SAMBHRAM
INSTITUTE OF TECHNOLOGY

Amba Bhavani Temple Road, M.S.Palya, Vidyaranyapura Post, Bengaluru-560097.

Website: www.sambhramit.com, Email : sait@sambhram.org

CYBER CRIME
SAFETY INITIATIVE
Hand Book

By

SaIT - Cyber Crime Awareness Cell

2024

Campus

Amba Bhavani Temple Road, M.S.Palya, Vidyaranyapura Post, Bengaluru-560097.
Website: www.sambhramit.com, Email : sait@sambhram.org

Total Number of Pages of this Hand book : 17

This manual is not for sale.

First Printed : 2022

Rewritten on : 2023

Updated on : 2024

First Written By: Dr.Ravishankar.C.V.

Rewritten & updated by: Dr. Sanjeetha.R

Updating done on 01.02.2024 by: Dr. Sanjeetha.R

Verified & Approved by : Dr.H.G.Chandrakanth,Principal,SaIT.

Next Updation : 2025

Campus & Registered office :

Amba Bhavani Temple Road,
M.S.Palya,
Vidyaranyapura Post,
Bangalore-560097

DO`S & DON`TS FOR STUDENTS & FACULTY TO SAFE GAURD AGAINST
CYBER CRIMES

Cyber Crimes

Cybercrime Overview

Cybercrime refers to criminal activities conducted through digital technologies and the internet. It includes a wide range of illegal activities, from hacking and data breaches to online fraud and identity theft.

Types of Cyber crimes

- **Hacking**: Unauthorized access to computer systems, networks, or devices to steal, manipulate, or disrupt data.
- **Phishing**: Sending deceptive emails or messages to trick recipients into revealing sensitive information or downloading malware.
- **Malware**: Software designed to harm or gain unauthorized access, including viruses, worms, Trojans, and ransomware.
- **Identity Theft**: Stealing personal information to impersonate an individual for financial gain or other malicious purposes.
- **Online Fraud**: Engaging in deceitful activities, like credit card fraud, auction fraud, or investment scams, through online platforms.
- **Cyber bullying**: Harassment, threats, or intimidation of individuals using digital communication methods.
- **Denial of Service (DoS) Attacks**: Overloading a system or network to make it unavailable to users.
- **Data Breaches**: Unauthorized access and release of sensitive information from organizations or individuals.
- **Cyber Espionage**: Illegally gaining access to confidential information, often for political, economic, or competitive advantage.
- **Online Harassment**: Persistent and harmful behavior directed at individuals, often via social media or other online channels.

- **Sextortion**: Blackmailing individuals by threatening to release compromising personal content.
- **Child Exploitation**: Creating, distributing, or accessing explicit content involving minors.
- **Cyber stalking**: Unwanted and persistent online attention or harassment towards a person.

Impact and Consequences

- **Financial Loss:** Individuals and businesses can suffer significant financial damage due to cyber crimes.
- **Privacy Violations:** Personal information can be exposed, leading to identity theft and other privacy breaches.
- **Reputational Damage:** Organizations and individuals can suffer reputational harm due to data breaches and other cyber crimes.
- **Legal Consequences:** Perpetrators can face legal action, including fines and imprisonment.
- **Economic Impact:** Cyber crimes can affect economies through lost revenue, increased security measures, and decreased consumer trust.
- **Emotional Toll:** Victims of cyber bullying, harassment, and other cyber crimes can experience emotional distress.
- **National Security:** Cyber crimes can have implications for national security when they target critical infrastructure or involve espionage.

Prevention and Protection

- **Strong Passwords**: Using complex and unique passwords for different accounts.
- **Software Updates:** Regularly updating operating systems, applications, and security software.
- **Two-Factor Authentication (2FA):** Adding an extra layer of security by requiring a second verification step.
- **Phishing Awareness:** Educating users about identifying and avoiding phishing attempts.
- **Secure Networks:** Using encryption and secure connections, especially on public Wi-Fi networks.

- **Regular Backups:** Keeping copies of important data to restore in case of ransomware attacks.
- **Antivirus and Firewalls:** Employing reliable security software to detect and block threats.
- **Employee Training:** Providing cyber security training for employees to prevent social engineering attacks.
- **Legal Frameworks:** Governments and international organizations developing laws and regulations to address cyber crimes.

Cyber Laws

Cyber Laws Overview

Cyber laws, also known as cybercrime laws or internet laws, are legal regulations that govern activities conducted in cyberspace. They address various aspects of digital interactions, including online behavior, data protection, and electronic transactions.

