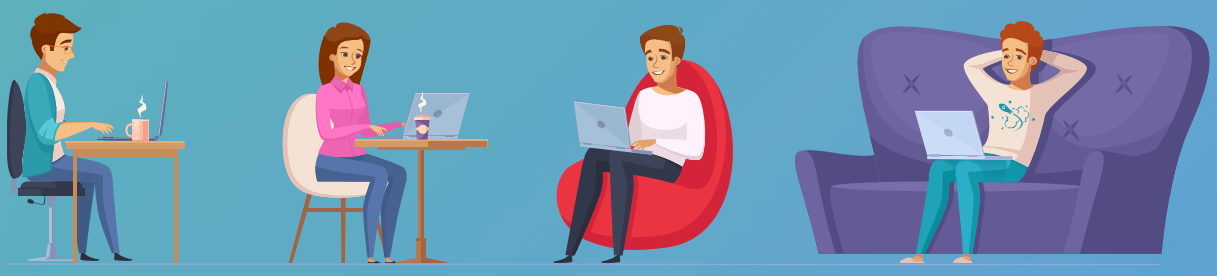
DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

DSCI ADVISORY

WORK FROM HOME – CYBER SECURITY BEST PRACTICES
FOR EMPLOYEES

A Cyber Security Best Practices Guide to keep Businesses Agile & Productivity Up amid the Pandemic

Table of Contents



Background

As the world is grappling with the Coronavirus Pandemic, it has led to massive lockdown in most parts of the world. While the COVID-19 scare has upended lives and led to major health concerns, it has also pushed organizations to adopt a full-scale Work from Home (WFH) model.

While the WFH model has been around for a while but managing an entire remote workforce is completely new for most businesses. Critical and essential services are far from safe to be introduced in a Work from Home culture. However, left without options, organizations have been forced to shift business models. Several bottlenecks include gap in process, policies and technologies that enable employees to work from home safely and securely. On top of it, cyberattacks are on the rise and cyber criminals are exploiting weak security controls and using social engineering to mislead employees, leaving businesses vulnerable.

Additionally, most employees are also not familiar or adequately prepared with the idea of working from home. While IT and security teams are scrambling with various security policies and options to ensure business and workforce safety, the onus lies on the employees as well to follow security guidelines and secure the organization's information and data.

In light of these developments, DSCI has prepared a simple end-user Cyber Security Best Practices guide for employees. These simple and easy tips will ensure basic security protocols are followed by employees, which in turn can minimize cyberattack risks.

General Productivity Best Practices

Work from Home starts with having the right infrastructure setup and mindset to ensure productivity. Follow the below to ensure you treat your home as the new office:

- Designate a workspace within your home as it allows to minimise distractions
- Set Work Hours aside and plan your workflow or make a To-Do list for the day
- Use apps/services such as Microsoft Teams, Google Hangout, Zoom, Cisco WebEx, GoToMeeting, etc. for meetings, collaboration and team communication
- Lock your screen when you aren't working to avoid any unintentional misuse of office resources
- Take periodic breaks for meals, coffee as you do in office to be energetic and ensure productivity

Home Network Security

As the Internet is the backbone of Work from Home, it starts with having a stable internet connection and a secure network. While home networks aren't as secure as a workplace, risks can be minimised by ensuring the below security controls:

- Do not use unsecure or open Wi-Fi for official purposes
- Change the default network name and password of your router used for login
- Secure your Wi-Fi router connections by enabling WPA2 + AES security
- Connect to office network strictly through company provided means

Software & Asset Security

The next important factor is to have the right software and infrastructure for a smooth workflow. Switching to Work from Home may require installation of various software services; however, ensure you strictly follow the installation guidelines issues by your organization's IT team.

What to Install

- Only licensed software versions of those approved by your office IT team
- Allow security updates to be installed when prompted by your system
- Contact your IT team before installing any third-party software, be it productivity tools

What not to Install

- Software over the Internet like games, browser plugins, etc
- Free antivirus to ensure security on your own
- Freeware/shareware or any unapproved software

Portable Media Security

Amid the lockdown, a lot of resources are also using their personal laptop/desktop for official purposes. While organizations instil security protocols when it comes to using USB devices with official systems, the same remains valid for both official & personal systems.

