacks, can be financially devastating. Effective cyber security is a primary defense against these threats.
- **Maintains customer trust:** Customers expect businesses to keep their personal information safe. Companies that demonstrate a strong commitment to cyber security build trust and loyalty, while security breaches can lead to lost customers and a damaged brand reputation.
- **Supports national security:** Critical infrastructure, such as power grids and government systems, are vulnerable to politically motivated cyberattacks from hostile entities. Strong cyber security is vital for safeguarding a nation's interests, public safety, and economic stability.
- **Helps meet regulatory requirements:** Many industries are subject to data protection regulations like GDPR or HIPAA. Implementing a sound cyber security strategy is necessary to comply with these rules and avoid heavy legal penalties.

Common cyber threats: Phishing, Malware, Ransomware, social engineering

Common cyber threats include Phishing, which tricks users into revealing sensitive data through deceptive messages; Malware, harmful software like viruses and spyware that damages or steals data from systems; Ransomware, a type of malware that encrypts data and demands a ransom for its release; and Social Engineering, a broad tactic of manipulating people to gain access to systems or sensitive information.

Phishing

- **What it is**:

  A type of social engineering attack using deceptive emails or messages, often from seemingly legitimate sources, to trick users into providing sensitive information or clicking malicious links.

- **Goal**:

  To steal sensitive data like login credentials, financial details, or personal information for monetary gain or identity theft.

- **Methods**:
  Includes email phishing, vishing (voice phishing), and smishing (text message phishing).
  Malware

- **What it is**: Malicious software designed to infiltrate, damage, or gain unauthorized access to computer systems and networks.

- **Examples**: Includes viruses, worms, Trojans, and spyware.

- **Function**: Can steal data, disrupt services, or harm system functionality.
  Ransomware

- **What it is**:

  A specific type of malware that encrypts a victim's data or locks their system, preventing access.

- **Goal**:

To demand a ransom payment from the victim in exchange for the decryption key or to restore access.

Social Engineering

- **What it is**:

  A broad category of cyber threats that relies on psychological manipulation and deception to trick people into divulging confidential information or performing actions that compromise security.

- **How it works**:

  Attackers use tactics like impersonation, creating a sense of urgency, or preying on curiosity to manipulate victims.

- **Relationship to other threats**:
  Phishing is a common form of social engineering attack, but social engineering can also involve in-person interactions where an attacker poses as a trusted individual, such as an IT professional, to extract passwords.

Types of phishing

**Spear phishing**: These email messages are sent to specific people within an organization, usually high-privilege account holders, to trick them into divulging sensitive data, sending the attacker money, or downloading malware. This hyper-targeted approach exploits the human tendency to trust communications that appear personalized and relevant.

**Whaling (CEO fraud)**: These messages are typically sent to high-profile employees of a company to trick them into believing the CEO or other executive has requested a money transfer.

- **Smishing**: Using SMS messages, attackers send a text message to a targeted victim with a malicious link that promises discounts, rewards, or free prizes. This technique exploits the increasing reliance on mobile devices and the quick, often less cautious way people interact with text messages.
- **Vishing**: Attackers use voice-changing software to leave a message telling targeted victims they must call a number where they can be scammed. Attackers also use voice changers when speaking to targeted victims to deceive them.

Types of Malware

- **Viruses:**

  Malicious software that attaches to a legitimate file and requires user action to spread to other files.
- **Worms:**

  Self-replicating malware that spreads across a network without any user interaction.
- **Trojans:**

  Disguised as legitimate or harmless software to trick users into installing them, allowing access to sensitive data.
- **Ransomware:**

  Encrypts a user's files, making them inaccessible, and demands a ransom for their release.
- **Spyware:**

Secretly collects user information, such as browsing activity and login credentials, and sends it to a remote user.

- **Adware:**

  Displays unwanted advertisements, often in the form of pop-ups, and can track user activity to serve targeted ads.

- **Rootkits:**

  Designed to hide their presence and other malicious activities from the user and security software.

- **Botnets:**

  A network of infected computers (bots) controlled by a single attacker to carry out coordinated attacks.

- **Cryptojacking:**

  Uses a victim's computing power to secretly mine cryptocurrency.

- **Fileless Malware:**

  Resides in a computer's memory rather than in files, making it difficult to detect and remove.

