Cyber Security Dos and Don'ts

Dear All,

Cyber Security is one of the most important criteria in today's technological era. Keeping this in mind a session regarding the same was taken for the students in our school auditorium.

Cyber Security is a shared responsibility of each and every individual. You play a key role in properly safeguarding and using private, sensitive information and resources. The following Dos and Don'ts remind us the actions we must take to remain vigilant.

DOs

1. Create strong passwords that are at least eight characters long, and including at least a numerical value and a symbol, such as #, to foil password-cracking software. Avoid common words, and never disclose a password online.
2. Change your password every ninety days.
3. Use different passwords for different accounts.
4. Perform regular backups of important data.
5. Create a password for your files in order to protect file sharing activities.
6. Physically secure your laptop.
7. Lock your computer or mobile when not in use.
8. Delete any message that refers to groups or organizations that you are not a part of.
9. Download and install software only from online sources you trust.
10. Never click on a link from an untrusted source.
11. Close windows containing pop-up ads or unexpected warnings by clicking on the "X" button in the upper most right hand corner of that window, not by clicking within the window.
12. Use antivirus software, and update it on a regular basis to recognize the latest threats
13. Regularly update your operating system, Web browser, and other major software, using the manufacturers' update features, preferably using the auto update functionality.
14. Set Windows or Mac updates to auto-download.
15. Save attachments to disk before opening them. Let your antivirus program automatically scan your attachments after saving them to disk.
16. Report stolen devices immediately.

DON'Ts

1. Never write down your password. Especially on a Post-It note stuck to your computer!
2. Never give out your password to anyone, whether you know them or not.
3. Never select the "Remember My Password" option. Many applications do not store them securely.
4. Never purchase anything promoted in a spam message. Even if the offer isn't a scam, you are only helping to finance and encourage spam.
5. Please refrain from opening an e-mail attachment, even from someone you know well, unless you were expecting it.
6. Never leave your devices unattended, even for a few minutes.
7. Do not post any private or sensitive information on public sites or social media.
8. Do not plug in unknown devices into your computer.
9. Avoid creating common passwords such as your name, date of birth, etc.
10. Never reply to e-mail(s) requesting financial or personal information.
11. Avoid Public Wi-Fi hotspots.
12. Avoid Public computers.
13. Avoid opening e-mail(s) or e-mail attachments from an unknown sender.
14. Please refrain from clicking on the close button within pop-up ads.
15. Under no circumstances should you install or use pirated copies of software.
16. Do not install P2P file sharing programs which can illegally download copyrighted material.
17. Never set your e-mail program to "auto-open" attachments.
18. Do not leave your wireless/Bluetooth turned on when not in use.