County Officials E-News

Promoting better county government through direct assistance to county officials and their associations

Recent CTAS Staff Changes

Carolyn Keith Retired September 29

Carolyn Keith, CTAS Administrative Support Assistant, retired on Friday, September 29 after 36 years of loyal, dedicated public service.

If you've ever called our office in Nashville, you were likely greeted by the "Voice of CTAS" in her warm, welcoming answer. Carolyn has been a constant source of exemplary customer service for both our external customers and internal staff. She has been our rock, our shoulder, our friend.

We hope you've had the chance to speak with or meet Carolyn. We will truly miss her sweet smile and wide open heart. ■

Kelsey Schweitzer Joins CTAS October 1

Join us in welcoming Kelsey Schweitzer to CTAS as our new County Government Consultant for the southern West Tennessee region. He previously worked for the Tennessee Comptroller of the Treasury as a legislative auditor. Kelsey also has experience in accounting. He earned a Masters of Business Administration degree in 2017 and a Bachelor of Science in Business Administration in 2010, both from The University of Tennessee at Martin. Welcome, Kelsey! ■

Kelsey Schweitzer
County Government Consultant
Southern West Tennessee
605 Airways Blvd., Suite 109
Jackson, TN 38301
Cell: (731) 336-3576
kelsey.schweitzer@tennessee.edu

Inside This Issue...

Nickajack Cave in Marion County is one of the most historical caves in Tennessee, located just over half a mile south of Shellmound Station on the west side of the Tennessee River. A paved hiking trail leads to an observation deck at the entrance to the cave where visitors can watch Gray Bats, an endangered species, leave the cave at dusk. In 1968 the cave was partially flooded when Tennessee Valley Authority constructed Nickajack Dam 6 miles downstream to replace the aging Hales Bar Dam. ■

County Spotlight

Marion County

County Seat:
2010 Census Population:
County Government Consultant:
Gary Hayes
gary.hayes@tennessee.edu

Jail Liability Seminar Series
Risk Assessment & Management

This seminar is designed to assist those law enforcement personnel that work predominately in correctional facilities. This course will provide attendees with a better understanding of the liability issues facing today's jails and provide them with tools to help avoid that liability. Click HERE for more info.

Who should attend: Sheriffs, Chief Deputies, Jail Administrators, Shift Supervisors, FTO's, County Safety Directors, Correction Officers, County Mayors, County Commissioners, Jail Medical/Nursing Staff

If your county is a Safety Designee member, it is a requirement that the Sheriff, Chief Deputy or Jail Administrator attend.

Schedule

◊   October 23, Monday, Chattanooga

◊   October 24, Tuesday, Murfreesboro

◊   October 25, Wednesday, Cookeville

Cyber Security
What to Know, What to Do

Are you worried about being hacked? Concerned your sensitive computer data may be subject to unauthorized release? October is Cyber Security Awareness Month and the focus is on preventing data breaches by establishing and following security measures to protect computer and web data. Read below to learn what hackers want and how to prevent their access.

What Type of Data Do Hackers Want?
Hackers want personal information. Driver license numbers, social security numbers, names, addresses, phone numbers, email addresses -- all of these data are valuable to hackers. Most county offices have access to some of these data. As public servants, county officials who handle personal information have a responsibility to protect it from unauthorized use.

Ransomware: The Next Big Thing
Local governments have become an increasingly attractive target for hackers. Ransomware is one method hackers use to access sensitive data. What is ransomware? It is malicious software hackers load onto computers that will lock down the entire computer, circumventing the county official's access, until a monetary ransom is paid. Ransoms demanded by hackers usually amounts to thousands of dollars.

How Do I Stop Hackers?
The one variable most people often forget when looking to secure their computer data is usually the most common cause of cyber security breaches: humans. People are their own worst enemy when it comes to cyber security. There is no amount of software protection or technological solution that can prevent human error. Ensuring staff are properly trained in cyber security and *continue to use established security protocols* are the best way to minimize human error.

Below are a few tips to get you started on establishing proper cyber security in your office. Some of these tips may seem to be common sense, but remember it only takes one user error to allow hackers in.

Password Strength
It can be annoying to have to constantly remember passwords for all of the login credentials we use every day. However, your passwords are your first line of defense against hackers. Be sure you are using a strong password -- use punctuation, spaces, or even entire sentences. Don't use easy-to-know names, dates, addresses, or other information for your password. And don't use the same password for every account you have. Here are some examples of strong passwords:
⇒ Where is my coffee!??
⇒ Surgeon format briefly explore
⇒ #*@gadw-32j#-qwU

If you have trouble remembering your passwords, you might consider using a password manager such as 1Password, Enpass, or Keypass. These programs have you create a master password and encrypt your data so it cannot be read by others. You are able to store login credentials, important information, and notes. Several also offer secure, encrypted browser access as well as the ability to automatically fill in your login information for you (if you choose).