- **Keyloggers:**
  Records keystrokes to steal information like passwords and credit card numbers.

## Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks their computer, preventing access until a ransom is paid, typically in cryptocurrency. Attacks can also involve holding sensitive data hostage, with threats to leak it publicly. Ransomware can spread through phishing emails, malicious links, or compromised websites, and organizations can protect themselves by backing up data, keeping software updated, and training staff to recognize threats.

How Ransomware Works

1. **Infection**:

   Attackers deliver ransomware via email attachments, malicious links, or compromised websites.

2. **Encryption/Locking**:

   Once on a system, the malware encrypts the victim's data, making it inaccessible.

3. **Demand**:

   The attackers then display a message demanding a ransom payment, often in a cryptocurrency like Bitcoin, to decrypt the files.

4. **Multifaceted Extortion**:
   Modern attacks often combine data encryption with data exfiltration (stealing sensitive data), threatening to publish the stolen information if the ransom isn't paid.
   Ways to Get Infected

- **Phishing emails**: Opening malicious links or file attachments in unexpected or suspicious emails.
- **Malicious websites**: Visiting unsafe or fake websites.
- **Vulnerable software**: Exploiting security flaws in outdated software or operating systems.
  How to Protect Against Ransomware
- **Back up your data**: Regularly back up important files to an offline or cloud storage location.
- **Keep software updated**: Install software and operating system updates as soon as they are released to patch security vulnerabilities.
- **Be vigilant with email**: Be cautious of unsolicited emails, suspicious attachments, and links.
- **Use strong security software**: Employ high-quality anti-malware and ransomware protection software.
- **Train your staff**: Educate users about the risks of clicking on malicious links or opening strange attachments.

## Digital Social Engineering

Social engineering is the set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions to release personal and financial information or hand over control over a computer system.

A malicious science, social engineering uses psychological manipulation, persuasion, and exploitation to deceive users into making security mistakes or relinquishing sensitive information. Social engineering attacks rely on human interaction and often involve conning victims into breaking normal security procedures. For instance, social engineering attacks can be highly effective because they're based on the human tendency to trust others or explore one's curiosity about new offers or information acting as bait.

Types of Social Engineering

- **Phishing:**

  Broadly uses emails, texts, or calls to trick people into providing personal information, transferring money, or clicking malicious links.
- **Spear Phishing:** A targeted phishing attack that uses personalized information to target specific individuals or organizations.
- **Whaling:** A type of spear phishing that targets high-level executives and government officials.
- **Vishing:** Phishing conducted over the phone, often using automated voice systems.
- **Smishing:** Phishing done through SMS (text) messages.
- **Baiting:**

  Lures victims with the promise of a reward, such as tempting ads or a physical object like a malware-infected USB drive left in a public place.
- **Scareware:**

  Uses fear to manipulate people into sharing information or downloading malicious software.
- **Watering Hole Attack:**
  Infects a legitimate website frequented by the target group with malicious code, hoping to compromise individual visitors.
  Physical Social Engineering
- **Tailgating/Piggybacking:**

  An unauthorized person follows an authorized person into a restricted physical area, often under the guise of being a new employee or delivery person.
- **Pretexting:**
  The attacker creates a believable but fake scenario or identity to deceive the victim and extract sensitive information.
  Exchange-Based Social Engineering
- **Quid Pro Quo:**

  Offers a desired good or service in exchange for the victim's sensitive information or a specific action.
- **CEO Fraud:**
  A high-level executive's persona is used to trick employees into a time-sensitive action, such as sending money to an offshore account.

# History and evolution of cyber threats

## Early Days (1970s–1980s)

- **First Viruses:** The first known virus, the experimental Creeper, appeared in 1971 on the ARPANET.
- **Malware Emerges:** The 1980s saw the first true malicious software (malware), with threats like the Morris Worm of 1988 causing significant disruption, according to Yeshiva University.
- **Prank-Based Threats:** These early threats were often created as experiments or pranks.

## The Rise of Mainstream Internet and Malware (1990s)

- **Increased Access:**

  With the growth of the mainstream internet and personal computers, cyber threats became more complex and widespread.
- **New Avenues for Attack:**

  Viruses, worms, and Trojans spread through email attachments and floppy disks.
- **Commercial Targets:**
  Website defacement, Denial-of-Service (DoS) attacks, and phishing scams started targeting the emerging e-commerce platforms and web servers.

