CYBER SECURITY DO’S (End User)

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Change your passwords at least once in 45 days.
3. Save your data and files on the secondary drive (ex: d:\).
4. Update your system with the latest updates/patches.
5. Install latest Antivirus client.
6. Use authorized and licensed software only.
7. When you leave your desk temporarily, always lock/log-off from your computer session. 1
8. **When you leave office, ensure that your computer and printers are properly shutdown.**
9. Keep the GPS, Bluetooth, NFC and other sensors disabled on your computers and mobile phones.
10. Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
11. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services.
12. 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.
13. Report suspicious emails or any security incident to incident@cert-in.org.in and incident@nic-cert.nic.in.

CYBER SECURITY DON’TS (End User)

1. Don’t save your passwords in the browser or in any unprotected documents.
2. **Don’t upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: google drive, dropbox, etc.).**
3. **Don’t install or use any pirated software (ex: cracks, keygen, etc.).**
4. Don’t open any links or attachments contained in the emails sent by any unknown sender.
5. Don’t disclose any sensitive details on social media or 3rd party messaging apps.