RAMTech
We Make IT Simple.

7 STRATEGIES TO SECURE WORK FROM HOME

People worldwide are working from home. Often on personal devices, using their own Internet connections. These seven strategies address challenges business face securing the work from home environment.

Even before the pandemic, remote work had momentum. Today’s widely available business collaboration software enables productivity and offers accountability.

The company could enjoy a larger talent pool and reduce technology and real estate costs. The employees were happier without a commute and greater work-life balance.

Yet, COVID-19 took working from home to another level. The health crisis challenged businesses to react quickly and get users up and running remotely. The urgency of the transformation left many businesses scrambling.

Yet the sudden shift to remote work doesn’t ease the need to:

- Protect personally identifiable information of customers and employees
- Secure valuable business data and proprietary information
- Prevent unauthorized access to business systems, networks and hardware
- Track access to business infrastructure to detect intrusions and defend against attack

Onsite, your business might have had workstation monitoring, firewalls, unified threat management appliances and more. Plus, a dedicated IT team providing comprehensive security. Locking down business done offsite, on many different devices, is more challenging. Rethink cybersecurity for the new work from home environment with these strategies.

#1 Require Antivirus & Malware Upgrades

Perhaps employees had business laptops. Or you asked them to cart home desktops and monitors. Otherwise, they’re working now on personal devices. They’re using personal computers, laptops, tablets, or smartphones — of any brand. You can’t be sure their devices have the same protections installed. Personal devices could lack firewalls and antivirus protection. Users may not have backups set up either.

Ensure that all business users working remotely install up-to-date antivirus and malware packages. Your business could buy a license for multiple remote employees. Remind users also to keep these current or have a Managed Service Provider manage it. Skipping a security patch could be disastrous.

#2 Provide Cloud-Based Software Solutions

In your office, everyone was on the same version of key software. Now, though, you can’t be certain that all your users have the same version. How do you know when they last updated their software?

The same with operating systems. Windows 7 reached its end of life on January 14, 2020. That means it’s no longer updated with security patches from Microsoft. Hackers know this. Mac users can also be using older operating systems to support their hardware. These employees may not have upgraded at home because their tech still works “just fine.” But, that’s not going to meet compliance requirements or secure your business systems.

Another issue could be that people are Mac users at home, but PC users at work. Or vice versa. This could cause difficulties in transferring work files.

Make things safe and consistent. Provide every user access to a cloud-based software solution. Office 365 is a subscription-based service providing Microsoft Office, Teams, SharePoint, and more. Or G-Suite is the Google equivalent.

Plus, most cloud-based solutions let an administrator monitor and manage user accounts. This helps with access management and maintaining a cybersecurity standard.

#3 Limit External Sharing

Your employees need to continue collaborating and communicating while working from home. Business collaboration software makes this possible in real-time and securely.

At the same time, your staff need to engage with vendors, suppliers, customers and clients too. You may want to limit file sharing outside of your business. You have fewer protections for that data or information once it is in other hands.

With a few setting changes in software like Microsoft 365 or G Suite, you can make it so that only people with a business account can view a file. Or it may be enough to share information on a read-only basis to prevent changes to any documents.

#4 Enable Multifactor Authentication

Cybercriminals have many ways to gain access credentials. Multifactor Authentication goes beyond entering a username and password to login. Two-factor or multifactor authentication (MFA) is increasingly common.

Any time you've entered your username and password and then provided a code sent by email or text, you've been using MFA. With MFA, the user has to provide more than one layer of evidence to gain access.

MFA adds more security, making it harder for bad actors to impersonate a legitimate user. They can't get in by knowing a user's password or PIN alone.

They'd also need access to the user's phone or email account.

This added layer of security is a good idea for any devices used offsite. It can also prevent exploitation if an employee's laptop gets stolen. Or reduce the danger of a child accidentally opening any work-related files.

#5 Educate Users about Wi-Fi Password Protection

A virtual private network (VPN) can secure business communications for work from home. A VPN creates a secure connection between the home user’s network and the business network. Data traffic between the two points is encrypted for added protection.

A business might load its laptops with a VPN or subscribe to VPN services for its users. There are free VPN options. They come at a price, though. They're often subsidized with advertising or they sell your browsing data.

Businesses that aren’t using a VPN should have a policy in place for connecting to the Internet from home. This should require employees to:

- Change the default username and password on a home Wi-Fi router
- Turn on wireless network encryption
- Hide the network from view
- Keep router software current
- Recommending users turn off their Wi-Fi network when not at home is also a good idea.

#6 Communicate Expectations for Ensuring Business Security

When employees work on-premises, you can monitor usage. People think twice about opening random files or graphics. Yet you can’t be sure they aren’t using pirated software at home. Plus, with the same device used for personal and professional reasons, acceptable use grows more blurry.

Clearly communicate what users should avoid. This would include recommendations to:

- Keep work devices shut down or locked when not in use
- Store work devices out of sight and in a safe place at the end of the workday

- Install password protection on any device used to access work files
- Keep personal and professional accounts separate — don’t send work-related emails from private addresses and vice versa
- Avoid public Wi-Fi
- Secure home Wi-Fi with a strong password
- Remain wary of phishing and other attempts to compromise business credentials
- Save and back up files as outlined by your IT team (How often? Where to?work remotely without compromising security or risking non-compliance?

#7 Make IT Support Available

Adding these cybersecurity requirements may feel like another imposition on employees right now. Make it easier for them by offering the IT support they need.

Ensure users have someone reliable they can contact when they encounter technical problems. Different employees will have varying comfort levels with work from home technology. What worked for them working remotely once or twice a month, may not fit the bill now. Providing tech support can go a long way to employee productivity and boost morale.

Conclusion

Good technologies and cybersecurity policies can go a long way. At the same time, educating your employees in security awareness is critical too.

Work from home may be a short-term solution for some. Others may identify long-term benefits and stick with it. The strategies outlined here can make remote work viable, reliable, safe and secure.

Need help setting up for remote work? Or implementing administrative controls for work from home? A managed service provider can help. Our experts can get you up and running. Or we can provide the IT help your people need. Contact us today at 678-999-2172!

RAM Tech

We Make IT Simple.

www.ramtechpcs.com

678-999-2172

• Managed IT Services • Network Security
• Backup Solutions • Computer Repair

RAM-Tech PC Solutions, LLC

Phone: **(678) 999-2172**

Email: **info@ramtechpcs.com**

Web: **ramtechpcs.com**

Facebook: **www.facebook.com/ramtechpcs**