7 Work from Home Security Tips to Include in Your Cybersecurity Checkup

A full year after the pandemic began, studies suggest that remote work is here to stay. Over 40 percent of employees work remotely and plan to continue to do so indefinitely. With that in mind, organizations should take the pandemic anniversary as a time to conduct a cybersecurity checkup. Be sure to include these work from home security tips in the strategy moving forward.

1. Ensure Endpoint Security

With an increasingly mobile workforce, the network perimeter has all but disappeared. Each laptop, tablet and smartphone that connects to the network adds another possible entryway for cyber criminals. Consequently, organizations need to pay special attention to endpoint security.

Start with mobile device management (MDM) to address access at the device level. MDM enforces acceptable use policies, manages encryption, determines whether a device can access the network and blocks risky activities. With MDM, for instance, you can enforce multi-factor authentication (MFA) policies and require that devices meet specific security standards.

2. Pay Special Attention to Protecting Email

Email represents the number one risk for security breaches. And when employees work remotely, they depend on email even more for sending links and sensitive documents. In addition to beefing up automated email policies, organizations should mandate multi-factor authentication for email accounts and ensure email encryption.

Along with technology safeguards, cover the human element, as well. Deliver regular bursts of cybersecurity training to remind users of security risks and best practices to counter them. For instance, all users should understand the elements of strong passwords and know how to recognize phishing emails.

3. Practice Safe Video Conferencing

With a large percentage of the workforce working remotely, video conferencing has become a fixture in daily life. We conduct meetings, do schoolwork, and even socialize over video. And because we spend so much time in front of a webcam, we sometimes forget that video conferencing brings inherent security risks. Take steps to minimize those risks.

For instance, to make sure that meetings remain private, use a waiting room or password to control guest entry to the meeting. And keep in mind that not all conferencing apps provide end-to-end encryption for video meetings. For meetings that will cover extremely sensitive information, be sure the software provides necessary encryption.

4. Strengthen Remote Connections

Remote connections form the backbone of work from home success. As a critical item on the cybersecurity checkup, organizations should review the infrastructure that enables your mobile workforce to access necessary applications and data. For instance, if you use a VPN, enforce MFA policies and make sure you have enough capacity to handle all remote workers.

As an alternative to using a VPN, reduce remote access to the network by using virtual desktops. And, where possible, migrate applications to the cloud. In addition to minimizing risk to the network, cloud computing offers significant benefits for remote work, including flexibility and scalability.

5. Enforce Centralized Storage

One important benefit of cloud computing includes access to scalable, centralized document storage. Whether your organization utilizes cloud storage or server storage, make sure all employees use it. Centralized storage simplifies backups and ensures business continuity. Documents stored on local computers do not benefit from the same security measures.

6. Update Security Policies

Hopefully, you already review security policies at least annually. With the upheaval of the past year, pay special attention to your policies now. Make sure they cover important aspects related to remote work. For example, security policies should include acceptable use policies for equipment and for internet access, password requirements, encryption and protocols for BYOD.

7. Separate Home and Office Computers

If you enjoy the privilege of working from home, this responsibility requires that you keep the computer you use for work separate from the family computer. If you are using a personal device for work, sharing it with spouses and kids is dangerous. Protect your systems from unauthorized use by family and ensure that your work-from-home computer is protected by company endorsed anti-virus and security software.

Implementing Work from Home Security Tips

Like many businesses, you may discover some gaps in your remote work cybersecurity. Messaging Architects can help. Our cybersecurity consultants can walk you through implementing automated email policies, migrating to the cloud, or building a comprehensive data security strategy tailored to your needs.