Progent™

https://www.progent.com/

5 Must-haves for a safe and secure WFH environment

Do you have staff working from home? With the pandemic still around, the answer to that question is most likely a “Yes”. And, that makes sense.

Why risk the safety of your staff when you can operate equally well or even better with them working from the safety of their homes. But, did you know that the WFH model can put your data at risk? When you have your employees work remotely, inadvertently your data becomes more vulnerable to cybercrime. This whitepaper discusses 5 things you should invest in to ensure the WFH environment is safe--for both your employees and your data.

#1 Anti-malware tools

Any discussion about data security has to start with anti-malware applications. These applications keep your computers safe from viruses, worms, adware, and other malware. When your employees are working remotely, they are most likely to use their own devices such as their laptops or the desktop computers at their home. Plus, with working schedules blurring, and the trend to “be there” 24/7 catching on, personal devices used for work include smartphones and tablets as well. It could so happen that your employee’s devices are not up-to-date on the latest anti-malware software. These software programs do not come cheap and so your employees may not have them at all or maybe using an outdated or free version of the tool, which may not be of much help. So, one of the first things you should do as a company is to provide the latest version of powerful anti-malware software to your staff to install on their devices. Again, if they are using personal devices, you may not be able to make this mandatory, but considering it safeguards their private data as well, most will happily take advantage of this offer.

#2 Firewalls

Firewalls protect your data by monitoring network traffic and allowing/blocking data exchange based on preset rules. For example, a firewall lets you dictate what websites can or cannot be accessed from a particular device, or what software programs may be installed, etc. Sounds great, doesn't it? Using a firewall you can weed out the risk of your employees compromising your data security unwittingly by visiting unsecured places on the web. Firewalls also generate alerts for the system administrator if there's an attempted breach. For example, someone tries to visit a site that has been firewalled. But, there's a caveat. You can only install a firewall on company property, that is, if you are providing your employees with laptops or desktops to use for work purposes. You can't Firewall your employee's devices that they are using to access work files when operating from home.

#3 Multi-factor authentication

When you are going away on a vacation, do you just close the screen door behind you and take off? No, right? You close all the doors and windows to your home, lock them--probably with multiple locks, and then activate your home security system. Multi-factor authentication is somewhat like that. Instead of using a single password for data access, multi-factor authentication adds more layers to security. If WFH has your employees accessing their work computers remotely, then you simply cannot skip multifactor authentication. Multi-factor authentication works by confirming the identity of the user across 3 areas

a) What they know: Examples include asking for User IDs, passwords, answers to 'secret questions', verification of their date of birth, etc.
b) What they have: This includes physical tokens, access cards, OTPs sent via text or email, etc.
c) Who they are: This authentication mechanism includes biometric authentication such as retina scan, fingerprint, or voice recognition.

While the 3rd kind of authentication (who they are) may not be easy to implement in a WFH scenario, you can still use multi-factor authentication to include the first 2 options.

#4 The Cloud

Using the Cloud to store your files presents a lot of advantages in the WFH environment. It certainly saves time and effort as files don't have to be mailed back and forth, eliminates version control challenges, and ensures timely access to data. But, did you know that you can also leverage the Cloud to thwart security threats presented by the WFH scenario? The Cloud lets your employees work safely from anywhere and offers more safety than local data storage mechanisms. Any data in the Cloud is encrypted, which means it is not that easy to access confidential information as it would be when someone hacks a PC. Plus, the chances of data loss are almost zero. Unlike your employees storing work files on their computer, which can be lost or misused if their device malfunctions or is stolen or hacked into, any data put on the Cloud stays there.

#5 Training

Did you know that lack of knowledge is one of the major reasons behind companies and individuals becoming victims of cybercrime? All it takes is one wrong click to open the floodgates, and the only way to stop that from happening is to train your employees on cybersecurity best practices. Training will not only provide them with a clear set of do's and don'ts but also help them identify situations where they may be a possible target. Training on cybersecurity best practices can cover a wide range of topics, but here are a few that should not be missed.

- Password hygiene
  - What does a good password look like?
  - Why is password sharing an absolute no-no?
- How to identify phishing attempts?
- Why is it important to install software updates and patches on a timely basis
- Data storage best practices
- The risks associated with public WiFi such as those at malls, coffee shops, or airports

You can also conduct mock drills and check who grasped these concepts right and who needs further training.

WFH opens up whole new horizons in terms of flexibility, productivity, and cost savings. But, it also opens your business up a little more to cybercriminals, as you can't have a hands-on approach to cybersecurity, especially if your employees are using their own devices for work. An experienced MSP can help you overcome the cybersecurity challenges propelled by the WFH scenario. They can put your mind at ease by taking care of everything--from anti-malware solutions to employee training, and beyond.

For more information please contact,
Tony Ciangiarulo | Progent
Phone: 408-240-9429 | Email: Tony.Ciangiarulo@progent.com