CS-27
Cyber Security Journal

Index

Unit 2

Unit 3

Unit 4

Unit 5

Prepared By: Prof. Harsh Joshi

Unit 2

1) Checklist for reporting cybercrime at Cyber crime Police station.

Ans.

checklist for reporting a cyber crime at a Cyber Crime Police Station in India:

Before You Go:

- **Gather Evidence:**
  - Take screenshots or printouts of relevant online activity (e.g., phishing emails, scam messages, social media posts).
  - Save any chat logs or online conversations.
  - Note down any time stamps, reference numbers, or usernames associated with the crime.
- **Write a Complaint:** Briefly describe the incident, including the date, time, and nature of the crime. Mention the websites or platforms involved and the extent of damages incurred.

At the Police Station:

- **Report the Crime:** Report the incident to the officer on duty and express your desire to file a First Information Report (FIR).
- **Provide Details:** Provide a clear and concise account of the crime, including the evidence you've collected.
- **Cooperate with Investigation:** Be prepared to answer questions and cooperate with any investigation procedures.

Documents Required (May vary depending on the station):

- A written complaint
- Photo identification proof (e.g., Aadhaar card, PAN card, Driver's license)
- Copy of the FIR (if available)
- Evidence related to the crime (screenshots, printouts, chat logs)
- Complaint reference number (if available in online complaints)

Additional Tips:

- **Be calm and composed.**
- **Maintain a clear chronology of events.**
- **Avoid sharing confidential information on social media.**
- **If unsure about the procedure, ask the officers for guidance.**

By following these steps, you can effectively report a cyber crime and assist law enforcement in their investigation.

Here are some resources that you might find helpful:

- National Cyber Crime Reporting Portal: https://cybercrime.gov.in/
- Cyber Crime Helpline: 1930

2) Checklist for reporting cyber crime online.

Ans.

Online Reporting:

- **Find the Right Platform:**
  - Look for your country's dedicated cyber crime reporting portal (search online for "[your country] cyber crime complaint").
  - If no such portal exists, report to your local police department's website (search for "[your city/state] police department online reporting").
  - Consider reporting to relevant platforms where the crime occurred (e.g., social media platforms).
- **Fill Out the Report:** Provide accurate and detailed information about the crime, including:
  - Date and time of the incident
  - Description of the crime
  - Any usernames, websites, or platforms involved
  - Financial losses (if applicable)
  - Upload your evidence (screenshots, etc.)
- **Submit the Report:** Follow the online instructions for submitting your report. You might receive a reference number for future reference.

3) Reporting phishing emails.

Ans.

Phishing emails are a specific type of cybercrime and reporting them can help protect yourself and others. Here's what you should do:

Don't Click or Reply: Clicking links or replying to phishing emails can be dangerous. It can download malware or expose your information.

Report the Email:

- **Email Provider:** Most email providers have a way to report phishing emails directly. Look for options like "Report Phishing" or "Report Spam."
  - Here are some specific examples:
    - Gmail: Open the email and click "More" then "Report phishing." (https://support.google.com/mail/answer/8253?hl=en)
    - Outlook: Select the email and choose "Junk" then "Phishing." (https://support.microsoft.com/en-us/office/phishing-and-suspicious-behavior-0d882ea5-eedc-4bed-aebc-079ffa1105a3)
- **Anti-Phishing Working Group (APWG):** You can also forward the suspicious email to reportphishing@apwg.org. This is a central reporting body that helps identify and takedown phishing campaigns.

4) **Demonstration of email phishing attack and preventive measures.**

Ans.

Scenario: You receive an email that appears to be from your bank, [Bank Name]. The subject line is: "Urgent Action Required: Verify Your Account Information." The email body looks professional and uses your bank's logo. It claims there has been suspicious activity on your account and prompts you to immediately verify your information by clicking a link. The email warns that failure to do so could result in account suspension.