## Financially Motivated Attacks (2000s)

- **Sophisticated Social Engineering:**

  Phishing became a major threat, using social engineering to trick users into revealing sensitive information or installing malware.
- **Botnets and DDoS:**
  Hackers created botnets (networks of infected computers) to launch distributed denial-of-service (DDoS) attacks, overwhelming servers and disrupting services.

## Organized Crime, APTs, and Exploitation (2010s)

- **Ransomware:**

This decade saw the explosion of ransomware, which encrypts a victim's data and demands payment for its release.

- **Advanced Persistent Threats (APTs):**

  Well-funded groups and nation-states began using stealthy, long-term APTs to infiltrate systems, remain undetected, and steal data over extended periods.

- **IoT and Supply Chain:**
  Attackers started exploiting vulnerabilities in Internet of Things (IoT) devices and the software supply chain to expand their reach and impact.

**Modern Threats and Artificial Intelligence (2020s)**

- **Lowered Barrier to Entry:**

  Ransomware-as-a-Service (RaaS) models now make it easier for amateur criminals to conduct sophisticated attacks.

- **AI and Deepfakes:**

  Artificial intelligence (AI) is being used to create deepfakes and other tools, enabling new methods of extortion and identity theft.

- **Increased Sophistication:**
  Attacks continue to grow in both frequency and sophistication, posing significant challenges for cybersecurity professionals

# Cyber security in daily life: online shopping, banking and social media notes

When shopping online, practicing good cybersecurity habits is essential for protecting your personal and financial information from theft and fraud. By taking a few practical steps, you can significantly reduce your risk of falling victim to scams.

## Shopping on secure websites

- **Verify the URL:** Always check that a website's address begins with "https://" and displays a padlock icon in the address bar. The "s" stands for secure and means that the website uses encryption to protect your data during transmission.
- **Trust reputable retailers:** Stick with well-known retailers and marketplaces that have established security measures and positive customer reviews. Scam websites often mimic legitimate stores with subtle misspellings in the URL, hoping you won't notice.
- **Be wary of unbelievable deals:** If an offer seems too good to be true, it likely is. Unfamiliar websites promising steep discounts can be a ploy to steal your information.

## Protecting your financial information

- **Use a credit card or secure payment service:** Credit cards generally offer better fraud protection than debit cards, with many card issuers capping your liability at $50 for unauthorized charges. Secure payment services like PayPal and Apple Pay also add an extra layer of protection by not sharing your actual card details with the merchant.
- **Avoid saving payment details:** While convenient, saving your credit card information on retailer websites increases your risk during a data breach. Enter your card details manually for each purchase to keep your data from being stored in multiple locations.
- **Use virtual or temporary card numbers:** Some credit card companies offer virtual card numbers that are temporary or for one-time use. This prevents hackers from using your real card number for future fraudulent purchases if the merchant's data is compromised.
- **Regularly monitor statements:** Keep an eye on your bank and credit card statements for any unusual or unauthorized charges. Report any suspicious activity to your bank immediately.

## Securing your accounts and devices

- **Use strong, unique passwords:** Create complex passwords for all your online shopping accounts, using a combination of letters, numbers, and symbols. A password manager can help you generate and securely store unique passwords for each site.
- **Enable multi-factor authentication (MFA):** Use two-factor authentication (2FA) or MFA wherever possible. This requires a second form of verification, such as a code

sent to your phone, making it much harder for cybercriminals to access your accounts even if they have your password.

- **Shop on secure networks:** Avoid making purchases while connected to public Wi-Fi networks in places like cafes or airports. These networks are often unsecured and can be easily intercepted by hackers. Use a secure private network or a Virtual Private Network (VPN) for extra protection.
- **Update your software:** Install software and app updates for your devices as soon as they become available. These updates often contain critical security patches that protect against new threats.
- **Consider a dedicated email address:** Using a separate email address for your online shopping can help you manage spam and better identify potential phishing emails.

