# Remote Working Cyber Security Best Practices


Remote work has long been an option for many newer and smaller companies. Now that the world is dealing with the coronavirus pandemic, millions of people across the globe are working remotely.

With remote work comes a great deal of freedom and flexibility, but as with everything in life, there is a downside, too.

Businesses must focus on cybersecurity more now than they've ever done before because with teams spread out, comes an increased risk of data breaches due to cyber attacks.

As a business with a remote workforce, there are some security measures you and your team can take to protect company data.

## 1. Avoid Public Wi-Fi

Your remote workers should make every effort not to use any public wi-fi network. Using these networks introduces a major security risk because others have access to that same network without a firewall between them.

Interested parties on that network, or any public network your data travels between you and your company can monitor the traffic as it flies by.

If working anywhere away from your private network at home, use a personal hotspot either from your phone or a dedicated device.

The traffic won't be encrypted between the hotspot and its destination, it does eliminate the risk of hacking by others on the public network. With the majority of mobile carriers, you can pay a small fee for the option to set up a private network on your cell phone plan.

Using it will count toward your data, but the cost is much more affordable than a data breach. In many cities, the 4G and 5G service is almost as fast as your home network, so there's no reason to rely on public wifi.

For the majority of remote access applications, use a virtual private network, or VPN. It gives you a way to protect your traffic as you use various websites, emails, SQL servers, and so on.

It's worth noting that not all VPNs are created equally, and the ones provided for privacy only protect the data as it moves to and from the VPN provider, not to the destination, so those aren't suitable for remote access protection.

## 2. Use a Work-Only Device, If Possible

If you're tempted to take care of a few small work-related tasks before bed, do so only on your work computer.

Use secure wi-fi, a VPN, anti-virus, encrypted drives, and endpoint protection. This is the only way to make sure you're protecting sensitive data. Using your personal devices, even over a secure network, can still make it possible for cybercriminals to access data.

If your organization has a strong IT team, they are likely working to block malicious websites, regularly updating software with security patches, running antivirus scans, and a number of other activities design to protect your data without you even realizing it.

Using a personal computer likely means you've not followed those same protocols,

and are risking your information security being compromised by a third party.

One way to make using a personal device less risk is to use remote access environments online, rather than downloading or syncing files to your computer.

## 3. Use a Privacy Screen

If you decide to go work from a coffee shop for a change of scenery, there's more than the public wi-fi security issues you need to worry about.

Sightlines are another consideration because if someone is behind you, they can see everything you type.

The right people can easily watch what you're doing and find confidential information.

Other than sitting in an area where it makes it hard for people to see your screen, you can use a privacy screen. It darkens your screen from a distance but still allows you to see up close so you can work. Onlookers won't see anything.

## 4. Encrypt Data to Protect It

When possible, avoid sending emails with sensitive information. It's always a risk because a third party can intercept it and see it. If you must send emails with sensitive data, encrypt it in an attachment.

This step prevents people from being able to view the information along the way. Set your device so that all stored data is encrypted so that it is protected in the event of theft.

## 5. Keep Devices in Your Possession at All Times

If you're going to be anywhere outside of your home office, take your devices with you.

Even if you're only going to be away for a few minutes using the restroom, that's all it takes to plug in a USB drive with pre-programmed sequences running at

1,000 words per minute.

Don’t leave them in your car, or even put them in your trunk. Keep them on your person at all times while you’re on the road. You never know when people could be watching you in the parking lot from a distance.

## 6. Lock Your Doors

Working remotely puts corporate information at risk. Always lock the door to your home and to your office to prevent someone from being able to come in and steal your computer.

In highly regulated industries, losing certain data could result in massive fines. Keeping the data encrypted, in many states, ensures disclosure laws don’t come into effect if the information is ever compromised.

## 7. Only Use Flash Drives You’re Familiar With

Many people aren’t aware of this classic hacking method. Hacks will drop a large number of flash drives near the company they want to attack.

They are hoping an employee will pick up one of the drives and use it.

When tested anecdotally at another company, it was found that a high percentage of people actually opened the files on the drive. For hackers, that’s the jackpot.

Do not use a flash drive if you’re not sure where it came from. Do not continue to use the one you’ve got plugged into your system if you cannot vouch for its safety.

## 8. Use a USB Data Blocker

If you’re travelling for work and the only option is to charge your phone at a public station, you don’t know the USB port and could put all the data on your phone at risk.

To solve this issue, you use a USB data blocker to protect against malware while also preventing data exchange.

This device allows your phone to connect to power but doesn't expose the data pins inside your device.

## 9. Implement Multi-Factor Authentication and Single Sign-On

Based on information from TechRepublic, without multi-factor authentication (MFA) and single sign-on (SSO), employees may have to remember as many as 85 different passwords, and while password management tools help, there's still the issue of knowing the employee is who they say they are.

MFA is a feature that requires users to authenticate their identity another way before resetting a password, or when logging in for the first time via an unrecognized device.

This may be with a phone call that provides a code like Google, via email with a link to click, or via a mobile app where you're also signed in, like Facebook's Code Generator.

SSO is a feature that allows your team to use a single set of credentials to sign into multiple platforms across the company. That's why it's also important to implement MFA alongside SSO.

Implementing SSO for cloud services and web apps allows your IT team to track and manage access control from a remote location.

If employees leave the company or are terminated from their position, IT can change that single password so that former employees do not have access anymore.

> *Using good technology and policies does help, but it's the employees who make the business work that is a primary avenue of risk. That's why it's so important to educate them.*

PLANERGY offers the option to use SSO as part of its software for better procurement cybersecurity, to help IT better authenticate remote workers.

# Creating Formal Remote Work Policies

CISOs and IT managers can easily implement and enforce these security strategies with technical and administrative controls.

Once you outline the policies you expect your team to follow, have a meeting to train them on the policies, and give them a chance to ask questions.

Work this security awareness training into your new hire onboarding process, and host them any time your company updates its security policies.

Even when the COVID-19 pandemic is under control and remote employees can return to the office, data privacy and security must remain a priority in your business. Phishing attacks and scams are rampant cybersecurity risks that won't disappear any time soon.

# What's your goal today?

## 1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

## 2. Download our guide "Preparing Your AP Department For The Future"

Download a free copy of our guide to future proofing your accounts payable department. You'll also be subscribed to our email newsletter and notified about

new articles or if have something interesting to share.

download a free copy of our guide

### 3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

## Related Posts