Asigra.

Recovery is Everything™

# MSPs Guide to Enabling Secure Remote Work

## Here are11 tips how to stay safe

# Table of Contents

**Now's the time for good tech hygiene, too.** ..... **3**

**Security implications of remote work** ..... **4**

**What MSPs can do to enable secure remote working** ..... **6**

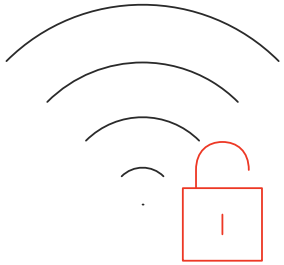
- Educate employees about basic home IT security ..... 6
- Update their software ..... 6
- Multi-Factor Authentication ..... 7
- Deploy a trusted VPN ..... 7
- Use a secure SSO platform ..... 8
- Back up their data ..... 8
- Secure file sharing ..... 8
- Provide secure collaboration tools ..... 9
- Review privileged access ..... 9
- Encrypt, geo locate & remote wipe sensitive data on edge devices ..... 9
- Plan for upcoming Helpdesk needs ..... 10


## Now's the time for good tech hygiene, too.

In just a few short weeks, remote work has morphed from a perk offered mostly by tech companies to an absolute necessity, as the COVID-19 epidemic continues to disrupt the daily lives of millions of people. Suddenly, companies are forced to enable their employees to work from home on a massive scale, while keeping their productivity up. By now nearly everyone is moving to remote work to some degree, at least temporarily, many more people are forced to work on their personal computers or phones exposing organizations, their data and their backups to a higher risk of hackers, even in normal times, and these aren't normal times.

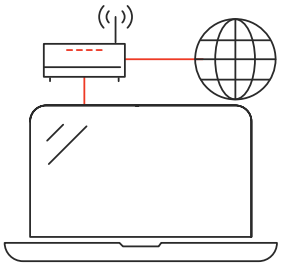
# Security implications of remote work

Remote working might be a critical risk management tool that can make the difference between surviving a pandemic or global disaster and sustaining unrecoverable damage, however it also creates a much wider target for hackers to infiltrate your network and possibly even your backup repositories. This introduces new risks and challenges for MSPs managing these corporate IT infrastructures. Some of the risks include:



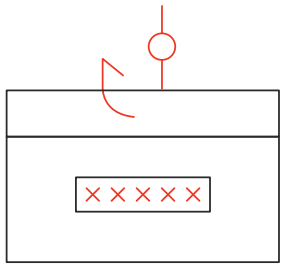
## Unsecured WIFI networks

Some workers may connect to enterprise assets through unsecured networks, potentially giving access to malicious parties to spy on the enterprise and collect confidential information.



## Using personal devices and networks

Home devices will often lack the tools built into business networks such as robust antivirus software, customized firewalls, and automatic online backup tools.

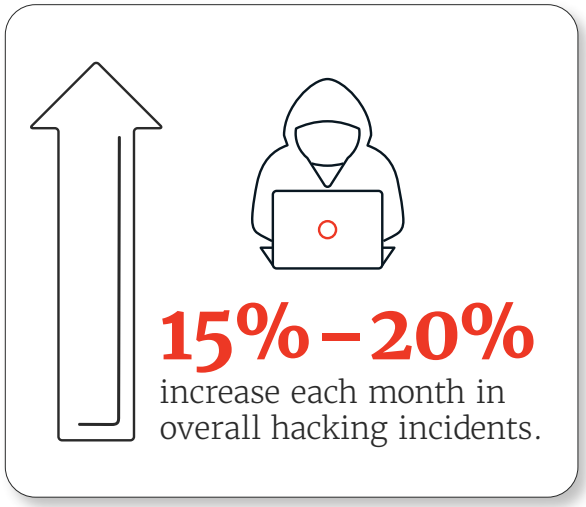


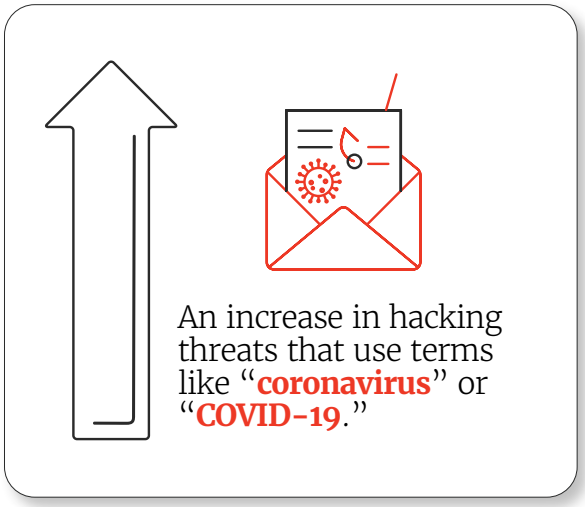
## Phishing

As more and more people work from home, we'll likely see an increase in malicious phishing campaigns targeting remote workers as they browse more personal sites and lower their guard.