Recognizing online scams

- **Beware of phishing emails:** Be cautious of emails or text messages promising deals that are "too good to be true" or claiming an issue with your account. Check the sender's email address for authenticity, and never click on suspicious links. Instead, go directly to the retailer's official website by typing the address in your browser.
- **Look for website red flags:** Poorly designed websites with misspellings, grammar errors, or a lack of contact information are common signs of a scam. Likewise, an abundance of fake or overly positive reviews should raise suspicion.
- **Don't overshare personal information:** Never provide sensitive information beyond what is necessary to complete a transaction, such as your Social Security number or date of birth. A legitimate retailer will not require this data for a simple purchase.

## Banking

When banking, practicing good cybersecurity habits is essential to protecting your finances from evolving threats like phishing, malware, and scams. While banks employ robust security measures like encryption, customers must also remain vigilant.

Protecting yourself from common banking scams

- **Be wary of phishing attempts.** Fraudsters may send emails or text messages that appear to be from your bank, often creating a false sense of urgency. These scams pressure you to click malicious links that install malware or lead to fake websites that steal your login credentials. Always verify the sender's email address and contact your bank directly through official channels to confirm any urgent request.

- **Recognize vishing (voice phishing) calls.** Cybercriminals may call you pretending to be a bank official, insurance agent, or government officer to gain your trust. Remember that legitimate bank officials will never ask you to disclose confidential information over the phone, such as your PIN, OTP, password, or card details.

- **Guard against SIM swap fraud.** In this scam, a fraudster obtains a duplicate SIM card, using it to receive the one-time passwords (OTPs) needed for digital transactions. Stay cautious if your mobile network disappears for an extended period and immediately contact your mobile operator if you suspect an issue.

Securing your devices and accounts

- **Use strong and unique passwords.** Your passwords are your first defense. Create complex, long passwords using a mix of uppercase and lowercase letters, numbers, and special characters. Avoid common phrases or personal information like your birthdate. Consider using a reputable password manager to generate and store unique passwords for different accounts.

- **Enable multi-factor authentication (MFA).** MFA adds a crucial second layer of security beyond just a password. This often involves a one-time passcode sent to your phone or a biometric verification like a fingerprint or facial scan. Always enable MFA for your banking apps and other important accounts.

- **Install antivirus and keep software updated.** Use genuine antivirus and anti-malware software on your computer and smartphone. Enable automatic updates for your operating system and apps, as these updates often contain important security patches that protect against new vulnerabilities.

- **Secure your mobile device.** Password-protect your phone with a strong PIN or biometric authentication. Avoid rooting or jailbreaking your device, which exposes it to malware. Also, disable Wi-Fi and Bluetooth when not in use.

Exercising caution during online transactions

- **Avoid public Wi-Fi for banking.** Public Wi-Fi networks in hotels, airports, or cafes are often unsecured, making it easy for hackers to intercept your data. Use a secure, private connection or a Virtual Private Network (VPN) for all banking transactions.

- **Manually type your bank's URL.** Instead of clicking a link from an email or a search result, type your bank's website address directly into your browser's address bar. Before entering your login details, check that the URL begins with "https://" and that there is a padlock symbol in the address bar.

- **Always log out properly.** After finishing an online banking session, be sure to click the "Log Out" button instead of simply closing the browser window. This is especially important when using a shared or public computer.

Monitoring your accounts and cards

- **Monitor your accounts regularly.** Frequently check your account balances and statements for any unauthorized transactions. Most banks offer transaction alerts via SMS or email, which you should enable to get immediate notification of any activity.
- **Protect your ATM card and PIN.** When using an ATM, always cover the keypad with your hand while entering your PIN to prevent "shoulder surfing". Do not share your PIN with anyone, and memorize it instead of writing it down.
- **Be present for card swipes.** When using your card at a store or petrol pump, ensure the transaction is done in your presence. Keep an eye out for any suspicious devices attached to card readers that could be "skimmers" designed to steal your card data.

What to do if you are a victim

If you suspect or discover fraudulent activity on your account, act immediately:

- **Report to your bank.** Contact your bank's customer service or fraud hotline immediately to report the fraud and freeze your account. Many banks have a zero-liability policy for incidents reported promptly.
- **Report to the authorities.** File a report with the police or the national cybercrime portal in your region.
- **Change all passwords.** Change the passwords for your financial accounts as well as any other accounts that used the same credentials.
- **Monitor your credit.** Check your credit reports for any new accounts or inquiries you did not initiate.



