SAFETY
Nebraska Building Chapter

AGC Safety Initiative E-News
May 11, 2022

OUR Safety MISSION: Help each other enforce safety rules to ensure that every person on construction site goes home safe and healthy at end of the workday.

Calendar of Events – Learn more

OSHA withdrew its Vaccination and Testing Emergency Temporary Standard and will focus on a permanent **COVID-19 Healthcare Standard**

Many employees don't unplug from work while on vacation: survey

Nearly half of U.S. employees say they work while on vacation, according to the results of a recent survey.

Researchers from software company Qualtrics surveyed more than 1,000 adult full-time workers. They found that 49% work for at least an hour a day while on vacation, and 24% of respondents reported working at least three hours.

Results also showed that 27% of respondents used all of their allotted vacation time in the past year, while 26% had a week or more of unused vacation time at the end of last year. The top three reasons cited for not using all of their vacation time: fear of falling behind at work, fear of letting down their team and pressure from co-workers.

Nearly 1 out of 3 of the workers (31%) feel they're expected to answer phone calls or texts while on vacation, 27% are expected to respond to emails, and 20% are expected to be online. Perhaps not surprisingly, 27% of the respondents said they don't feel refreshed after their vacations.

The respondents suggested that organizations can help by making sure employees don't have to do any work when they're off the clock, ensuring they're not contacted when off duty and giving employees greater freedom to use vacation time when they want instead of working around co-workers' schedules.

"Two years into the pandemic, employees and organizations have experienced an immense amount of stress while continuously adjusting to work as it evolves," Benjamin Granger, head of employee experience advisory services at Qualtrics, said in a press release. "If companies are serious about the well-being of their people, they must evaluate existing norms around time off and encourage employees to completely disconnect during their allotted vacation days, without guilt. This is not only healthy for people, but essential for ensuring long-term productivity and retention."

35% of Workplace Injuries Occur During First Year

A new study by Travelers of workers compensation claims found that 35% of injuries occur during employees' first year on the job, regardless of age or industry experience.

"Our data underscores the importance of comprehensive onboarding and training programs for employees, particularly as we continue to navigate the challenges of COVID-19 and see many workers starting new jobs," said Chris Hayes, assistant vice president, Travelers Risk Control – Workers Compensation and Transportation. "While new employees are among the most vulnerable, many injuries sustained by employees of any tenure can often be prevented if the proper safety measures are in place."

The leading workers compensation carrier on May 3 released its 2022 Injury Impact Report. The study analyzed more than 1.5 million workers compensation claims over a five-year period (2015-2019).

The study provided insights in a number of areas related to first-year injury claims.

Most Common and Costliest Claims

The most common causes of first-year injuries were overexertion (27% of claims); slips, trips, and falls (22%); being struck by an object (14%); cuts and punctures (6%); being caught in or between objects (6%); and motor vehicle accidents (6%). The most expensive claims, accounting for just 8% of total claims but 26% of total claim costs, were amputations, multiple traumas, electric shock, and dislocations.

Industries Most Affected

The restaurant industry experienced the most claims from first-year employees, with 53% of the claims involving the newest workers and representing 47% of total claim costs. The construction industry was a close second, with nearly half of all claims coming from those who were new to the job, driving 52% of the industry's claim costs.

Missed Workdays

First-year injuries led to more than 6 million lost workdays over the five-year period studied, representing 37% of all lost days. Among all worker injuries over the same period, construction workers on average missed the most workdays (98) due to an injury, followed by employees in transportation (88) and those in services (69), which includes businesses such as legal, engineering and accounting firms.

Dislocation and inflammation injuries resulted in the most time away from work on average, at 132 and 82 workdays, respectively. Strains and falls both caused workers to miss an average of 69 workdays, followed by motor vehicle accidents (61) and being struck by an object (59).

About the Injury Impact Report

Travelers analyzed more than 1.5 million workers compensation claims it received between 2015 and 2019 from a variety of industries and business sizes. Findings were based solely on indemnity claims, where the injured employees could not immediately return to work and incurred medical costs. This is the second analysis of its kind conducted by the company. The first was in 2016 and included data between 2010 and 2014.

