TechCERT
HELPING YOU SECURE
YOUR INFORMATION ASSETS

Security Awareness Guide

Secure Work From Home

COVID-19 Edition

Document Version: Secure-Work-From-Home-v3.1-Covid-19e

Executive Summary

In response to COVID-19, organizations worldwide are implementing Work from Home (WFH). However, this transitioning their workforce to work from home can be a challenge as many organizations lack the policies, technology, and training. Additionally, many employees may be unfamiliar or uncomfortable with the idea of working from home. The following guide will help you to create a more secure Work from Home setup.

This guide was written to enlighten both WFH employees and employers to explain underlying security threats and how to stay securely. And this guide is composed especially matching to Sri Lankan context with special evaluation threats.

How to Use this Guide

This guide has two sections with providing a technical outline for both WFH employees and employers. In the section 'As an Employee, what can You Do to Securely Work from Home?' is the employees' guide and the section 'As an Employer, what can You Do to Provide a Securely Work from Home for Your Workforce?' is the employer or enterprise set up guide. But keep in mind, if you feel any additional security measure is required which is suitable for you or your organization, please proceed. Please find the Further Reading & Resources section for more WFH guides that are published.

As an Employee, what can You Do to Securely Work from Home?

If you want to do WFH, probably there are two scenarios.

1. Your Employer already technically control your WFH devices with Mobile Device Management (MDM) system

2. Your Employer only provide guidelines on how to do WFH with adhering to corporate policies

In the first case, your employer may have already pushed security policies to enhance security such as restricting the Encryption, Removable media restriction, Remote Antivirus software configuration, etc. However, the real challenge comes, if you are using your device, totally controlled by yourself. You need to strictly adhere to the following steps if you are in case scenario 2. You are also recommended to adhere even if you belong to scenarios 1.

1. **Don't use Public or Shared Computers with Less Known People** - Security state of public or shared computers with less known people cannot be assured in any manner. Attackers can plant rootkits to steal your credentials maybe therein such a system. Therefore, do not use such devices for WFH activities. Refrain using such devices for WFH.

2. **Make sure Physical Security of Your Device** - In typical office environments, there may be security checkpoints, biometric fingerprint readers between your PC and outsiders. Remember if you are using your devices in public places and do your work stuff, then the physical protection is not there. Lost and stolen mobile devices and laptops are easy pickings for cybercriminals if insufficient security measures are in place. Therefore, always keep your WFH devices with you and in-sight.

3. **Use Secure Networks** - Do not use public or untrusted networks (e.g. Open Wi-Fi network, Wi-Fi network of your neighbor) to perform your WFH activities. Even though your employer provides a VPN, refrain the use of public or untrusted networks. A public or untrusted network often targets to Man-in-Middle-Attacks to steal sensitive data.

4. **Secure Passwords + MFA** - Use Unique & Strong passwords for all accounts and use Password Managers to properly secure them. In reality, it is not possible to remember so many passwords without a password manager. With excellent password hygiene, use Multi-Factor Authentication every possible occasion. Multi-Factor Authentication is often called Two-factor Authentication or Two-Step Verification.

5. **Antivirus Software** - Make sure your Antivirus Solution is properly installed and have the latest signature updates. If you are using your own devices to WFH activities, switch to enterprise-level security-enhanced commercial AV software than free AVs. Free AVs often collect your data and use it for their business purposes which could be problematic with corporate sensitive data.

6. **Security Updates** - Make sure the latest security updates are installed not only for your operating system, but every application installed in your Computer or Mobile Devices.

7. **Removable Devices** - USB pen drives and other removable devices can be a source of malware and should be checked first.

8. **Negligence and Accidental Risks in the Home** - Make sure your cat is not allowed to walk on your keywords while you are working a business transaction. Keep in mind in the home environment, your family member can accidentally perform a click which can cause huge issues for your business transactions.

As an Employer, what can You Do to Provide a Securely Work from Home for Your Workforce?

Remote working is a vast field in enterprise security. Security needed to be taken care of multiple approaches. Here is a list of areas needed to be taken as a baseline.

- Securing remote working devices
- Using a secure network connection
- Restricting to minimal access level to internal systems and data
- Enabling strict monitoring
- Implementing proper incident response mechanism
- Properly enforcing adopted enterprise IT security practices and remote working policies

Securing WFH Devices

First, the Physical security of working from home devices should be taken care of with proper guidance to employees. Then technical controls can be implemented on top of it. A remote workforce device can be operated with the following two methods.

1. With enterprise-managed devices such as laptops and mobile phones/tabs through enterprise mobile device management solution
2. Without any device management solution. (E.g. Employees use their laptops)

The enterprise managed devices have the flexibility to enforce security enhancements. If you have enterprise-managed devices, make sure they are enforcing to enterprise remote working policy. Enterprise WFH policy typically contains

- Keep the Antivirus solution up with latest updated
- The device operating system supported, and the latest security updates are installed
- Removable devices are restricted etc.