Red Flags (Signs this is a Phishing Attempt):

- **Sense of Urgency:** Phishing emails often create a sense of urgency or panic to pressure you into acting quickly without thinking critically.
- **Generic Greeting:** The email might use generic greetings like "Dear Customer" instead of your actual name.
- **Suspicious Link:** Don't hover over the link! The link text might say "Verify Account" but the actual destination URL could be completely different.
- **Threat of Suspension:** Legitimate companies won't threaten to suspend your account via email.

Preventive Measures:

Don't Click Links in Suspicious Emails:

- Never click on links or download attachments from emails you don't recognize or suspect might be phishing attempts.

Verify Sender Information:

- Check the sender's email address carefully. Phishing emails often use email addresses that closely resemble the real company's address, but with slight variations (e.g., misspelling a letter).

Go Directly to the Source:

- Instead of clicking the link in the email, navigate to your bank's website directly by typing the web address you know is legitimate (e.g., [Bank website address]) into your browser.

Check Login Information:

- Once on the legitimate bank website, log in to your account and check for any suspicious activity or requests to update information.

Report Phishing Emails:

- Report the phishing attempt to your email provider and consider forwarding it to the Anti-Phishing Working Group (APWG) at reportphishing@apwg.org.

Enable Two-Factor Authentication (2FA):

- Many banks and online services offer 2FA, which adds an extra layer of security by requiring a code from your phone or another device in addition to your password when logging in.

Unit 3

1) Basic checklist, privacy and security settings for popular Social media platforms.

Ans.

This checklist covers some general settings to consider for popular social media platforms. Remember, specific options might vary slightly depending on the platform you use.

General Settings:

- **Review Privacy Settings:** Find the privacy settings section within your account settings. This will allow you to control who can see your profile, posts, and activity.
- **Limit Who Can See Your Posts:** Choose who can see your posts (public, friends only, or custom settings).
- **Review Profile Information:** Control what information is publicly visible on your profile.
- **Location Sharing:** Disable location sharing by default or limit who can see your location.
- **App Permissions:** Review and manage permissions granted to third-party apps connected to your social media account. Revoke access for apps you no longer use.

Password & Login Security:

- **Strong & Unique Passwords:** Use a strong and unique password for each social media account. Consider using a password manager.
- **Enable Two-Factor Authentication (2FA):** Enable 2FA for an extra layer of login security. This typically requires a code from your phone in addition to your password.
- **Beware of Phishing Attempts:** Don't click on suspicious links or attachments in messages or emails claiming to be from the social media platform.

Additional Considerations:

- **Review Tagged Posts:** Choose who can tag you in posts and whether you want to approve tags before they appear on your profile.
- **Direct Messages:** Control who can send you direct messages or limit messages to friends only.
- **Public vs. Private:** Consider making your account private if you only want to share content with a limited audience.

- **Regular Reviews:** Make it a habit to review and adjust your privacy settings periodically as your needs or the platform features evolve.

Here are some resources for specific social media platforms:

- **Facebook:** https://www.facebook.com/help/193677450678703
- **Instagram:** https://help.instagram.com/196883487377501
- **Twitter:** https://twitter.com/settings?lang=en

2) **Reporting and redressal mechanism for violations and misuse of Social media platforms.**

Ans.

Social media platforms have reporting and redressal mechanisms in place to address violations and misuse. Here's a breakdown of the typical process:

Reporting:

- **In-Platform Reporting:** Each platform has built-in reporting tools. You can typically find a "Report" button or option next to the content you find offensive or violating their terms of service. This might include hate speech, bullying, harassment, spam, or copyright infringement.
- **Report Content Type:** Select the specific reason for reporting (e.g., hate speech, bullying, etc.). Some platforms allow you to report entire accounts or profiles.
- **Provide Details (Optional):** While optional, consider adding details about the violation to help the platform review the content effectively.

Review Process:

- **Platform Review:** The platform will review your report based on their community guidelines and terms of service.
- **Response Time:** This can vary depending on the platform and severity of the violation. Some offer time estimates for addressing reports.

