CYBERSECURITY CENTRE of EXCELLENCE

A joint initiative of DSCI & Government of Telangana

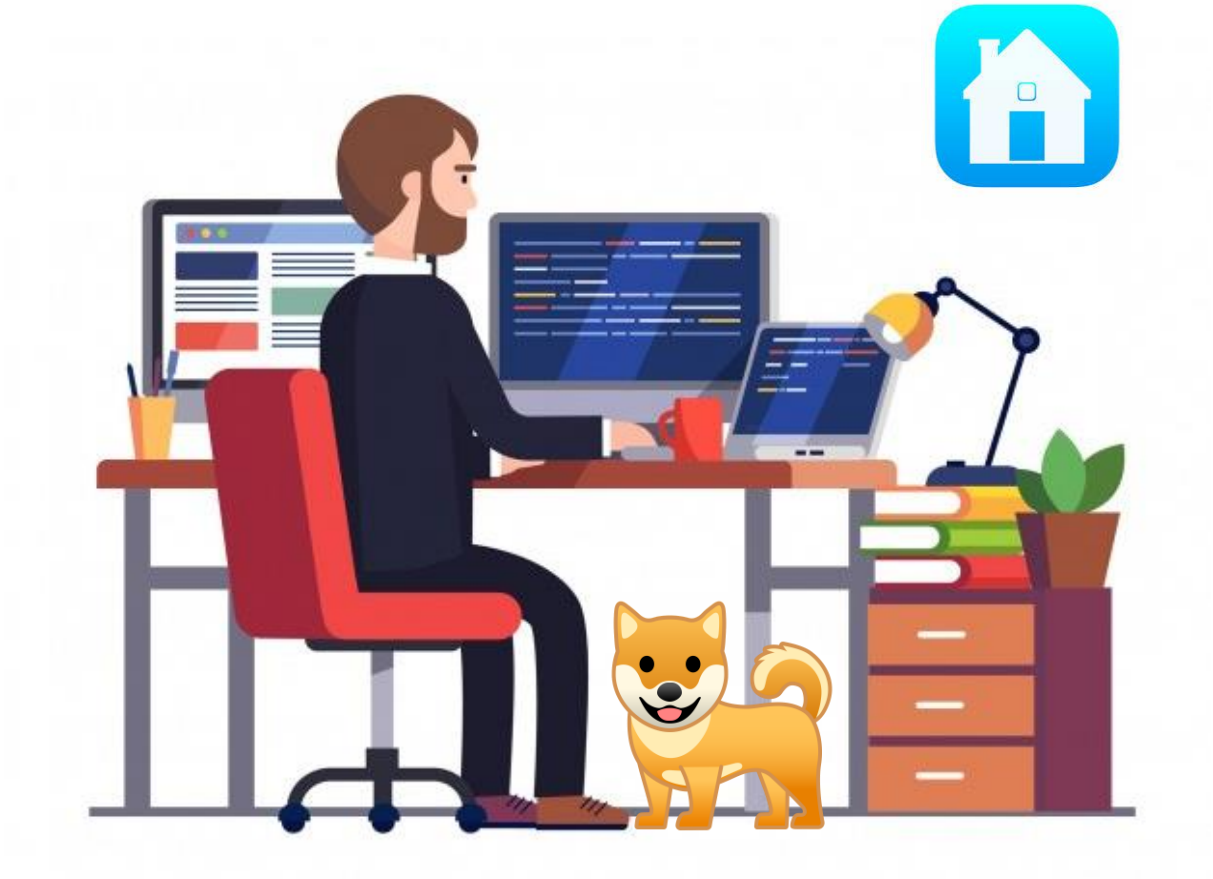
DSCI PROMOTING DATA PROTECTION

A NASSCOM® Initiative

WORK FROM HOME - BEST PRACTICES

- ADVISORY

BY THE DATA SECURITY COUNCIL OF INDIA (DSCI) ALONG WITH THE CYBERSECURITY CENTRE OF EXCELLENCE, HYDERABAD.



For any queries, please reach out to: safewfh@dsci.in

Background

Due to the global pandemic of COVID-19, home has become the new office!

Work from home (WFH) has become the need of the hour and the utmost priority is to keep the workforce safe and ensure productivity. In light of these conditions, understanding the available options and working with quality IT services providers, we can safely navigate the cyber world and keep our businesses seamless and protected.

As an industry body, it is DSCI's continuous endeavour to help you stay connected throughout the COVID-19 pandemic and support organisations and employees through best practices.

Below are some of the basic requirements to secure your network while allowing remote access to employees and guidelines for them to follow.

1. Secure Connection to Workplace

A. **VPN Gateway**: - should only be used on a company-owned hardware device

Virtual Private Network (VPN) gateways create secure connection to your network from employee devices which are on public networks.

- Choose the best VPN gateway, which extends business firewall rules to the user computer to minimize risk.
- Make sure to use VPN only on company-owned hardware with up-to-date security features, else infected data may transmit over VPN to subsequent networks if the client system is infected/compromised.
- The best choice for SMBs is to establish a site-to-site VPN.

