Warren County · Ohio

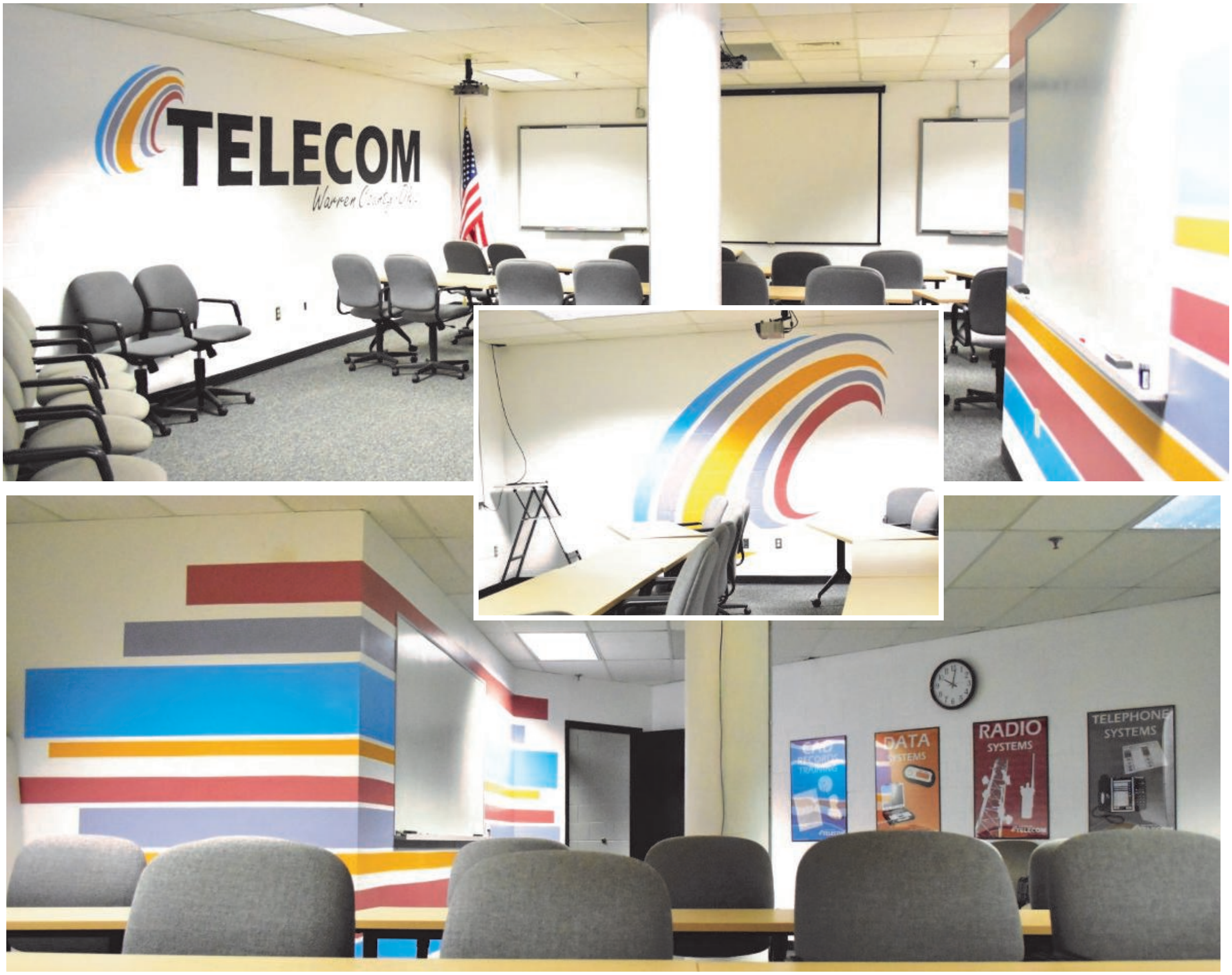
January 2016

TELECOMatters

our monthly newsletter of things that matter. all things Telecom.

Check out Telecom's *NEW* Training Room!

Last month we shared digital renderings of our training room design plans: the painting & wall art is done; proper conference/training tables are in! Come gather and learn at Telecom!



Why You Should Care About Computer Security

Computers help us maintain our financial, social, and professional relationships. We use them for banking and bill paying, online shopping, connecting with our friends and family through email and social networking sites, researching data posted on the Internet, and so much more. **We rely heavily on our computers** to provide these services, yet **we sometimes overlook our need to secure them.** Because our computers play such critical roles in our lives, and we input and view so much personally identifiable information (PII) on them, it's imperative to maintain computer security that ensures the safe processing and storage of info.