Cybersecurity in daily life: social media

To practice social media cybersecurity, focus on strengthening your accounts by using strong passwords and multi-factor authentication, and be vigilant about privacy by limiting oversharing and adjusting your settings. Additionally, protect yourself from threats like phishing by being cautious with links from unknown sources and avoiding sensitive activities on public Wi-Fi.

Account security

- **Use strong passwords:** Create strong, unique passwords for each social media account.
- **Enable multi-factor authentication (MFA):** Add an extra layer of security for your accounts.

- **Enable automatic updates:** Ensure your social media apps and operating systems are always up to date to patch vulnerabilities.
- **Log out:** Log out of your accounts, especially on public or shared computers.
  Privacy and data protection
- **Be mindful of oversharing:**

  Limit the amount of personal information you share online, as it can be used for identity theft or scams.
- **Adjust privacy settings:**

  Regularly review and tighten your privacy settings to control who can see your posts and information.
- **Turn off location services:**

  Be cautious about sharing your location by disabling geolocation on your apps.
- **Limit third-party access:**

  Review and restrict permissions for apps connected to your social media accounts.
- **Monitor your accounts:**
  Periodically check for suspicious activity and review your settings for any changes.
  Threat prevention
- **Be wary of phishing:**

  Be cautious of links and attachments, especially in messages from people you don't know.
- **Verify identities:**

  Be skeptical of friend requests from strangers and verify who you are interacting with.
- **Avoid public Wi-Fi for sensitive tasks:**

  Public Wi-Fi networks can be risky. Use a VPN or avoid sensitive activities like logging in when on them.
- **Be aware of scams:**
  Stay informed about common social media scams, such as those involving fake threats to extort money.

# Digital hygiene practices

This is the idea behind cyber hygiene: to create a structured and intelligent environment that reduces the risks of external contamination *without* having to consistently spend lots of IT effort on these processes. This way, you and your team have more time to use the same environment in more productive and strategic functions, generating good business and operational results.

Cyber hygiene is basically a structured approach to cybersecurity across an organization., though it's less formalized than cyber frameworks.

Cyber hygiene practices include using strong, unique passwords and multi-factor authentication, regularly updating software, backing up data, being cautious of phishing attempts and suspicious links, and using security software like antivirus and firewalls. Practicing these habits is essential for protecting your digital life, networks, and data from cyber threats and vulnerabilities.

## Account Security

- **Use strong, unique passwords:**

  Create complex passwords that are different for each account to prevent attackers from accessing multiple accounts with a single password.
- **Enable multi-factor authentication (MFA):**
  Add an extra layer of security by requiring a second verification step, like a fingerprint or a code from your phone, in addition to your password.
  Software and Device Maintenance
- **Keep software updated:**

  Regularly update operating systems, applications, and devices to patch vulnerabilities and protect against known security flaws.
- **Use antivirus and anti-malware software:**

  Install reputable antivirus and anti-malware programs and keep them updated to detect and remove malicious software.
- **Secure your network:**
  Use a strong password for your Wi-Fi network and consider using encryption like WPA2 or WPA3.

# Data Protection

- **Back up your data:**

  Regularly back up important files to a secure location, such as a cloud service or an external hard drive, to ensure you can recover data in case of loss or ransomware attacks.

- **Encrypt sensitive data:**
  Encrypt your data to maintain its privacy and security, especially if it needs to be transmitted or stored.
  User Vigilance

- **Be wary of phishing attempts:**

  Do not click on suspicious links or download attachments from unknown or untrusted sources.

- **Educate yourself and others:**

  Stay informed about the latest cyber threats and best practices for online safety.

- **Monitor account activity:**
  Regularly check your accounts for suspicious transactions or activity to detect potential fraud.

# UNIT 3 - Legal and ethical aspects of cyber security

## OVERVIEW OF INDIAN IT ACT AND RELEVANT LAWS

The Indian Information Technology (IT) Act, 2000 is the primary law governing cybercrime and electronic commerce, providing legal recognition for digital transactions and promoting digital governance. Key aspects include recognizing electronic records and digital signatures, defining and punishing cybercrimes like hacking and data breaches, establishing rules for digital communication and cybersecurity, and amending other Indian laws like the Indian Penal Code. The Act was supplemented by the IT (Amendment) Act, 2008 and has been further updated through various IT Rules, notably the IT Rules, 2021, which enhance data protection and platform accountability.

