CYBERSCOUT

7 Tips to Protect Your Business from the Risks of Remote Work Environments

With a rapid increase in telecommuting, every device, email server and WiFi network accessed outside the business network is a new potential access point or vulnerability for hackers to exploit. Business leaders must establish strict policies and employee guidelines to ensure that we don't have a cybercrime crisis during this unprecedented push to work remotely. Follow these seven tips to reduce threats:

1. **Issue security policy guidance and rules.**
   Annual trainings and email reminders from the IT department are not enough to keep good cyber habits top of mind for employees. A fresh reminder can go a long way to reinforce security best practices.

2. **Set up a VPN**
   A VPN system creates an encrypted tunnel that your internet traffic travels through so it can't be seen by third parties. Setting up a virtual private network (VPN) can seem daunting but just requires a couple hours to configure and isn't technically difficult. VPN with multi-factor authentication should be used as it is the strongest defense.

3. **Require Use of Encryption and WiFi Protected Access (WPA) to Secure Networks.**
   While no WiFi is totally secure, private, password protected networks are significantly more secure than public WiFi networks - especially those offered in cafes, hotels and other public places. You can always ask a business that offers public WiFi if private password protected networks are available.

4. **Password-Protect Devices Used By Employees and Third Parties.**
   Require employees to use strong passwords that contain letters, numbers and special characters. Avoid using the same password on multiple devices/accounts.

5. **Maintain Anti-Virus and Anti-Malware Software**
   Remind employees to install and regularly update adequate security software on all electronic devices they use to perform work remotely. That can be a phone, tablet, laptop, etc. Some employers are eliminating BYOD options and mandating that employees use only employer-supplied equipment and devices.

6. **Power Down**
   Encourage employees to power down computers when not in use. Powered off, computers are not accessible or susceptible to attacks or intrusions from the internet.

7. **Back Up Data.**
   Regularly backup sensitive information and, depending on the importance of the data, make sure it is encrypted. Secure backups are the best strategy to prevent critical business disruptions in case of a ransomware attack.