Remote Employees and Network Security

Tips, tricks, and tech to keep remote workers, and company data, safe

LOCKNET
AN EOJOHNSON COMPANY

LOCKNET
AN EOJOHNSON COMPANY

Table of Contents

DID YOU KNOW?

445 M

cyber attacks were reported in the first quarter of 2020

We can all agree now that working from home isn't going anywhere.

In some way, shape, or form your employees will be working from home at least part of the time. Nationwide, research shows that post-pandemic 42% of employees who worked strictly from the office or a company-based location will not return to the office.

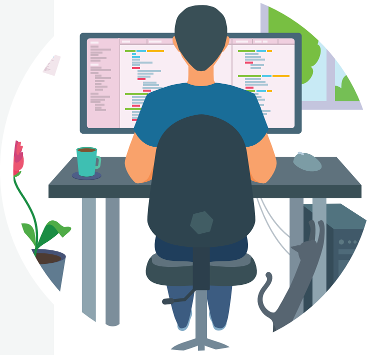
How will that impact your business? Do you have an effective strategy for maintaining your digital security while workers are in potentially unsecure environments? Have your clients begun to ask about your employees' digital security? Do you know what your responsibility is for your clients' data?

At this point in time, laptops are still in scarce supply and lead times on newly-deployed laptops can be 4-8 weeks. This raises some particular concerns.

So, before we get into specific technologies and strategies, here's our first tip for your work-from-home strategy:

First off, **do not allow your employees to connect their personal computers to your remote desktop, VPN, or other company network connections.** The reasons for this are many, but specifically that device contains none of your corporate security measures: unknown antivirus, no webfilters, etc. By connecting that device, you are trusting every single data point on it, and you trust every website that the employee has ever accessed from that device. In addition, providing corporate access from personal computers presents a multitude of legal and compliance issues. As tempting as it may be as a short-term fix, just do not do it.

So, what if you have no other option? If no laptops are available to the employee and it is absolutely necessary for them to have connectivity, have your employees go to the office and bring home their desktop device. It will be bulkier to haul and set up, and may need to have wireless added to it, but it will be a better solution.



Do not allow employees to use personal computers while working from home

- Unknown antivirus
- No webfilters
- Legal and compliance issues

DID YOU KNOW?

78%

of the organizations in the U.S. have experienced a cyber attack in the past year

Now, let's talk technology.

At Locknet Managed IT, we're passionate about protecting our clients, so we recommend tools that will ensure a lock-tight environment. These are the tools you simply need to have in place in our new working reality—according to our team of experts—to protect your client data and network, and ensure the continued productivity of your employees.

1

Remote Monitoring and Management Technology

A proper Remote Monitoring and Management (RMM) tool will increase the impact of your internal IT department. This tool allows multiple solutions to be deployed from a single pane of glass. Your IT team can automatically and remotely update and patch your company PCs, remote on to those PCs to help fix any IT issues, monitor third-party software and much more.

Why is this important to your business? Patching and monitoring your PCs is critical to the security of your environment. A patch deployment repairs or "patches" the pieces of code that have been manipulated by cybercriminals to gain access to your devices and network. Patching essentially closes and locks the open door. But patches only are as effective as the patching schedule and technology used to patch. In other words, if a patch is not applied, the "door" is still open.

How is this more efficient than what you are doing now? To be frank, while you may already have an all-in-one RMM solution, but most small to medium size businesses do not due to the cost and the complexity to deploy and administer. Often businesses are cobbling together several free tools to do all that RMM technology does in one. Those free tools may appear to be comparable, but they usually do nothing exceptionally well, and are typically unstable and unreliable. Putting all of these functions, and more, into a single tool could save up to one FTE of time within your IT organization. How? Patching an environment correctly and monitoring warning signs of potential failure is a time-consuming, manual process. It easily falls to the bottom of a to-do list and can often go ignored. With an all-in-one solution, you'll have the peace of mind that comes with knowing you're protected, while also freeing staff up for the rest of their responsibilities.

DID YOU KNOW?

57%

of data breaches can be attributed to lackluster patch management

A proper Remote Monitoring and Management tool will increase the impact of your internal IT department.

2

Managed Antivirus Software

We all know that antivirus software is important, but how do you choose one, and how do you know which is best for you?

When considering an antivirus solution, you want to consider:

- the virus definitions;
- how many types of threats it protects against;
- and most importantly, how the antivirus software will impact the performance of your network devices

Most antivirus applications include protection against malware, phishing, and system viruses. The virus definitions and updates are constantly changing, so it's essential to look for a trusted antivirus application that continually updates and looks for new viruses as part of your package.

The third item may be the most important. How many times have you started a virus scan or even worse, had the scan start when you were in the middle of an important project? The resources used by your antivirus is an incredibly important consideration when selecting a commercial grade antivirus. Antivirus software can use a lot of computing power and compete with other applications for processor speed, RAM and more. With the correct anitvirus software these processes can be done in the background with minimal interruption to the user. Work continues as normal.

Antivirus Management

- 24/7 monitoring
- Central management
- Rapid response
- Cost effective
- Peace of mind

DID YOU KNOW?