- Perform a full scan of hard drives, pen drives & SD cards with an updated antivirus before you open/use them
- Avoid sharing official USB drives with other personal computers of family/friends around you
- Use additional read/write security controls and if required, enable event logging

Password Security

Passwords are the gatekeepers to your devices, user accounts, social accounts and subscribed web/app services. Ensure to have strong password security protocols by following the below tips and maintain password hygiene.

- Use complex passwords with strict password policy like 8 characters with a combination of alphanumeric and special characters (@#$%*)
- Frequently change account passwords while working from home network
- Use a unique password on every account/device to ensure that all accounts are not compromised in one go
- Use two-factor authentication (2FA) to ensure that just the password is not enough to gain access
- Beware of shoulder surfing at home while entering passwords

Web Surfing Security

Surfing the web for research, data collection and information access is required in most cases today. However, the web is also the space where a legion of cyber criminals waits to gain access through baits and end user mistakes.

- Visit only trusted sites and always check for *https or the lock sign* while browsing
- Do not browse the Internet using system admin credentials

- Keep an eye on any automatic content download. These can be trojans, viruses.
- Stay away from links leading to malicious websites. They may look identical to a legitimate site, but the URL will have a variation in spelling or a different domain (e.g., .com vs. .org).
- Verify full URL using mouse hover before clicking any button or shortened link
- Never activate 'save password' feature in your browser for official accounts

Privacy Protection

Apart from security, ensuring Data Privacy is equally important. Be extra careful if you deal with Personally Identifiable Information (PII) of your customers. Follow the below steps to uphold privacy in & around your new workspace.

- Ensure you don't store and share PII inadvertently
- Sense the sensitivity of information you are dealing with
- Respect rights associated with the kind of data you handle
- Be observant of people around to avoid becoming the reason for data leakage
- Be mindful of data obligations and liabilities that your organisation is compliant with

Email Security

Email is an essential part of official communication. It is also one of the most common methods that hackers use to gain access to sensitive information. Follow the below email security tips to stay away from possible fraud attempts.

- Use strict spam filtering for official and personal emails
- Never forward a company email containing sensitive info to personal email accounts
- Better not to access personal emails on official email clients
- Do not open password protected PDF, PPT, Excel or zip files from unknown senders, especially when the password is mentioned within the email itself
- Never enable macros in word files received from unknown senders
- Report suspicious emails to your IT department by making it an attachment. Do not forward it directly and aware others by the subject name.

Phishing

Cyber criminals are now exploiting the COVID-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating trustworthy organizations.

Phishing uses fraudulent email messages designed to impersonate a legitimate person or organization and trick the recipient into downloading harmful attachments or divulging sensitive information, such as passwords, official data, bank account numbers, etc.

Few common indicators of phishing attempts are:

- **Suspicious sender's address** imitating a legitimate business closely resembling one from a reputable company by altering or omitting a few characters
- **Generic greetings and signature** such as "Dear Customer" or "Sir/Ma'am" and lacking direct contact information in the signature block
- **Spoofed hyperlinks and websites:** Hover the cursor over any link in the email body. If the link doesn't match the text that appears onscreen, it may be spoofed.
- **Spelling and layout:** Poor grammar, spelling mistakes and inconsistent formatting are other indicators
- **Suspicious attachments** are a common delivery mechanism for malware. Unsolicited emails request users to download and open an attachment.
- **Email forms** creating urgency or lottery wins asking users to fill personal/financial information

There are a lot of phishing and scam attempts related to WHO. The World Health Organisation has released a Cyber Security Scam Alert to stay away from such fraudulent attempts. Know more: https://www.who.int/about/communications/cyber-security

Social Engineering Scams

Apart from phishing, cyber criminals forge a host of other social engineering attempts to trick employees into giving away sensitive information. Fraudsters first investigate the background of their targets and then use email, voice, SMS to make them commit security mistakes. Stay away from such common fraud attempts:

