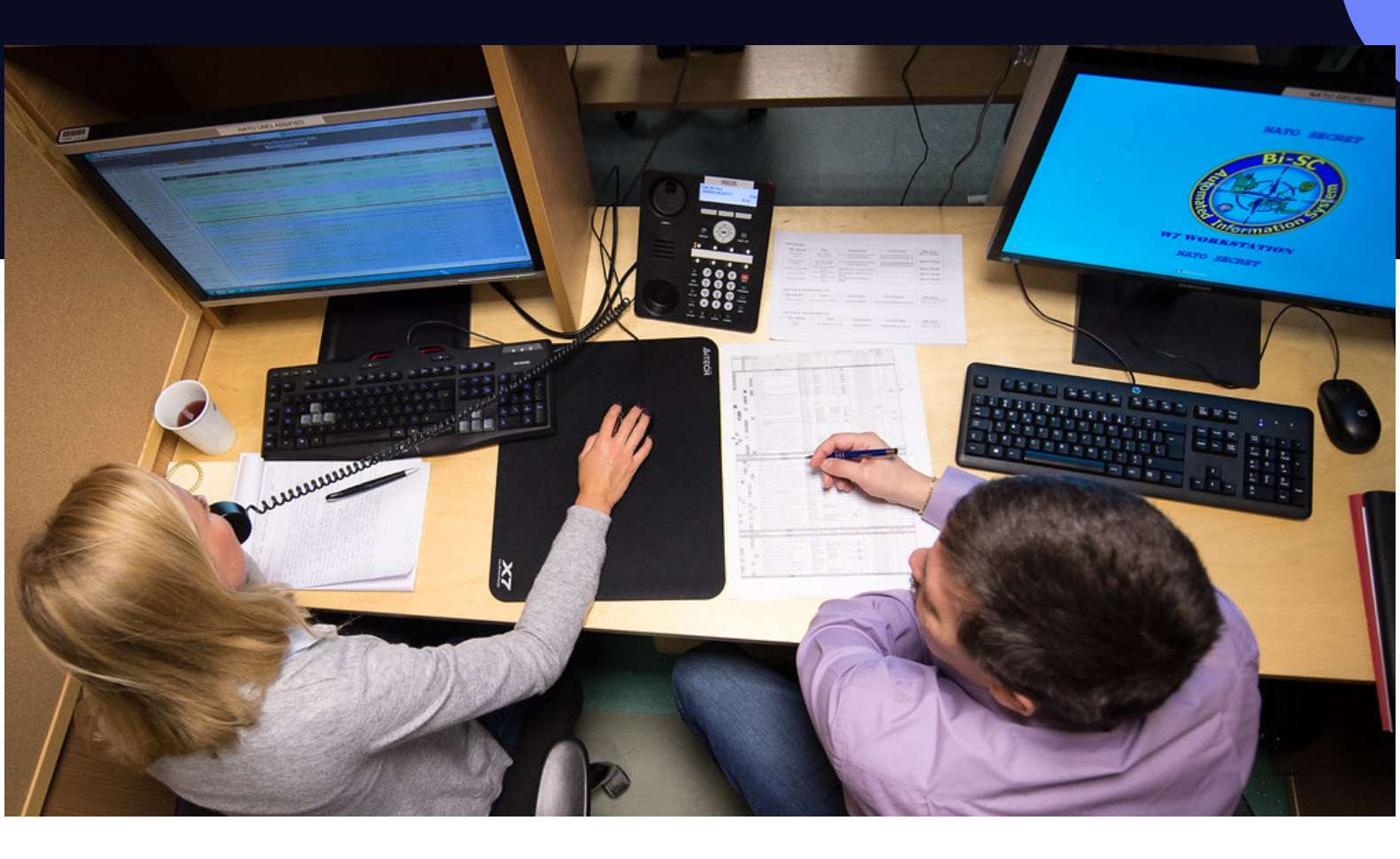
Online Privacy: Guide for Securing Your Remote Work Environment from Cyber Threats



Working Remotely

A staggering **43%** of cyber-attacks are now aimed at small businesses, and **64%** of companies have experienced web-based attacks, as per a recent report by Cybint.
In line with this, Microsys., a leading Canadian tech solution company, is committed to empowering businesses by offering state-of-the-art IT solutions. With a robust understanding of contemporary cyber threats and how they evolve, Microsys. safeguards organizations by streamlining their cyber security infrastructure.