5-Step Plan for Employers to Defeat Text Message 'Smishing' Scams

Have you received a text from a random number in the last few days? Perhaps the text looks quite obviously suspicious, but it could pass as legitimate – especially if you are distracted or multitasking while scrolling through your device. The text contains a link asking you to confirm the delivery or receipt of a package. Or it tells you that you have just paid a bill. Or need to pay an outstanding bill. Or it could just be advertising a random product. These texts are actually scams that have been dubbed "smishing" – combining "SMS" and "phishing" – and your employees are no doubt receiving them, too. In a remote-work era where a multitude of attackers are attempting to gain access to your company network through digital vulnerabilities, the time is now for employers to guard yourself against this latest weapon in the cyberwar raging all around us. What are the five steps your organization can take today to best prepare?

What is Smishing?

"Smishing" is a version of phishing carried out over SMS (short message service, commonly known as texting) channels. The senders of these malicious texts are trying to get hold of personal information, passwords, and money. Smishers start by sending a text impersonating a reputable company. Typical smishing attempts specifically involve using the name of common parcel carriers informing you that your package has been delivered, or fake texts seemingly coming from a bank, company vendor, or other common company name. The messages almost always have a link. Unfortunate recipients who click that link will often end up having unsuspecting malware downloaded to their devices or will be lead to a legitimate-looking form to "log in" and voluntarily provide a trove of valuable data.

Smishing is the New Cyberattack

There is ample evidence indicating a rapid increase in smishing attempts. Smishing attacks increased 24% in the U.S. alone and 69% globally last year. According to data from the Federal Trade Commission, 21% of fraud reports that were filed in 2021 involved smishing. That's 377,840 out of the total 1,813,832 reports that identify a contact method. Of those hundreds of thousands of claims, a total of $131 million was lost, with an average of $900 per report. Work-from-home and hybrid work arrangements have led your employees to use their mobile phones and company devices at an increasing rate. This has led many of these smishing attacks to have a workplace component.

What Can Employers Do? A 5-Step Plan to Combat Smishing

So what can you do to address this latest cyber-concern? Here are five steps your organization can take to put yourself in the best position.

1. **Develop Strong BYOD Policies**
   First, you should have – and enforce – strong BYOD policies. They should include employee obligations relating to data security on company devices, with a new emphasis on smishing scams. Among other things, the policy should advise employees that they must protect confidential, proprietary, and non-public information, and that they should not allow non-employees to copy or download such information. The policy should also require employees not to share remote access addresses, logins, or passwords with anyone, even if they believe that the individual requesting the information has already been approved for remote access.
2. **Stay Up to Date**
   Next, you should make sure you keep company issued phones' software and web browsers up to date to take advantage of build-in protection features. Ask your employees to do the same for personal devices being used for business purposes.
3. **Keep Things Need-to-Know**
   You should also take steps to make confidential or other sensitive information available only on a need-to-know basis. This will minimize the spread of the information and opportunities for cybercriminals to access company data if a device is compromised. You should advise employees who do have access to such information not to provide it in response to a request delivered through text message.
4. **Enable Multi-Factor Authentication**
   You should also consider requiring multi-factor authentication to access company systems. This will provide extra security in the event an employee has their password compromised.
5. **Train, Train, Train**
   Finally, and perhaps most importantly, you should instruct employees to be wary of unsolicited requests for information sent by text and phone call. Educate your employees on the typical hallmarks of smishing schemes, including the sense of urgency often embedded into the message, such as a "limited-time offer" or other call for immediate action. You should caution employees not to tap links in an unexpected text message.

   If employees are unsure if the text is legitimate, you should train them to contact the company associated with the text request through a separate source, such as a previously verified phone number. If they receive a text from an unknown number from someone indicating they are a co-worker, you should train the recipient to follow up with the purported sender via company email or phone to confirm the text message.

Safety Initiative Goals:

As an AGC Nebraska Building Chapter member, are you participating with:

- 100% of all AGC members and other contractors on AGC jobsites enforcing OSHA standards as they apply to falls, electrical safety and possible another topic.
- 100% of all AGC members will have set their own company goals to improve safety in their firm and have a way to measure progress towards the goal.
- 100% of all AGC members will encourage and support all contractors on their jobsites to set their own company goals for improving safety.