Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

CERT-In Advisory CIAD-2020-0026

Security Best Practices for Telecommuting

Original Issue Date: May 02, 2020

Severity Rating: High

Description

Many organizations has considered remote work options for their employees in order to counter the possible impacts of Corona virus Disease 2019 (COVID-19). Rather than travelling to the office, the employee "travels" via telecommunication links, keeping in touch with co-workers and employers via telephone, online chat programs, video meetings, and email.

There are many risks associated with telecommuting. A remote attacker can compromise the security of the organisation if proper security measures are not taken while telecommuting. Firewalls, physical security tokens, passwords, encryption, employee awareness and limiting the availability of confidential data to only those in the organisation who need to know it are some ways to minimize damage from security threats.

Best practices

- Use devices owned, managed, and protected by the organisation, such as laptops or smart phones whenever possible.
- Separate your work and your private life as much as possible. Ideally you will have a designated room or a separate work space and your own device for working.
- Use organisation's approved methods to share files. Be mindful of distribution and dissemination even when utilizing organisation -approved platforms.
- Do not forward work emails to a personal email account
- Log off of your remote connection at the end of the work day
- Follow your organisation’s acceptable use and telecommuting policy on physical and information security.
- If you must use a personal device, first ensure use of personal devices is permitted by your department/organization’s policies, then:
  - Follow organisation's policy for encrypting and signing emails
  - Use passwords to log into the device, use strong passwords, and change them frequently
  - Only use non-privileged profiles for daily activities and only use elevated privileges when administering the device
  - Close all other non-work related windows and applications before and during work related use
  - Create a separate user profile with minimal privileges for work-only use
  - Close all work-related windows, applications, files, and documents when not in use
  - Clear browser cache when switching from work to personal use
  - Keep the operating systems and all relevant applications up-to-date and fully patched
  - Turn on automatic patching and run anti-virus software
- Don't install unapproved clients. When joining meetings initiated by third parties that use collaboration tools not approved by your organization, do not attempt to install software-join web (browser) based session instead. Do not use work email addresses to sign up for unauthorized/free tools.
- Provide clear policy on telecommuting, on accessing organizational/corporate resources and whom to contact in case of problems.
- Grant access to your employees to corporate network only though a company-approved VPN with multi factor authentication (MFA).
- Store work-related content on Government approved services only.
- Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms.
- Update router software and ensure your Wi-Fi is encrypted with current protocols (such as WPA2 or WPA3), and confirm that legacy protocols such as WEP and WPA are disabled.

Best practices for video conferencing

- Verify the links sent by unfamiliar addresses, and never click on a link to a meeting sent by a suspicious sender. Verify that meeting links sent via email are valid.
- Do not make meetings "public" unless they are intended to be open to anyone.
- For private meetings, require a meeting password and use features such as a waiting room to control the admittance of guests. For enhanced security, use randomly generated meeting codes and strong passwords and do not reuse them.
- Do not share a link to a teleconference on an unrestricted, publicly available social media post.
- Provide the link to the meeting directly to specific people and share passwords in a separate email.
- Manage screen-sharing, recording, and file sharing options. Consider saving locally versus in the cloud based on the specific circumstances. Change default file names when saving recordings.
- Check and update your home network. Change default settings and use complex passwords for your broadband router and Wi-Fi network and only share this information with people you trust.

References

CERT-In
CIAD-2020-0008 Cyber security during covid-19 outbreak
CIAD-2020-0013 Securing mobile devices and applications
CIAD-2020-0020 Web conferencing security

CISA
https://www.cisa.gov/telework

ENISA
https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home
https://www.enisa.europa.eu/news/enisa-news/tips-for-selecting-and-using-online-communication-tools

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India