



Preventing Tech Support and Internal Help Desk Scams

Cyber-criminals' methods for infiltrating networks and stealing sensitive data are constantly evolving. Among the most deceptive tactics they use are technical support scams and internal IT help desk scams. In tech support scams, attackers pose as representatives from well-known technology companies, claiming they will fix non-existent issues. They may use unsolicited pop-up messages, social media adverts or phishing calls or emails in these fraudulent communications. They then attempt to run a fake "scan" of the computer, finding non-existent issues and claiming they need remote access to remedy them. Once granted, the hackers may install malware, request enrolment in a fake support contract, or demand payment for fraudulent software or services.

In IT help desk scams, cyber-criminals pretend to be internal IT staff, often using urgent language to manipulate employees into granting access to secure networks or sharing confidential information. Tactics commonly include voice phishing (vishing), text message phishing (smishing), fraudulent emails, and fake messages sent via collaboration platforms.

Through both types of scams, cyber-criminals employ social engineering strategies to fool employees, communicating with urgency and utilising technical jargon and scare tactics (eg stating it is a major issue) to pressure employees into divulging sensitive information. When someone believes they're speaking with a legitimate authority figure who is offering help, they may be more likely to comply with requests that compromise security.

The consequences of falling victim to these scams can be severe. Beyond the immediate loss of data or financial assets, organisations may suffer long-term damage to their reputation, face regulatory penalties and experience operational disruptions. Recovery can be costly and time-consuming, especially for organisations without robust incident response plans. Fortunately, raising employee awareness is an effective way to reduce the risk of these attacks. Employees

should be mindful of the following red flags:

- **Unsolicited contact** (eg calls, emails, pop-up messages) from someone claiming to be tech support or IT staff.
- **Credential requests** for passwords, multifactor authentication (MFA) codes or remote access.
- **Urgent language or threats** of consequences if immediate action isn't taken.
- **Anomalous payment requests** through non-conventional methods (eg untraceable gift cards, cryptocurrency, bank transfers, links to enter payment details).

Prevention Strategies

Employers can take several proactive steps to protect their organisations, such as the following:

- **Implement regular cyber-security training** that includes real-world examples of scams and phishing attempts.
- **Establish clear protocols** for IT support communications, including verification steps.
- **Use MFA** to add a layer of security.
- **Limit administrative privileges** to reduce the potential impact of a compromised account.
- **Foster a culture of cyber-security** where employees feel comfortable questioning suspicious requests, even if they appear to come from internal sources.

In addition, businesses should maintain up-to-date security software, monitor network activity for unusual behaviour and have a response plan in place in case of a breach.

Contact us today for additional cyber-security resources.

Preparing Commercial Properties for Autumn and Winter

As the cooler months approach, proactive maintenance of commercial properties becomes a top priority for organisations. Autumn and winter can present numerous seasonal risks, including wet leaves, icy walkways, heating system failures and frozen pipes. Such risks can compromise occupant safety, disrupt day-to-day operations and potentially lead to costly liability claims from slips, trips and falls.

To mitigate these risks, building managers should implement a robust maintenance plan that addresses both safety and operational resilience. Consider these maintenance tips for autumn and winter:

- **Service heating systems.** Before temperatures drop, arrange for boilers, radiators, and HVAC systems to be professionally inspected. This helps prevent breakdowns during cold spells and ensures a comfortable environment for occupants.
- **Clear gutters and drains.** Gutters can quickly become clogged with leaves and debris, potentially leading to water ingress and damp. Regular cleaning ensures proper drainage and helps avoid costly repairs.
- **Insulate exposed pipes.** Frozen pipes can burst and cause significant property damage. Apply insulation to vulnerable pipework, especially in unheated or external areas, to reduce the risk.
- **Weatherproof the building.** Inspect windows, doors, and roofs for gaps or damage. Sealing cracks and applying weather stripping helps prevent heat loss and water intrusion and can improve energy efficiency.
- **Maintain footpaths and car parks.** Keep outdoor areas clear of leaves, moss, and ice to reduce slip hazards. Stock grit and ensure surfaces are treated during frosty conditions to protect staff and visitors.

- **Improve outdoor lighting.** Check that all external lighting is working properly, particularly in car parks and along footpaths. Good visibility is essential during darker mornings and evenings.
- **Test fire safety systems.** Check that fire alarms, smoke detectors, and sprinkler systems are fully operational ahead of the colder months. Increased use of heating equipment and reduced ventilation during winter can heighten fire risks, making regular testing and maintenance essential for occupant safety and regulatory compliance.
- **Deliver autumn and winter safety training.** Equip employees with the knowledge to identify hazards, report issues, and respond appropriately to autumn and winter-related risks. This supports a safer and more resilient workplace.

Conclusion

Proper building maintenance in autumn and winter is essential to aid organisations in avoiding unexpected expenses and remaining fully functional during the colder months. In addition, commercial property insurance can provide vital financial protection against a range of unforeseen events that could occur in the colder months, including weather-related damage.

Contact us today for further commercial property guidance and insurance solutions.