Cyber Awareness

Information leakage may lead to great loss as in many cases it can be avoided if the person involved has a better knowledge and awareness in data protection/cyber security. Users are recommended to develop information security mindset, build and reinforce a good security practice through regular updates on information security awareness.

The DOs

- While banking, shopping or paying the bills online, check if the website's URL begins with 'https'. Also look for the padlock icon 🔒, which strongly suggests that the connection is secure.
- Access your bank's website by manually typing its URL in the address bar. Never access it from an email or a text message.
- Download software's from authentic and genuine verified publishers only.
- Go for unique, and hard to guess passwords. Never keep the same password for different online accounts. Create a password with a combination of uppercase and lowercase letters, special characters, and numbers.
- Always change default **PASSWORDS** of your home network Wi-Fi router, phone hotspot or any other devices.
- Do change passwords in regular intervals and never disclose them to anyone.
- Always shred confidential/sensitive documents, such as password, ATM slips etc., which are no longer useful/needed.
- Do lock your computers, laptops and mobile phones etc. when not in use. This protects data from unauthorized access and use.
- Always make sure to log out of online accounts when you are done. This is especially important when you are using a public computer to avoid any unauthorized access to your account.
- Do use privacy settings on social media sites to restrict access to the personal information.
- Use primary email address to stay in touch with people you know or are acquainted with.
- For social media sites, use an email address that you do not use for important communications.
- Do use Add-Blocker Extensions on Web Browsers for preventing unwanted ads from popping up.
- Delete old accounts which are not in use anymore.
- To prevent data loss, always make sure to take regular backups of all important files.
- Ensure that the latest firewalls, antivirus, antispyware, security patches are installed on your devices to help detect and disable malicious content.
- Always keep devices up to date.

The DONT’s

- Do not use free, public Wi-Fi for shopping or banking on the Internet and even for accessing your social media profiles as these WIFI’s may be insecure.
- Do not visit any unknown websites.
- Do not respond to unwanted pop-up ads, that may come up on your screen while accessing any websites. Close such pop-ups from the task manager.
- Do not tick the box of save password while logging or accessing into any sites.
- Do not use your official email address for social media sites.
- Do not share personal information on internet or social media.
- Do not post any official, private or sensitive information, such as credit card numbers, passwords on public sites, including social media sites, and do not send them through email unless authorized to do so.
- Do not include your personal information such as name, date of birth, address, etc., to create your password.
- Do not save your credit/debit card details on any websites and web browsers.
- Do not share your personal/bank details on phone, email or SMS, even if the unknown caller/senders seem genuine.
- Do not click on links or download attachments in unwanted, unexpected emails, even if such emails look like they are from a known source.
- Do not respond to phone calls or emails requesting confidential data.
- Do not 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.
- Do not leave sensitive/confidential information lying around unattended.
- Do not leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured.
- Do not attach unknown devices to your USB ports.