No. 19-78/2019-SA
Government of India
Ministry of Communications
Department of Telecommunications
Sanchar Bhawan, 20, Ashok Road
New Delhi-110 001
(Security Assurance Wing)

New Delhi, Dated: 09.09.2020

OFFICE MEMORANDUM

Subject: **Unsafe practices to be avoided at Workplace for Cyber Security:**

The Covid-19 pandemic has resulted in an increase in cyber attacks including state-sponsored attacks. The cyber security incidents like spreading of virus/Botnets/spyware, spoofing and phishing attacks, attacks on servers, attacks on critical infrastructure, etc. are increasing in sophistication with each passing day.

2. In this context, kindly find attached **"Ten Unsafe Practices to be avoided at Workplace for Cyber Security".** It is requested to kindly avoid these practices to help in strengthening security posture of the Department/Organization.

3. This is issued with the approval of Chief Information Security Officer (CISO) & DDG (Security Assurance), DoT.

Enclosure: As stated above.

Kanika 09.09.2020.
(Kanika Gambhir)
ADET(Security Audit)

To,

1. All Sr. DDG/ DDG/CVO/JS level Officers of DoT Hq.
2. Heads of all Attached Offices/ Subordinate Offices/ Field Offices/ Autonomous bodies/ Statutory bodies/Training Centers/ CPSEs of DoT

Copy to:

1. PSO to Secretary (T)
2. Sr. PPS/PPS to Member(S), Member(T), Member(F)
3. Sr. PPS/PPS to Additional Secretary
4. Sr. PPS/ PPS to Advisor(O), Advisor(T), Advisor(F)

Annexure

UNSAFE PRACTICES TO BE AVOIDED AT WORKPLACE FOR CYBER SECURITY

1. **Using Common Passwords for all:** Password recycling or using easy-to-guess passwords are just two common mistakes that we make when protecting ourselves from cyberworld. The gravest problem with password recycling is that it leads to credential stuffing which is an account takeover attack that leverages bots to hammer sites with login attempts using stolen access credentials from data breaches at other sites until they stumble upon the right combination of new site and "old" credentials. So, it becomes important to diversify the passwords for digital identities.

2. **Leaving your devices unlocked:** Spies can install malware on an unattended device and download stored information remotely at their convenience. It might also expose your classified information and increases risk to organization's safety and security. Leaving your devices locked while not working, protects you from this risk.

3. **Ignoring Operating System (OS) and Software Updates:** When OS and software vendors discover a weakness in their current version; they release updates to fix them. If we don't apply these updates, we are still vulnerable. Outdated OS and software's are prone to malware infections and other cyber concerns.

4. **Clicking on hyperlinks from unknown sources:** The basic method for cyber criminals is to send out bulk e-mails containing an attachment or a hyperlink. The attachment is malware and any hyperlink will to be a website masquerading as something legitimate. The goal is to trick the e-mail recipient into downloading the attachment (exposing their PC to the malware), or clicking the link to a website that may be infected with malware. or asks for Confidential/Personal data such as credit card numbers to be entered.

5. **Downloading files without scanning:** Malicious files are even making their way onto legitimate download sites. So, it becomes important to scan the file using online website Virus & Malware Scanning, before downloading to determine whether the file to be downloaded is free from malwares.

6. **Connecting unsafe devices to office network:** Allowing users to connect to the network with their own devices has the potential to wreak havoc, as it is difficult for IT departments to control the devices having security aspects other than that of the organization. One of the front-line defenses is the network access control (NAC) and its ability to restrict network by MAC (Media Access Controller) binding and Port binding which allow access to devices and users that are authorized and authenticated.

Jamika 09.09.2020

7. **Using Public Wi-Fi without a VPN:** Connecting public WiFi without a VPN can potentially leave our devices open for criminals to access any sensitive data stored on your device.When using Wi-Fi with a VPN, the privacy and security is protected at all times.

8. **Carelessly handling devices with sensitive data:** The mishandling of devices with sensitive data leads to a security breach faster than any other process. The devices with classified information need to be hardened to eliminate a means of attack by patching vulnerabilities, turning of non-essential services and configuring system with security controls. Kindly ensure that the sensitive information is kept at Airgap Computer to avoid any malware attack and other cyber concerns.

9. **Downloading Unauthorized software:** Unauthorized software increases the risk of outsiders gaining access to sensitive data. Any software that is not authorized is likely managed without proper patching, updates, configurations, and security protocols. Buying and using genuine and legal software — as opposed to pirated, counterfeit, illegal or unlicensed versions is to be followed to avoid any leakage of information.

10. **Leaving Sticky Notes with passwords:** It is one of the common practices observed in employees for easy access/visibility in today's password intensive world. However, it should not be forgotten that each user's password credentials holds some level of access to sensitive information, which if leaked or stolen can cause significant damages.Therefore, the employees need to understand the associated risks and such practices should be immediately stopped.

09.09.2020