There are simple steps you can take to limit the risk, though. That's good, because cybersecurity firms say it appears hackers have become more active lately. Researchers at Zscaler say since January 2020, they've seen a 15% to 20% increase each month in overall hacking incidents and an increase in hacking threats that use terms like "coronavirus" or "COVID-19" to trick users into handing over sensitive information or installing malicious software.

Limiting hacks could help prevent headaches at work sites, and it could also stop hackers from stealing data that your company is protecting.

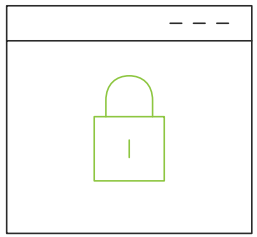



Source: Researchers at Zscaler, January 2020

# What MSPs can do to enable secure remote working

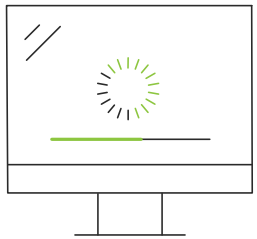
MSPs must ensure that the remote workers are adequately secured, and security teams have the right infrastructure in place, including such capabilities as remote access, remote wiping or bricking, and secure channels for communication. Here are 11 tips:



## 1 Educate employees about basic home IT security

Home environments are inherently less secure, potentially risking business-related assets. At home, it's less likely workers are protected by the corporate software that can scan every link they click and file downloaded for signs of danger.

Even though this step might seem like a no-brainer, this is the most important step. A simple email to staff reminding users, especially those handling sensitive business data, to practice basic tech hygiene, to set their own passwords on routers and smart devices and take other basic measures.



## 2 Update their software

An obvious policy in most organizations which is usually done automatically, but because workers aren't in the office, MSPs could have a harder time making adjustments to deploy remotely, keeping software updated automatically. And believe it or not, these end-users might not even realize that to stop hackers, the most important thing one can do is keeping software up to date.

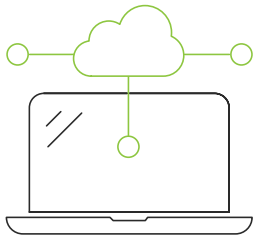
When software companies release updates that fix security flaws, they're essentially handing hackers a key that helps them access devices running the older version of the software. When you update your software, you're essentially changing the locks, and it'll be a lot harder for hackers to get in. It's not just the applications and operating systems running on their laptops and phones that need updating, even routers need to be secured. Of course, there are potential drawbacks. Software updates themselves can sometimes cause problems for the MSP, breaking programs that are essential to remote workers. However, these problems typically get noticed and addressed

quickly by the MSP, but still requires unwelcome time and resources spent fixing it. It thus pays to wait and make sure there aren't any surprise problems with a specific update, but don't wait too long.

## 3 Multi-Factor Authentication

Phishing is on the rise and attackers acted fast to take advantage of the current Coronavirus health scare. Research shows that customized phishing campaigns intended to steal credentials and spread malware are increasing.

Remind and educate employees about these risks – do not click links or open attachments unless sure about the source. And make sure employees use a **MFA solution** to decrease credential theft risks.



## 4 Deploy a trusted VPN

Access to company assets is most likely already dependent on a VPN. For people using a work computer at home, corporate anti-virus software and other security tools are often running by default. If workers have access to a corporate VPN, remote workers can use it to access the company network, where the MSP can better protect them from afar. This won't work for all companies, which might not be prepared to have their entire workforce use the VPN at once, so it's worth checking with the customer. Remote workers can also use a personal VPN, but that's mostly to protect their own privacy, as these services aren't meant to protect them from malicious software and apps.

If workers have access to a corporate VPN, remote workers can use it to access the company network, where the MSP can better protect them from afar. This won't work for all companies, which might not be prepared to have their entire workforce use the VPN at once, so it's worth checking with the customer. Remote workers can also use a personal VPN, but that's mostly to protect their own privacy, as these services aren't meant to protect them from malicious software and apps.

## 5 Use a secure SSO platform

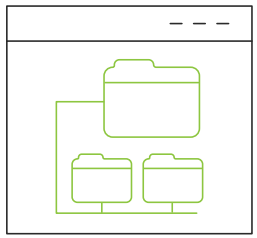
For organizations relying on cloud services and online platforms, one user's compromised credentials could be especially devastating these days.