Possible Outcomes:

- **Content Removal:** If the platform finds a violation, they might remove the reported content.
- **Account Suspension/Termination:** For repeated violations or severe offenses, the platform might suspend or even terminate the offending account.
- **No Action Taken:** In some cases, the platform might decide the content doesn't violate their policies and take no action. You might have the option to appeal this decision.

Additional Options:

- **Blocking:** You can block the offending user to prevent them from contacting you or seeing your content.

- **Law Enforcement:** For serious crimes like online threats or harassment, consider reporting the incident to law enforcement officials.

Limitations of Platform Reporting:

- **Subjectivity:** Defining violations can be subjective. What one person finds offensive, another might not.
- **Resource Constraints:** Social media platforms handle massive amounts of content. Reviewing every report thoroughly can be challenging.
- **Platform Bias:** Platforms might be hesitant to take action against influential users or content that generates engagement.

Alternative Reporting Mechanisms:

- **Government Agencies:** Some countries have government agencies that handle complaints about online content.
- **Industry Bodies:** Industry bodies might have reporting mechanisms for online abuse or harmful content.

Unit 4

1) **Configuring security settings in Mobile Wallets and UPIs**

Ans.

Securing Your Mobile Wallets and UPI Apps

Mobile wallets and UPI (Unified Payments Interface) apps offer convenient ways to transact digitally. However, safeguarding them is crucial to protect your financial information. Here's a checklist for configuring security settings in these apps:

App-Level Security:

- **Enable Strong Passwords or PINs:** Set a strong and unique password or PIN for your mobile wallet or UPI app. Don't use easily guessable codes like birthdays or anniversaries.
- **Enable Biometric Authentication (if available):** Many apps offer fingerprint or facial recognition for logins. These features add an extra layer of security.
- **App Updates:** Keep your mobile wallet and UPI apps updated with the latest security patches. Updates often address vulnerabilities that could be exploited by hackers.
- **App Permissions:** Review and adjust app permissions. Grant only the permissions essential for the app to function. Disable access to features you don't use (e.g., location sharing for a non-location-based mobile wallet).

Transaction Security:

- **Beware of Unknown Senders:** Always verify the recipient's name and virtual payment address (VPA) before initiating a transaction. Double-check for typos or mismatched information.
- **Review Transaction Details:** Before confirming a transaction, carefully review the amount, recipient details, and purpose of the payment.
- **Scrutinize Links:** Don't click on suspicious links received through messages or emails claiming to be from your bank or UPI provider. These could be phishing attempts to steal your login credentials.
- **Transaction Limits:** Consider setting transaction limits on your mobile wallet or UPI app. This can minimize damage in case of unauthorized access.

Additional Security Measures:

- **Multi-Factor Authentication (MFA):** If available, enable MFA for added security during transactions. This typically involves a one-time code sent to your registered phone number or email.

- **Public Wi-Fi:** Avoid making transactions on public Wi-Fi networks as they might be less secure. If necessary, use a VPN (Virtual Private Network) for an extra layer of protection.
- **Suspicious Activity:** Report any suspicious activity or unauthorized transactions to your mobile wallet or UPI provider immediately.

Here are some resources for specific Mobile Wallets and UPI Apps:

- **PhonePe:** https://cms.phonepe.com/en/myhelp/getting-started-phonepe/complete-your-phonepe-profile/secure-your-phonepe-account/
- **Google Pay:** https://cloud.google.com/security/products/security-command-center (Select "Google Pay" from the product list)
- **Paytm:** https://paytm.com/
- **BHIM:** https://www.bhimupi.org.in/

2) **Checklist for secure net banking**

Ans.