How Do I Improve the Security of My Home Computer?

Following are important steps you should consider to make your home computer more secure. While no individual step will eliminate your risk, together these defense-in-depth practices will make your home computer's defense stronger and minimize the threat of malicious exploit.

1. **Connect to a Secure Network**—Once your computer is connected to the Internet, it's also connected to millions of other computers, which could allow attackers access to your computer. Information flows from the Internet to your home network by first coming into your modem, then into your router and finally into your computer. Although cable modem, digital subscriber line (DSL), and internet service providers (ISP) purport some level of security monitoring, it's crucial to secure your router—the first securable device that receives information from the Internet. Be sure to secure it before you connect to the Internet to improve your computer's security

2. **Enable and Configure a Firewall**—A firewall is a device that controls the flow of information between your computer and the Internet, similar to a router. Most modern operating systems include a software firewall. In addition to the operating system's firewall, the majority of home routers have a firewall built in. Refer to your user's guide for instructions on how to enable your firewall. Once your firewall is enabled, consult the user's guide to learn how to configure the security settings and set a strong password to protect it against unwanted changes.

3. **Install and Use Antivirus and Antispyware Software** - Installing an antivirus and antispyware software program and keeping it up to date is a critical step in protecting your computer. Many types of antivirus and antispyware software can detect the possible presence of malware by looking for patterns in the files or memory of your computer. This software uses virus signatures provided by software vendors to look for malware. Antivirus vendors frequently create new signatures to keep their software effective against newly discovered malware. Many antivirus and antispyware programs offer automatic updating. Enable that feature so your software always has the most current signatures. If automatic updates aren't offered, be sure to install the software from a reputable source, like the vendor's website or a CD from the vendor.

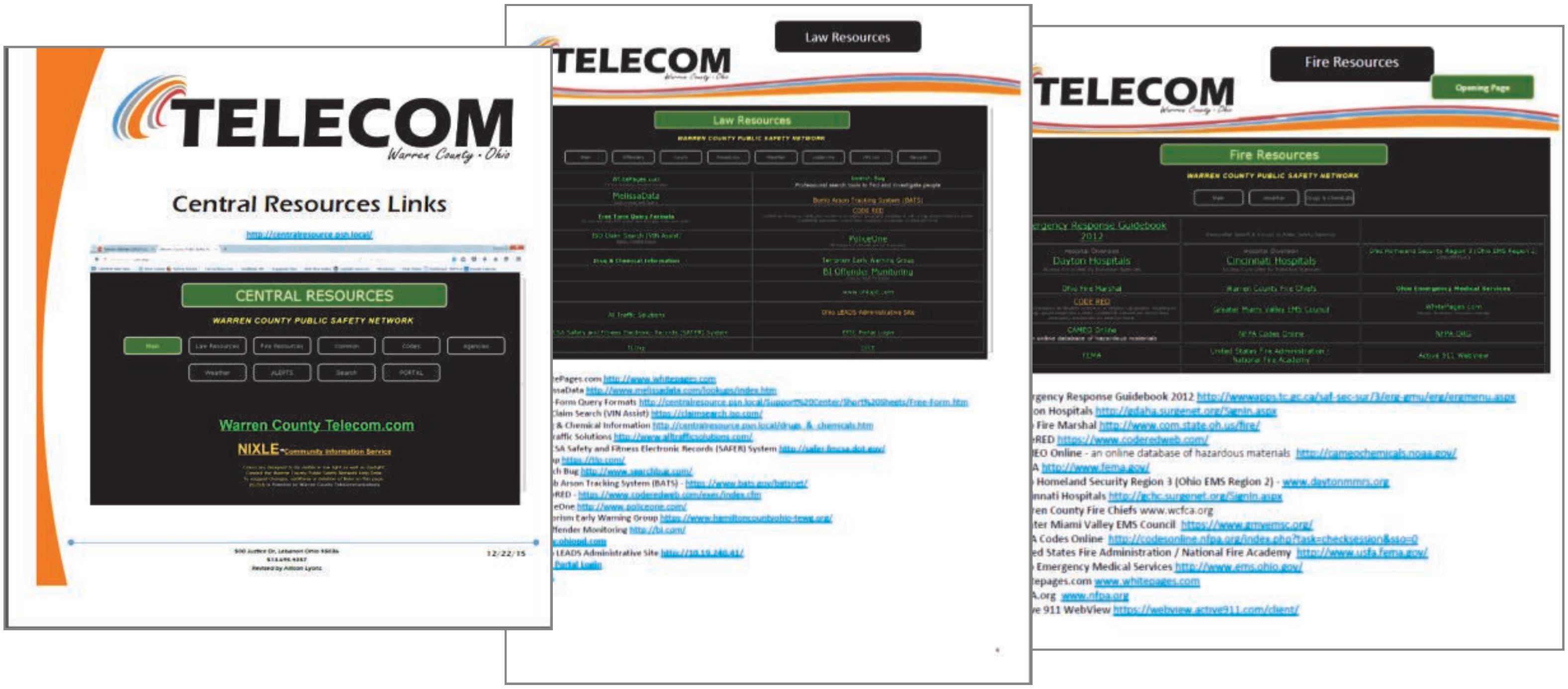
4. **Remove Unnecessary Software**—Intruders can attack your computer by exploiting software vulnerabilities (that is, flaws or weaknesses), so the less software you have installed, the fewer avenues for potential attack. Check the software installed on your computer. If you don't know what a software program does and don't use it, research it to determine whether it's necessary. Remove any software you feel isn't necessary after confirming it's safe to remove the software. Back up important files and data before removing unnecessary software in case you accidentally remove software essential to the operating system. If possible, locate the installation media for the software in case you need to reinstall it.

