Cyber Security Awareness

Prepared by:

NIC-WCD

Cyber Security Awareness

Cyber Security is the state or process of protecting and recovering computer systems, networks, devices, and programs from any type of cyber-attack. Cyber security measures are designed to combat threats against networked Systems and applications, whether those threats originate from inside or outside of an organization.

Need of Cyber Security- Our society is more technologically reliant than ever before and various aspects of our being are heavily driven by technology e.g. power, industries, law and order, safety etc. Cyber security thus gains paramount importance as it is imperative for protecting these data sources and IT infrastructure from being misused. This includes sensitive data, official data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property etc.

Goals of Cyber Security- To ensure CIA by keeping out unwanted intruders while providing authorized access.

1) Confidentiality
2) Integrity
3) Availability

Attackers usually target –

- Hardware
- Software
- Data
- Internet/Network
- Disruption of services

Dos & Don'ts

Email

- **Do** check the URL before clicking any link sent via email.
- **Do** report all suspicious activity and cyber incidents to competent authority.
- Official E-mail account should be used for official purpose only.
- Official E-mail should not be forwarded to personal E-mail account.

- **Don't** respond to emails received from strangers
- **Don't** click on links from an unknown or untrusted source
- **Don't** send any personal or sensitive information, such as credit card numbers, passwords or other private information, through email.

Password

- Always follow password policy for creating password to avoid risks involved.
- **Do** use hard-to-guess passwords or passphrases. A password should have a minimum of 10 characters using uppercase letters, lowercase letters, numbers, and special characters
- **Do** change password at regular intervals.
- **Do** use different passwords for different accounts.
- **Do** keep your passwords or passphrases confidential.
- **Do** change password immediately if it is suspected to have been disclosed / compromised and a security incident shall be reported to the competent authority.
- Be careful while entering a password when someone is sitting beside you.

- **Don't** share passwords with others or write them down.
- **Don't** use a password that was used earlier.
- **Do not** use the name of things located around you as passwords for your account.
- **Don't** use the words from dictionary. They can be cracked easily.

Computer / Laptop

- **Do** lock your computer and laptop when not in use.
- **Do** keep all devices, such as laptops and computer physically secured.
- If a device is lost or stolen, report it immediately to competent authority.
- **Antivirus** software should be installed on computer and it should be kept updated.

- **Don't** install unauthorized programs on your work computer / laptop.
- **Don't** leave devices unattended.

Mobile

- **Do** lock your mobile phone when not in use.
- **Do** keep mobile devices, IP phones etc. physically secured.
- **Personal information** should be guarded properly. Requests for personal or account information over the mobile should be avoided.
- If a device is lost or stolen, report it immediately to competent authority.
- Always check what permissions are asked by mobile app which you want to install.
- Advisable to check the reputation of the application before installing it.
- Be cautious about using **geo-location** services. Stalkers can easily access one's location.

- **Don't** respond to phone calls requesting confidential data.
- **Don't** leave mobile unattended.
- **Don't** be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner.

Portable Media

- **Do** lock portable media containing sensitive information in a drawer to reduce the risk of unauthorized disclosure.
- **Do** destroy information properly when it is no longer needed.
- Do use official portable storage media for official purpose and should not be handed over to unauthorized person.
- In case of loss of official portable storage media, it should be reported to the competent authority at the earliest.

- **Don't** leave portable media containing sensitive information on your desk.
- **Don't** plug in portable devices without permission. It may contain virus or may be corrupted.

Wireless Connectivity

- **Do** remember that wireless is inherently insecure. Avoid using public Wi-Fi hotspots.
- When you must to use Wi-Fi, use VPN to protect the data and the device.
- **Do** ensure that the wireless interfaces are disabled by default.

- **Don't** leave wireless or Bluetooth turned on when not in use.
- **Secure websites** using **public Wi-Fi should not** be used

Internet Usage

- **Do** use latest version of Internet browser.
- **Do** log-out from web based services, like web mail, before closing the browser session.
- **Do** close the browser session, after completing the activity in the current web based application.
- Cookies should be allowed from the trusted web sites only.

- **Don't** enable "save password" and auto-complete features of the browser.
- **Don't** download or distribute malicious software and tools.
- **Don't** violate any copyright or license agreement by downloading and distributing protected material.

Security from Virus & malicious Code

- **Do** ensure that client system is configured with authorized centrally managed anti-virus software**.**
- **Do** ensure that anti-virus software and the virus pattern files are up-to-date.
- In case a virus does not get cleaned, incident shall be reported to the competent authority.

Web Browser Security

- In case a virus does not get cleaned, incident shall be reported to the competent authority.
- **Latest version** of web browser should be used.

- **Don't** forget to delete browsing history which deletes all the cookies, temp files, history and ActiveX filtering.
- **Don't** forget to turn off all JavaScript or ActiveX support in your web browser before you visit any unknown websites.
- **Don't** give any personal information in any untrusted links.
- **Don't** allow pop-ups and plugins; disable them in the browser settings.

Web Application

- **Security patches and software updates** should be installed as soon as they are available.

Printouts / Faxes

- **Do** lock printouts containing sensitive information in a drawer to reduce the risk of unauthorized disclosure.
- **Do** be aware of your surroundings when printing or faxing sensitive information.
- **Do** pick up information from printers, copiers, or faxes in a timely manner

- **Don't** leave sensitive information lying around the office.
- **Don't** leave printouts or portable media containing private information on your desk.

Social Networking

- **Do** use privacy settings on social media sites to restrict access to your personal information.
- Only add people you KNOW offline.
- If must add strangers, keep your guard up.
- **Convincing imitations** of banks, card companies, charities and government agencies should be watched out carefully.
- **Privacy settings** of profile should be checked and make sure they are set to the right level.
- Even if **social network** is **set to private**, it doesn't guarantee that information is completely private. It should be remembered that friends' friends might be able to see posts and updates even if they are not friends with them. So be careful.

- **Don't** tolerate being uncomfortable
- **Don't** post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites.
- **Don't** over share the information. Sensitive information like birth date, mother's maiden name, pet's name or any other identifying information should not be shared on social-media platforms such as **Facebook, LinkedIn or Twitter.** Social media has made cyber stalking much easier. A stalker can easily locate and track their target's every move. Personal titbits collected over time can give them a whole picture of who you are, where you work, live and socialize

Always remember that, once the internet gets hold of personal or sensitive information, there has no control over it. Anything which can be put up that can be grabbed, copied and saved on someone else's computer and mirrored on other sites.

"Do your part, Be Cyber Smart"