Don’t forget home office security: A guide to keeping remote workers safe and secure

DIGITAL ORCHARD I.T

If you could bundle an office worker from the year 2003 into a time machine and bring them to the present day, they wouldn't believe how different things are.

And not just how much better the tech is. Our work environment has changed just as much.

The traditional office has undergone a radical transformation. For many of us, we no longer have to suffer the daily commute, the stress of making it on time when traffic's bad, and the constant interruptions from people passing your desk.

Today, your office can be the kitchen table, the local coffee shop, or even a hammock in your garden (weather permitting).

Sounds idyllic, doesn't it?

But hold on a moment. There's a catch.

Whilst this newfound freedom and flexibility has undeniably boosted productivity, employee engagement, and retention rates, it has also thrown open a Pandora's box of security concerns.

Just picture this: You're sitting in your home office (or maybe on your sofa), sipping your morning coffee, and working on that important project when suddenly – something is seriously wrong.

It takes a little while for you to realise you're the victim of an unfolding cyber attack.

Your device is compromised, your business's data stolen, and your cup of coffee is not so comforting anymore.

Working in your pyjamas might be a dream come true. But keeping your business data and devices secure? That's a serious business.

From understanding the risks, to implementing robust security measures, this guide will arm you with everything you need to know to create an impenetrable home office fortress for you and your team. Because working from home might mean you can avoid office politics, but it doesn't mean you can ignore cyber criminals.

There's a lot to cover. We've broken it down to make it super simple for you.

The risks

According to the Future of Cyber 2023 report by Deloitte, a staggering 95% of cyber security events are caused by human error. That's right, in most cases, we are our own worst enemy.

Imagine the potential pitfalls when your workforce is scattered across multiple locations, each with their unique security challenges. Have you got that sick feeling in the pit of your stomach yet?

Working from home presents a playground for cyber criminals. Why?

When you're in an office environment, you're protected by layers of protection, including corporate-grade firewalls and security protocols. But at home? You're often reliant on the family Wi-Fi network that's shared with lots of other people, some of whom have really bad security practices (do your teenagers use a different randomly generated password for every app they sign up to???)

The result? An open invitation to cyber criminals far and wide.

And it's not just about your network security. Your teams could be using their personal devices for work, devices that might not have the same level of protection as company-issued hardware.

Add to that the fact that important business data is now being accessed, stored, and transferred outside of your secure office environment... and you've got yourself a ticking time bomb.

Believe it or not, all it takes to compromise your entire business is:

- One easily guessed password reused across multiple sites
- One unsuspecting click on a phishing email
- One unsecured Wi-Fi connection

Sounds terrifying, doesn't it? But don't worry, all is not lost. With the right measures, you can mitigate these risks and protect your business. Ready or not, you need to take action.

The essentials

Remember your grandma used to say, "safety first"? Well, it's not just for crossing the road – it applies to your home office too. And the best place to start is at the beginning. That means you need to get those basic security measures completed before anything else.

You probably already do all of these in your office, but it's essential you implement them in your employees' home offices too if you want robust security.

Strong passwords

You wouldn't use "123456" as your building's alarm code. So, don't use it as your digital key either. Encourage your remote workers to use complex, unique passwords for all their accounts. A good password should be a combination of letters, numbers, and special characters.

Pro tip: For a higher level of protection, consider using a trusted password manager to generate random passwords for each application or site, and remember them for you.

Multi-factor authentication (MFA)

Imagine having two or more locks on your office door instead of one. That's what MFA does for your accounts. It adds an extra layer of protection by requiring two or more verification methods. That could be something you know (your password) and something you have (like a code sent to your phone). You can even add biometric factors, such as your fingerprint or Face ID.

Update

Outdated software and operating systems are like open windows in your fortress. They provide easy entry points for cyber criminals.

Make sure your remote workers regularly update their devices and enable automatic updates where possible. You may even want to make it a policy, with serious repercussions if an update isn't installed in good time.

Wi-Fi key

Make sure every Wi-Fi network is protected with a strong password, also known as a "Wi-Fi key." If your router came with a default password, change it ASAP. You wouldn't leave your front door key under the welcome mat, right?

Pro tip: Consider naming your network something that doesn't scream "This is my house!" An obscure name like "BananaStand867" is much better than "SmithFamilyHome."

Educate and empower

Knowledge is power, and in the realm of cyber security, it's your most potent weapon. Educate your remote workers about phishing emails, suspicious links, and the dangers of downloading attachments from unknown sources.

Pro tip: Consider organising regular cyber security training sessions for your entire team. It's an investment that pays off ten-fold in the long run. We can help with this.

Backup

A wise man once said, "hope for the best, but prepare for the worst". Regularly back up all data with an automated service that stores data in the cloud. This way, even if you suffer data loss or a breach, your data will be safe.