5. **Modify Unnecessary Default Features**—Like removing unnecessary software and disabling nonessential services, modifying unnecessary default features eliminates opportunities for attack. Review the features that came enabled by default on your computer and disable or customize those you don't need or plan on using. As with nonessential services, be sure to research these features before disabling or modifying them.

6. **Operate Under the Principle of Least Privilege**—In most instances of a malware infection, the malware can operate only under the rights of the logged-in user. To minimize the impact the malware can have if it successfully infects a computer, consider using a standard or restricted user account for day-to-day activities and only logging in with the administrator account (which has full operating privileges on the system) when you need to install or remove software or change system settings from the computer.

(continued on page 4)

DOWNLOAD YOUR CENTRAL RESOURCES REFERENCE GUIDE: Head over to http://ftp.wcoh.net/public/User_Information/Training/ and download the Central Resources Links document to learn what all is available from this web-based library of links and documents.



TELECOM Warren County • Ohio

Central Resources Links

http://centralresource.psn.local/

CENTRAL RESOURCES

WARREN COUNTY PUBLIC SAFETY NETWORK

Warren County Telecom.com

NIXLE-Community Information Service

12/22/15

Revised by Allison Lyons

Law Resources

TELECOM

Law Resources

WARREN COUNTY PUBLIC SAFETY NETWORK

WhitePages.com	Search Bug Professional search tools to find and investigate people
MelissaData	Bomb Arson Tracking System (BATS)
Free Form Query Formats	CODE RED
ISO Claim Search (VIN Assist)	PoliceOne
Drug & Chemical Information	Terrorism Early Warning Group BI Offender Monitoring
	www.ohiopd.com
All Traffic Solutions	Ohio LEADS Administrative Site
FMCSA Safety and Fitness Electronic Records (SAFER) System	PPSC Portal Login
TLOxp	OSCE

ePages.com http://www.whitepages.com
saData http://www.melissadata.com/lookups/index.htm
-Form Query Formats http://centralresource.psn.local/Support%20Center/Short%20Sheets/Free-form.htm
Claim Search (VIN Assist) https://claimsearch.iso.com/
& Chemical Information http://centralresource.psn.local/drugs_&_chemicals.htm
raffic Solutions http://www.alltrafficsolutions.com/
SA Safety and Fitness Electronic Records (SAFER) System http://safer.fmcsa.dot.gov/
p https://tlo.com/
ch Bug http://www.searchbug.com/
b Arson Tracking System (BATS) - https://www.bats.gov/batsnet/
RED - https://www.coderedweb.com/ews/index.cfm
eOne http://www.policeone.com/
rism Early Warning Group https://www.hamiltoncountyohio-tewg.org/
ffender Monitoring http://bi.com/
.ohiopd.com
LEADS Administrative Site http://10.19.240.41/
Portal Login

