Government of India

National Critical Information Infrastructure Protection Centre
(A Unit of NTRO)

**Date:** 25 Mar 2020

## Advisory No: Adv/2020/Mar/017

## Cyber Security Advisory: Precautions for CII in COVID-19

This data is to be considered as **TLP:GREEN**

Due to outbreak of COVID-19, Government of India has issued order for lock-down/curfew in whole nation and requested organisations (Government/Private) for use of "work from home" in order to maintain business continuity. A pandemic of this scale has resulted in dependency on digital communications many folds and many operations may be under remote monitoring mode. A cyber attack on critical sector organisations to access to their devices, data or the Internet could be devastating in present case. In a worst-case scenario, broad-based cyber attacks could cause widespread infrastructure failures that take entire communities or cities offline, obstructing healthcare providers, public systems and networks.

**Possible Attack Vectors:**

**Social Engineering Attacks:**
Phishing emails with links claiming to have important updates on Coronavirus from World Health Organisation (WHO). The links, if clicked may lead the devices being infected with malware/ransomware.

**Remote Login Attacks: Remote User Credential Theft**
An attacker may target increase use of remote login credentials to organizational resources.

**Malware Attacks:**
Users working with home systems for official work could fall for "free" access to obscure websites or pirated shows, opening the door to likely malware and attacks.

Latest news from open source have indicated that many unique files dubbed as Coronavirus spread related documents (PDF, MP4, and Docx) are circulating on the web which are filled with malevolent infections such as file-encrypting malware, crypto-mining malware and browser details siphoning digital adjectives and those which exfiltrate sensitive data

**Precautions for Cyber Security in Present Case:**

**Organisational Policy measures:**

- Remote login for maintenance tasks to be enabled only after proper authentication and session management. Monitoring of all such sessions pertaining to critical resources.
- Secure systems that enable remote access.
- Ensure Virtual Private Network and other remote access systems are fully patched.
- Enhance system monitoring to receive early detection and alerts on abnormal activity.
- Implement multi-factor authentication
- Ensure all machines have properly configured firewalls policies.
- Implementation of anti-malware and anti-intrusion prevention.
- Test remote access solutions capacity or increase capacity as per assessment.
- Ensure continuity of operations/ plans or business continuity plans are up-to-date.
- Increase awareness of information technology support mechanisms for employees who work remotely.
- Update incident response plans to consider workforce changes in a distributed environment.

**Individual Protection Measures:**

- Change default passwords on you home Wi-Fi router to prevent hackers accessing your network
- Ensure not to reuse passwords across the web.
- Don't click on links from unknown emails. When signing up to new services, verify the source of every URL and ensure the programmes or applications installed are the original versions from a trusted source.
- Use strong and unique passwords on every account and device.
- Keep all devices, apps and operating systems up-dated.
- In case of working in public place use a privacy screen and tether using a 3G/4G connection instead of an untrusted Wi-Fi hotspot.
- Only use authorised software /trusted source to share files. Refrain from using personal email or 3rd party services unless reliably informed otherwise.
- Use separate logins for home system for wok purpose.
- Before using own device for work, install antivirus software.
- Disk encryption is an option available in most operating systems. In many cases it is optional that can be enabled as and when required.
- Encrypt sensitive data in emails and on devices.
- Don't use random thumb drives for official work at home.

**Reference:**


- https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

- https://www.computerweekly.com/news/252480079/NCSC-issues-coronavirus-cyber-security-alert
- https://www.cybersecurity-insiders.com/now-meet-the-cyber-threat-in-the-name-of-coronavirus/
- https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus
- https://www.cisa.gov/cybersecurity
- https://www.ncsc.gov.uk/

**Disclaimer:**



**With Best Regards,**
**Knowledge Management System**
**National Critical Information Infrastructure Protection Centre**
**Block-III, Old JNU Campus, New Delhi - 110067**
**Website: www.nciipc.gov.in**
**Toll Free: 1800-11-4430**