# How to Maintain Security in the Age of Remote Work

**kimcubitt.alphalifestyleacademy.com**

Remote work is quickly becoming the new normalfor modern companies. In a world where many offices were forced to shut down during the 2020 pandemic, team leaders discovered something. **Remote and hybrid working seems to be effective at improving productivity.**

Countless studies show that remote workers are more invested in their work than their counterparts, often working up to 1.4 days more per month. Remote staff members also demand fewer overheads and don't require massive real estate investments.

Unfortunately, **there's a downside to the remote working trend.**

86% of business executives agree that remote workers could increase a company's chances of a security breach. So, how do you ensure that your remote workers are secure in this new landscape?

Follow this process...

**Step 1: Create a Cybersecurity Policy**

The first step in defending company data is ensuring that all your employees are following the right guidelinesfor data protection. **Employees are often the main cause of security issues,** as they often take shortcuts when it comes to setting passwords and protecting data.

Employees may assume they're logging into a system from a secure environment when they're opening the door to criminals.

**A strong cybersecurity policy will outline everything your team members need to do to stay secure.** This includes making sure that they're using strong passwords for their accounts and that they never log into services from a public connection.

Your cybersecurity policy could also determine which applications and tools are safe for your remote employees to use when dealing with business data.

**Step 2: Secure Network Connections**

Access to an unsecured Wi-Fi network is one of the most common ways for companies to stumble into a security breach.

Unfortunately, a lot of remote workers have shifted to using their standard Wi-Fi connections and home routers to connect to the office. These services aren't always as protected as they should be.

**The easiest option for companies in search of better network protection may be to implement VPNs.** Asking your employees to use VPNs ensures that they have a direct and secure way to connect to the business network and access important information.

Make sure that any VPN you choose covers every level of encryption that's important for your team.

**Step 3: Consider Password Managers**

Password safety is another critical part of running a secure business in the age of remote work. Unfortunately, now that today's team members are using a wide range of software solutions and accounts each day, the number of passwords they must remember is increasing.

The result is often more employees using repetitive and simple passwords to access tools.

53% of people admit to reusing the same password for multiple accounts. While you

can support your team with information on how to choose more secure passwords, a password management solution may be a better option.

**Password managers allow team members to access a range of tools with just one set of credentials.** That means they only have a single code to remember.

**Step 4: Explore Two-Factor Authentication**

A password manager can help to make your accounts more secure – but passwords still only offer a single layer of protection. Two factor authentication could be an excellent choicefor companies who want to strengthen the security of remote teams.

That's because even if someone was to figure out your employee's password, that wouldn't be enough to get them into an account.

**Multi-factor authentication requires an additional input of a limited-time code or something similar to unlock access to an account or service.**

Multi-factor authentication is increasingly becoming more advanced. Today, it's possible to build strategies that use a password and biometric data to secure services. Your employees could protect their data with a fingerprint or retina scan.

**Step 5: Remember the Basics**

Technology like biometric securityis opening the door to a new level of protection for today's businesses. While these advanced offerings could be an exciting step forward for a lot of companies, it's worth remembering that the fundamentals are still important.

**Using encryption software with your video conferencing and messaging software is a must-have in the remote world.**

It's also worth ensuring that your employees have up-to-date systems for security on any devices they use, such as antivirus software, anti-malware, and phishing protection. Firewalls are even available to cover everything from tablets and

computers to smartphones and other mobile devices.

Remember, mobile device management tools can also help your team leaders to ensure that apps and security services remain up to date on your team's devices.

These services allow you to implement patches remotely, remove dangerous data from an employee's hard drive, and even blacklist certain apps.

**Avoid Jeopardizing Security**

Remote work doesn't have to jeopardize data security. Once remote workers are fully educated in the demands of secure working, and you have the right tools in place, you can enjoy all the benefits of flexible working without the security threats.