Online Security: Do’s and Don’ts

Online security, also known as cybersecurity, refers to the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access. It encompasses a wide range of measures and technologies designed to safeguard the confidentiality, integrity, and availability of digital information. One can safeguard their data and confidential information from online frauds and scams by following the Do's and Don'ts.

Do’s

- Keep your passwords or passphrases confidential. Don’t share them with others or write them down. You are responsible for all activities associated with your credentials.
- Pay attention to phishing traps in email and watch for telltale signs of a scam. Don’t open mail or attachments from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message and report it to IT Cell.
- Destroy information properly when it is no longer needed. Place paper in designated confidential destruction bins throughout the office or use a crosscut shredder.
- Be aware of your surroundings when printing, copying, faxing, or discussing sensitive information.
- Lock your computer and mobile phone when not in use. This protects data from unauthorized access and use.
- Avoid using public Wi-Fi hotspots for confidential browsing. Always use virtual private network tunnels to protect the data and the device.
- Report all suspicious activity and cyber incidents to the IT Cell or call 1390. Keep all areas containing sensitive information physically secured and allow access only to authorized individuals.
- Always use hard-to-guess passwords or passphrases. A password should have a minimum of 8 characters using uppercase letters, lowercase letters, numbers, and special characters. To make it easy for you to remember but hard for an attacker to guess.
- It is suggested to use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.

Dont’s

- Don’t install unauthorised programs on your work computer. Malicious applications often pose as legitimate software.
- Don’t respond to phone calls or emails requesting confidential data.
- Don’t leave sensitive information lying around the office.
- Never click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.
- Don’t be tricked into giving away confidential information. It’s easy for an unauthorised person to call and pretend to be an employee or business partner.
- Don’t leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorised disclosure.

- Don’t post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites, and Don’t send it through email unless authorised to do so. (Use privacy settings on social media sites to restrict access to your personal information)
- Don’t leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment.
- Don’t leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. If a device is lost or stolen, report it immediately to your manager and ISO/designated security representative.
- Don’t plug in portable devices without permission from your management. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer.