Cyber Suraksha Dishaanirdesh Vol. 11

Information security cannot exist in a vacuum, every individual's contribution is imperative! All swasth sarathis must follow the following guidelines to maintain information security and data privacy at NHA.

1. KEEP A CLEAN MACHINE

Plug and scan: USBs and other external devices can be infected by viruses and malware. Always scan the device before transferring information.

Automate Software Updates: Many software programs will automatically connect and update to defend against known risks. Always turn on automatic updates for security software.

Use internet safely: Secure online habits reduces the opportunities for attackers to install malware or steal personal information of beneficiaries enrolled. Avoiding malicious sites, never ignore warning messages from your browser, never ignore 'Website security certificate' error.

2. PROTECT YOUR PERSONAL DATA

Lock down your login: For protection of key accounts, just username and password aren't enough. Fortify online accounts by enabling the strongest authentication tool available, such as biometrics, security keys, or a unique one-time code through an app on your mobile device.

Use strong and unguessable passwords: Passwords that are found in common password lists or permutations of your username are examples of passwords that can be cracked easily. It is advisable to make your password a sentence, about 8-12 characters long with numeric values and special characters.

Unique account, Unique password: Always use separate passwords for every account. This helps to thwart cybercriminals and help prevent them from leveraging a compromised password to access firm services.

3. CONNECT WITH CARE

When in doubt, throw it out: Links and attachments in emails, tweets, posts and online advertising are common ways cybercriminals try to compromise your information. If it looks suspicious, its best to delete it.

Cyber Suraksha Dishaanirdesh Vol. 11

4. SECURING YOUR MOBILE DEVICES

SMS Phishing: SMS messages are quickly becoming a common method for cybercriminals to attack or fool people. Never reply or click on URLs as they are laid as baits by cybercriminals to gain access to the device to either steal information or infect the device.

Bluetooth: Bluetooth allows your mobile devices to wirelessly communicate with other devices, such as your headphones or with your computer. However, Bluetooth is kept if kept on servs as a entry point for cybercriminals as they can remotely connect using Bluetooth and then either steal information or infect the device.

5. SECURITY GUIDLEINES FOR WORKPLACE

Shield yourself from shoulder surfers: someone may see you type your password or see any sensitive information on your desktop/ laptop screen.

Strictly follow Clean Desk and Desktop Policy: Always remember to shred unwanted documents and keep important documents locked in cabinets.

Since our work devices contain confidential information, never share your work devices such as cellphones, tablets or laptops with others.

Lock the system: If you leave your computer on and walk away from it, make sure you password lock the screen (Windows + L) . This means that if anyone walks up to your computer, they cannot access your information.

6. BE AWARE OF SOCIAL ENGINEERING

Never disclose potentially sensitive information to an unknown source, and never give out more information than seems necessary.

When asked for potentially sensitive data by someone you don't recognize, always ask to see their identification. Be wary of emails or websites that ask you to confirm sensitive information belonging to you or your member firm.

Cyber Security is a shared responsibility and we each have a role to play.