Key Elements of Cyber Laws:

- **Data Protection and Privacy:** Laws that regulate the collection, storage, and processing of personal information to protect individuals' privacy rights.
- **Cybercrime Offenses:** Laws that define and penalize various cyber crimes, such as hacking, identity theft, and online fraud.
- **Electronic Transactions:** Laws that recognize the legal validity of electronic contracts and transactions.
- **Intellectual Property**: Laws that safeguard digital intellectual property rights, including copyrights, patents, and trademarks.
- **Digital Signatures:** Laws that establish the legal status of digital signatures for authentication and authorization purposes.
- **Jurisdiction:** Determining which laws apply to cross-border cyber crimes and disputes involving parties from different countries.
- **Cyber bullying and Harassment:** Laws that address online harassment, cyber bullying, and harmful digital communications.

- **Cyber security and Incident Reporting:** Laws that require organizations to implement cyber security measures and report data breaches.
- **Online Defamation:** Laws that address false statements made online that harm an individual's reputation.
- **Freedom of Expression:** Balancing individuals' rights to freedom of speech with regulations against hate speech and incitement of violence.

Examples of Cyber Laws:

- **General Data Protection Regulation (GDPR):** European Union regulation that protects the privacy and data of EU citizens and residents.
- **Computer Fraud and Abuse Act (CFAA):** U.S. federal law that addresses computer-related crimes and unauthorized access to computer systems.
- **Cybercrime Prevention Act:** Philippines law that deals with cybercrime offenses, including hacking, identity theft, and online fraud.
- **Information Technology Act, 2000:** Indian law that covers electronic transactions, digital signatures, and cyber security.
- **Personal Data Protection Act (PDPA):** Singaporean law regulating the collection, use, and disclosure of personal data.

Challenges and Considerations

- **Jurisdictional Issues:** Determining jurisdiction in cross-border cyber crimes can be complex due to the global nature of the internet.
- **Rapid Technological Changes:** Cyber laws must continually adapt to new technologies and emerging threats.
- **Balancing Rights:** Striking a balance between protecting privacy, freedom of expression, and security can be challenging.
- **Enforcement:** Cyber laws may be challenging to enforce across different jurisdictions, leading to gaps in prosecution.
- **Global Harmonization:** Achieving consistent international cyber law standards is a complex task due to differing legal systems and cultural norms.

Importance of Cyber Laws

- **Protection:** Cyber laws provide legal safeguards for individuals, businesses, and governments against cyber crimes and digital rights violations.
- **Framework for Digital Transactions:** They establish a legal framework for electronic contracts, transactions, and electronic signatures.
- **Deterrence:** Cyber laws deter individuals from engaging in illegal cyber activities by outlining penalties and consequences.
- **Consumer Confidence:** Strong cyber laws contribute to consumer trust in online transactions and data security.
- **International Cooperation:** Cyber laws promote collaboration among countries in addressing cybercrime and creating consistent global standards.

Do’s and Don’ts

Accessing unknown/non trusted website/portals:

Communicating with unknown or non-trusted websites or portals can expose you to various cybercrime risks, including phishing attacks, malware infections, and data breaches. To protect yourself from these risks, it's important to follow these guidelines:

1. **Verify the Website's Legitimacy:** Before interacting with a website, ensure that the URL is spelled correctly and matches the official website of the organization or service you intend to use. Check for "https://" in the URL, indicating a secure connection.

2. **Avoid Clicking on Suspicious Links:** Don't click on links in unsolicited emails, messages, or pop-ups. Hover your mouse over links to see the actual URL before clicking.

3. **Unsolicited Communications:** Be cautious of emails, messages, or calls asking for personal or financial information, especially if they pressure you to provide information quickly.

4. Use Strong and Unique Passwords: If you need to create an account on a new website, use a strong, unique password. Consider using a password manager to generate and store passwords securely.

5. Enable Two-Factor Authentication (2FA): If the website offers 2FA, enable it. This adds an extra layer of security.

6. **Keep Software and Systems Updated:** Keep your operating system, browsers, and antivirus software up to date to protect against known vulnerabilities.

7. **Personal Information:** Only provide personal or sensitive information to trusted websites that have a legitimate need for it. Avoid sharing unnecessary personal details on social media platforms.

8. **Check for SSL Certificates:** Look for a padlock symbol in the browser's address bar, indicating that the website has a valid SSL certificate and is secure for data transmission.

9. **Use Security Software:** Install and regularly update reputable antivirus and anti-malware software on your devices.

