Best Practices - Cyber Security (User level)

- Always use genuine software. Install the latest updates/ patches for Operating System, Antivirus and Application software.
- Limit user privileges on the computer. Always access Internet as a standard user but not as Administrator.
- Restrict remote access. If file sharing is not required in your day-to-day work, disable file and print sharing.
- Beware of storing personal information on various Social Media and other platforms.
- Do not share financial details, e-wallet details or banking details with anyone.
- Beware of unsolicited contacts from individuals in person, on the phone, or on the Internet who are seeking organizational or personal data
- Do not share usernames, passwords, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems or schedules and travel itineraries.
- Do not provide information about yourself that will allow others to answer your security questions- such as when using "I forgot my password" feature. Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends and co-workers on Social Media platforms.
- Check and verify email sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
- Be cautious of tiny URLs in Email contents.
- Do not open attachment having extension: VBS, U64, SHS, PIF and SCR.
- Protect against social engineering attacks. Pushing emails and SMS are used to get user Credentials like username, passwords, credit card and PIN numbers etc.
- Regularly check the last log-in details of emails accounts.
- Internet-connected computers Should not be used for drafting storing classified Official documents/correspondences.