This issue of our newsletter is dedicated to helping you understand the significance of online privacy, the nature of cyber threats targeting remote environments, and various strategic measures to secure your digital ecosystem. With this knowledge, you'll be better prepared to steer your enterprise towards safer digital pathways.

Understanding Cyber Threats in Remote Work

Remote work has many advantages, including flexibility and cost savings. However, it also presents unique challenges in terms of cybersecurity. **Gartner's analysis** indicates that by the end of 2024, nearly half of global companies will have retained a significant remote workforce, thus spotlighting remote work cyber threats.

Exploring the world of cyber threats, we find that they majorly affect remote workers through phishing attacks, ransomware, and unsecured Wi-Fi connections.

Phishing attacks:t

Cybersecurity Ventures predicts that in 2021, businesses will fall victim to a phishing attack every 11 seconds, resulting in $6 trillion annually by the end of the year. Phishing attacks continue to be a favorite tool for cybercriminals to exploit remote workers, who might not have the same level of security infrastructure as they would in a traditional office environment.

Ransomware:

Ransomware is another growing threat in the cyber world. According to PurpleSec's report, a ransomware attack will occur every 14 seconds. It's a type of malicious attack where the attacker encrypts a victim's data and then demands a ransom to restore access.

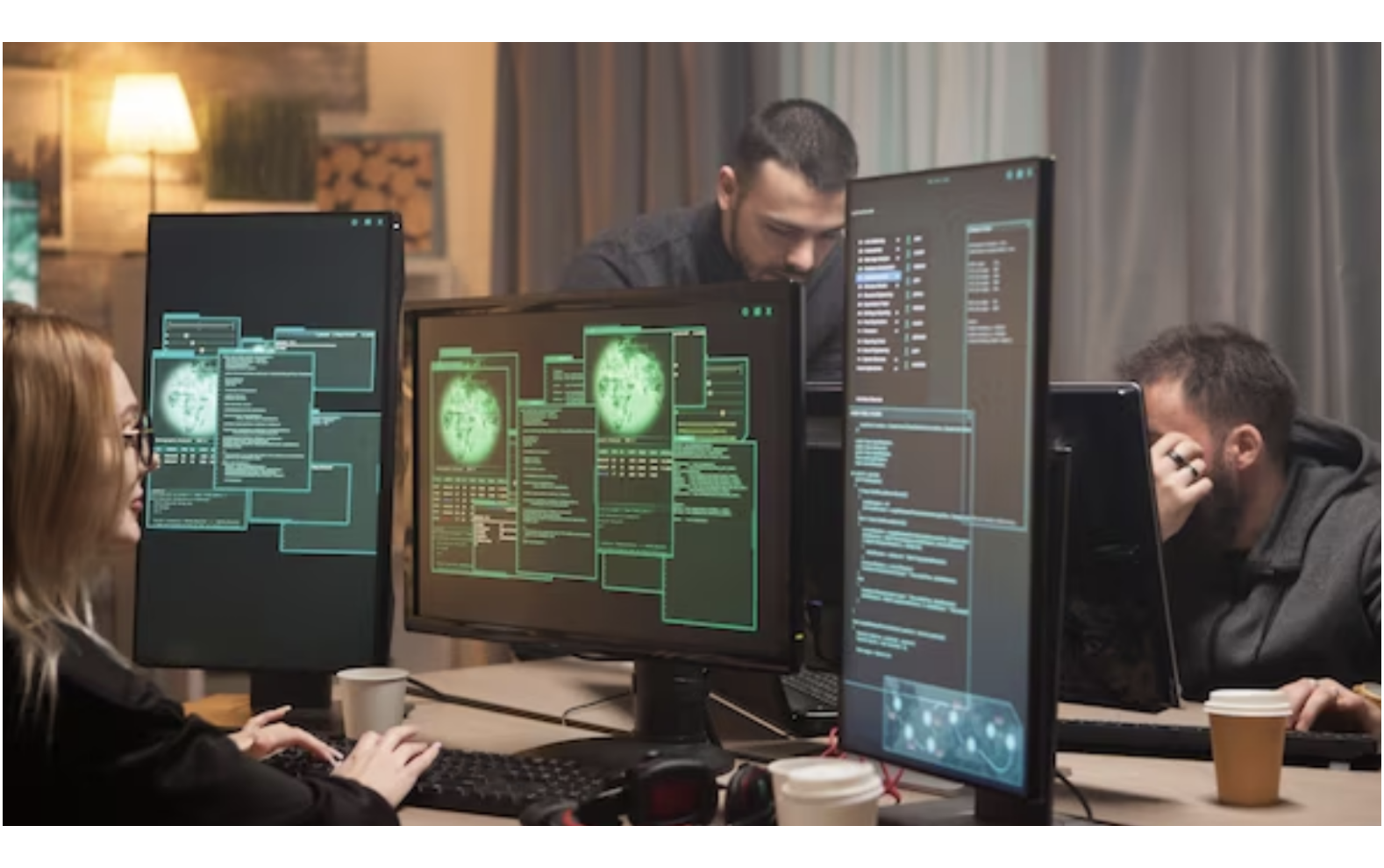
Unsecured Wi-Fi connections:

Remote workers often connect through unsecured public Wi-Fi networks, significantly increasing the risk of cyber-attacks. A study by Symantec revealed that 87% of users have potentially put information at risk while using public Wi-Fi.

In one real-world example, a global software provider, TeamViewer, became a victim of a large-scale cyber-attack in 2016. The attackers targeted remote workers through fake emails and infected their devices with malware to gain unauthorized access to sensitive company information.

Building a Secure Foundation

Before dwelling on advanced protection measures, it is essential to establish a sturdy cyber security foundation. Recognize the fact that data breaches caused by human errors account for nearly **24%** of all breaches, according to the Office of the Australian Information Commission, warranting a strong emphasis on cyber security policies and employee training.



Cybersecurity Policy

A well-formed cyber security policy outlines how an organization must respond during a security breach, providing clear guidelines on access controls, managing customer data, and incident response processes

Employee Training and Awareness

Cyber security training is an effective deterrent against cyber threats. A report by **Proofpoint** suggests **22%** of organizations experienced a successful phishing attack in 2022. Addressing this, continuous security awareness training can play a crucial role in helping employees identify and react appropriately to phishing emails. It also gives employees an understanding of **password best practices**, a key aspect considering weak or compromised passwords account for **81%** of hacking-related breaches.

Secure Tools

It's critical to use secure tools for communication and collaboration. Leverage tools certified by **SOC2 Type II,** an internationally recognized security standard. Microsys.'s IT Infrastructure and Support services offer secure and reliable digital solutions to facilitate streamlined workflow.

Implementing Advanced Security Measures

When a robust foundation is in place, it's prudent to combine it with advanced security measures. Ponemon's Cost of Cyber Crime Study indicates that businesses that use security technologies were able to reduce the cost of a cyber-attack by an average of **27%.**

Cybersecurity Solutions

Microsys. provides Cyber Security services harnessing the latest tech advancements along with Cyber Security Training Modules, Network Infrastructure Security, Data Storage & Recovery services. Use these solutions to amplify your defense against cyber threats.