Fire Resources

TELECOM

Opening Page

Fire Resources

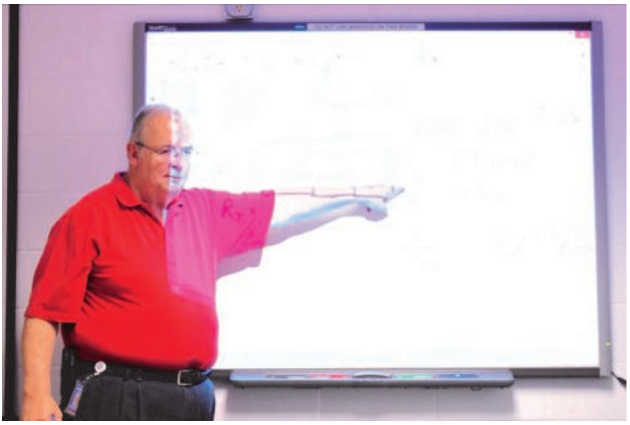
WARREN COUNTY PUBLIC SAFETY NETWORK

Emergency Response Guidebook 2012		
Dayton Hospitals	Cincinnati Hospitals	Ohio Homeland Security Region 3 (Ohio EMS Region 2)
Ohio Fire Marshal	Warren County Fire Chiefs	Ohio Emergency Medical Services
CODE RED	Greater Miami Valley EMS Council	WhitePages.com
CAMEO Online an online database of hazardous materials	NFPA Codes Online	NFPA.ORG
FEMA	United States Fire Administration / National Fire Academy	Active 911 WebView

rgency Response Guidebook 2012 http://wwwapps.tc.gc.ca/saf-sec-sur/3/erg-gmu/erg/ergmenu.aspx
on Hospitals http://gdaha.surgenet.org/Signin.aspx
Fire Marshal http://www.com.state.oh.us/fire/
RED https://www.coderedweb.com/
EO Online - an online database of hazardous materials http://cameochemicals.noaa.gov/
A http://www.fema.gov/
Homeland Security Region 3 (Ohio EMS Region 2) - www.daytonmmrs.org
nnati Hospitals http://gchc.surgenet.org/Signin.aspx
ren County Fire Chiefs www.wcfca.org
ter Miami Valley EMS Council https://www.gmvemsc.org/
A Codes Online http://codesonline.nfpa.org/index.php?task=checksession&sso=0
ed States Fire Administration / National Fire Academy http://www.usfa.fema.gov/
Emergency Medical Services http://www.ems.ohio.gov/
tepages.com www.whitepages.com
A.org www.nfpa.org
ve 911 WebView https://webview.active911.com/client/

Lunch & Learns

Radio Systems Manager, Wally Hardwick has been hosting Lunch & Learns for Telecom employees in pursuit of their HAM (Amateur Radio) Technician licenses. Conducted during unpaid lunches, Wally has taken it upon himself to invest in his coworkers by offering his industry expertise and study aides. Data Systems personnel, being cross-trained in Radio Systems, will make them more effective in the field when troubleshooting agency issues regarding antenna work, cabling issues, etc.



Why You Should Care About Computer Security (continued)

7. **Secure Your Web Browser**—Web browsers installed on new computers usually don't have secure default settings. Securing your browser is another critical step in improving your computer's security because an increasing number of attacks take advantage of web browsers.

8. **Apply Software Updates and Enable Future Automatic Updates**—Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software. Because intruders can exploit these bugs to attack your computer, keeping your software updated is important to help prevent infection.
When you set up a new computer (and after you have completed the previous practices), go to your software vendors' websites to check for and install all available updates. Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won't have to remember to do it yourself. Many operating systems and software have options for automatic updates. As you're setting up your new computer, be sure to enable these options if offered. Be cautious, however, because intruders can set up malicious websites that look nearly identical to legitimate sites. Only download software updates directly from a vendor's website, from a reputable source, or through automatic updating.

9. **Use Good Security Practices**—You can do some simple things to improve your computer's security. Some of the most important are:

- Use caution with email attachments and untrusted links. Malware is commonly spread by people clicking on an email attachment or a link that launches the malware. Don't open attachments or click on links unless you're certain they're safe, even if they come from a person you know. Some malware sends itself through an infected computer. While the email may appear to come from someone you know, it really came from a compromised computer. Be especially wary of attachments with sensational names, emails that contain misspellings, or emails that try to entice you into clicking on a link or attachment (for example, an email with a subject like that reads, "Hey, you won't believe this picture of you I saw on the Internet!").

