RUDRAM DYNAMICS

IITM PRAVARTAK CATALYSING INNOVATION

SURAKSHIT BHARAT

CYBERSECURITY AWARENESS WORKSHOP

KEY TAKEAWAYS NOTES

1. Phishing Attacks

How It Works:

Cybercriminals send fraudulent emails, messages, or websites pretending to be legitimate entities (e.g., banks, government agencies) to trick individuals into revealing personal information.

Example:

An email that looks like it's from your bank asking you to verify your account details by clicking on a link that leads to a fake website.

What to Watch Out For:

- Verify the sender's email address: Ensure the email is coming from a legitimate source by looking closely at the email address.
- Check the return path: Ensure the return address is the same as the sender’s email domain.
- Inspect the URL: Hover over any links to ensure they lead to the correct domain

---

2. Malware

How It Works:

Malware can be installed on your device without your knowledge, often through malicious websites or downloads, enabling cybercriminals to capture sensitive data.

Downloading a free game from an untrusted website that installs a keylogger.

What to Watch Out For:

- Use reputable antivirus software: Ensure your device is equipped with up-to-date antivirus programs.
- Be cautious when downloading files: Avoid downloading from untrusted sources or websites.

---

3. Social Engineering

How It Works:

Attackers manipulate individuals into voluntarily giving up personal information by impersonating someone trustworthy.

Example:

A scammer calls you, pretending to be from your bank, and asks for account verification details.

What to Watch Out For:

- Verify identity: Ask for verification details to the call, that only the legitimate party would know.
- Avoid sharing sensitive data over the phone: When in doubt, hang up and call the official customer service number directly.
- Stay calm under pressure: Scammers often use urgency to trick you into acting quickly without thinking.
- Never share OTP or any personal information with **ANY** authorities like bank, telephone ,police etc. **NEVER**

RUDRAM DYNAMICS

IITM PRAVARTAK CATALYSING INNOVATION

4. Use Strong Passwords

How It Works:

Using weak passwords or reusing the same password across multiple accounts makes it easier for hackers to compromise your accounts.

Example:

A hacker gains access to your email using a weak password and resets passwords for other accounts.

What to Watch Out For:
Use strong, unique passwords: A combination of uppercase, lowercase, numbers, and symbols is more secure. 10-12 chars password is strong

- Enable two-factor authentication (2FA): For added security, use 2FA on your accounts.

---

5. Public Wi-Fi and Unsecured Networks

How It Works:

Information sent over unsecured public Wi-Fi can be intercepted by attackers using techniques like man-in-the-middle attacks.

Example:

Logging into your bank account on public Wi-Fi, allowing a hacker to capture your login details.

What to Watch Out For:

- Avoid sensitive transactions on public Wi-Fi: Do not log into sensitive accounts over public networks.
- Use a VPN: Virtual Private Networks (VPNs) encrypt your data, making it harder for hackers to intercept.
- Disable automatic connections: Ensure your devices do not automatically connect to public Wi-Fi.

6. Identity Theft via Social Media

How It Works:

Attackers gather personal information from public social media profiles to steal your identity.

Example:

An attacker gathers your birthday and location from social media to guess your passwords or impersonate you.

What to Watch Out For:

- Limit the personal information you share: Avoid sharing sensitive data such as your address or birthdate publicly.
- Adjust privacy settings: Make sure your social media profiles are set to private.
- Be mindful of what you post: Think carefully about the personal information in your posts and profiles.

---

7. Publicly Available Information

How It Works:

Attackers use publicly available information, such as home addresses or phone numbers, to impersonate you or answer security questions to gain access to your accounts.

Example:

An attacker uses your publicly listed phone number and email to reset your account password.

What to Watch Out For:

- Limit what you share publicly: Be cautious about where you post your personal information.

- Use stronger security questions: Make sure your security questions are difficult to guess based on publicly available information.

---

8. Fake Apps and Software

How It Works:

Attackers create fake apps or websites that look legitimate, but upon download or interaction, they install malware or collect sensitive information.

Example:

Downloading a fake banking app that collects your login details.

What to Watch Out For:

- Only download apps from official stores: Stick to trusted sources like the Google Play Store or Apple's App Store.
- Check app reviews: Look for reviews and app ratings before downloading.
- Inspect app permissions: Be mindful of the permissions requested by apps; they should make sense for the app's function.

---

9. Shoulder Surfing and Physical Snooping

How It Works:

Attackers physically observe or "shoulder surf" while you enter sensitive information in public places, such as ATMs or cafes.

Example:

An attacker watches you enter your PIN at an ATM.

What to Watch Out For:

- Be aware of your surroundings: Shield your screen or keypad when entering sensitive information in public.
- Use strong passcodes: Ensure your devices are protected with strong passwords or PINs.
- Enable encryption: Protect sensitive data on your devices by encrypting files and drives.

---

10. Ransomware

How It Works:

Ransomware encrypts your files and demands payment in exchange for the decryption key, potentially locking away personal information.

Example:

Ransomware infects your computer, encrypting files, and demands payment to unlock them.

