




CYBER SECURITY AWARENESS



DOs

1. While doing banking transactions, paying your bills etc. online, check if the website's URL begins with 'https'. Also look for the padlock  icon, which indicates a secure connection.
2. Go for unique, and hard to guess passwords. Never keep the same password for different online accounts. Create a password with a mix of uppercase and lowercase letters, special characters, and numbers. Change passwords at regular intervals.
3. Avoid using free, unsecured Wi-Fi for shopping or banking on the Internet and even for online social media profiles.
4. Delete old accounts (Email, social media etc.) that you do not use anymore.
5. Never click on links or download attachments from unwanted & unexpected emails, even if such emails look like they are from a known source.
6. Take regular backups of all your important files. Doing this is more important now that ransomware attacks are becoming so rampant.
7. Do not leave system unattended. Log out or lock your computer when stepping away, even for a moment. Always log out of online accounts when you are done.
8. Treat sensitive data very carefully.
9. Use system's screen locking functionality to protect against physical access, such as a screen saver.
10. Scan all the files after you download from websites or links received from e-mails.
11. Be wary of storing personal information on Internet.
12. Verify those you correspond with. It is easy for people to fake identities over the Internet.
13. Make a habit of clearing history from the browser after each logout sessions.
14. Try to avoid cloud services (Dropbox, iCloud, Evernote, etc.) that are based outside India.
15. Be cautious of what you are clicking on / downloading.
16. In general, block all pop-ups and scripts.
17. Avoid Internet access through public / free Wi-Fi.
18. Avoid posting of photos with GPS coordinates.
19. Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for personal / financial information.
20. Before opening any attachment, the same should be scanned through an updated anti-virus for malicious contents.
21. Lock your computer and mobile phone when not in use. This protects data from unauthorized access and use.



CYBER SECURITY AWARENESS



DON'Ts

1. Avoid making your personal information public on social media sites and the Internet in general.
2. Avoid checking 'Keep me logged in' or 'Remember me' options on websites especially on public computers.
3. Never use your official email address for social media sites.
4. Never use any of your personal information such as name, date of birth, address, etc., as your password.
5. Never respond to pop-up ads.
6. Avoid visiting inappropriate websites or websites that you are not fully aware of.
7. Do not install software that comes as an attachment in emails.
8. Avoid saving your banking / financial information on websites and web browsers.
9. Never share your personal / bank details on phone, email or SMS, even if the caller / sender seems genuine.
10. Auto save of password should not be enabled.
11. Do not click any URLs mentioned in the body of the E Mail text.
12. Do not open attachment having extension EXE, DLL, VBS, U64, SHS, PIF , SCR
Typical example: .txt.exe , .doc.exe
13. Don't enter personal or sensitive information online unless you are using a trusted, secure web page.
14. Don't leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured.
15. Don't leave wireless or bluetooth turned on when not in use.
16. Never write down your password, especially on a Post-It note stuck to your computer. Never give out your password to anyone, whether you know them or not.
17. Never reply to e-mail(s) requesting financial or personal information.