B. **Wi-Fi Connectivity -** Ensure you use a secure Wi-Fi network to connect to your organization network. Avoid Public Hotspots or open Wi-Fi.

C. **Zoning or Subnetting** - To keep network integrity protected, incorporate network segregation wherever appropriate (using subnetworks) to keep publicly accessible components off internal networks, and monitor and control communications at key boundary points.

D. Closure of Unwanted Ports – It is strongly recommended to close unnecessary network ports with the help of your IT/Security teams.

E. End Point Security with Up-to-date Security and DLP Policies – Antivirus should be up to date with remote access policy configuration for auto-update of virus definition, client machine should be properly patched before connecting to the organization network.

2. Portals /VDI: - Virtual Desktop should be the first choice

It is strongly recommended that employees should access company data and applications through a browser-based webpage or virtual desktop. Ensure that all applications and data are stored on the portal's server and cannot be downloaded or saved on an employee's device without permission. This is a good way to keep control over who is accessing your data and how it is used. It's mandatory to restrict employee's access to other programs while the portal is in use else there may be a high risk of overexposure.

3. Remote Access Services: - Choose secured and trusted third-party services

It is noteworthy to document remote access requirements, authorize remote access before allowing connections, monitor and control remote access, encrypt remote access connections from the organization's firewall and threat detection. Try to ensure employee systems/desktops are fully protected and has the same protection as office workstations.

4. Direct Application Access: Low Risk

Employees can remote login into a single application such as Webmail. The employee doesn't have access to the entire network; the user can access the application as per his access profiles, so there is a very low risk to the internal network.

5. Live Support Mandate

A. It is strongly recommended to establish 24*7 live IT support to handle queries from all shifts.
B. Live monitoring of all events and responses must be ensured.

6. Basic Mandate Hygiene – for organisations and employees alike

A. Enforce strong password policies and ensure employees use a password manager.
B. Change your router password, and Encryption should be set to WPA2 and WPA3.
C. Set up session time-out on all remote connections and automatic screen locking feature on all computers.
D. Turn off networking capabilities (such as Bluetooth) for mobile and laptop when not necessary for work.
E. Turn on personal firewalls, if available
F. Restrict other applications allowed on the mobile device
G. Add additional security authentication layers to company data on mobile devices.
H. Set up restrictions to keep unknown or unnecessary browser extensions from being installed. Many extensions have tracking codes which users are unaware of, while others are used to spread malware. Stick with trusted and needed browser extensions only.
I. If possible, physically secure computers with locking cables
J. Employees should know how to spot and respond to unusual computer activities, which can be an indicator for any suspicious activity.
K. Employees must be aware whom to contact for IT support, and how to verify the genuinity of the person asking for access to their computer.
L. Avoid clicking on links in unsolicited emails and be wary of email attachments. See 'Using Caution with Email Attachments' and 'Avoiding Social Engineering and Phishing Scams' for more information.
M. While checking personal emails on work machine, be extra cautious and make sure you open attachments only from known and verified senders.
N. Use this as a thumb rule everywhere - neither click on any link nor open any attachment from an unknown source.
O. Use customized spam filter settings for personal email accounts, like in Gsuite, you can configure it in Gmail advanced settings – scroll to "**Spam, phishing, and malware and at Spam**" option and configure it, you can also opt for aggressive spam filter settings.
P. In case of financial approvals/ dispatch of payments, please cross verify with the concerned person before you issue any payments.
Q. Non-technical staff, while working from home, should take care of the confidentiality of valuable transactions and sensitive financial documents.

R. Avoid delivery of sensitive physical documents other than office address and collect them as required with utmost care.
S. No recording of client calls, no screen recording, no clicking pictures, and video capturing
T. Screen capture functionality should be disabled on mobiles
U. Enforce strict email policies with visual markings enablement to restrict print, snip and saving confidential emails. It is every employee's responsibility to follow the same best practices, even if restrictions are not in place by the organization.

7. Right Work Environment

Working from home also largely involves sharing the space with other family members/housemates. It's important to set guidelines to indicate when you are at work so as not to be disturbed. Hence there must be an isolated space for work.

8. The right set of tools and environment should be available to ensure smooth functioning, like a wireless headset for call center operations, quiet workplace, allowed only whitelisted devices in USB ports; Sys Admins should be proactive and allow USB ports only for authorized devices.

9. Please review and seek clarity for NDA/ legal undertaking to protect client/business information that you have signed while joining, and it is every employee's responsibility to adhere to it strictly while working from home.

10. Ensure to be complaint as per company work from home policies.

11. Risk Assessment: Risk assessment should be performed as part of selecting a remote access method (tunnelling, application portals, remote desktop access, direct application access).

12. Awareness: Be wary of COVID-19 precaution messages as they may contain malware

Be vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19. Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.

13. Information is Key:

For a pandemic which the world is still grappling with and when there are new developments every day, it is obvious for everyone to keep tab of the latest updates. However, social media, multitude of news portals contain outdated or ill information. It is important to seek for the current information from trusted sources only. Refer to legitimate government websites, WHO, Ministry of Health —for up-to-date, fact-based information about COVID-19.

For any queries, please reach out to: safewfh@dsci.in