Employer Flexible™

Monthly Safety Newsletter

October 2014

In This Issue

Acknowledgements

- Why is Cyber Security a Problem? by Mindi McDowell and Allen Householder
- Using Caution with USB Drives by Mindi McDowell
- Choosing and Protecting Passwords by Mindi McDowell, Shawn Hernan, and Jason Rafail
- Cybersecurity for Electronic Devices by Mindi McDowell and Matt Lytle

Cybersecurity at a Glance

From U.S Computer Emergency Readiness Team National Cyber Awareness System

We have all heard the news reports about credit card numbers being stolen, email viruses being spread, and major companies data being compromised. Understanding the risks and what some of the basic terms mean can start to help protect us from them.

- **Hacker, attacker, or intruder:** People who seek to exploit weaknesses in software and computer systems for their own gain.
- **Malicious code:** Malicious code, sometimes called malware, is a broad category that includes any code that could be used to attack your computer. Malicious code can have the following characteristics:
  - It might require you to do something before it infects your computer, like opening an email attachment or going to a web page.
  - Some forms propagate without user intervention and typically start by exploiting a software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and affect other computers. This code can also propagate via email, websites, or network-based software.
  - Some malicious code claims to be one thing while in fact it does something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

  Viruses and worms are examples of malicious code.
- **Vulnerability:** In most cases, vulnerabilities are caused by programming errors in software. Attackers try and take advantage of these errors to infect your computer, this is why it is important to apply updates and patches that address known vulnerabilities.

USB Drive Security Tips

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks. Here are some tips for protecting your data:

- **Disable the "Autorun" feature**
- **Take advantage of security features**
- **Keep personal and business USB drives separate**
- **Backup the USB drive date in case your drive is lost**
- **Do not plug an unknown USB drive into your computer**
- **Use and maintain security software, and keep all software up to date**

News & Notes

- Any piece of electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities.
- Vulnerability increases if the device is connected to the internet or a network that an attacker may be able to access.
- If an attacker infects your cell phone with a virus, steals yours phone, or accesses your data on your phone your personal information may be at risk, in addition this could have serious consequences if you store corporate information on the device.

Password Protection

Sometimes a password is the only barrier between a criminal and your companies information. There are several program attackers can use to help guess or "crack" passwords. By choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.

Here are some tactics to use when choosing a password:

- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Don't use words that can be found in any dictionary of any language.
- Develop a mnemonic for remembering complex passwords.
- Use both lowercase and capital letters.
- Use a combination of letters, numbers, and special characters.
- Use passphrases when you can.
- Use different passwords on different systems.

Example: Basketball23 (23 is LeBron James' jersey number) vs.

Better: LBJwMVPi1213 [L]e[B]ron [J]ames [w]on [MVP] [i]n 20[12] and 20[13]

Employer Flexible Safety & Risk
Risk Main: 1.888.983.5881
Injury Reporting: 1.888.983.4802
risk@employerflexible.com

Cybersecurity for Electronic Devices

When we think of cybersecurity we often think of laptops and PCs and often forget that all of our electronic devices, like smartphones, tablets, video games and even car navigation systems can be vulnerable to attack. There are several tips to keep in mind to help protect yourself:

- **Remember Physical Security:** Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your devices unattended in public or easily accessible areas.
- **Keep software up to date:** If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.
- **Use good passwords:** Choose devices that allow you to protect your information with passwords. See the above article for tips on choosing good passwords.
- **Disable remote connectivity:** Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.
- **Encrypt files:** If you are storing personal or corporate information, see if your device offers the option to encrypt the files. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it.