Workers' Compensation Group Self-Insurance Fund and Group Insurance Pool

MARYLAND ASSOCIATION OF BOARDS OF EDUCATION

Niovember / December 2011

Volume 20 / 6

safetynews

"MEMORY LOSS"

You probably have used or are currently using a portable flash drive that holds important files that are either personal or confidential and business in nature. Either dangling from a keychain or strung to a lanyard, Flash drive memory sticks have become a great utility for transporting data from one place to the other quite easily.

Flash drives are compact storage devices that can store large amounts of data (usually gigabytes worth) and can be transported from location to location. Flash drive media can

IN THIS ISSUE:

FEATURED STORY:
MEMORY LOSS

SAFETYNEWS WORD SCRAMBLE

NEWS BRIEFS

CASE STUDY: AFTER THE FALL

TECHINCALLY SPEAKING

easily be concealed in a bag or a jacket pocket. Flash drives have become so commonplace that organizations are giving these drives away at conventions and meetings as promotional media. Flash drives are an inexpensive and have become an industry standard when it comes to having a backup of an important document or financial data.

Although these drives have helped revolutionized how we transport data, they also pose a great security risk to the content that is stored on the drive and other devices as well. It is important not only how these devices work but how to keep the information on them from prying eyes.

HOW FLASH DRIVES WORK:

Just slide any flash drive into any USB (Universal Serial Bus) port on a computer and you can move information from computer-to-computer quickly and with little risk of theft or viral infection from the computer you install it on. Flash drives have replaced large and bulky media such as the compact disc and floppy diskette.

The computer the flash drive is plugged into uses a technology called plug-and-play to see the flash drive, install the necessary drivers on to the computer to access the device. Once the computer has recognized the flash drive, it will assign the next drive letter available on the computer and allow data to be moved easily between the device and the computer. Flash drives can be scanned by anti-virus software that is active on the computer to protect the computer from an infected file before it is downloaded, however, not all software can stop a possible malware attack on your computer.

MORE DATA WITH LESS SPACE

Some flash drives today hold up to in excess of 32 gigabytes (GB) of data. A typical 2 GB drive is the equivalent of about 3 full compact discs worth of data. Flash drives have become more compact over the years and thanks to technology more robust and best-of-all; inexpensive.

What many unsuspecting users may not know is that some of these drives could possibly be loaded with MALWARE (Malicious Software). Malware is software that can wreak havoc on your computer once the infected file is run and you might unsuspectingly infect your computer with the corrupt file.

Because there are so many variants of virus and malware, all flash drives should be thoroughly scanned and disinfected using your computer's anti-virus program before using the flash drive for the first time. It only takes a few minutes to scan the flash drive and will save hours trying to repair the damage a malicious file may cause.

THE FEAR OF LOSING DATA

Since flash drives are small they can easily be lost or stolen. Attaching your flash drive securely to a lanyard or a keychain can give a false sense of security. Lanyards and key rings can break and the flash drive can fall freely to the ground leaving your data vulnerable to whomever finds it.

Some of the newer flash drives come with encryption software that will run when you plug the device into the computer every time. The software will ask you for a password before allowing anyone to access the files and folders that are on the drive. If you navigate through the Windows Explorer to the flash drive location, you will not see any of the files or media that is on the drive until you provide the appropriate password. But beware, there are still utilities on the Internet that can thwart this authentication mechanism and bypass the security altogether. So please keep this in mind when placing valuable data on the storage drive. Also, store your passwords in a safe location just in case you forget it. You might need to refer to this document should this occur.

There are some free utilities available on the Internet to help encrypt your files, but there are limitations to support

in case you are unable to remember the right password.

LAPTOP HARD DRIVE FEARS

What people may not realize is that this applies for laptops and personal computers as well. If your laptop or computer, with all of your important personal and business data falls out of your hands, the drive can easily be accessed without even having to turn the computer on. Hard drives can be accessed with little to no effort. With just two cables ALL data that is stored on your hard drive can be compromised without the use of a password.

TIPS ON PROTECTING DATA

1) Always zip the files and folders of important information and password protect ALL of your data. Products like PKZIP or WINZIP allow you to set passwords on files and folders. Data that is sensitive in nature (i.e., tax documents, social security numbers, proprietary information (etc.)) should always have some level of encryption for your safety.