Securing Your Computer:

- **Firewall & Anti-virus:** Ensure a robust firewall and up-to-date anti-virus software are installed and running on your computer. These programs help block unauthorized access and detect malicious software.
- **Operating System Updates:** Keep your operating system updated with the latest security patches. These updates often address vulnerabilities that could be exploited by hackers.
- **Limited User Accounts:** Avoid using administrator accounts for everyday tasks. Create a standard user account with limited privileges for net banking activities.
- **Suspicious Software:** Be cautious of downloading and installing software from untrusted sources. This can introduce malware that steals your information.

Net Banking Practices:

- **Official Website:** Always access your bank's website by directly typing the legitimate URL into your browser address bar. Don't rely on links from emails or search results, as they could be phishing attempts.
- **Look for "HTTPS":** Verify the website address starts with "https://" and displays a security lock symbol in the address bar. This indicates a secure connection.
- **Strong & Unique Passwords:** Create a strong and unique password for your net banking account. Don't use the same password for other online accounts. Consider using a password manager.
- **Two-Factor Authentication (2FA):** If available, enable 2FA for your net banking logins. This adds an extra layer of security by requiring a code from your phone or another device in addition to your password.

- **Beware of Phishing Emails:** Don't click on links or attachments in emails claiming to be from your bank. These emails might try to steal your login credentials.
- **Public Wi-Fi:** Avoid accessing your net banking account on public Wi-Fi networks. These networks are less secure and could be vulnerable to eavesdropping.
- **Logout Properly:** Always log out of your net banking session completely after you finish your transactions. Don't rely on the "back" button to exit.
- **Regular Monitoring:** Regularly review your account statements for any unauthorized transactions. Report any suspicious activity to your bank immediately.

Additional Security Measures:

- **Dedicated Computer:** Consider using a dedicated computer for net banking, especially if you use your computer for other online activities like browsing or checking email.
- **Virtual Keyboard:** Some banks offer virtual keyboards on their net banking platforms. This can help prevent malware from capturing your keystrokes when entering your password.
- **SMS Alerts:** Enable SMS alerts from your bank to receive notifications about transactions and login attempts.

Unit 5

1) Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).

Ans.

1. Windows with Local Accounts:

- BIOS Password: BIOS password settings are typically accessed during system startup, often by pressing a specific key (e.g., DEL, F2). These settings are usually independent of the operating system and may have limited configuration options beyond enabling/disabling password protection and setting a basic password.
- Administrator and Standard User Accounts: Windows offers local account management tools. You can configure password policies like minimum password length, complexity requirements (uppercase, lowercase, symbols), and password history (preventing reuse of recent passwords) using the Local Security Policy:
    1. Press **Windows Key + R** to open the Run dialog.
    2. Type **secpol. msc** and press Enter.
    3. Navigate to **Account Policies > Password Policy**.
    4. Here you can configure settings like:
        - **Minimum password length**
        - **Require passwords to meet complexity requirements**
        - **Enforce password history** (number of previous passwords users cannot reuse)
        - **Maximum password age** (how often users must change passwords)

2. Windows in a Domain Environment:

If your computer is part of a Windows Domain, password policies are likely centrally managed through Group Policy. Local Security Policy settings might be greyed out or inaccessible. In this case, IT administrators will manage domain-wide password policies.

3. Other Operating Systems:

Mac, Linux, and other operating systems may have their own built-in tools for managing user accounts and password policies. Consult your system's documentation for specific instructions.

2) Setting and configuring two factor authentications in the Mobile phone.

Ans.

Two-factor authentication (2FA) adds an extra layer of security to your online accounts. Here's how to set up and configure 2FA on your mobile phone:

General Steps:

1. **Enable 2FA on the Account:**
   - Sign in to the online account you want to secure with 2FA (e.g., social media, email).
   - Navigate to the account security settings. This might be labeled "Security," "Two-factor authentication," or something similar.
   - Look for an option to enable 2FA and choose your preferred method (more on methods below).
2. **Install an Authenticator App (if needed):**
   - Many services rely on authenticator apps to generate unique codes for 2FA. Popular options include Google Authenticator, Microsoft Authenticator, and Authy. Download one from your phone's app store.
3. **Link the App to your Account:**
   - The account you're enabling 2FA for might provide a QR code or a secret key. Open your authenticator app and follow the instructions to scan the QR code or enter the secret key. This links the app to your account.
4. **Verify with a Code:**
   - The next time you log in to the account, you'll likely be prompted for a code after entering your username and password.
   - Open your authenticator app and locate the code for the specific account. Enter the code to complete the login process.

