

## Remote Workers



## Checklist



### Workspace Security and Productivity

- 1 Setup your office in a place free of distractions.
- 2 Lock your computer and devices when not in use.
- 3 Limit work computer use to work activities.
- 4 For productivity, maintain an regular schedule (take lunch/coffee breaks etc.)



### Home Office Computer Security

- 1 Ensure computers are running company approved antivirus and anti-malware software.
- 2 Ensure your work computer is fully patched and up-to-date (OS and applications).
- 3 Use a **Virtual Private Network** <sup>2</sup> when connecting to your office resources.
- 4 Enable **Two-Factor Authentication** <sup>3</sup> (2FA) on all critical accounts (VPN, Bank, Email etc.)



### Wireless Network Security at Home

- 1 Set wireless networks to WPA-2 **encryption**. <sup>1</sup>
- 2 Update your Wireless Router firmware.
- 3 Change your wireless router's default password to a passphrase. Store in a Password Manager.
- 4 Follow your company's mobile device management policy.



### Prepare for Online Dangers

- 1 Learn the signs of **Phishing attack** <sup>4</sup> emails to spot and avoid them.
- 2 Use strong, unique passwords on all your accounts by **adopting a Password Manager**. <sup>5</sup>
- 3 Do some Cybersecurity Training. Learn in your favorite pajamas.
- 4 Backup your critical data to two locations; one should be online and one offline.

By following this advice, you will **Become more Aware** and in doing so, you will **Become more Secure**

<sup>1</sup> <https://cyberhoot.com/cybrary/encryption/>

<sup>2</sup> <https://cyberhoot.com/cybrary/virtual-private-network-vpn/>

<sup>3</sup> <https://cyberhoot.com/cybrary/two-factor-authentication/>

<sup>4</sup> <https://cyberhoot.com/blog/cyber-hoot-wednesday-avoiding-phishing-attacks/>

<sup>5</sup> <https://cyberhoot.com/blog/cyberhoot-wednesday-passwords-passphrases-and-password-managers/>