2) Never store data that is proprietary or secure in nature on an unprotected flash drive. Use a flash drive that provides a basic level of encryption so that your information is protected. There are other ways to transfer this information besides flash drives that should be considered, including hosting the data on an FTP (File Transfer Protocol) server so the data can be accessed through secure authentication methods.

3) If you absolutely MUST store data on a flash drive, please make sure to delete and reformat the drive once you are done accessing or moving the data. With some flash drives, even deleted files can still be recovered if the flash drive itself has not been completely reformatted.

4) Password protect all data on your flash drive and hard drives whenever practical. The tougher you make it to reach the data the better.

COPIERS HAVE HARD DRIVES TOO!

Believe it or not, there are other areas where data is being stored that when compromised can be a detriment. Copier machines now have become one of the more popular targets for housing personal data. Every file that is scanned to the copier's drive is stored on an internal hard drive. If this internal hard drive is not removed when the copier is disposed, your personal and business information can be accessed the same way data on a stolen or lost flash drive or hard drive can. Most copier companies do offer a pay-for-services that will drill holes through the hard drive to ensure that no one can access the drive once the copier has been decommisioned.

To keep yourself and your information safe, it is best to store all data in a safe and secure manner. Though there are constant forces and people looking to get at your data, keeping flash drives, laptops and other storage devices from getting lost or stolen is as important as the data on the device itself.

SAFETYNEWS WORD SCRAMBLE

Accident	Compensable	Insurance	Risk
Alarm	Contractor	Lockout	Safety
Asbestos	Disability	Mitigation	Security
Attorney	Emergency	Pandemic	Survey
Audit	Ethics	Plaintiff	Tort
Benchmark	Exposure	Policy	Transportation
Benefits	Hazard	Property	Underwriter
Certification	Incident	Risk	Volunteer
Claim	Injury	Safety	Waiver

Answers to this month's Word Scramble will be available in our next issue.

NEWS BRIEFS

OSHA'S OUTREACH TRAINING

OSHA's 10- Hour Outreach Training Course in General Industry Safety and Health was presented over two days, October 26th and November 2nd. Hosted by Caroline County Board of Education, 15 people from Allegany, Caroline, Queen Anne's, Saint Mary's, Somerset and Wicomico County Boards of Education attended.

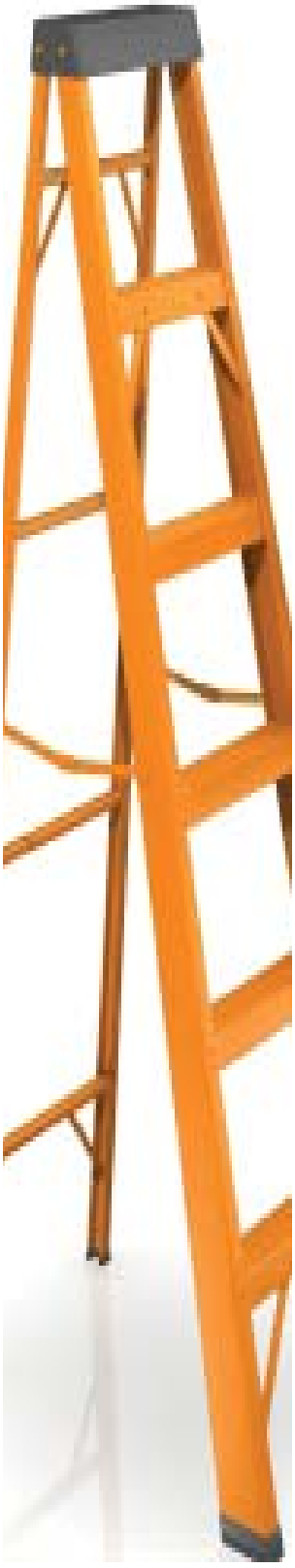
Boiler Safety Training Provided

Instructors Tony Fragale and John Wich from CNA Insurance presented helpful information on problems and potential hazards commonly found in the educational institution environment. A total of 169 people attended from Calvert, Cecil, Charles, Dorchester, Harford, Queen Anne's, Somerset, Washington and Wicomico County Boards of Education. We thank our members from Charles, Dorchester, Harford and Washington County Boards of Education for hosting this year's training course.