10. **Educate Yourself:** Learn about common phishing and online scams so you can recognize suspicious behavior.

11. **Use a Firewall:** Enable firewalls on your devices to prevent unauthorized access.

12. **Limit Permissions:** When using apps or services, only grant necessary permissions and access. Avoid giving access to sensitive data unless it's essential.

13. Trust Your Instincts: If something seems too good to be true or feels suspicious, it probably is. Trust your instincts and exercise caution.

Sharing information with unknown persons/through social media platforms.

Sharing personal information with unknown individuals or through social media platforms can put you at risk of various cyber crimes and privacy breaches. Here's how you can protect yourself from these risks:

1. **Limit Personal Information:** Be cautious about what personal information you share online. Avoid sharing sensitive details like your full address, phone number, financial information, and Social Security number.

2. **Check Privacy Settings:** Review and adjust the privacy settings on your social media accounts. Limit who can see your posts, profile information, and contact details.

3. **Be Wary of Friend Requests:** Be cautious when accepting friend requests or connections from people you don't know personally. Cyber criminals may create fake profiles to gather information.

4. **Don't Share Financial Information:** Never share your credit card details, bank account information, or other financial information on social media.

5. **Avoid Posting Travel Plans:** Refrain from posting travel plans in real-time. This can alert potential burglars that your home might be vacant.

6. **Be Skeptical of Unsolicited Messages:** If you receive messages or friend requests from strangers asking for personal information or money, be skeptical and avoid responding.

7. **Use Strong Privacy Settings:** Familiarize yourself with the privacy settings of the platforms you use. Opt for the highest level of privacy to limit who can access your information.

8. **Educate Yourself About Scams:** Stay informed about common online scams, phishing attempts, and social engineering tactics. This awareness can help you recognize and avoid potential threats.

9. **Think Before You Share:** Before posting anything online, consider whether the information could be used against you in any way. Once information is shared, it's often challenging to fully retract it.

10. **Don't Overshare:** Be mindful about the amount of personal information you share in your public profiles. Cyber criminals can piece together details from different sources to build a comprehensive profile.

11. **Use Discretion with Photos:** Avoid sharing photos that reveal sensitive information, such as your location, workplace, or other identifiable details.

12. **Use Strong Passwords:** Ensure that your social media accounts have strong, unique passwords to prevent unauthorized access.

13. **Be Careful About Geo location Tags:** Be cautious about tagging your location in posts or photos. This can reveal your whereabouts and daily routines.

14. Regularly Review Friend Lists: Periodically review your friends or connections list and remove individuals you no longer interact with or don't recognize.

Using Mobile Phones & other Digital equipment’s.

The usage of mobile phones and other digital devices has become an integral part of our lives, but it also exposes us to various cybercrime risks. Here are some common ways cybercrime can occur through the usage of mobile phones and digital equipment, along with tips to protect yourself:

1. **Malware and Mobile Apps:** Malicious apps can be downloaded from unofficial app stores or disguised as legitimate apps. Once installed, they can steal data, track your activities, or gain control over your device. **Protection:** Stick to official app stores (e.g., Google Play Store, Apple App Store) and only download apps with good reviews and a significant number of downloads. Keep your device's operating system and apps up to date to patch vulnerabilities.

2. **Phishing and Smishing:** Cyber criminals send fraudulent messages (phishing) or SMS (smishing) to trick you into revealing personal or financial information. **Protection:** Be

cautious of unsolicited messages and avoid clicking on links or providing sensitive information. Verify the sender's identity through official channels.

3. **Stolen or Lost Devices:** A stolen or lost mobile device can provide access to sensitive data if not properly secured. **Protection**: Use strong PINs, passwords, or biometric locks to protect your device. Enable remote tracking and data wiping features in case your device is lost or stolen.

4. **Public Wi-Fi Risks:** Using public Wi-Fi networks can expose your data to hackers who can intercept your traffic. **Protection:** Avoid accessing sensitive information on public Wi-Fi networks. If you must use them, consider using a Virtual Private Network (VPN) to encrypt your data.

5. **Unsecured Bluetooth Connections:** Cyber criminals can exploit vulnerabilities in Bluetooth connections to gain unauthorized access to your device. **Protection:** Keep Bluetooth off when not in use and only pair your device with trusted devices.

6. **Social Engineering:** Attackers may use social engineering tactics to manipulate you into divulging sensitive information or performing actions that compromise security. **Protection:** Be skeptical of unsolicited communications and avoid sharing personal information or taking actions based solely on requests through digital channels.