If you do not have MDM in solution, you need to ask you, employees, to strictly adhere to the above device security measurements. Otherwise, there is a large probability of malware running on employees' devices would infect corporate enterprise systems.

Securing WFH Network Connections

A secure network connection from WFH users to the enterprise system is essential in secure WFH. The following baseline is needed in the approach of a secure network connection.

- Remote users should only use Secure VPN Connection to connect an enterprise network
- A secure network should be used to connect to VPN service endpoint without using public or untrusted Wi-Fi connections

Securing a VPN Connection

A secure VPN is a mandatory requirement for WFH to connect internal enterprise systems. VPN connections are typically created by perimeter firewalls and special servers such as OpenVPN servers. A VPN a connection setup should adhere to the following.

- **Multi-Factor Authentication (MFA)** - MFA is a mandatory requirement for VPNs. If you are using perimeter firewalls to provide VPN connection, enable TOTP support. Then mobile apps like Google Authenticator can be used for MFA. If you are using OpenVPN, use Key+Password approach
- **Security Updates** - The Firewall device or VPN server should be running supported OS or not reach End of Life (EOL). All security updates should have been applied to the VPN server/Firewall.
- **Security Hardened** - The Firewall device or VPN server should have gone through the security hardening process within line with industry-accepted security guidelines.
- **Restricted Access** - If the workforce only resides in Sri Lanka, allow only Sri Lankan IP addresses to VPN servers

Secondary Defense Line

Any system or server which can be connected through VPN should have gone through proper security hardening before opening through VPN connections as follows.

- No open systems without authentication
- No systems with default or easily guessable passwords
- Security updates should be installed
- No file shares with global write access

Jump Servers

A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. However, jump servers often configured poorly with access to a lot of internal systems with inadequate monitoring. Due to these reasons, there are incidents with compromised jump servers. If you have placed an MDM for your WFH workforce better to use VPNs with strict controls. However, if you do not have MDM, using a secured Jump Server with the following guidelines would minimize the risk to internal systems.

- Reducing the subnet size and securing those VLANs using a firewall or router.
- Using higher security authentication, such as multi-factor authentication.
- Keeping the operating system and software on the jump server up to date.
- Using ACLs to restrict access to only the people that require it.
- Do not allow outbound access to the rest of the internet from the jump server.
- Restrict which programs can be run on the jump server.
- Enable strong logging and pushing logs to a SIEM system.

Please note, jump servers would be problematic when handling many simultaneous users.

ISP Provided VPN Connections (VPN Dongles)

It is possible to obtain VPN connections from ISPs that are bound into SIM cards. Small set up in the organization side will be required for connecting VPN connectivity and end-users will get USB internet dongles. Above mentioned securing VPNs are still valid for these VPN connections. Additionally, losing such a device can be problematic and additional physical security for these devices is essential for these VPN USB dongles.

Restricting to Minimal Access Level to Internal Systems and Data

There is malpractice allowing all IT systems made available to the WFH workforce. Some system administrators make access to the entire high-security zone network subnets while WFH user needs to access only a single URL. Therefore, make proper user groupings and allow only what they need to carry out a business function. Always adhere to the Principle of Least Privilege (POLP) which is an important concept in computer security. POLP states the practice of limiting access rights for users to the bare minimum permissions they need to perform their work.

Enable Strict Monitoring

The usage of strict monitoring is a mandatory requirement for WFH. Both failure and success access attempts to VPN servers should be specially monitored. Additionally, the following baselines should have adhered with strict monitoring.

- Make sure IPS/IDS functionalities enabled in both perimeter and internal firewalls or other monitoring devices
- Make sure IPS/IDS are updated with latest threat signatures
- Make sure alerts are generated in an attempt of intrusion and adequate staff is attending to the alert by 24/7 and 365 days
- Monitor applications for unusual errors messages

Implement Proper Incident Response Mechanism

It is highly recommended have some type of technology or forum where you can answer peoples' questions and/or report incidents, preferably in real-time. This can be implemented through a dedicated email alias, a chat channel, or some type of online forum. The goal is you want to make security as approachable as possible and help people with their questions. Also, having such an interactive platform with your workforce enables you to quickly identify and respond to incidents.

Properly Enforce Adopted Enterprise IT Security Practices and Remote Working Policies

It is happy to see today many enterprises have adhered to basic information security hygiene. However, it is very important not to comprise such best practices due to the high requirements of WFH. Proper approval process and security hardening processes are needed to be carried out any information security-related activity even though the workforce is performing WFH. Even though the workforce switched to WFH, the positions of attackers have not changed.

Additionally, if your organization has existing policies for remote working, BYOD or COPE, make sure there enforced properly without dilutions.

Further Reading and Resources

- SANS: Work-From-Home Deployment Kit - https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit
- NCSC UK: Home working: preparing your organization and staff - https://www.ncsc.gov.uk/guidance/home-working
- ENISA: Top Tips for Cybersecurity when Working Remotely - https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely
- Norton: Keep your home Wi-Fi safe in 7 simple steps - https://us.norton.com/internetsecurity-iot-keep-your-home-wifi-safe.html