

How to secure a remote workforce



Table of Contents

	Introduction	3
---	--------------	---

Security Issues IT Admins Need to Consider When it Comes to Remote Work

	Substantially increased online communication	4
---	--	---

	Scanning and patching remote devices	5
---	--------------------------------------	---

	Home network security	7
--	-----------------------	---

	Backup all data with encrypted backups	10
---	--	----

	How difficult is it to secure a remote workforce?	11
---	---	----

	Protect your business with Unlimited Network Security	11
---	--	----



Introduction

Your small business has changed in ways you never expected. Even if you aren't operating in a location with mandatory stay-at-home orders, you want to keep your employees safe. As a consequence, your business may have either partially or fully shifted online.

This complicates the necessity of keeping all files and communications safe. The machines driving your business may no longer solely be located in your offices.

Where do you go from here? Your budget is stretched thin. You don't have remote IT experts on your team. Your business plan was likely not prepared to keep things safe in case of a catastrophic event in which all employees must stay home.

Many businesses began making the switch to remote employees before the COVID-19 pandemic. For others, this means there are established best practices and cost-efficient software to make your life easier, keep your company secure,

Security Issues IT Admins Need to Consider When it Comes to Remote Work



Substantially increased online communication

Now that so much interaction and communication has switched to online, you need to ensure that you have robust email and communication security.

While being secure with video chat generally comes down to choosing the most privacy-friendly software for your needs, email choices are more nuanced. Email needs to be kept safe from numerous threats, including unauthorized access or loss.

Email intrusions may be phishing attacks, spam, or malware, with deceptive subjects, content, attachments, or links that entice users. You need a comprehensive anti-spam service coupled with employee education about the nature and appearance of these attacks.

Targeted phishing attacks for at-home workers will likely increase as malicious actors know there will be more people in this new and potentially less-protected position.

There are numerous work-from-home and other attacks that could cost people money, risk vital information, and open your company to other attacks. Potential hacking attempts can be recognized if people know what to look for. Offer a refresher course for employees to make them aware of current email scams and phishing attacks.

Malicious actors may still use unsecured email as an access point to enter your network. To prevent this, make sure everyone has a strong password and MFA (multi-factor authentication) turned on.

As a best practice, your company should also consider an automated email encryption solution that analyzes outbound email traffic to recognize sensitive material and encrypt such emails deemed sensitive.



If you are using a large, browser-based email client such as Gmail, you are already encrypting each email with Transport Layer Security (TLS). This type of encryption isn't as secure as end-to-end encryption, so you should still use a different service for sensitive data. As long as everyone in your company follows the advice listed above to keep their accounts safe, avoid malware links, and recognize phishing schemes, your communications should be secure for remote working.

Tool(s) You Need for This Security Issue

- ✓ Anti-virus with built-in email scanning
- ✓ Phishing and Internet Security Protection Tools (typically integrated into your browser)

Best Practices

- Educate your employees on all common phishing and spam attacks
- Be hyper-attentive of all links and attachments sent through email, particularly from unknown senders
- Enforce proper password regulations
- Enforce two-factor authentication
- Use more secure, end-to-end encrypted methods for sending sensitive data



Scanning and patching remote devices

In normal circumstances, your IT team follows a schedule and practice, issuing vital patches immediately and following schedules to push non-vital patches overnight or during non-work hours to reduce interference with staff. Now, your network includes machines no longer just in-office.

To keep everyone secure while working from home, you need software that scans and patches all remote devices. [One in three breaches](#) are caused by unpatched vulnerabilities. These security breaches could be prevented by simply making sure your machines are fully patched.

This is more difficult when you switch to remote staff but it's not impossible. There are software options built for this exact purpose. Your IT team can follow their in-place security plan with slight modifications. Your staff's devices can stay up-to-date and secure, even if they're remote.

Tool(s) You Need for This Security Issue

- ✓ Network monitor
- ✓ Remote management software

Best Practices

- Assess your network and develop a full inventory. Regularly scan your network for missing patches
- Make sure all operating systems in your network are covered (something you might not have had to worry about when not working remotely, if every computer in your office ran only Windows, for example)
- Schedule time to push patches while still being aware of vital updates that must be pushed immediately
- Test after deployment and be prepared to rollback patches that cause problems until a solution is found or a new patch is issued
- Identify all vulnerabilities with remote scans, even those not due to missing patches





Home network security

Another important step towards securing remote workers is ensuring their home network security system is ready and robust.