Two-Factor Authentication and VPNs

Two-factor authentication (2FA) adds an extra layer of security for user accounts beyond just passwords. According to **Symantec**, implementing 2FA can prevent **80%** of data breaches. VPNs, on the other hand, allow remote workers to securely connect to the organization's network, even over public Wi-Fi. Juniper Research shows that remote workers using VPNs can reduce the risk of cyber-attacks by **75%.**

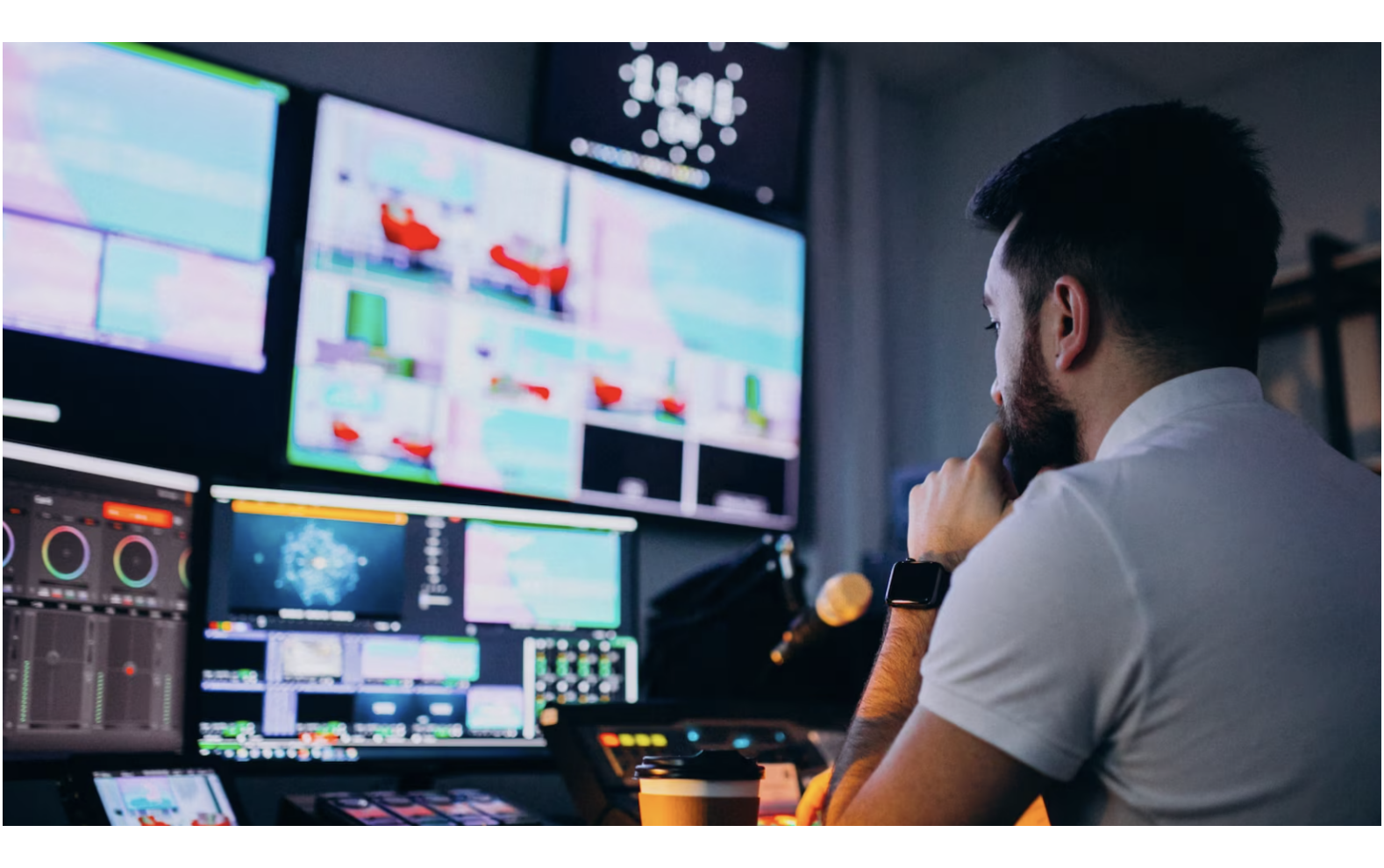
Mobile Device Management

As per the iPass Mobile Security Report, **94%** of IT professionals think that mobile work is a significant security risk. Thus, Mobile device management (MDM) plays a critical role in securing company data, especially when employees are using personal devices for work.

