Is Your Business New to Working Remotely? Start Here.

As our community works together during this difficult time to practice "social distancing," we would like to share our best practices for small to medium size businesses whose employees need to work remotely and/or whom are looking to conduct business remotely. Below are three areas in which we receive the most questions and therefore recommend that businesses start considering first when adopting remote work practices.

- **Remote collaboration.** Does your business need a way for employees and clients to virtually meet? If you need meeting collaboration software, first check to see if your business already has a Microsoft Office 365 or G-Suite license. If so, you may have access to collaboration tools like Microsoft Teams, Skype, or Google Meet are already included in your license or available for a low additional fee. If you prefer a different solution, and/or do not already have a meeting solution, we recommend Zoom meetings https:/www.zoom.us/. Zoom is known for its intuitive user experience and also integrates with most calendar software to make it easy to add meetings to calendars and manage meeting changes.

- **Home office equipment.** A high-quality headset and/or webcam can make all the difference between a frustrating meeting and a seamless professional experience. Here are a few recommendations:

  - Headphones: COWIN 37 Active Noise Cancelling Bluetooth Headphones ($49.99) or Logitech USB Headset H390 Noise Cancelling Headphones ($39.95).

  - Webcam: Logitech B525 Foldable Business Webcam ($64.99).

  - Want to easily share drawings and other "whiteboard" conversations? Online you can use Office365's Whiteboard or G-Suite's Jamboard, etc. If you prefer a physical solution try a Rocketbook Smart Reusable Notebook ($28.16) to easily digitize notes.

  - Lighting: High quality lighting is inexpensive. Try Emart 6" LED Ring Light ($32.99).

- **Secure business data.** As your business works virtually, your business may need to take extra steps to secure company and client data. Here are some solutions to consider:

  - 2-Factor Authentication. Mobile 2-Factor Authentication solutions like Duo Mobile provide increased protection against unauthorized access to cloud systems and data by requiring users to verify their identity before logging in. Users are sent a time-bound passcode, receive a phone call, or SMS before authenticating. We highly recommend these solutions, especially if employees are accessing business systems on personal devices.

  - Virtual Private Network (VPN). VPN solutions like Express VPN encrypt network data on devices and route the traffic through a secure server before connecting users to sites. VPNs add a layer of user privacy protection. As your employees use a home network or public WiFi to work remotely, this extra step will make it harder for those with ill intent (hackers, etc.) to track their activity. Ultimately a direct VPN solution to your office or using Chrome Remote Desktop to your office computer will be the most secure but a hotspot VPN is a start when working on public WiFi.

Working remote does require adjustments to processes and tools. If your organization is new to working remotely and has more than **5** employees, be sure to use a full remote work readiness assessment. While working remote is a change, planning and proven tools can reduce unnecessary user frustration and lost productivity.

For more information and a complete assessment on working remote readiness, contact us at:
https://omnitechpro.com/covid-19-remote-work-readiness-self-assessment