Benefits Administrators' Group Meets

Thirteen people representing 10 member school systems were able to attend our first School Benefits Administrators' Group meeting on October21, 2011. Health plans, wellness programs and a wide variety of services were discussed. This meeting was an opportunity for persons involved in Benefits Administration for Maryland Public Schools to compare notes, ask questions, share knowledge and to network. A second meeting is scheduled for January 19, 2012. For more information, please contact Lisa Spencer at lspencer@mabe.org.

CASE STUDY: AFTER THE FALL



Location: White Oak Middle School

Event: On the afternoon of Friday April 2nd, 2010, art teacher Robert Thompson was proudly hanging his student's artwork from a wall when the step-stool he was on rocked backwards and Robert began to fall. Reaching out and upward for something to stop him, Robert grabbed a sprinkler head and was able to regain his balance. Then, the sprinkler head snapped from the ceiling into his hand causing a pulsing rush of water to shower the entire contents of Mr. Thompson's art room.

Costs: $41,500 for repairs and replacement of materials.

Investigation: Robert explained that he was standing on a step-stool, hanging his student's artwork when he felt the wobble of the step-stool underneath him. Robert admitted grabbing the sprinkler head above him to prevent his fall. Upon close inspection, the step-stool was missing a rubber cap from one of the legs. That would have prevented the step-stool from rocking or wobbling when he was on it. Neither Mr. Thompson nor the other custodians know how long the rubber cap had been missing prior to this event. There was enough visible wear on the step-stool leg to determine that it had been used before without the rubber cap attached. It was discovered that step-stools delegated for classroom usage were not inspected and teachers were not properly informed on how to inspect them to insure they were in good working order.

Lesson: Providing sturdy step stools with hand bars and non-skid feet gives employees a safe alternative to standing on chairs and desks. Step stools, just like other equipment, need to be inspected to make sure they are in safe working condition. Users need to understand how to safely use step stools. It takes just a little time and effort to train employees, including teachers, on how to safely use step stools and how to look for problems that would make a step stool unsafe.

- **Choose step stools that will be compatible with the tasks for which they are needed**
- **Explain how much weight the step stool will hold**
- **Instruct users to:**

  - **Open a folding step stool completely, making sure it locks in the open position**
  - **Never lean a folded step stool against a wall or other structure and climb upon it**
  - **Always look at the step stool to make sure the steps, non-skid feet, hand holds and rails are in good condition**
  - **Put all your weight on the first step to make sure the step stool does not wobble before proceeding to climb**
  - **Always face the step stool when climbing it**
  - **Use the hand holds (if present) as you climb and make sure you are balanced before letting go of the hand holds**
  - **Never use a step stool in front of a door or in areas where people could come upon you and possibly knock you down**
  - **Obtain a higher step stool or ask for help if you can't reach the desired height safely**

TECHINCALLY SPEAKING

GETTING THE MOST OUT OF FREEMAIL!

Years ago, you used to have to pay for an e-mail account. But as technology and security has evolved, so has the availability of many good electronic resources that you can send e-mail to with a degree of confidence. Best of all, these e-mail accounts are FREE.

Google, which has graciously divvied out “Gmail” accounts over the past few years to millions of online users, has even upped the ante and provided one of the top spam-filtering giants, Postini, as an added measure of security in stopping malware and viruses from reaching your inbox. Hotmail and Yahoo offer excellent alternatives if you are looking to create an e-mail account for a personal or business use.

Many “Freemail” accounts today offer the ability to send and receive e-mail regularly with a good degree of reliability. You can also chat with friends in a chat room environment as well as join social networks offered by most Freemail companies today. There used to be a limitation or restriction on how much e-mail can be stored and how much data could be transferred. But since bandwidth is so inexpensive, many of these restrictions have been lifted and communication is constant and unfettered. Most Freemail accounts can be accessed by most smart phones, you won’t need to be in front of a computer to get your Freemail.

So, why not take advantage of what Google, Hotmail, and Yahoo have to offer in terms of a Freemail account? Chances are a friend or family member of yours already has.

MABE SAFTEYNEWS STAFF

Steve James
Deputy Director

Lisa Spencer
Risk Manager Officer

John Magoon
Risk Manager Officer

Lynn Gaston
Editor

Safetynews is published six times a year by the MABE Group Insurance Pool & Workers’ Compensation Group Self-Insurance Fund.

The Pool and Fund self insure property, casualty & workers’ compensation risks for Maryland school boards.