A Single Sign-On portal with secure authentication will prevent multiple passwords and minimize the risk for takeovers. Users never have to recall or enter another password and enjoy simple "touch-and-go" authentication across all business systems. And businesses improve their security posture by replacing vulnerable passwords with a high-assurance authenticator.

## 6 Back up their data

When work is done at home it's less likely to be constantly backed up, unless employees have an easy tool that does that for them.

Not only should employees understand the importance of regular backup, they must also know how to verify it's actually working. By backing up critical data located on mobile endpoints to a secure data center, you can easily recover a worker's data if a device is lost, stolen, or damaged. A point in time backup copy previously taken from their old mobile device is used to restore data to a replacement device.

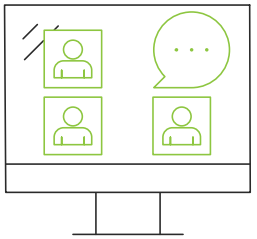


## 7 Secure file sharing

The alternative to a VPN is to give remote workers access to a file sharing service. VPN might be a good solution for larger companies with the IT staff to set up and manage these connections. For others, a file sharing solution is the simpler option.

VPN speeds don't compare favorably to regular internet connections. There can also be connectivity issues, which can disrupt the working day if the remote workers are in a different time zone to your IT staff. For distributed teams who are working around the globe, then file sharing may be a better solution. An excellent file sharing service is not just about user experience but also more about efficient synchronization and security. A further advantage of this approach is that data could be backed up from a centralized location, enabling additional ransomware and malware prevention.

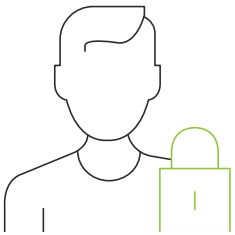
This can be performed through sophisticated **signature-less malware detection** engines which identify and quarantine unauthorized or malicious embedded code, including unknown and "zero day" attacks, from penetrating backup and replication streams, if your data protection solution is enabled to perform that.



## 8 Provide secure collaboration tools

The need for remote collaboration tools is higher than ever, and the temptation to approve anything that helps employees is high as well.

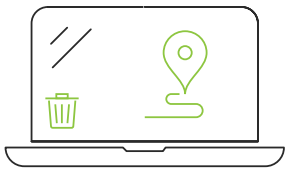
As with File Sharing, it is important for MSPs to be proactive in providing organizations and their remote workers with a list of recommended collaboration tools. Without official tools, workers are very likely to use free products and personal accounts that are, at best, less secure.



## 9 Review privileged access

Privileged accounts always pose a potential threat, even more so when IT reaction time is slower.

This is a good time as any to review organizational privileges and make sure **principles of least privilege** are met.

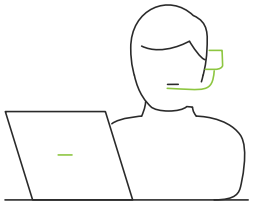


## 10 Encrypt, geo locate & remote wipe sensitive data on edge devices

When work is done remotely, loss or theft of laptops and storage devices is simply more likely to happen at some point.

Full disk encryption is natively available in most modern laptops and mobile devices, using it (or another encryption solution) can prevent major data breaches. Further safety measures can be taken to protect the organization from potential disgruntled employees by locating and remotely wiping endpoint devices before data gets compromised. Wipe any data included in the backup

policy that you have defined—without touching any data excluded from that backup policy. While other mobile device wipe options reset devices back to factory settings, this selective data destruction allows you to retain control over corporate data without impacting employee's personal data if you have a BYOD policy.



## 11 Plan for upcoming Helpdesk needs

Moving to remote work is bound to bring some unexpected IT needs from employees placing additional strain on the MSP helpdesk teams.

The MSP's helpdesk teams are crucial at times of change to guarantee continuity of work. They should not be overwhelmed with preventable issues such as password resets and renewals. Taking the time plan and develop a Business Continuity Plan and basic internal procedures can go a long way in serving your customers with confidence.

### About Asigra

Asigra's trusted technology is proudly developed in and supported from North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global partner network of Managed IT service providers. As the industry's most comprehensive data protection platform for servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, and eliminates silos of backup data by providing a single consolidated repository with 100% recovery assurance and anti-ransomware defense. Asigra's software has won numerous awards in the Best Enterprise Backup and Recovery Software and Storage Innovation categories for its unmatched defense of backup data against the rapidly growing threat of ransomware infiltrating backup repositories.



Asigra.
Recovery is Everything™