- A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first
- **Vishing:** Never respond to hoax calls which claim to be from banks/hospitals asking for sensitive information. Beware of VoIP attacks as it allows caller identity (ID) to be spoofed
- **Pretexting:** Hackers create a false sense of trust by impersonating a remote co-worker or figure of authority and ask for account login and passwords or sensitive official information
- **Smishing:** Beware of attacks that exploit SMS or text messages which can contain links to webpages, email addresses or phone numbers that when clicked may automatically open a browser window, email message or dial a number
- **Quid pro quo:** Amid the lockdown, hackers may pose as a technical support staff from various services that the organisation uses and offer to upgrade/patch the software in exchange of critical data or credentials. Immediately inform your IT team to validate such calls.

The golden rule is to avoid responding to inbound calls, email support requests. In case any such support is needed, initiate it from your end keeping your IT team in the loop.

Donation Scam Alerts

One of the fastest proliferating scams amid these times are donation scams related to Coronavirus. Cyber criminals are exploiting empathy and helping nature of citizens by tricking them and con money. Whenever you decide to donate, be extra cautious and ensure you donate at legitimate & official charity sites.

- Ignore emails and messages with links urging for donations. Always initiate a donation from your end at official websites.
- Always crosscheck all account details/UPI handles before making any donation on PM or CM relief funds
- Do not scan unrecognized QR codes while extending financial support
- Beware of fake websites and malicious donation links. Check URLs for authenticity.
- Before sharing your donation information on Social Media, impart caution to avoid sharing any personal/financial information online

Other Security Tips

Apart from the above-mentioned security aspects, here are few other measures to ensure better security.

- Inform your organization if you come across any discrepancies
- Frequently backup your data as advised by your company against accidental data corruption or device failure
- Stay away from PC cleaning/RAM booster software/freeware
- Don't play online games on company devices as they may download trojans unknowingly
- Be mindful of time zones while WFH and check for suspicious activities at odd hours
- Ensure Virtual Private Network (VPN) and other remote access systems are fully patched
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19

Conclusion

The goal of this guide is to make security concepts simple and implementable for everyone and help end users follow basic guidelines to stay away from common pitfalls. While IT teams are putting forth all efforts to identify risks which can have the greatest impact on their respective business model, it is a collective responsibility of all employees, at every level, to ensure security and business continuity of their organization.

COVID-19 has fast changed the business security landscape of organizations globally. However, it is also an opportunity to prepare for such newer work models which are becoming a reality and strengthen the cyber security posture of every organization and employee alike.

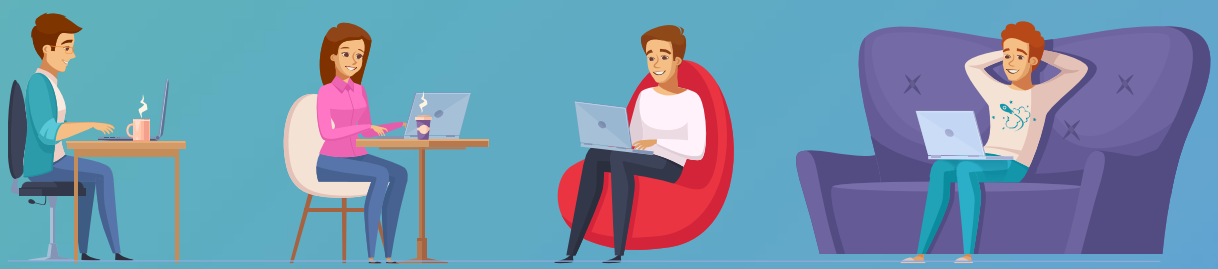
Additional References

You can also refer to the below advisories for more information on Work from Home Best Practices and policies.

- https://infosecawareness.in/gallery/handbooks/ISEA-Handbooks/secure-remote-desktop-access.pdf
- https://workfromhome.globalcyberalliance.org/
- https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final
- https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

---

- For any Work from Home issues, reach out to your office IT & Admin teams.
- For any query related to the advisory or for more information, reach out to: safewfh@dsci.in



Stay Home, Stay Safe!