80%

of reported cyberattacks are phishing

3

Remote End User Protection

When working from the office, your employees are protected by your network firewall, website filter included. When working from home they, and your corporate devices, lose that protection.

A remote end user protection technology will allow your corporate firewall settings to be replicated to remotely protect your remote and roaming users.

From a productivity standpoint you are assured that your employees are not accessing potentially undesirable sites such as social networking, adult themed, gambling, etc. All these settings, like your firewall settings, are customizable per user.

4

Secure Passwords and Password Management

A password policy gets a lot of attention when implemented. You may hear grumbling such as, “I just changed my password,” or, “Why does it need to be so long?”

A properly-deployed domain password policy is essential for your business. To protect your data, passwords should be required to be long (at least ten digits, but fifteen is ideal) and complex (including combinations of lower and upper case letters, symbols, and numbers), and they should also expire every 45 or 90 days.

What about other application-specific passwords? A password management tool can help you and your employees address the frustrations of managing multiple complex passwords. How many times have you seen a password on a post-it note on an employee desk? Now imagine that password written on their desk at home for any visitor to their home to see. Makes you cringe a little, right? How about the headaches caused when a shared password changes? Along with constant emails asking who changed the password, the dreaded password-in-an-email scenario is bound to happen.

A proper password management tool can help with all of these things.

By remembering only the one password needed to access the password management tool, your employees can access the tool which does several things:

1. **PASSWORD CREATOR**
   It helps generate complex passwords that will meet your length and complexity requirements.

2. **PASSWORD VAULT**
   This will, based on the website visited, automatically input your username and password with a single click.

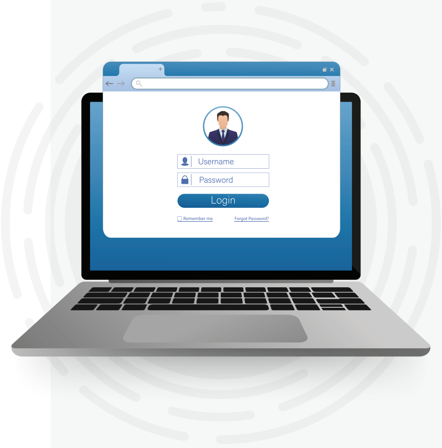
3. **SHARED PASSWORD FUNCTION**
   This is perhaps the most impressive feature. Based on permissions and user profiles you can share the password amongst a group, meaning that the application will store the most recent password and when it’s changed, it gets updated for everyone.

DID YOU KNOW?

Cybercrimes increased by nearly

300%

following the COVID-19 outbreak



Cybercriminals know the instant they capture your employees’ passwords they have what they need to have full access to your network data.

5

Multi-factor Authentication

Multi-factor Authentication (MFA) is something that most of us are already using now in our personal lives, but ironically we are rarely using in our professional settings.

MFA is the technology that your personal email provider, financial institutions, investment managers and others use to confirm your identity prior to logging you into the account to view any proprietary data.

When used in a corporate environment, this technology can consolidate MFA into a single application. In other words, you can use the same MFA tool for the Microsoft 365 suite of services, Virtual Private Network access, third-party integrations, and much more. This technology can even push the alert to your phone so all you have to do is confirm you are logging in; you may not even have to enter a six digit pin.

These days, with employees working from wherever they are, the risk of hackers harvesting credentials is greater than ever—meaning there's no time like the present to up your cybersecurity game.

6

Virtual Private Network

It is extremely easy to set up and use a remote desk top server to connect your employees to the office-based server resources. It is also extremely insecure. Simply put, for most businesses it can be an open door to your entire network.

Setting up a Virtual Private Network (VPN) is the most secure way to facilitate remote access by your employees.

A VPN controlled by your firewall is a best-in-class solution, and ensures the access is secure and can be monitored. When paired with an MFA tool the result is an extremely secure access tool that all of your employees can use.

DID YOU KNOW?

68%

of business leaders feel their cybersecurity risks are increasing

7

Security Awareness Training

Your employees probably participate in training regularly, whether that be job specific or related to company policies. But, are your employees regularly taking trainings related to IT security?

Security awareness training puts your employees through a number of modules chosen by you, to help increase their awareness of IT security threats. The best prepared businesses ensure staff are kept up-to-date on the latest threats (which are always changing), receiving training on a quarterly or even monthly basis. Online training should be performed on a regular basis to ensure it is top-of-mind (we recommend quarterly) and completion by employee should be tracked to ensure that 100% of employees are completing it. Remember, it only takes one employee to click on the wrong attachment in a malware-infected email to cause tremendous damage to the company.

As with all trainings, you want to make sure the behaviors are being learned, not just forgotten about once the certificate of completion hits their inbox.

To "test" your employees, make sure you choose a security awareness training application that has the ability to put together real-world tests, for example, fake phishing emails.

DID YOU KNOW?

$3.9M

is the average cost of a data breach

Network Security is within reach—even with a remote workforce.

Ready to take the next step in network security for your remote workforce? We can help! Contact us for a free network examination, to determine which of these tools would make the most sense for your business.

LOCKNET
AN EOJOHNSON COMPANY

844-365-4968
locknetmanagedit.com