Security TIPS for Working from Home

End-Users

Make sure to update your antivirus software on the machine you're using to access corporate information.

Make sure to update your Operating System to the latest stable version and update all security patches.

Validate all email addresses for incoming email for legitimacy, especially the ones requesting information.

Don't click on unknown links in emails and attachments.

Validate all URLs that request you to sign in.

If you're not 100% sure of the legitimacy of the email, links, or attachments, contact your local IT for validation.

Avoid the use of USB sticks.

Don't connect to unknown, unsecure or open WIFI's. Remember that other people may be able to monitor your online activity.

Do not allow others to connect other devices to your laptop (i.e. USBs and USB related devices)

Only install software that has been approved by your IT department.

Enterprise

Always keep track of your devices and don't leave them unattended.

Assume the worst – Spare the cost of hiring a penetration tester and deploy defenses by assuming the worst.

Enable MFA on all compatible services. If MFA can't be implemented, require users to use strong passwords.

With increase in remote work, update your VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.

Alert employees to an expected increase in phishing attempts.

Assume that employees will use their personal devices on the corporate network, even if they are told not to.

Ensure IT security personnel test VPN limitations to prepare for mass usage and implement modifications such as rate limiting to prioritize users that will require higher bandwidths.

Assume employees value convenience more than security – They will find a way around cumbersome or inconvenient security policies.

An organization's first and last defense against a security breach is its own employees. Train employees on good security practices.