- Use caution when providing sensitive information. Some email or web pages that appear to come from a legitimate source may actually be the work of an attacker. An example is an email claiming to be sent from a system administrator requesting your password or other sensitive information or directing you to a website requesting that information. While Internet service providers may request that you change your password, they will never specify what you should change it to or ask you what it is.

- ***Create strong passwords. Passwords that have eight or more characters, use a variety of uppercase and lowercase letters, and contain at least one symbol and number are best.*** Don't use passwords that people can easily guess like your birthday or your child's name. Password detection software can conduct dictionary attacks to try common words that may be used as passwords or conduct brute-force attacks where the login screen is pummeled with random attempts until it succeeds. The longer and more complex a password is, the harder these tools have to work to crack it. Also, when setting security verification questions, choose questions for which it is unlikely that an Internet search would yield the correct answer.

NEMSIS Version 3 Compliance

Warren County ePCR Agency Administrators and Fire/EMS Chiefs,

In regards to the email sent from the State of Ohio regarding becoming NEMSIS version 3 compliant prior to April 1, 2016, the response from Zoll is as follows:

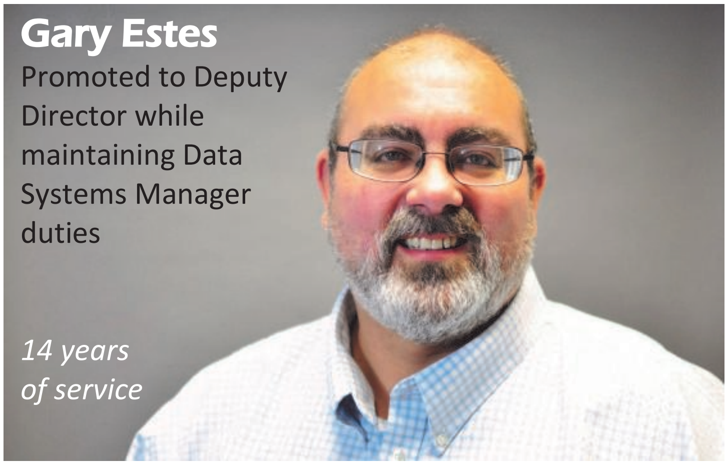
"... we will be able to meet this deadline and we will be in touch just after the first of the year to talk about some work that will need to be done prior to upgrading to ePCR 6.0 and becoming NEMSIS 3 compliant."

Telecom will be in touch as soon as we have any further updates on this.

Telecom Personnel Updates

Thanks to the County Commissioners' approved 2016 budget, Telecom is set to expand and grow this coming year!

Promotions



Gary Estes

Promoted to Deputy Director while maintaining Data Systems Manager duties

14 years of service

Becky Trovillo

Promoted from Switchboard Operator to Administrative Support, Telephone division

10 years of service

Jessica Johnson

Promoted from Administrative Support to Administrative Assistant, Telephone division

10 years of service

New Hires

Corey Burton
Radio Systems Technician

corey.burton@wcoh.net
513.695.1177
4T42

Before coming to Telecom, I worked at P&R Communications in Dayton. My education and industry training include Commercial and Public Safety radio programming and utilization.
Key skills I plan to utilize here at Telecom include knowledge of radio capabilities and new ideas on how to use the radio system. In my spare time, I spend time with my children and read books. A fun fact about me is I also work on radio systems in the Air National Guard.

Joseph Newton
Data Systems Applications Analyst I

joseph.newton@wcoh.net
513.695.1321
4T32

Before coming to Telecom, I worked as a Media Team Manager for Hewlett Packard. My education and industry training include Linux Networking & Administration education and Media Management. Key skills I plan to utilize here at Telecom include problem solving and critical thinking. In my spare time I enjoy partaking in craft beers while watching football and gaming. A fun fact about me is I try to visit Jekyll Island and enjoy a blizzard (from Dairy Queen) on the beach at least once a year.

“The Telephone Ladies” have moved offices!

When visiting Telecom for phone or billing inquiries, engraving orders, or Directory changes, the Telephone Administrative staff has moved across and down the hall, directly across from Director Kindell’s office. Those familiar with the basement remember this as the former Dispatch Supervisor/Trainer offices. This is one more piece of the relocation/ renovation since Emergency Services left the building in February 2015. Next up: moving CAD/RMS to the former EMA room and Data Systems to the former Dispatch Center.