Secure video conferencing

In the age of virtual meetings, don't forget to secure your video meetings. Use password protection and meeting IDs wisely and avoid sharing sensitive information during public video conferences.

Advanced security

Covered the basics? Good. But we're not there yet.

Now, it's time to climb the security ladder and delve into some more advanced strategies that will add yet another layer of protection for your data, at your team's homes.

VPN

A Virtual Private Network (VPN) is like an invisibility cloak. Provide a reputable VPN service to all your employees to encrypt their internet connection. It's a secure link between their home and the office, that's almost impossible to peer into. This ensures that sensitive data stays safe from prying eyes.

Pro tip: Don't be tempted to use a free VPN service - you get what you pay for. And choose a VPN provider that doesn't keep logs of your online activities.

Security on each device

Every device that's used to access business data should be protected against malware, ransomware, and other cyber threats. Invest in reliable software and what's known as endpoint detection and response (EDR) tools (an endpoint is a device).

Pro tip: Keep these defences up-to-date and regularly scan your devices for hidden threats. Think of it as a digital health check-up for your equipment.

Secure file sharing and collaboration

We've come to rely on file sharing and collaboration tools in recent years. We'd struggle without them. But check your software offers end-to-end encryption and robust access controls. This makes sure that only people with the proper credentials can access your documents.

Intrusion Detection and Prevention Systems

An Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) monitor network traffic for signs of suspicious activity and can automatically respond to threats.

Employee training

Education has already been mentioned (well spotted). But continued education is key in the ever-evolving realm of cyber security. Regularly update your remote workers on the latest threats and tactics. Knowledgeable and aware employees are your best defence… combine that with software to help protect them, and this is best practice.

Pro tip: Consider conducting simulated phishing exercises to test your team's readiness.

Incident response plan

You will never be 100% protected from threats. Prepare for the worst by creating an incident response plan. This blueprint outlines how to react when a security breach occurs. Remember, swift action can save your business a lot of time, money, and stress. For remote workers, plan how you can properly support them if they have no access to their devices.

Third-party risk management

Your security chain is only as strong as its weakest link. Assess the security practices of vendors and third-party partners who have access to your data. Make sure they are as committed to security as you are.

Data encryption

Encryption conceals your messages from prying eyes. Enforce the use of end-to-end encryption for communication tools like email and messaging apps. This way, even if your messages are intercepted, they remain indecipherable.

Anything else?

One thing it's important to realise is that the world of cyber security is in a constant state of flux. To stay ahead of the game and safeguard your remote workers and business data, you must embrace the principles of continuous monitoring and adaptation.

Real-time threat detection

Imagine having a security guard that scans the horizon for incoming threats 24/7. Real-time threat detection systems do this in the digital world. They monitor network traffic, looking for unusual patterns and known attack signatures. When danger is detected, they raise the alarm.

Security Information and Event Management (SIEM)

SIEM tools collect and analyse data from various sources, providing a complete view of your security posture. By identifying trends and anomalies, SIEM helps you uncover hidden threats and vulnerabilities.

Pro tip: Consider partnering with a trusted IT support provider to implement and manage your SIEM solution. We not only bring the expertise needed to interpret the SIEM data effectively, but we can implement and monitor all the other security solutions mentioned in this guide too.

Threat intelligence

Threat intelligence provides information on emerging threats and tactics used by cyber criminals. Subscribe to threat intelligence feeds and services to stay ahead of the curve.

Security audits and penetration testing

Regular security audits and penetration testing simulate cyber attacks to expose any vulnerabilities within your network. This helps you find and patch weak points before the enemy can take advantage.

Security patch management

Vulnerabilities are the chinks in your armour. Keep your software, operating systems, and applications up to date with the latest security patches. Cyber villains often exploit known vulnerabilities, so timely patching is crucial.

Incident response refinement

Your incident response plan should evolve with your business's needs. After every security incident, conduct a post-mortem analysis. Learn from the past and refine your response strategy to be more efficient and effective.

Employee training

Remember the earlier advice on employee training? It still applies here. Cyber security education should be an ongoing effort. After all, a well-trained team is your strongest defence. Training can be done online meaning everyone can access it.

Compliance and regulation

Stay informed about cyber security regulations and compliance standards applicable to your industry. Ensure your remote workers adhere to these guidelines, as non-compliance can lead to hefty penalties.

And there you have it – the essential guide to keeping your remote workers and home office secure. We've covered a lot of ground, from strong passwords to advanced security strategies, and the need for continuous vigilance in this ever-evolving digital landscape.

Don't forget, you're not in this alone. We can help you bring your security up to scratch for your remote workers as well as your office-based systems.

Whether you're wrestling with a new threat or just looking for advice, we'd be happy to help.

Get in touch.

CALL: 0131 500 0310
WEBSITE: www.digitalorchardit.co.uk

DIGITAL ORCHARD I.T