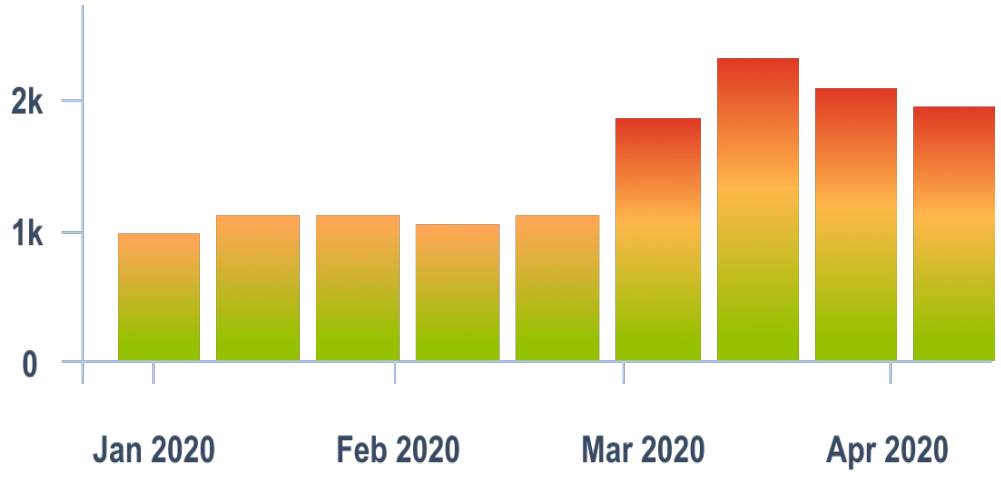
5 Must-do Steps to Make Working from Home Secure

Freelancers and consultants may know the best practices for working from home, but the COVID-19 pandemic has more people than ever working remotely. If you're not used to it, you've got to realize that you've got to take steps to ensure your computer and the software you're using to work from home is secure.

That's because cybercriminals know that attacking remote workers is much easier since home networks are typically less secure than office environments, which is why there's been a tremendous spike in cyberattacks since the pandemic started.



Source: Acronis Cyber Protection Operations Center, April 2020

A successful attack can give them access to an organization's servers, confidential documents, and valuable company data. Taking steps to protect your remote work can save tremendous headaches and lots of money.

Here are five recommendations for securing your home office during these difficult days.

Tip #1: Use a VPN

Whether you are connecting remotely to company resources and services, or you are just browsing web resources and using telecommunication tools, use a Virtual Private Network (VPN). VPNs encrypt all of your online traffic to prevent hackers from capturing your data in transit.

Your company may have a VPN policy, so you can get instructions from your admin or MSP technician. If not and you have to secure your home office, use a well-known respected VPN app and service.

Tip #2: Be wary of phishing attempts

New phishing websites pop-up every day using themes like COVID-19 to trick you into entering personal details, login credentials, or financial information. The good news is these can often (but not always) be blocked at the browser level with URL filtering.

Avoiding those malicious sites entirely is the safer bet. Typically those links are delivered in instant messages, emails, forum posts, etc. – so don't click any links you don't need to click on, and always avoid those that you did not expect to receive.

If you're looking for information about COVID-19 or other hot topics, go to official sources and agencies instead of opening links or emails from unknown sources.

Tip #3: Be sure to have good anti-malware up and running properly

---

Having a good anti-malware solution installed is a must nowadays. With Windows, where the majority of threats are targeted, the built-in Windows Defender does a good job of stopping threats.

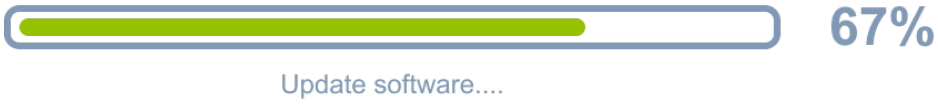
Simply having an anti-malware defense in place is not enough, however:

- Have a full scan performed at least once a day
- Be updated daily or hourly, depending on how often they are available
- Allow on-demand and real-time scans anytime new software installed

Also, don’t ignore the messages coming from your anti-malware solution. If you’re using a paid service, you don’t want your license to lapse

---

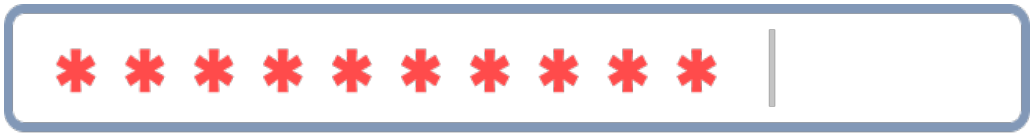
Tip #4: Patch your OS and apps



And speaking of not ignoring messages from software providers, keeping your operating system (OS) up to date is crucial, as a lot of attacks succeed due to unpatched vulnerabilities. The only reason the WannaCry ransomware attack from a few years ago was so virulent and damaging was because victims had not applied the Windows patch that Microsoft delivered months beforehand.

If you don't use any patch management software, keep track of the updates available for all of your applications can be hard. Be sure that at least your operating system gets all the updates it needs and that they are quickly installed. Then, be sure that auto-updates to popular software vendors like Adobe are enabled and such apps like PDF Reader are also updated promptly.

Tip #5: Protect your passwords



Maintaining good password practices is always the top piece of security advice, but it's even more important when working from home. Make sure your passwords are strong and known only to you. What's considered

strong? Think of 20 characters, since the old eight-character passwords are easily opened by brute-force attacks now. Creating a set of long phrases that you can remember is more effective than random combinations of letters, numbers, and symbols.

Of course, you should never share passwords with anyone, and use different passwords for every service you use. Password management software makes that juggling easier and is infinitely more secure than keeping a list of passwords on a Post-It note where anyone can find them.