CYBER SECURITY DO’S AND DON’TS

✓ BEST PRACTICES AGAINST PHISHING

- Think before you CLICK
- Practice good cyber hygiene practices both
- Use Multi-Factor Authentication (MFA)
- Verify a website’s legitimacy
- Check all online accounts including social media regularly
- Keep Browser up to date
- Beware of Pop-Ups
- Never disclose Personal Information
- Use genuine and updated software
- Use updated antivirus
- Report the incident
- Periodic Individual awareness

✓ CYBER SECURITY DO’S

- Use complex passwords.
- Change your passwords at least once in 45 days.
- Use multi-factor authentication, wherever available.
- Save your data and files on the secondary drive (ex: d:\).
- Maintain an offline backup of your critical data.
- Keep your Operating System and BIOS firmware updated with the latest updates/patches.
- Install enterprise antivirus client and ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
- Use authorized and licensed software only
- Ensure that proper security hardening is done on the systems
- When you leave your desk temporarily, always lock/log-off
- When you leave office, ensure that your computer and printers are properly shutdown.
- Keep your printer’s software updated with the latest updates/patches.
- Setup unique passcodes for shared printers.
- Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centers.
- Keep the GPS, Bluetooth, NFC and other sensors disabled on

- your computers and mobile phones. They maybe enabled only when required.
- Download Apps from official app stores of google (for android) and apple (for iOS).
- Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user-base, etc
- Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
- Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortened services.
- Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
- Report suspicious emails or any security incident to incident@cert-in.org.in

✓ CYBER SECURITY DON'TS

- Don't use the same password in multiple services/websites/apps.
- Don't save your passwords in the browser or in any unprotected documents.
- Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
- Don't save your data and files on the system drive (Ex: c:\ or root).
- Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: google drive, dropbox, etc.).
- Don't use obsolete or unsupported Operating Systems.
- Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).
- Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.