7. **App Permissions Abuse:** Some apps request unnecessary permissions that can be used to access personal data without your knowledge. **Protection:** Review app permissions before installing and regularly review permissions granted to installed apps. Only grant necessary permissions.

8. **Phony Mobile Banking and Shopping Apps:** Fake mobile banking or shopping apps can steal your login credentials and financial information. **Protection:** Download banking and shopping apps only from official app stores, and verify app details and developer information before installation.

9. **Email and Account Breaches:** Access to personal email accounts can expose sensitive information and lead to further cyber crimes. **Protection:** Use strong, unique passwords for email accounts and enable two-factor authentication (2FA).

10. Device Tracking and Stalking: Location services can be abused to track your movements and gather personal information. **Protection:** Review app settings and permissions related to location services, and only grant access when necessary.

What to do if you became Cyber Crime Victim

Victim of fraudulent online / offline Bank Transactions

If you become a victim of online or offline bank transaction cybercrime in India, it's important to take immediate action to minimize the damage and report the incident to the appropriate authorities. Here's what you should do:

1. **Contact Your Bank:** For online transactions, contact your bank immediately to report the unauthorized transaction or fraudulent activity. They can guide you through the process of blocking your account or card, initiating an investigation, and recovering any lost funds.

2. **Change Passwords/PINs:** If you suspect your online banking credentials have been compromised, change your passwords, PINs, and other access details for your online accounts. Ensure that your new passwords are strong and unique.

3. **Preserve Evidence:** Take screenshots or photos of any suspicious activities, transactions, or communications related to the cybercrime. These can serve as evidence if needed.

4. Lodge a Complaint: For online transactions, file a complaint with the Cyber Crime Cell of the local police. Provide them with all the relevant details and evidence you have gathered. They will issue you a copy of the First Information Report (FIR) once your complaint is registered.

5. Contact Cyber Helpline: You can also reach out to organizations like CERT-In (Indian Computer Emergency Response Team) or the Cyber Crime Helpline for guidance and assistance in dealing with cybercrime incidents.

6. **Report to RBI and Bank Ombudsman:** If your bank is not responsive or if you are not satisfied with their resolution, you can file a complaint with the Reserve Bank of India (RBI) and the Banking Ombudsman. The Banking Ombudsman is a designated authority that handles customer complaints against banks.

7. **Monitor Your Accounts:** Regularly monitor your bank accounts, credit card statements, and other financial accounts for any suspicious activities. Report any discrepancies immediately.

8. **Inform Credit Bureaus:** If your personal information has been compromised, consider informing credit bureaus to place a fraud alert on your credit report. This can help prevent identity theft and further financial fraud.

9. **Be Cautious with Personal Information:** Be cautious about sharing personal information online and offline. Avoid clicking on suspicious links, and only provide sensitive information to trusted sources.

10. Educate Yourself: Stay informed about cyber security best practices and common scams. Being aware of potential threats can help you avoid falling victim to cybercrime.

Victim while using social media platforms

If you become a victim of cybercrime on social media in India, you should take immediate action to protect your account, personal information, and report the incident to the relevant authorities. Here's what you should do:

1. Secure Your Account: Change your password immediately to a strong and unique one. Enable two-factor authentication (2FA) if the platform offers this option. Review your account settings, privacy settings, and connected apps to ensure there are no unauthorized changes or access.

2. **Document Evidence:** Take screenshots or photos of any suspicious posts, messages, or activities on your account. This evidence will be helpful when reporting the incident.

3. **Report the Incident:** Report the cybercrime to the social media platform through their reporting mechanisms. Use platform-specific tools to report hacked or compromised accounts, impersonation, harassment, and other types of cyber crimes.

4. **Preserve Information:** Keep any communication or messages related to the incident. These could be useful for legal purposes or while dealing with authorities.

5. **Lodge a Complaint:** File a complaint with the Cyber Crime Cell of the local police. Provide them with all the evidence and details you have gathered. Provide a copy of the complaint to the social media platform as well, if required.

6. **Contact Cyber Helplines:** Reach out to organizations like CERT-In (Indian Computer Emergency Response Team) or the National Cyber Crime Reporting Portal for guidance and assistance in dealing with cybercrime incidents.

7. **Educate Yourself:** Stay informed about common social media scams and phishing techniques to better protect yourself in the future.

8. **Inform Contacts:** If your account was used to send harmful content to your contacts, let them know that your account was compromised to prevent them from becoming victims.

9. Review Other Online Accounts: If you've used the same password for other accounts, change those passwords to prevent further unauthorized access.