Dickering cyber threats require advanced security measures. The combination of sophisticated cybersecurity solutions offered by Microsys., prudent use of security-enhancing tools like 2FA and VPNs, regular updating practices, and efficient mobile device management can fortify your remote work environment against the most potent cyber threats.

Continuously Monitoring and Responding to Threats

Merely implementing security measures isn't enough; organizations must be relentless in monitoring and responding to cyber threats. To mitigate these risks, continuous monitoring and threat detection become indispensable.



Continuous Monitoring and Threat Detection

Microsys.'s 24/7 support services, along with their remote monitoring services, provide organizations with timely alerts and insights into potential vulnerabilities. In fact, a **Forrester report s**tates that AI-driven monitoring solutions can help identify and respond to security incidents **60%** faster.

Incident Response Plan

Having an incident response plan in place helps businesses contain the impact of a cyber-attack. CrowdStrike's **2020 Global Security Attitude Survey** shows that companies with an up-to-date incident response plan report **39%** less downtime following a cyber-attack.

Regular Security Audits and Assessments

Proactive security audits and assessments enable the identification and remediation of vulnerabilities. A Symantec study found that organizations that conducted regular security assessments witnessed a 48% improvement in their security posture.

Microsoft Office 365 and Security

Microsoft Office 365 is a top choice for businesses due to its comprehensive suite of productivity tools. It also boasts robust security features to protect businesses from cyber threats. According to a recent Microsoft survey, companies adopting Office 365 have experienced a 36% increase in their security stature.

Microsoft Office 365 Security Features: Some notable security features in the Office 365 suite include:

- **Advanced Threat Protection (ATP):** ATP effectively detects, prevents, and responds to zero-day threats, ransomware, and phishing attacks.
- **Data Loss Prevention (DLP):** DLP helps organizations comply with data protection regulations, significantly reducing potential data breach financial repercussions.
- **Secure Score:** Office 365 offers a built-in security dashboard called Secure Score. It provides recommendations and insights to help organizations understand and improve their security policies. According to Microsoft, customers with higher Secure Scores experienced 63% fewer breaches than those with lower scores.

Microsys. and Microsoft Office 365

Microsys. has the expertise and resources to consult businesses on the implementation and optimization of Microsoft Office 365, ensuring that you benefit from the suite's top-notch security provisions.

By appreciating the essence of ongoing monitoring and efficient response strategies, as well as integrating powerful, secure tools like Microsoft Office 365 into their workflows, businesses can significantly enhance their defense against evolving cyber threats.

The Human Factor - Your Last Line of Defense

As organizations strengthen their cyber security practices and deploy sophisticated technologies, one crucial aspect remains – the human factor.

Simulated Phishing Exercises

Conducting simulated phishing exercises to test employees' vigilance and awareness is a powerful way to gauge the organization's vulnerability to phishing attacks. As per a **KnowBe4 study**, after participating in a phishing simulation, **85%** of employees exhibited a higher degree of attentiveness to phishing emails.

Regular Refresher Seminars

Organizing regular refresher seminars on cyber security can boost employees' ability to recognize and respond suitably to new threats. A study conducted by the University of Texas at San Antonio posits that employee vigilance can be maintained through drills and consistent reminders about security policies.

Reward and Incentivize

Encouraging employees to stay vigilant and report incidents by rewarding them with recognition or incentives can significantly enhance the company's overall cyber security posture. The SANS Institute contends that organizations with token rewards for reporting spear-phishing attempts have shown an 86% reduction in susceptibility to such attacks.

Conclusion

Embracing online privacy and robust cyber security measures is no longer optional but imperative for organizations navigating the complex and evolving digital landscape. Remember, standing tall in the face of a challenge isn't about invincibility; it lies in enveloping oneself with the strongest armor. Simultaneously, it's about retaining the agility to adapt and evolve as the challenge changes its course.

At Microsys., we firmly believe that cybersecurity isn't just a destination—it's a journey. A journey of commitment, vigilance, and steady progress. Let's embark on this journey together, paving the way not only for a secure digital environment but also for trust and confidence that empowers you to shine in an ever-more digital world.

Click here to contact us