Common 2FA Methods:

- **Authenticator App:** As mentioned above, this is a popular method where the app generates temporary codes for logins.
- **SMS Verification:** You might receive a verification code via text message to your phone number.
- **Security Key:** A physical device you insert into your computer's USB port or use wirelessly (like NFC) to verify your identity.

3) Security patch management and updates in Computer and Mobiles.

Ans.

Computers:

- **What are Patches and Updates?**

    - Patches are updates released by software vendors to fix security vulnerabilities in their programs.
    - Updates can also include bug fixes, performance improvements, and new features.

How to Manage Patches and Updates?

- **Automatic Updates:** Most operating systems (Windows, macOS) offer built-in automatic update features. Enable them to ensure automatic download and installation of critical security patches.
- **Manual Updates:** You can also check for updates manually through your system's settings menu.
- **Third-Party Software:** Software vendors often release updates outside the operating system. Check their websites or within the application itself for update options.

Mobile Phones:

- **The Importance of Updates:** Similar to computers, mobile operating systems (Android, iOS) and apps require updates for security and performance reasons.
- **How to Manage Updates:**
    - **Automatic Updates:** Enable automatic updates in your phone's settings. This ensures timely installation of critical security patches and improvements.
    - **App Updates:** App stores (Google Play Store, Apple App Store) notify you when updates are available for your installed apps. Update them promptly.

4) Managing Application permissions in Mobile Phone.

Ans.

Managing app permissions on your mobile phone is essential for protecting your privacy and security.

Managing Permissions:

1. Open the **Settings** app on your Android phone.
2. Navigate to **Apps & notifications** or **Apps** (depending on your device).
3. You'll see a list of installed apps. Tap the app you want to manage permissions for.
4. Look for a section labeled **Permissions**. Here you'll find a list of all permissions the app has requested.
5. Toggle the switch next to each permission to **Allow** or **Deny** access.

Additional Tips:

- Review app permissions carefully before granting access.
- Only allow permissions that are essential for the app's functionality.

- Android allows some granular controls for certain permissions, like allowing location access only while the app is in use.
- Consider using a privacy-focused app review website or resource to get insights into app permissions before installing.

5) Installation and configuration of computer Anti-virus.

Ans.

1. Choosing an Antivirus:

There are many reputable antivirus programs available, both free and paid. Here are some factors to consider when choosing one:

- **Features:** Look for features like real-time protection, malware scanning, phishing protection, and firewall capabilities.
- **Performance:** Antivirus software can impact system performance. Choose one that offers a good balance of protection and resource usage.
- **Reputation:** Opt for antivirus software from a well-established and trusted security company.

2. Downloading the Antivirus:

- **Official Websites:** Download the antivirus software installer from the official website of the vendor you choose. Avoid downloading from untrusted sources.
- **Free vs. Paid:** Some antivirus programs offer free versions with basic features, while paid versions offer additional functionalities.

3. Installation Process:

- **Double-click the downloaded installer file.**
- **Follow the on-screen instructions.** This typically involves accepting a license agreement and choosing installation settings.
- **In some cases, you might need to disable your existing antivirus software (if any) before installing the new one.**

4. Configuration:

- **Most antivirus programs offer a user-friendly interface for configuration.**
- **Here are some common settings you might want to adjust:**
  - **Real-time protection:** Ensure real-time protection is enabled to continuously monitor your system for threats.
  - **Scheduled scans:** Schedule regular automatic scans to proactively check your system for malware.
  - **Email protection:** Enable email protection to scan incoming and outgoing emails for malicious attachments.
  - **Firewall settings:** Some antivirus programs have built-in firewall functionalities. You can configure these settings to control incoming and outgoing network traffic.