- Encrypting data in transit

When working from home, it's important that your employees encrypt their data. To keep materials private, everyone in your company should be using a VPN at home when accessing sensitive information.

A VPN delivers an encrypted tunnel that protects your web traffic and unties you from your specific IP address. This gives your company and employees more privacy.

Depending on your VPN, employees may add more risk to your network through connections to potentially unsecured devices. Make sure employees are aware of this risk and only use the VPN when accessing work-related data.

- Encrypted wifi

While it is rare that a personal wifi becomes compromised, if it occurs the attacker can intercept everything you send or enter online: bank info, email accounts, corporate access credentials, and more.

Ensure your network is properly configured and you encrypt your connection. WPA2 or now WPA3 is typically considered the best option for wifi encryption, and your wifi password must be strong.

- Router changes

You should change your router login and password. These can arrive as standard (such as 'admin') and may be weak or easy to guess. Malicious actors take advantage of this to capture the router, turning it into a bot or allowing attackers to spy on you as your online information is sent through the router. Ensure firmware updates are automatically installed to address security vulnerabilities.

Depending on the level of security your business requires, you could also take the extra steps of having employees restrict inbound and outbound traffic, select the highest level of encryption offered in their router settings, and turn off WPS. These steps are not user-friendly, so deploy them only if absolutely required.

- Firewall adjustments

Double-check your firewall settings to reinforce your home network security. Firewalls create a barrier to prevent threats that attempt to get into your system. This helps in two ways: stopping malicious programs from entering your network; and preventing data from leaking from your home devices.

Typically, firewalls are already built-in for your devices; make sure they are enabled in your settings. Small businesses may need a more comprehensive security plan through a third-party vendor to strengthen the firewall.







- Put anti-virus solutions in place for personal devices

While machines you keep at the office may already have anti-virus protections in place, many employees are now using personal devices that might not. Even if they follow the other advice given, poorly secured devices are a significant security risk.

Make sure that the computers your employees are using at home include powerful anti-virus solutions. Because of the circumstances, that might include buying a trusted anti-virus solution for your employees' devices, at least while they are required to have private company information on it.

It is critical that you protect all information related to your business, and that includes securing personal devices and ensuring on-time updates for these solutions.

Tool(s) You Need for This Security Issue

-  VPN
-  Bandwidth management
-  Enhanced firewall tools
-  Anti-virus solution

Best Practices

- Always use a VPN with untrusted networks
- Be mindful of bandwidth capabilities from a company's remote VPN
- Only download your company's remote VPN on devices you use to work
- Make sure the VPN authentication method and encryption are the strongest possible
- Constantly monitor inbound and outbound network communications for suspicious activity
- Have a strong password set for your wireless network
- Use a personally owned router rather than one given to you by your ISP and change the factory username and password
- Employ the strongest available firewall capabilities that still allow you to access the internet as desired
- Implement WPA2 or WPA3 on your wireless network
- Keep your router up-to-date
- Keep your anti-virus solution up-to-date



Backup all data with encrypted backups

Data is not properly secured without regular, encrypted backups. This is true whether or not your employees are working from home, but it's even more important with remote workers.



You have less control over remote workers' devices, therefore you can never be quite as sure that everything is fully functional and secure. Even something as simple as a coffee spill on a device could mean lost work or data if it isn't properly backed up.

A well-secured system ensures all company data can be encrypted, uploaded, and backed-up to a centralized source (often on the cloud, but it doesn't have to be), so you don't have to worry about losing important information from human error or malicious actions.

Tool(s) You Need for This Security Issue

- ✓ Encryption-enabled storage software

Best Practices

- Perform backups frequently and regularly
- Encrypt data during storage
- Decide how long it's necessary to keep a backup for depending on your business and its compliance regulations
- Consider storing the most important data in more than once place (ensuring that it is still encrypted and properly protected)



How difficult is it to secure a remote workforce?

Much of these suggested actions require small alterations to practices you already have in place or have been doing, such as an automated patch management service or regular backups of your data.

Some changes may require an adjustment at first, but there are many products to support companies switching to partially-remote or fully-remote employees. By following some simple best practices and adding a few necessary tools, your business and employees will be able to work remotely and securely, and stay safe.



Protect your business with GFI's security solution set

Unlimited | Network Security

Multilayer security to prevent, detect, and address threats to your network

Secure Network with **Firewall & Intrusion Prevention**

Secure Traffic with **Web & Email Antivirus**

Secure Endpoints with **Vulnerability Monitoring & Patching**

[Learn More](#)

