PiSYS .net

A COMCEN COMPANY

Mastering Home Office Security: Shielding Remote Workers with Cyber Safety

We make IT easy

Stepping into the modern workplace, your can't help but marvel at the transformation it has undergone. This shift extends far beyond technological advancements; it encompasses a fundamental evolution in our work environment.

The conventional office is no longer the exclusive hub of productivity. The era of enduring daily commutes, battling traffic and wrestling with desk-side distractions has faded into history. Nowadays, your workspace knows no bounds – it could be your tranquil library nook, the vibrant rooftop garden, or even the sun-drenched park bench just around the corner.

It all sounds remarkably idyllic, doesn't it? However, there's a twist in this tale.

Amidst the freedom and flexibility, which have undeniably boosted productivity, employee engagement and retention, a new set of security concerns has emerged.

Imagine this: You're comfortably stationed in your home office, or maybe you're nestled in your reading nook, enjoying a steaming cup of morning coffee while diligently tackling an essential project. Suddenly, a sense of unease washes over you.

It takes a moment to grasp the severity of the situation - you're under attack by cybercriminals. Your device is compromised and your business data exposed.

Though the allure of working in comfort is undeniable, safeguarding your business data and devices becomes a vital mission. This is precisely where we step in.

Our guide is your map through the labyrinth of home office security. It's your shield against the perils of remote work, ensuring cyber safety for you and your team. Because working from home might free you from office politics, but it also opens the door to relentless cyber threats.

In this guide, we demystify the complexities of security, providing step-by-step insights to fortify your digital sanctuary.

Safety begins at home, and we're here to make sure your digital home office is nothing short of impregnable.

'Mastering Home Office Security.' It's your first step towards securing the future of remote work.

Cyber Security Risks in the Home Office

In the ever-evolving landscape of the digital age, the landscape is fraught with challenges. According to Deloitte's 2023 Future of Cyber report, a staggering 95% of cyber security incidents stem from human error. Yes, you read that correctly, we often become our own worst adversaries.

Now, picture a scenario where your workforce is dispersed across diverse locations, each with its own unique security intricacies. **Can you feel that nagging unease in the pit of your stomach?**

Working from home opens the door to a cyber playground cyber criminals. Why? Well, in an office setting, you benefit from layers of protection, including robust corporate firewalls and stringent security protocols. But at home, you might find yourself sharing the Wi-Fi network with various household members, some of whom may not prioritise the best security practices. (Ever wonder if your teenagers employ different, randomly generated passwords for each app they sign up for?)

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

And it doesn't stop at network security. Your teams might be using personal devices for work, devices that may not match the level of protection of company-issued hardware.

Furthermore, vital business data is now traversing the digital realm beyond the secure office perimeter, like a ticking time bomb.

It's astounding how just a few vulnerabilities can jeopardise your entire business:

- One easily guessable password reused across multiple platforms
- One click on a phishing email
- One unsecured Wi-Fi connection

It may seem daunting, but fear not. With the right safeguards in place, you can neutralise these risks and fortify your business. The time for action has come, and your business's digital defense begins now.

Vital Security Fundamentals

Recall those wise words from your elementary school teacher, **"Preparation is key"**? Well, it's not just about studying for a test; it's crucial for your home office as well. The foundation of a secure digital workspace lies in the basics. This implies tackling essential security measures before anything else.

These are steps you likely follow diligently in your traditional office setting, but it's paramount to extend the same rigor to your employees' home workspaces. To ensure unwavering security, these fundamentals are non-negotiable.

Strong passwords

You wouldn't use "123456" as your building's alarm code. Encourage your remote workers to use complex, unique passwords, use random sentences such as 'eggs@thefarm86p!'. 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) with Pisys Security Defaults

Enhance Online Security: MFA, is adding multiple locks on your digital door, using two or more verification methods (e.g., password and a code sent to your phone). For extra defense, integrate biometrics like fingerprint or Face ID. Pisys automates fundamental security settings for all 365 tenants, including multi-factor authentication, blocking legacy protocols and protecting privileged accounts.

Update

Outdated software and operating systems act as vulnerabilities in your digital infrastructure, granting cyber criminals easy access. Pisys employs remote software management, ensuring your remote workforce's devices remain up to date. Employees are granted a reasonable window for manual updates, after which automatic updates take charge, offering a robust shield against vulnerabilities.

Wi-Fi key

Ensure your home office stays secure with our top tips! Safeguard your Wi-Fi network by setting a robust password, your virtual "Wi-Fi key." Don't risk using default passwords; change them now. Treat it like hiding your house key - no one leaves it under the welcome mat!

Pro tip: Opt for a discreet network name, like "BananaStand867," over revealing ones such as "SmithFamilyHome." Prioritise your home office security with Pisys.

