Cyber Security: Some Suggested Dos & Don'ts

Over the years the Internet has become an essential tool for carrying out personal and professional activities. It has drastically changed our lives. We spend significant time while performing activities on the Internet. With increasing use and dependence, the Internet is also emerging as a serious security threat to confidentiality, integrity and availability of information and resources. The advancement in ICT have also equally helped the criminals. Cybercrimes are now growing rapidly. In fact, today's Cyber Threats are not only limited to mere slowing down of PC due to virus infection or identity loss, but the nature of crimes has grown to become extremely threatening. Cyberattacks now include cyber bullying, financial frauds, espionage, terrorism & warfare.

It is thus very important to exercise care while carrying out online activities. To minimize the Cyber threats, all IT users in Jamia Millia Islamia are advised to follow the "dos and donts" given below while working online.

Dos for PC/Laptops

- Always install Licensed Operating System and other Application Software.
- Update all software installed on your systems regularly.
- Use an up-to-date antivirus software. Windows 7, 8 & 10 users may use Windows Defender which comes bundled with the operating system.
- Activate the Operating System firewall.
- Create an exclusive account for the "Administrator". Create separate users accounts for each user of the PC/Laptop. Use Administrator accounts only to install or modify software and to change system settings.
- Use Strong and unique Passwords with at least 8-characters containing combination of upper & lower cases, numerals and special characters.
- Always lock the system if you intend to leave it unattended even for a short time.
- Before making any Online transaction, check the following:
    - The site uses https protocol. (Hyper Text Transfer Protocol Secure).
    - The name of the site is correctly spelled. Lookout for similar looking characters such as 0 (zero) and O (letter O) or 1 (one) and l (letter L)
    - The SSL certificate is trusted i.e. the owner name is valid and the certificate has not expired.
    - To check the certificate, click the "lock" icon in the beginning of the address bar in the browser.
- Download software from trusted sites only.
- Regularly Backup data on external disks/cloud. While saving locally or on cloud consider encrypting the data, if it is confidential. Utilities such as 7-zip or pkzip etc may be used for this purpose.
- Never click a link or download attachment from an email coming from unknown source. When suspicious someone else who could help you in ascertaining the identity of the source.

Browser Security:

- Use standard browsers such as Chrome, Edge, Firefox etc. and keep them updated with latest patches.
- Use privacy or security settings which are inbuilt in the browser. Only make changes to these settings when necessary.
- If your antivirus software flags suspicious cookies, delete them.
- Do not save sensitive information such as passwords in the browser.
- Activate "Safe Search" to filter out explicit contents in search result.

Cyber Security: Some Suggested Dos & Don'ts

Dos and don'ts for Mobile Device

- Keep your mobile Operating System up to date.
- Take a note of the unique 15-digit IMEI number of your mobile phone. In case your Mobile phone is stolen or lost, this number is required for registering complaint at Police Station. The number also helps in tracking your mobile phone through service provider.

  *Note: On most phones, the IMEI number can be found by dialing *#06# on most of the phones. You may also look for it below the battery.*
- Setup "**Find my Phone**" feature on your phone.
- Activate auto lock to automatically lock the phone or keypad lock protected by passcode/biometric/security patterns to restrict access to your mobile phone.
- Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen.
- Report lost/stolen devices immediately to the nearest Police Station and concerned service provider.
- Keep the Bluetooth & WiFi Off unless you require them.
- Review and understand the details of an app before downloading and installing onto your device.
- Download applications form secure stores only such as PlayStore (Android) or Apple App Store (iOS).
- Delete App(s) which you don't use regularly.
- Backup data regularly and set up your phone such that it backs up your data when you sync it.
- When a phone is permanently given to another user to make sure to reset to the factory settings to wipe off your data.

Don'ts:

- Never leave your mobile device unattended. Avoid giving your phone to children.
- Turn off applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections on may pose security issues and cause to drain out the battery.
- Don't use public WiFi facility for making financial or other important transactions. Avoid accessing your key accounts such as emails or others.

Social Media

- Review the Privacy and security settings and adjust them to control who sees your post/pictures.
- Think twice before posting. Your messages must not be abusive, vulgar or promote hatred & extremism.
- Avoid accepting unknown friend requests.
- Keep personal information access to public to bare minimum.
- If someone harasses or threatens you, remove them from your friends list, block them and report them to the site administrator.

To report all types of cybercrime complaints online please visit http://www.cybercrime.gov.in/

For Cyber-safety and Cybersecurity awareness follow **@CyberDost** handle maintained by Ministry of Home Affairs, Government of India.

Resources/References:

1. National Cyber Crime Reporting Portal: https://cybercrime.gov.in/
2. Indian Computer Emergency Response Team: https://www.cert-in.org.in
3. National Cyber Security Alliance: https://staysafeonline.org/

Cyber Security: Some Suggested Dos & Don'ts

4. Ebook: For Students on Cyber Safety. https://cybercrime.gov.in/UploadMedia/index.html