waystone | Compliance Solutions

Cyber Security Awareness for Businesses and Employees: Best Practices and Common Pitfalls

Mohammad Momani January 15, 2025

In today's digital world, cyber security is more than just an IT issue, it's a business-critical concern.

Cyberattacks can lead to financial losses, reputational damage, regulatory and legal consequences. As cybercriminals become more sophisticated, businesses of all sizes need to take proactive steps to protect their data, systems and customers.

A recent statistic shows that nearly 60%[1] of small businesses close within six months of a cyberattack, emphasizing that cyber security is essential for long-term business success. Below, we highlight some of the most common cyber security mistakes businesses make and how to avoid them.

Common Cyber Security Issues That Can Be Prevented

Phishing Attacks

Phishing remains one of the most common and damaging cybersecurity threats. Cybercriminals often send fraudulent emails or messages that appear to come from trusted sources, tricking employees into disclosing confidential information.

Prevention tip: Educate employees on how to spot phishing attempts, such as checking for suspicious sender addresses or spelling errors. Encourage them to avoid clicking on links or downloading attachments from unknown sources, and to verify any suspicious messages with your IT team. Testing employees on a quarterly basis is an effective way to reinforce awareness and encourage continuous learning.

Weak Passwords

Weak or reused passwords are a major vulnerability. Cybercriminals use simple techniques to guess passwords and gain unauthorised access to sensitive systems.

Prevention tip: Set clear policies requiring employees to use strong, unique passwords for every system. Encourage the use of password managers and ensure that systems are protected with two-step verification to add an extra layer of security.

Lack of Software Updates

Outdated software can have vulnerabilities that cybercriminals easily exploit. Many cyberattacks target unpatched systems, putting businesses at risk.

Prevention tip:Automate software updates and encourage employees to regularly update their devices. Regularly review and patch any security flaws in operating systems and applications to stay ahead of threats.

Unprotected Networks

Using public Wi-Fi networks without protection is a common mistake. Cybercriminals can easily intercept unencrypted data, compromising sensitive information.

Prevention tip: Advise employees to avoid accessing company data on public Wi-Fi networks. Encourage the use of mobile hotspots or personal data connections when working remotely. Remind employees of the risks associated with unprotected networks and ensure secure, trusted connections for all work-related tasks.

Insufficient Data Backup

Data loss can occur for various reasons, including cyberattacks like ransomware or hardware failure. Without secure, regular backups, businesses risk losing critical data.

Prevention tip: Implement regular, automated backups for all important data. Store backups securely (preferably offsite or in a secure cloud environment) and regularly test your restoration procedures to ensure they work effectively.

Employee Negligence

Sometimes, the biggest security threat comes from within the organisation. Employees may unknowingly compromise security through careless behaviour, such as using unsecured devices or sharing sensitive information through unencrypted channels.

Prevention tip: Regularly train employees on the risks of negligent behaviour and best practices for protecting data. Establish clear policies for device use, communication methods and data handling to promote a security-conscious culture.

Best Practices for Improving Cyber Security

Building a Cyber Security Culture

Fostering a culture of cyber security awareness throughout your organisation is key. Leaders should lead by example, demonstrating a commitment to protecting sensitive data and security. Encourage employees at all levels to take ownership of their role in safeguarding company assets.

Promote transparency, open communication about potential threats and continuous learning. Cyber security isn't a one-time effort, it's an ongoing process that must evolve alongside new technologies and emerging threats.

Training and Awareness Programs

Continuous training is key to ensuring that employees understand cyber security risks and their role in safeguarding company data. Provide clear guidance on how to identify threats, report incidents and follow proper security protocols.

Multi-Factor Authentication ("MFA")

Protect critical systems by requiring two-step verification (MFA) for all access. This adds an extra layer of security, making it harder for cybercriminals to gain access, even if a password is compromised.

Access Control and Segmentation

Limit access to sensitive information based on employee roles. Implement role-based access controls to ensure that employees only have access to the data they need to do their job.

Incident Response Plan

Prepare for the worst-case scenario by having a clear incident response plan in place. This plan should outline the steps to take in the event of a cyberattack, from containing the attack to notifying stakeholders and recovering data.

Regular Security Audits

Perform routine security audits to identify potential vulnerabilities in your systems. These audits help detect weaknesses before they become problems and ensure that your security measures remain effective.

Secure Third-Party Relationships

Third-party vendors can sometimes introduce cyber security risks. Ensure your vendors follow best security practices and make cyber security a top priority when selecting partners.

Conclusion

Cyber security is essential for safeguarding your business, customers and reputation. As businesses in the UAE and broader financial sectors face increasing cyber threats, adhering to the regulatory frameworks set out by the Dubai Financial Services Authority ("DFSA") and the Financial Services Regulatory Authority ("FSRA") is critical. Both regulators emphasize the importance of implementing robust cyber security measures to protect sensitive data and financial systems.

Taking action today to align with these standards and regulations will not only minimize risks but also ensure the long-term sustainability of your business in a highly regulated and competitive environment.

How Waystone Can Help

Waystone is a leading provider of cyber security consulting and compliance services to the financial services industry. If you would like to find out how Waystone can help you to assess your current cyber security measures, please reach out to your usual Waystone representative, or contact us below.

Contact Us →

[1] According to a report by Ponemon Institute, nearly 60% of small and medium-sized businesses ("SMBs") go out of business within 6 months of a cyberattack. This figure is frequently cited in discussions about the critical need for small businesses to invest in cybersecurity. The reason for the high failure rate is often attributed to the financial impact of cyberattacks, including the costs of recovery, legal consequences, and reputational damage.

The National Cyber Security Alliance ("NCSA"), supports the idea that small businesses are highly vulnerable to cyberattacks and face significant challenges in recovery after an attack. However, this 60% figure can vary depending on the study.