

# 7 TOP CYBERSECURITY TIPS FOR A SECURE REMOTE WORKPLACE

- (1) All WFH (#WorkFromHome) personnel should have access to a VPN (Virtual Private Network) for secure remote connectivity.
- (2) Do NOT use split tunnels. Send ALL traffic through the VPN, including Internet traffic, and ensure the proxy and HTTP/HTTPS protection you have in your office, is also applied to every remote workstation.
- (3) 2FA (2-Factor Authentication) must be enabled on all devices and user accounts, to add an additional layer of security.
- (4) WFH personnel should divide home WiFi networks into separate accounts. One for personal use and one for business use, each with distinctly different login credentials. These must not use easy-to-crack passwords but instead focus on passphrases (phrases, special characters/symbols, mix of upper/lowercases, foreign words, etc).
- (5) Employees need to avoid linking work and home devices, i.e., home Bluetooth speakers to work laptop. They also mustn't use personal home devices, (which could be shared by family members) for work.
- (6) WFH staff must increase vigilance where phishing attempts/scam emails claiming to contain "reliable updates" on COVID-19, are concerned. Trust ONLY news from known and legitimate media outlets, and do NOT click.
- (7) Now, more than ever, it's VITAL that everyone patches and updates. Patch your computers. Update your AV (Anti Virus) to ensure protection is up to date.

## CHECKING-IN ON YOU

These are difficult times for everyone around the world, and we wanted to reach out, to check in on you as we all stand united in this fight against COVID-19. As always, you are our top priority. From answering any questions you may have regarding your network to concerns about maintaining adequate security while working remotely, we're committed to doing whatever we can to lessen some of the weight you're presently shouldering - no matter where you're geographically located. During such a global crisis (*that's poised to escalate further and rapidly*), it's even more vital that everyone bands together and remains strong.

“

WHEREVER YOU MAY  
BE WORKING  
REMOTELY FROM,  
OUR TEAM IS READY  
TO HELP IN ANY WAY  
WE POSSIBLY CAN

”

Regardless of whether you view COVID-19 as an economic crisis first, and health risk second (*or vice versa*), the fact that we're standing knee deep in an outbreak that's quickly running rampant is irrefutable. So too the fact that remote working has become the new norm, AND even more critically, the many (*inevitable*) security risks that have come to light as a result thereof. These must be addressed (*and as we've always advocated*) proactively versus putting out fires after the fact.

Need help on network and/or remote cybersecurity-related issues? Just email us at [communications@networkboxusa.com](mailto:communications@networkboxusa.com) and we'll do our very best to assist.