MST INSURANCE SOLUTIONS

August 2025

COMMERCIAL

Risk Advisor

Keeping Young Workers Safe From Heat Illness

Young workers often bring energy and enthusiasm to the job and a willingness to embrace long shifts and physically demanding tasks. However, these traits can increase their risk of heat illness, a range of serious and potentially life-threatening conditions. Employers must recognize this hazard and take proactive steps to protect all workers, especially younger ones.

What Causes Heat Illness?

As temperatures rise, the body works to cool itself by increasing its heart rate and sweating. Heat illness occurs when these mechanisms fail, causing core body temperature to rise to dangerous levels. Symptoms range from mild (heat cramps) to life-threatening (heat stroke). Early recognition and response are critical to preventing medical emergencies.

Why Are Young Workers at Heightened Risk?

Young workers face increased heat illness risks due to several factors:

- Inexperience and unfamiliarity with heat illness symptoms
- Lack of knowledge about workplace safety protocols
- High energy and risk-taking tendencies
- Hesitancy to voice concerns or ask questions
- Overestimation of physical capabilities
- Longer shifts and physically intense roles
- Seasonal or temporary status, leading to improper or incomplete acclimatization

Industries That Pose a Higher Risk of Heat Illness

While all industries pose some risk, young workers are especially vulnerable to heat illness in sectors involving physical labor and high heat exposure. These include construction, utility work, machine operation, factory jobs, warehousing, maintenance, food service, moving, agriculture, landscaping, painting, and outdoor entertainment and recreation. These roles often involve long hours, strenuous activity, and limited access to shade or cooling, making targeted heat safety measures essential in these environments.

Heat Illness Prevention Tips

Heat illness prevention programs are vital for protecting all workers, including young workers, during periods of high heat. Employers should consider the following when developing and implementing their heat safety plans:

- **Conduct regular assessments** to identify heat hazards such as temperature, humidity, the sun, workload and personal risk factors.
- **Appoint a trained heat safety leader** and ensure backup coverage.
- **Train all workers** on heat illness risks, symptoms, and prevention in a language and format they understand.
- **Encourage appropriate attire** for hot conditions, including hats and breathable clothing that is still safe around equipment and wearable with protective gear.
- **Acclimatize new and returning workers gradually** using OSHA’s 20% rule; full adjustment may take two or more weeks.
- **Adjust schedules** to avoid peak heat and reduce fatigue.
- **Ensure adequate staffing** and rotate or split shifts to limit exposure.
- **Pause work if conditions are unsafe**, monitor for symptoms of heat illness and use a buddy system.
- **Provide shaded breaks** and cool water while encouraging hydration without overconsumption.
- **Use technology** like the OSHA-NIOSH Heat Safety Tool App and monitor weather alerts.
- **Have an emergency plan** for when an individual is showing severe heat illness symptoms, including how to contact emergency services and first-aid measures to provide while waiting for medical services to arrive.
- **Follow safety regulations**, which may vary by state, and regularly update and communicate the heat safety plan.

Implementing a strong heat illness prevention program is essential to protecting young workers. By proactively assessing hazards, training staff and enforcing safety measures, employers can create a safer work environment. Contact us today for more information.

This document is not intended to be an exhaustive source of information nor should any discussion or opinions be construed as legal advice. Readers should consult legal counsel or a licensed insurance professional for appropriate advice.

Preventing Tech Support and Internal Help Desk Scams

Cybercriminals use multiple tactics to accomplish their malicious goals. Schemes like technical support and internal help desk scams, where they pose as trusted personnel to breach networks, are often employed. Small and midsize businesses are especially vulnerable to these scams due to limited IT resources. Raising awareness and implementing preventive measures can protect a company from these cyber incidents and safeguard its data, finances and reputation.

Threat Landscape

Cybercriminals' 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 nonexistent issues. They may use unsolicited pop-up messages, social media advertisements, or phishing calls or emails in these fraudulent communications. They then attempt to run a fake "scan" of the computer, finding nonexistent issues and claiming they need remote access to remedy them. Once granted, the hackers may install malware, request enrollment in a fake support contract, or ask for payment for dishonest software, programs or services.

In IT help desk scams, cybercriminals pretend to be internal IT staff, often using urgent language to manipulate employees into granting access to secure networks or sharing confidential information. Voice phishing (or vishing) tactics are often utilized, as well as text message phishing (or smishing), illegitimate emails or phony collaboration platform messages.

Through both types of scams, cybercriminals employ social engineering strategies to fool a business's staff, communicating with urgency and utilizing technical jargon and scare tactics (e.g., 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.

Small and midsize businesses are especially attractive targets. With limited IT oversight, fewer cybersecurity resources and often no dedicated security team, these organizations may lack the infrastructure to detect or respond to such threats quickly. Additionally, employees in smaller organizations may not receive regular cybersecurity training, making them more susceptible to social engineering tactics.

The consequences of falling victim to these scams can be severe. Beyond the immediate loss of data or financial assets, businesses may suffer long-term damage to their reputation, face legal liabilities and experience operational disruptions. Recovery can be costly and time-consuming, especially for organizations without robust incident response plans. Fortunately, raising employee awareness is an effective way to reduce the risk of these attacks. When staff are trained to recognize the signs of a scam, they're better equipped to respond appropriately. Red flags to be mindful of include:

- **Unsolicited contact** (e.g., 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 nonconventional methods (e.g., untraceable gift cards, cryptocurrency, wire transfers, links to enter payment details)

Prevention Strategies

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

- **Implement regular cybersecurity 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 cybersecurity** 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 behavior and have a response plan in place in case of a breach.

Cybercriminals will continue to exploit human behavior as a way into systems, but with the combination of awareness, training and technical safeguards, businesses can significantly reduce their risk. Staying informed and vigilant can enable organizations to protect their data, finances and reputations from these increasingly sophisticated threats.

The FBI reports that many people don't realize they're the victim of a tech support scam until it's too late. Therefore, it's essential to take proactive steps to protect networks, accounts and data.