Educate and empower

Empower your remote workforce with the ultimate defense – knowledge. In the cyber security arena, awareness is your strongest asset. Educate your team on recognising phishing emails, avoiding suspicious links, and steering clear of unknown attachments.

Pro tip: Unlock the full potential of your team's security with regular cyber security training sessions. It's an investment that yields substantial returns. Let Pisys eCampus be your partner in fortifying your employee home offices against potential threats.

Backup

Protect your home office with a crucial strategy – backup. Embrace the wisdom of preparing for the unexpected by routinely safeguarding your data through our automated cloud storage service. In the face of data loss or breaches, rest easy knowing your valuable information remains secure. Pisys is your ally in fortifying your employees home office security.

Secure video conferencing

Elevate your virtual meetings with Pisys home office security expertise. Safeguard your video conferences by employing strong password protection and judicious use of meeting IDs. Keep sensitive information secure during public meetings.

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

Empower your remote workforce with the virtual invisibility cloak – a robust Virtual Private Network (VPN). Pisys recommends a reputable VPN service to encrypt your team's internet connection, creating a secure link between home and office, guarding sensitive data against prying eyes.

Pro tip: Remember, quality matters; avoid free VPNs and opt for a provider committed to your privacy without logging your online activities. Secure your home office with Pisys for unparalleled VPN solutions.

Security on each device

Ensure a fortress of security on every device accessing your business data. Safeguard against malware, ransomware and other cyber threats with robust software and endpoint detection and response (EDR) tools. Trust Pisys to fortify your devices.

Pro tip: Maintain up-to-date defenses and conduct regular scans for hidden threats - an essential digital health check-up for your equipment. Prioritise home office security with Pisys expertise.

Secure file sharing and collaboration

Experience seamless and secure file sharing and collaboration with Pisys. As essential tools in the modern workspace, ensure your software provides end-to-end encryption and robust access controls. Trust us to safeguard your documents, allowing access only to those with proper credentials. Elevate your home office security with Pisys expertise.

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

Pisys understands the importance of ongoing education for remote workers. Access our Pisys eCampus for FREE Training covering Cyber Security, Microsoft 365 and more, including topics like Well-being and Leadership. In the dynamic landscape of cyber threats, well-informed employees are your first line of defense.

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

Incident response plan

Shield your business with Pisys's comprehensive incident response plan. While 100% protection is elusive, preparation is key. Our blueprint guides your swift reaction to security breaches, saving time, money and stress. Tailored for remote workers, it ensures proper support even when they face device access challenges. Plan for resilience with Pisys, your partner in proactive home office security.

Third-party risk management

Pisys emphasises third-party risk management for robust home office security. Strengthen your security chain by evaluating the practices of vendors and partners with data access. Ensure their commitment to security aligns with yours, fortifying your digital defenses comprehensively. Trust Pisys to safeguard your home office ecosystem.

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 detection

Elevate your home office security with Pisys's real-time threat detection, akin to having a vigilant digital security guard. Our onsite SOC Security Operations Centre, coupled with our Datto Platinum Partnership, monitors network traffic for anomalies and known attack signatures, promptly alerting you to potential dangers. Trust Pisys for unparalleled threat monitoring.

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: Partner with us to implement and manage your SIEM solution. Beyond interpreting SIEM data, trust Pisys for seamless implementation and monitoring of all mentioned security solutions, ensuring robust protection for your digital workspace.

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

Strengthen your home office security with Pisys expertise in security audits and penetration testing. Our site surveys can reveal network vulnerabilities, allowing proactive patching of weak points before potential threats exploit them.

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

Pisys recommends a continuous evolution of your incident response plan to meet your business needs. Post-security incident, conduct a thorough analysis, learning from the past to refine and enhance your response strategy for greater efficiency and effectiveness. Speak to Pisys for proactive incident response solutions.

Employee training

Don't forget the crucial aspect of employee training in home office security, echoing our earlier advice. Cybersecurity education remains an ongoing effort because a well-trained team is your strongest defense. Accessible online training ensures everyone can participate. Rely on Pisys eCampus for comprehensive training solutions.

Compliance and regulation

Pisys encourages staying informed on cyber security regulations and industry compliance standards. Ensure your remote workers adhere to these guidelines, as non-compliance may result in substantial penalties. Contact Pisys for comprehensive compliance information.

Explore the comprehensive guide to fortifying your remote workers and home office security. From robust passwords to advanced strategies, we've covered it all.

Pisys stands with you, offering support for both remote and office systems. Whether facing threats or seeking advice, reach out – we're here to help.

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

Get in touch.

CALL: 01792 464748
EMAIL: hello@pisys.net
WEBSITE: www.pisys.net

PISYS .net
A COMCEN COMPANY