## Key Provisions and Objectives

- **Legal Recognition of Electronic Transactions:**

  The Act provides legal validity to electronic documents and digital signatures, vital for e-commerce and digital filing with government agencies.
- **Cybercrime Prevention:**

  It defines and penalizes various cybercrimes, such as unauthorized access to computers, data breaches, hacking, identity theft, and online obscenity, with specified penalties like imprisonment and fines.
- **Digital Signatures and Authentication:**

  The Act establishes a framework for secure electronic communication and the use of digital signatures to ensure authenticity.
- **E-Governance:**

  It facilitates electronic filing of documents with government bodies and promotes digital transactions with them.
- **Cybersecurity Measures:**
  The Act includes provisions for authorities to intercept, monitor, and block websites to protect national sovereignty and integrity, particularly against hate content and child pornography.

## Relevant Amendments and Rules

**Information Technology (Amendment) Act, 2008:**

This amendment introduced controversial provisions, such as Section 66A, which allowed authorities to arrest individuals for posting "offensive" content online, though it was later struck down.

- **IT Rules, 2021:**
  These rules significantly updated the framework by introducing new accountability for digital platforms and intermediaries, mandating grievance redressal mechanisms, data privacy, and content moderation.

Key Considerations

- **Extraterritorial Jurisdiction:**

  The Act has extraterritorial reach, applying to individuals outside India if their actions involve a computer system or network located in India.

- **Data Protection:**

  While the IT Act established a framework for cybersecurity, specific aspects of personal data protection have been further addressed by subsequent legislation like the Digital Personal Data Protection Bill 2022, as part of India's evolving digital policy landscape.

- **Intermediary Liability:**
  The Act and its subsequent rules address the liability of intermediaries, such as social media platforms, for the content posted by their users.

## Cybercrime reporting in india

To report cybercrime in India, use the 24x7 National Cybercrime Helpline number 1930 or file a complaint online via the National Cyber Crime Reporting Portal at cybercrime.gov.in. For financial fraud, you'll need bank account and transaction details. The portal is a user-friendly platform managed by the government to report offenses like identity theft, online fraud, hacking, and cyber bullying, allowing you to track your case and provide evidence.

**Methods to Report Cybercrime**

- **Call the Helpline:**

  Dial the national helpline number 1930 for immediate assistance, especially for online financial fraud.

- **Use the Online Portal:**
- Visit cybercrime.gov.in to access the National Cyber Crime Reporting Portal.
- Register using your name and a valid Indian mobile number, receiving an OTP for verification.

- Select the appropriate category for your complaint, such as online financial fraud, hacking, or cyber bullying, and provide relevant details and evidence.
- You can track the progress of your complaint after submission.
  Information to Have Ready
- **For Financial Fraud:**

  Your bank account number, bank transaction ID or UTR number, and details of the suspect (phone numbers, etc.).
- **For Other Cybercrimes:**
  Any suspicious messages, emails, or other forms of digital evidence related to the incident.

  Important Considerations
- The 1930 helpline operates 24/7 to help victims protect their funds, especially in financial frauds.
- The National Cyber Crime Reporting Portal is an initiative by the Indian government to provide a secure and anonymous platform for reporting various cybercrimes.
- Ensure you provide accurate details to facilitate prompt action and tracking of your case.
  Filing a Complaint on National Cyber Crime Reporting Portal

**Digital rights and responsibilities**

Digital rights are the privileges and freedoms to access, use, and create digital media, while digital responsibilities are the obligations to act ethically, respect others' rights, and ensure a safe and responsible digital environment. Together, they form digital citizenship, requiring users to uphold principles like freedom of speech and privacy, and simultaneously practice digital etiquette, intellectual property respect, and data security to maintain a positive online community.

Digital Rights

- **Access and Inclusion:** The right to use computers, electronic devices, and communication networks.
- **Freedom of Expression:** The ability to express ideas and opinions freely in the digital world.
- **Privacy:** The right to keep personal information private and to be secure online.
- **Digital Safety:** The right to be free from harassment, threats, and infringement of rights online.
- **Creation and Sharing:** The freedom to create and share digital content.
  Digital Responsibilities
- **Respectful Communication:** Communicating respectfully with others, even during disagreements.