Firewalls and Antivirus Protection

A firewall is a security system on a computer that monitors incoming and outgoing network connection traffic (i.e., the system watches to see how much data is being transferred between the computer and the internet connection). Monitoring this traffic will develop a baseline of "typical" network usage. If you have been hacked, chances are large amounts of network usage can occur. Your firewall will notice this and close down the network connection as a means of protection.

If you have a Windows or Mac computer, you have a firewall already. By default, it is turned on so you should not need to turn it on. You can find the firewall settings in the Control Panel for Windows or System Preferences for OS X.

Antivirus protection is software that periodically scans your computer for specific files. The companies that create the antivirus software also create libraries of known malicious files. When you have to update your antivirus software, what you are doing is downloading the latest library catalog so your computer is able to recognize the virus software. It is a good idea to use antivirus protection software and periodically scan your computer for infections.

Be Careful When You Click

Clicking on a bad link is one of the most common ways user error gives hackers a way in. Hackers will often send emails with malicious attachments or links disguised as legitimate websites. Always verify that the link in a email will take you to where it says it will. To do this, point your mouse cursor over the link without clicking. A bar at the bottom of the window will display the actual link. If they match, then the link is probably safe. However, it is much safer to go directly to the website by typing its address into your browser.

Ever get an email from someone you don't know that has an attachment? Never open attachments from people you don't know or were not expecting -- they are usually malicious. Further, sometimes hackers gain access to email accounts and then use the stolen account to trick others. If you receive an email from a friend that seems out of character for them, give them a call. They may have been hacked.

When browsing websites, be careful of links or ads that pop up on your screen. Links found on reputable websites such as federal or state agencies are usually safe to click. Links found on the website of a checkout-stand magazine, however, may be questionable. A good rule of thumb: If it seems suspicious, don't click!

What Do I Do If I've Been Hacked?

If you believe you have been hacked and are the victim of ransomware -- do not do anything with the computer. Immediately call (don't email!) your local FBI office (Knoxville or Memphis) to report the ransomware attack. The FBI issued a public service announcement in September 2016 that describes how to report ransomware attacks as well as details about the use of ransomware.

If you have not been attacked by ransomware but are still concerned about hacking, a good action to take is to immediately change all of your passwords. Make the new ones stronger and/or more complex.

Additional Resources

Need more info? Check out these websites below to learn more about cyber security and other tips to help prevent hacking.

FBI Resources on Scams and Safety https://www.fbi.gov/scams-and-safety/on-the-internet

FBI Internet Crime Complaint Center (IC3) https://www.ic3.gov/default.aspx

FBI IC3 Ransomware Brochure https://pdf.ic3.gov/Ransomware_Trifold_e-version.pdf

NACo. "Ransomware attacks on the rise in 2017." http://www.naco.org/articles/ransomware-attacks-rise-2017

National Cyber Security Alliance, Online Safety Basics https://staysafeonline.org/stay-safe-online/online-safety-basics/

U.S. Department of Homeland Security, Cybersecurity https://www.dhs.gov/topic/cybersecurity ■

A good rule of thumb:

If it seems suspicious, don't click!

Training Opportunities

All classes are 8:30am-12:30pm local time.
<u>Managing Conflict & Difficult Conversations</u>
(Part 1; Part 2 required for credit)
October 16 — Murfreesboro | Embassy Suites
<u>County Audit Issues</u>
October 18 — Murfreesboro | DoubleTree Hotel
October 19 — Dickson | Renaissance Hotel
October 20 — Jackson | Jackson Energy Authority
<u>County Purchasing</u>
November 8 — Johnson City | Carnegie Hotel
November 9 — Knoxville | UT Conference Center
November 16 — Jackson | Madison-Jackson Health Department
November 17 — Murfreesboro | DoubleTree Hotel

Register Today!

Reserve your spot in class now!
Visit k@te to register online.

COCTP
CTAS

k@te
UT
Knowledge and
Training Excellence

Upcoming Conferences

COUNTY OFFICIALS
ASSOCIATION OF
TENNESSEE

COAT 49TH
ANNUAL CONFERENCE

Embassy Suites - Franklin

November 1-3, 2017   Register Now!

THE PEABODY

64TH ANNUAL
TCSA
FALL CONFERENCE
& TRADE SHOW
NOVEMBER 1-3, 2017

Peabody Hotel - Memphis

November 1-3, 2017   Register Now!

UT **County Technical Assistance Service**
INSTITUTE FOR PUBLIC SERVICE

226 Capitol Boulevard, Suite 400, Nashville, Tennessee 37219
(615) 532-3555 ctas.enews@tennessee.edu