Reducing Workplace Stress

Prioritising mental health and implementing strategies to reduce stress are essential for a safe and productive workplace. Workplace stress and mental health issues can adversely impact employees by compromising safety, reducing productivity and decreasing engagement.

Causes and Impact of Workplace Stress

Several aspects of a job can cause employee stress, such as job security concerns, lack of training, scheduling challenges, job performance concerns and a poor work-life balance. Left unaddressed, employee stress can lead to distractions, reduced attention to detail and delayed reaction times, increasing the risk of workplace accidents. Moreover, workplace stress can lead to several negative emotions among employees, including low mood and fatigue, which can impair judgement and heighten safety risks. Additional negative consequences of workplace stress include inflated employee turnover rates, increased absenteeism and a poor workplace culture.

Fortunately, by taking proactive steps to reduce workplace stress and supporting employees' mental health, employers can improve their employees' well-being and job satisfaction, creating a safer and more productive work environment.

Stress Reduction Tips

Employers can consider the following strategies to reduce work-related stress:

- **Focus on a supportive workplace culture** where employees feel comfortable discussing any issues and seeking help without fear of retaliation.

- **Model healthy work practices** and be aware that employees may also have significant demands outside of work that they are trying to manage.

- **Uphold policies that aim to reduce stress,** including those that prohibit discrimination, harassment and bullying.

- **Promote safe work practices** and monitor the working environment, ensuring employees follow safety guidelines.

- **Provide comprehensive mental health resources,** such as an employee assistance programme with access to mental health services like professional counselling and peer support teams.

- **Establish workplace policies and procedures that create safe and healthy work environments** and ensure employees' schedules allow for adequate break times.

- **Provide comprehensive education and training** with regular mental health education, self-care guidance and stress management sessions. Training should include educating leaders to recognise, discuss and address mental health concerns within their teams.

- **Normalise mental health conversations to** encourage employees to feel more comfortable seeking assistance.

- **Provide clarity and allow flexibility** by ensuring job responsibilities are clear and have room for employees to have a work-life balance, adequate paid leave and access to mental health days.

- **Show empathy** by actively listening to employees and ensuring they know they are valued.

- **Consistently evaluate and adjust programmes** as personnel needs evolve, gathering feedback to ensure that programmes remain effective and accessible.

Reducing work-related stress is essential to individual well-being and operational success. By taking action to promote mental health, employers can make work environments healthier and safer while improving job performance, diminishing stress and mitigating organisational risks.

Contact us today for additional workplace well-being resources.

QR Codes' Cyber-security Risks

Quick response (QR) codes have become popular marketing, sales, payment and customer service tools. However, as the presence of QR codes increases, malicious actors have found ways to exploit them, including using them in phishing attacks and spreading malware. These vulnerabilities can lead to significant financial and reputational damage, and business owners should proactively address this exposure.

QR Codes and Their Risks

QR codes act like barcodes. They are a series of pixels arranged to form a large square that typically directs individuals to website URLs when scanned by a smartphone's camera. QR codes allow customers to access a business's information or leave a review. They can also be used to prompt users to take specific actions, such as making a payment or downloading an app.

Although they can be useful, the nature of QR codes allows cyber-criminals to exploit them. Since legitimate QR codes appear as a random scramble of pixels within a larger square, it can be difficult for users to determine if one is safe or malicious. Examples of how cyber-criminals can exploit QR codes include:

- Putting a counterfeit code over a legitimate one or tampering with a QR code.
- Placing QR codes in high-traffic areas or strategic locations where it might seem connected to a location or object (eg by parking meters) or where curious passersby may scan the malicious code.
- Sending fraudulent QR codes in an email or through a communications app.

Once the fraudulent QR code is scanned, a user may be vulnerable to security issues, including data breaches through QR code phishing—or "quishing"—attacks, uploaded malware on their devices and device hacking.

Mitigating the Risks of QR Codes

As cyber-criminals increase their exploitation of QR codes, business owners should mitigate their exposures by:

- Providing continuous education to employees on the dangers associated with QR codes
- Advising employees not to scan QR codes if they are unsure of their origin or if the QR code appears tampered with or altered
- Double-checking the URL to which the code directs
- Installing security software with content filtering that inspects links and attachments and prohibits access to suspicious items
- Maintaining strict access controls and utilising multifactor authentication systems to add a layer of protection
- Training employees on how to safely use their technology in a bring-your-own-device environment
- Keeping all devices updated and patched and turning off automatic QR code scanning settings
- Reviewing default permissions regarding the sharing of sensitive information
- Reducing the use of QR codes in electronic business communications to disincentivise cyber-criminals from using them to target customers

Businesses electing to use QR codes can also take steps to protect their customers. Strategies to consider include:

- Only using reputable QR code generators
- Customising QR codes with company branding
- Testing the QR code before distribution
- Ensuring the linked website is strongly encrypted and has visible indications of SSL protection

QR codes can be useful tools, but they can be exploited by cyber-criminals to compromise business and customer data, causing significant financial and reputational damage. Through risk reduction strategies, organisations can safeguard their business, employees and customers.

Contact us today for further cyber-security guidance.

Insurance Profile COMMERCIAL

A recent Phishing Threat Trends report from cyber-security firm Egress revealed that QR code payloads contained in phishing emails accounted for 0.8% of attacks in 2021 but rose to 10.8% in April 2024.