6) Installation and configuration of Computer Host Firewall.

Ans.

Most computers already have a built-in firewall, so installation typically isn't necessary. Here's a guide on configuring your computer's firewall:

1. Identifying Your Firewall:

- **Windows:** Windows comes with a pre-installed firewall called "Windows Defender Firewall."
- **macOS:** Mac computers have a built-in firewall called "Firewall."
- **Linux:** Linux distributions often come with firewall software like "iptables" or "firewalld." You might need to consult your specific distribution's documentation for details.

2. Accessing Firewall Settings:

Windows:

1. Click on the **Start** menu and search for "Windows Security."
2. Open **Windows Security**.
3. Click on **Firewall & network protection**.
4. You'll see options to manage settings for each network profile (e.g., Public, Private).

macOS:

1. Click on the **Apple** menu and go to **System Preferences**.
2. Select **Security & Privacy**.
3. Click on the **Firewall** tab.

Linux:

Accessing and configuring a Linux firewall can vary depending on the specific distribution and software used. Refer to your distribution's documentation for detailed instructions.

3. Configuring the Firewall:

Basic Firewall Settings:

- **Enable/Disable Firewall:** You can usually enable or disable the firewall completely. Disabling it is **not recommended** as it leaves your computer vulnerable.
- **Network Profiles:** Some firewalls allow configuration for different network profiles (e.g., Home, Public). You might have stricter rules for public Wi-Fi networks compared to your home network.

Advanced Firewall Settings:

(These options may not be available on all firewalls)

- **Inbound & Outbound Rules:** You can create rules to allow or block specific programs or ports from accessing the network. This allows granular control over what applications can communicate externally.
- **Public Network Behavior:** Configure how the firewall behaves when connected to public Wi-Fi networks.
- **Logging:** Enable logging to monitor firewall activity and identify potential security incidents.

7) Wi-Fi security management in computer and mobile.

Ans.

Wi-Fi security management is essential for protecting your devices and data on both computers and mobiles.

Securing your Wi-Fi Network:

1. **Strong Password:** Change the default password of your Wi-Fi router to a strong, complex password with a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using easily guessable words or personal information.
2. **Encryption:** Most modern routers support WPA2 (Wi-Fi Protected Access II) encryption. Ensure WPA2 encryption is enabled on your router. Avoid using older and less secure encryption methods like WEP (Wired Equivalent Privacy).
3. **Guest Network:** Consider creating a separate guest network for visitors. This allows them internet access without exposing your main network and devices.
4. **Network Name (SSID):** Change the default SSID (network name) of your router to a non-descriptive name. Avoid including any personal information.
5. **MAC Address Filtering:** Some routers allow MAC address filtering, which restricts access to devices with specific MAC addresses (unique hardware identifiers). While not foolproof, it can add an extra layer of security. (Note: MAC address spoofing can bypass this filtering).
6. **Disable Remote Management:** If you don't need to remotely manage your router settings, disable remote access for added security.
7. **Firmware Updates:** Keep your router's firmware up-to-date. Router manufacturers release updates to address security vulnerabilities.

Securing Wi-Fi on your Devices:

- **Connect to Known Networks:** Only connect to Wi-Fi networks you trust. Avoid connecting to open or public Wi-Fi networks without proper protection (like a VPN).

- **Verify Network:** Double-check the network name (SSID) before connecting to ensure you're joining the intended network.
- **VPNs for Public Wi-Fi:** If using public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your internet traffic and add an extra layer of security.
- **Disable Automatic Connections:** On your devices, disable automatic connection to Wi-Fi networks to avoid accidentally connecting to unsecured networks.
- **Strong Passwords for Devices:** Use strong passwords for your Wi-Fi connections on each device to prevent unauthorized access.