What to Watch Out For:

- Keep regular backups: Ensure that important files are regularly backed up to a secure location.
- Avoid suspicious downloads: Be cautious when downloading files or clicking on links in emails.
- Keep your software and AntiVirus updated: Regular updates help protect against known vulnerabilities.

---

11. QR Code Scams

How It Works:

Attackers create malicious QR codes that direct victims to phishing websites or prompt them to download malware when scanned.

Example:

Scanning a QR code at a restaurant that leads to a fake payment site where you enter your banking details.

What to Watch Out For:

- Verify the source: Only scan QR codes from trusted sources.
- Double-check URLs: When scanning QR codes, always inspect the URL you are directed to before entering personal information.
- Before paying anyone, make sure that the name of the shop owner is the same as the one that you see on your mobile phone after scanning the QR code (before you pay)

12. Safe Browsing

How It Works:

When you browse the internet, it's essential to protect yourself from tracking, cookies, and other methods that may compromise your personal information

Example:

Many websites use cookies to track your online activity, often for advertising, personalization

What to Watch Out For:

- Ensure the site uses HTTPS: A secure website will display “https://” at the beginning of the URL.
- Avoid unfamiliar or suspicious websites.

13. Secure Communication

How It Works:

Sensitive information shared over unsecured channels can be intercepted by attackers.

Example:

Sending personal information via unencrypted email.

What to Watch Out For:

- Use end-to-end encrypted messaging services for sensitive information.
- Avoid sharing personal information over unsecure communication methods.
- Verify the recipient's identity before sharing sensitive data.
- User encrypted emails like proton mail (https://proton.me/mail) for secure comms

---

14. Honey Trapping

How It Works:

An attacker uses fake relationships or social connections to extract sensitive information or financial assets from victims.

Example:

A cybercriminal befriends you online, gaining your trust, and later uses this to ask for money or personal information.

What to Watch Out For:

- Be cautious of new connections that seem too good to be true.

- Do not share personal or financial details with people you just met online.
- Verify the authenticity of individuals before trusting them with sensitive information.
- Never pick up video calls on whatsapp or any other such apps , if you don’t have the incoming contact number, in your contact list
- If at all you are compromised, DON’T PANIC. Talk to your family and friends, file an FIR to the police and submit the FIR copy with other details to the social media platforms

---

15. ALWAYS KEEP YOUR SOFTWARE UPDATED WITH THE LATEST VERSIONS

16. ALWAYS USE ANY REPUTED ANTI VIRUS IN YOUR PHONE AS WELL AS COMPUTER

RUDRAM DYNAMICS

IITM PRAVARTAK CATALYSING INNOVATION

WHAT TO DO IF YOUR INFORMATION SECURITY HAS BEEN COMPROMISED

If you are a victim of cyberbullying or have been hacked, it's important to act quickly to safeguard your data and well-being. Here's a step wise guide on what to do:

1. **Collect Evidence:**
    - Save screenshots of any abusive messages, posts, or harmful content.
    - Record dates, times, and the nature of the incident (for example, what accounts were compromised or the type of cyberbullying received).
    - Keep all related emails, texts, or messages as proof.

2. **Change Passwords and Secure Accounts:**
    - If your account is hacked, immediately change your passwords for all compromised accounts.
    - Enable two-factor authentication (2FA) on all accounts to add an extra layer of security.
    - Check for any suspicious activity in your account history, such as unauthorized logins.

3. **Lodge a Complaint with Cyber Crime Authorities:**
    - India's cyber crime cells work on investigating offenses such as cyberbullying, hacking, and online fraud.
    - You can file an online complaint with the National Cyber Crime Reporting Portal.

Online Complaint>

- Visit the National Cyber Crime Reporting Portal: cybercrime.gov.in
- Submit the necessary details along with any evidence (screenshots, messages, etc.).
- You can also file the complaint anonymously if you wish.

Local Cyber Crime Cell>

- You can visit your nearest police station or a dedicated cyber crime cell to file an FIR in person.
- You can find your nearest Cyber Crime Cell through this link: State-wise Cyber Crime Cells

4. **Report to Social Media Platforms:**
    - Most social media platforms, such as Facebook, Twitter, Instagram, and YouTube, have specific mechanisms to report abusive content or accounts.
    - Block the bully/hacker immediately on all platforms.
    - Check for any suspicious activity in your account history, such as unauthorized logins.

RUDRAM DYNAMICS

IITM PRAVARTAK CATALYSING INNOVATION

KEY HELPLINE NUMBERS AND RESOURCES

1. **Cyber Crime Helpline (National):**
    - Helpline Number: 1930 (24x7 helpline for financial cyber fraud complaints)
    - National Cyber Crime Reporting Portal: cybercrime.gov.in
2. **Indian Computer Emergency Response Team (CERT-In):**
    - Website: cert-in.org.in (for technical assistance in cases of hacking and data breaches).
    - Incident Reporting: Report incidents of cyber security breaches.
3. **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):**
    - Website: cyberswachhtakendra.gov.in
    - Provides free tools to remove malware from your device.
4. **Online Financial Fraud Reporting Helpline:**
    - Helpline Number: 1930
    - If you have been financially hacked or duped, immediately call 1930 and report the fraud to block transactions and trace the hacker.