02 Apr 2020

MINISTRY OF DEFENCE
CYBER CELL

CYBER SECURITY ADVISORY 04/2020: CYBER SECURITY DURING COVID-19 OUTBREAK

1. In the prevalent lockdown scenario most personnel of MoD have been encouraged to work from home. CERT-In has reported an increase in the number of cyber-attacks on computers, routers and unprotected home networks used by employees who have switched to remote working. Cyber criminals are exploiting the Covid-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating trustworthy organizations.

2. In this scenario, the following cyber security best practices are strongly recommended:

(a) Ensure that your PC / computer's operating system is licensed and updated with the latest patches from the OEM. Also ensure that there is a licensed anti-virus / Total security software application installed and updated on your machine.

(b) Change default passwords on your home Wi-Fi router to prevent hackers accessing your network. Passwords must be minimum 8 characters, have at least one numeral, one special character and one capital letter. WPA2 with AES or other suitable encryption is recommended to secure one's home Wi-Fi. Restrict inbound and outbound traffic, use the highest level of encryption available, and switch off WPS.

(c) Use strong and unique passwords on every account and device - consider using two-factor authentication for your IT devices.

(d) Refrain from using personal email or third party services for communication involving official matters. Only NIC email ids are to be used for this purpose.

(e) All information communicated through NIC email bearing CONFIDENTIAL or above classification or sensitive information must be encrypted / password protected prior to uploading as attachment in a mail. All sensitive and / or classified information must be contained in an encrypted attachment only and not in the body of the email.

(f) Do not share your PC at home with others if any sensitive matters are being edited or communicated through it to reduce the risk of inadvertent access to protected information. Use of open source encryption software such as "Veracrypt" is recommended to store sensitive information on disk. Password complexity as suggested in sub para (a) above is to be maintained.

(g) "Remember password" functionality should always be turned off when logging into Govt information systems and applications from their personal devices.

(h) Consider Mobile Device Management (MDM) and Mobile Application Management (MAM). These tools can allow organizations to remotely implement a number of security measures, including data encryption, malware scans, and wiping data on stolen devices.

(j) Do check the previous log-in details whenever logging into email portals and financial portals. Ensure that sessions automatically time out after a specified period of inactivity and that they require re-authentication to gain access.

(k) Do not communicate sensitive / classified information through IM / chat applications even though they claim to be encrypted. Such information may be communicated through NIC email services as detailed in sub para (e) above.

(l) Dispose of unnecessary copies of classified files (created or stored) on one's personal computer using a file shredder software (Eraser / PeaZip). Globally accepted standards/ methods such as Pseudo Random Data, DOD 5220.22-M (8-306. C), DOD 5220.22-M (8-306. E), Gutmann etc. may be used to securely wipe classified data.

(m) Be wary and suspicious of phishing emails/ websites and perform necessary authentication before opening/ clicking on fake looking or suspected emails.

(n) Don't allow access to remote desktop tools to your home PC/ computer without proper authentication/ validation.

(o) Do not share the virtual meeting URLs on social media or other public channels (Unauthorized third parties could access private meetings in this way).

(p) Do not connect to freely available public Wi-Fi, open networks/ Unsecured networks to transmit information. These hotspots may be insecure and are prone to snooping, hijacking etc.

3. These guidelines may be disseminated to all concerned agencies within the MoD.

Reference: CERT-In Advisory CIAD-2020-0008