- **Protecting Privacy:** Refraining from sharing others' private information and protecting one's own logins and passwords.
- **Respecting Intellectual Property:** Giving proper credit for others' work and not violating copyright.
- **Avoiding Misinformation:** Declining to share false or misleading information.
- **Security:** Understanding what information should not be shared and protecting personal data.
- **Ethical Behavior:** Acting ethically and responsibly to contribute to a safe and positive digital environment for all users.

Ethical use of digital content and resources

Ethical use of digital content and resources involves respecting intellectual property by giving proper credit and avoiding plagiarism, protecting user privacy by handling personal data responsibly and obtaining consent, ensuring content accuracy by using reliable sources and avoiding misinformation, practicing responsible communication by treating others with respect and avoiding harmful online behavior like cyberbullying, and maintaining digital wellness by balancing online and offline activities and being aware of technology's impact on well-being.

**Respecting Intellectual Property**

- **Give Proper Credit:**

  Always acknowledge original creators when using their digital content, be it text, images, or software.
- **Avoid Plagiarism:**

  Do not present others' work as your own; cite your sources and use digital resources legally.
- **Understand Copyright:**
  Be familiar with copyright laws and fair use principles to ensure you have the legal right to use digital materials.
  Protecting User Privacy and Data
- **Secure Personal Information:**

  Take steps to protect your own data and be cautious about sharing sensitive information online.
- **Respect Others' Data:**

Obtain consent before sharing someone's personal information or content, and be mindful of data protection regulations.

- **Be Transparent:**
  If you collect user data, such as for a mailing list, ensure transparency and provide easy options to unsubscribe.
  Ensuring Content Accuracy and Reliability
- **Use Reliable Sources:**

  Prioritize using well-researched and accurate information to maintain credibility and avoid spreading misinformation.
- **Critically Evaluate Content:**

  Assess the reliability and bias of online content before using it for any purpose.
- **Cite Credible Sources:**
  When using data or information from other sources, cite them to support the accuracy and integrity of your content.
  Practicing Responsible Communication
- **Engage Respectfully:** Treat others with respect online and use constructive, polite language, similar to face-to-face interactions.
- **Avoid Harmful Behavior:** Do not engage in cyberbullying, harassment, or forward negative or offensive content.
- **Promote Constructive Dialogue:** Encourage positive and respectful conversations on online platforms.
  Promoting Digital Wellness
- **Balance Activities:**

  Develop habits that balance virtual and physical activities to promote overall safety and well-being.
- **Understand Impacts:**

  Be aware of the physical and psychological effects of excessive digital technology use.
- **Cultivate Digital Citizenship:**
  Integrate ethical online behavior into educational settings and promote digital literacy for all users.



## CYBERSECURITY TOOLS AND SOFTWARE AWARENESS

Cybersecurity tools are software and hardware designed to protect systems, while cybersecurity awareness is the user's knowledge of how to use these tools and avoid threats like phishing and malware. Key tools include firewalls, anti-malware software, and vulnerability scanners, while

awareness training covers recognizing social engineering, practicing strong password habits, and securing devices.

Cybersecurity tools and software

- **Firewalls:** Act as a barrier between a secure internal network and an untrusted external network like the internet.
- **Anti-Malware and Anti-Virus Software:** Protect against malicious software, including viruses and ransomware.
- **Vulnerability Scanners:** Identify weaknesses in networks and systems that could be exploited by attackers.
- **Network Intrusion Detection/Prevention Systems:** Monitor network traffic for suspicious activity and can block malicious access.
- **Encryption Tools:** Scramble data to make it unreadable to unauthorized individuals.
- **Identity and Access Management (IAM) Tools:** Control who has access to what resources and enforce authentication.
- **Security Information and Event Management (SIEM) Tools:** Collect and analyze security logs from various sources to detect threats.
  Cybersecurity awareness
- **Phishing and social engineering:**

  Training to recognize and report phishing attempts, which often arrive via email or social media.
- **Password security:**

  Emphasizing the use of strong, unique passwords and multi-factor authentication.
- **Removable media:**

  Teaching safe practices for using USB drives and other portable storage devices.
- **Browser and email security:**

  Providing guidance on safe browsing habits and email attachments.
- **Remote and mobile work:**

  Educating users on the risks of public Wi-Fi and how to secure their devices when working remotely or using mobile devices.
- **Incident reporting:**
  Instructing users on what to do and who to contact if they encounter a suspicious activity.