10. Legal Action: If the cybercrime involves serious threats, harassment, defamation, or other criminal activities, consult with legal experts to understand the potential legal options available to you.

11. Be Cautious Going Forward: Continue to monitor your social media accounts for any unusual activity, and be cautious about sharing personal information online.

Victim sharing personal & confidential information:

If you become a victim of personal and confidential information theft in a cybercrime incident, it's important to take immediate action to mitigate the damage and protect yourself from further harm. Here's what you should do:

1. **Stay Calm:** While it's natural to feel panicked, try to remain calm and focused so you can take the necessary steps to address the situation.

2. **Change Passwords:** Immediately change the passwords of any compromised accounts, including email, social media, financial accounts, and online services. Use strong, unique passwords for each account.

3. **Enable Two-Factor Authentication (2FA):** Wherever possible, enable 2FA for your online accounts. This adds an extra layer of security by requiring a second form of verification in addition to your password.

4. **Notify Financial Institutions:** If your financial accounts or credit card information is compromised, contact your bank or credit card issuer to report the incident. They can help monitor your accounts for suspicious activity and take appropriate actions.

5. **Contact Authorities:** File a complaint with your local law enforcement agency or cybercrime division. They may need to investigate the incident and gather evidence.

6. **Inform Credit Bureaus:** Consider placing a fraud alert on your credit report with credit reporting agencies. This can help prevent identity theft and unauthorized credit applications.

7. **Monitor Accounts:** Regularly monitor your financial accounts, credit reports, and any other accounts for unusual activity. Report any suspicious transactions immediately.

8. **Inform Contacts:** If your personal information was stolen and could be used for identity theft or phishing attacks, inform your contacts to be cautious and avoid falling for scams.

9. **Update Software:** Ensure that your devices, operating systems, and software are up to date with the latest security patches. Cyber criminals often exploit vulnerabilities in outdated software.

10. Be Wary of Scams: After a data breach or information theft, you might receive phishing emails or messages that try to exploit the situation. Be cautious of any communication asking for sensitive information or directing you to click on suspicious links.

11. **Consider Legal Action:** Depending on the severity of the theft and applicable laws, you might consider consulting with a lawyer to understand if legal action is necessary or possible.

12. Educate Yourself: Learn from the incident and educate yourself about cyber security best practices to prevent future occurrences.

SaIT - Cyber Crime Awareness Cell :

The establishment of a Cyber Crime Awareness Cell in our college is driven by the fundamental objective of cultivating a heightened understanding and consciousness regarding cyber security among students, faculty, and staff. The primary goal is to equip individuals with the knowledge and skills necessary to navigate the digital landscape securely.

Additionally, the Cyber Crime Cell endeavors to educate and raise awareness among the college community about the importance of cyber security. Through workshops, training sessions, and awareness programs, the cell aims to instill a proactive mindset, promoting responsible online behavior and ensuring that students, faculty, and staff are well-equipped to navigate the digital landscape securely. By creating a strong cyber security culture, the cell contributes to the overall resilience of the institution against evolving cyber threats and aligns with industry standards and regulations, positioning the college as a secure and compliant entity in the digital realm.

It is our endeavour to support faculty, students and staff of Sambhram Institute of Technology to fight against cyber crime .

We invite all our students,faculty and staff to come out openly if they come across any such cyber crime incidences with them /with their friends. You can meet below faculty members /contact the related cyber crime government officials or Government portals for suitable help.

Please Contact :

SaIT - Cyber Crime Awareness Cell :

Dr. Ravishankar.C.V. –HOD-ECE, NAAC Coordinator,
echodsait@gmail.com, 9986155861.

Dr. Sanjeetha. – HOD-CSE(Cyber Security),
sanjeetha@sambhram.org, 9880251131.

Students Grievance Menu at www.sambhramit.com

Email to : ccdcell.sait@gmail.com

Cyber crime Police Station :

Cyber Crime Police Station, CID Annexe Building, Carlton House, 1, Palace Road, Bengaluru, Karnataka 560001. Phone: +918022094480

Dial 112

Central Government :

Ministry of Home Affairs has operationalized a toll-free helpline number '1930' (which was earlier 155260) to help people immediately report any sort of financial fraud on the "Citizen Financial Cyber Fraud Reporting and Management System".

You can email (helpdesk@nr3c.gov.pk) or contact on 051-9106384, 051-9106690, 051-9106691, or 1991

National Cyber Crime Reporting Portal (Helpline Number - 1930 **(9.00 AM to 6 PM))**

https://cybercrime.gov.in/Webform/Helpline.aspx