Cyber Safety Awareness Month (NCSAM) - Cyber Hygiene

1. Use Strong, Unique Passwords

- Avoid simple passwords like "123456" or "password" or "pets name", "first/last name."
- Create passwords that are at least 12 characters long, using a combination of upper and lowercase letters, numbers, and symbols. Consider using a password manager to generate and store passwords.

2. Enable Two-Factor Authentication (2FA)

- Enable 2FA for all major accounts (email, banking, social media). Typically, 2FA sends a unique code to your phone or email to verify your identity. Some platforms also offer app-based authentication for added security.

3. Beware of Phishing Scams

Phishing emails or messages trick users into providing sensitive information or clicking on malicious links that install malware or steal credentials.

- Be suspicious of unsolicited emails or messages asking for personal information. Look for signs of phishing like poor grammar, unknown sender addresses, or urgent reply requests.
- Always verify the sender before clicking on any links or providing information. When in doubt, don't click.
- Don't click on suspicious links or attachments in emails and messages from unknown senders.

4. **Keep Your Software, Apps, and Operating Systems Up to Date**

- Regularly update your devices and apps. Software updates often contain security patches that protect you from new threats.
- Enable automatic updates on your devices, including your computer, smartphone, and apps. If manual updates are required, check for them regularly—especially for your antivirus software, browser, and operating system.

5. Use Antivirus and Firewall

- Install trusted antivirus software and keep it updated to protect against the latest threats. Make sure your firewall is turned on to block harmful traffic from reaching your network.

6. Secure Your Wi-Fi

- Use a strong password for your home Wi-Fi network.

- Change the default name (SSID) and password of your router. Use WPA3 encryption if available, or WPA2 as a minimum. Disable remote management of your router and ensure your firmware is up to date. Also, hide your network's SSID to make it less visible to potential hackers.
- Avoid conducting sensitive activities like online banking, shopping, or accessing personal accounts on public Wi-Fi. If you must use public Wi-Fi, connect through a VPN (Virtual Private Network) to encrypt your traffic and protect your privacy.

7. Be Careful with Personal Information

- Think before sharing personal details online. Avoid oversharing on social media, as it can make you a target for cybercriminals with valuable information to steal your identity or launch targeted attacks like social engineering or phishing.
- Review and adjust the privacy settings on your social media accounts to control who can see your posts and personal information. Avoid sharing details like your home address, phone number, and vacation plans publicly. Be cautious when filling out online forms that request unnecessary personal information.

8. Regularly Backup Your Data

- Backing up your data ensures that you don't lose important files in the event of a cyber-attack (such as ransomware), hardware failure, or accidental deletion.
- Set up automatic backups for important files. Use an external hard drive or cloud storage service to store your backups, and ensure they're disconnected from your system when not in use to prevent them from being compromised.

9. **Log Out of Accounts After Each Session**

- Staying logged into important accounts like email, banking, or social media on shared devices can expose your personal information to others.
- Always log out of accounts when you finish using them, especially on shared or public devices. On personal devices, configure them to lock automatically after a period of inactivity.

10. Monitor Financial and Online Accounts Regularly

- Early detection of suspicious activity can prevent financial losses or further identity theft.
- Regularly check your bank statements, credit card bills, and online accounts for unfamiliar transactions or changes. Set up account alerts for any unusual activity, such as login attempts from unknown locations or purchases exceeding a certain amount.

11. Be Mindful of App Permissions

- Some apps request excessive permissions to access data they don't need, potentially compromising your privacy.

- Review the permissions requested by apps before installing them. Disable access to unnecessary data like your location, contacts, or camera if the app doesn't require them to function. Only download apps from official stores like Google Play or the Apple App Store.

What to Do If You Suspect a Cybercrime

- **Report the Crime**: If you suspect you've fallen victim to a cybercrime such as identity theft, phishing, or hacking, report it immediately to the appropriate authorities. Incase of Financial frauds, contact National Cybercrime Helpline **1930** immediately, or visit **National Cybercrime Reporting Portal(NCRP): https://www.cybercrime.gov.in** or reach out to the nearest police station for help.
- **Take Immediate Action**: Promptly change any compromised passwords, monitor your financial accounts for unauthorized transactions, and disconnect any affected devices from the internet to prevent further damage, in case of financial frauds, immediately block your accounts by calling respective bank customer cares by visiting official bank website or calling the official customer care number provided by bank (do not search for bank or other agency customer care number on search engines as sometimes they might mislead).

Stay safe online – be vigilant, stay informed, and protect your digital life!

#BeAlert, #BeSecure, #BeSafe, #cybersafetyawareness #ncsam