भारतीय समुद्री विश्वविद्यालय
INDIAN MARITIME UNIVERSITY
(Central University, Govt. of India)
HEADQUARTERS

CIRCULAR – IT-01/2020

Cyber Hygiene during Work From Home / On-line Classes & Meetings

Due to the global pandemic of COVID-19, IMU remains closed and continues to work from home during this lockdown period. Most of the Teaching & Non-Teaching staff are working from home and students continue to learn from home using online classes. At this juncture, it is brought to the information of all concerned that there is an increase in number of Cyber Attacks world-wide even in this COVID-19 pandemic. Hence, the following Cyber Hygiene guidelines may be considered to be followed while working from home / on-line class & meetings:-

Please;

1. Avoid using pirated software / operating system (OS) as they do not receive software updates that are necessary for patching security vulnerabilities. Hence, they are at risk of getting exploited by attackers.
2. Make sure to turn on automatic updates in Windows update to keep Windows, Microsoft Office and other Microsoft applications up to date.
3. Setting Strong Password for all devices is a must. Password should be unique and complex. Periodic change in password is also recommended.
4. Ensure to use a secure Wi-Fi network / Mobile Data. Avoid using Public Hotspots and open Wi-Fi.
5. Updated Anti-virus may be used in Laptops/PCs used to do office work.
6. Update apps, web browsers and operating systems regularly to ensure the system is working with latest patches.
7. Use official email ids for official communications.
8. Set up restrictions to keep unknown or unnecessary browser extensions from being installed. Many extensions have tracking codes which users are unaware of, while others are used to spread malware. Stick with trusted and needed browser extensions only.
9. Neither click on any link nor open any attachments from an unknown source. They can appear in email, tweets, posts, online ads, messages or attachments and sometimes disguise themselves as known and trusted sources.
10. Video conferencing applications should be used securely. Keep your Video Conference applications patched and up to date. Avoid using Zoom app as instructed by Govt. of India.

East Coast Road, Semmencherry, Sholinganallur (P.O), Chennai - 600 119.
Tel : (044) - 2453 9020 Fax : (044) - 2453 9026 E-mail : registrar@imu.ac.in website : imu.edu.in

10.1 Information about the meeting may be given only to concerned individuals via authorized mail.

10.2 Keep an eye on uninvited guest during the web conference.

10.3 Do not share password of the meeting with anyone.

11. Keep mobile operating system and its app up to date. Mobile operating systems like Apple's iOS, Google Android platform and Microsoft's Windows phone provide regular updates to users.

12. Do not download from unknown source or untrusted sources.

13. Disable Remote Desktop and Remote Assistance in your PC / Laptop.

14. Avoid use of peer to peer software like BitTorrent, uTorrent..etc.

15. Log out from other apps, games, emails when you use online Google Meet / Class room / Video conferencing.

16. Use "Virtual Keyboard" while doing online banking & transactions using your password.

17. Avoid surfing, downloading, storing & sharing child-pornography which is a serious cybercrime.

18. Avoid creating & spreading unauthorised messages, contents, audios & videos..etc

19. Please be in touch with respective campus / HQ IT section for any information & cyber security related issues.

20. Know & learn Cyber Security norms and provision of Information Technology Act, 2000.

21. This issues with the approval of the Competent Authority.

// ENJOY SAFE & SECURED INTERNET & ON-LINE SERVICES //

(P. THANGAPANDIAN)
Asst.Registrar(Admin & Legal) &
Chief Information Security Officer, IMU.

Dated 29.04.2020.