

'Tis the Season to Be Cautious

The holiday season is upon us and millions of people around the world are looking to buy the perfect gifts. Many of us will choose to shop online in search of a great deal, avoiding long lines and impatient crowds. Unfortunately, this is also a criminal's favorite time of the year to commit online or financial fraud. This month, we explain the dangers of shopping online and ways you can protect yourself.



Fake Online Stores

While most online stores are legitimate, some are not; they are fake websites set up by criminals. Criminals create these fake websites by copying the look of or using the name of well-known stores. They then use these websites to prey on people who are looking for the best deal possible. When you search online for the absolute lowest prices, you may be directed to one of these fake websites.

When selecting a website to purchase a product, be wary of websites advertising prices dramatically cheaper than anywhere else or offering products sold out nationwide. The reason their products are so cheap or available is because what you will receive is not legitimate, is a counterfeit or stolen item or, in some cases, you never even receive anything. **Protect yourself by doing the following:**

- Verify the website has a legitimate mailing address and a phone number for sales or support-related questions. If the site looks suspicious, call and speak to a human.
- Look for obvious warning signs like poor grammar and spelling.
- Be very suspicious if a website appears to be an exact replica of a well-known website you have used in the past, but the website domain name or the name of the store is slightly different. For example, you may be used to going to the website <https://www.amazon.com> for all of your Amazon shopping. But be very suspicious if you were to find yourself at a website pretending to be Amazon with the URL <http://www.store-amazon.com>.
- Type the store's name or URL into a search engine and see what other people have said about the website in the past. Look for terms like "scam," "never again" or "fake." A lack of reviews is also not a good sign, as it indicates that the website is very new.

Remember, just because the site looks professional does not mean it's legitimate. If something about the site sets off warning bells, take time to investigate. If you aren't comfortable with the website, don't use it. Instead, find a well-known website you can trust or have safely used in the past. You may not find quite as great a deal or find that hot ticket item, but you are much more likely to end up with a legitimate product and a clean credit report.

(continued on page 4)

More on Warren County's **NEW 9-1-1 System**

The 9-1-1 Committee was made up of representatives from Lebanon, Franklin, Warren County Emergency Services, and Telecom. The process went as follows:

1. Committee reviewed the request for proposals (RFPs) from 9 vendors.
2. Committee ranked RFPs on price, technical merit, and capabilities.
3. Committee chose the top three companies to present vendor demonstrations.
4. Committee again ranked the 3 finalists.
5. The top vendor was informed, negotiations were held, and on September 22nd the Commissioners signed the contract to proceed with the system upgrade.

The winner of our contract is Indigital Telecom of Fort Wayne, Indiana. They provide most Next Gen 9-1-1 systems in Eastern Indiana and some Ohio counties including Butler and Van Wert. The system we purchased is made by a team at Solacom who also manufactured our old system under the company CML. Solacom took the solid design and features from the old system and brought them to the Next Generation iP world.

The new equipment has been delivered to Telecom with configuration and updates already underway. The new system is dependent on Fiber Optic lines as its main form of communications between Dispatch Sites and the Phone Company. The fiber line installation has begun and is scheduled to be completed by January 15th, 2016. We will be using the County Microwave plus new links from Lebanon and Franklin as backup connections should the fiber go down.

More next month!

Telecom Personnel Updates

- Please congratulate Jeff Cepin on his promotion to Applications Analyst 2. He has been filling the position for some time and finally holds the distinction. The Applications Analyst 1 position has been posted to fill.
- In light of Nick Yeazel's October departure, several applicant resumes have been reviewed and screened for the Radio Systems Programmer position. We will be filling the position soon.



t
h
e
f
a
c
e
s
o
f
T
e
l
e
c
o
m

Paul Bernard
CAD / Records Team
Manager

paul.bernard@wcoh.net
513.695.2800




Mike Callahan
Telephone Systems
Technician

mike.callahan@wcoh.net
513.695.1326




Dustin Flint
Data Systems
System Administrator

dustin.flint@wcoh.net
513.695.2812




Jeff Cepin
Data Systems
Applications Analyst II

jeff.cepin@wcoh.net
513.695.2814




Allison Lyons
Training Specialist
Newsletter Publisher
Webmaster

allison.lyons@wcoh.net
513.695.2802




Don Sebastianelli
CAD / Records Team
Applications Analyst II

don.sebastianelli@wcoh.net
513.695.2801




Gary Estes
Data Systems
Manager

gary.estes@wcoh.net
513.695.1810




David Shiverdecker
Data Systems
Technician

david.shiverdecker@wcoh.net
513.695.2819




Rich Short
Data Systems
Technician

rich.short@wcoh.net
513.695.2818




Paul Kindell
Telecommunications
Director

paul.kindell@wcoh.net
513.695.1318




Geezer Wilson
Telephone Systems
Supervisor

garrett.wilson@wcoh.net
513.695.1320




Becky Trovillo
Telephone Systems
Switchboard Operator

becky.trovillo@wcoh.net
513.695.2494




Rhonda Bernard
Data Systems
Applications Analyst I

rhonda.bernard@wcoh.net
513.695.2813




Glenn McKeehan
Radio Systems
Supervisor

glenn.mckeehan@wcoh.net
513.695.1316




Rebecca Morton
Telephone Systems
Administrative Assistant

rebecca.morton@wcoh.net
513.695.1317




Debbie Griffith
Administrative
Assistant

debbie.griffith@wcoh.net
513.695.1322




Wally Hardwick
Radio Systems
Manager

gary.hardwick@wcoh.net
513.695.2860




Jessica Johnson
Telephone Systems
Administrative Support

jessica.johnson@wcoh.net
513.695.2436




Not pictured: Matt Stapleton, Telephone Technician



www.WarrenCountyTelecom.com | www.facebook.com/WarrenCountyTelecom | www.twitter.com/wcoh_telecom | www.youtube.com/warrencountytelecom

Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 adela.dingman@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

'Tis the Season to Be Cautious (continued)

Your Credit Card

Keep an eye on your credit card statements to identify suspicious charges. You should review your statements regularly, at a minimum at least once per month. Some credit card providers give you the option of notifying you by email or text messages every time a charge is made to your card or when charges exceed a set amount. Another option is to have one credit card just for online purchases.



That way, if it is compromised, you can easily change the card without impacting any of your other payment activities. If you believe fraud has been committed, call your credit card company right away and explain the situation. This is also why credit cards are better for online purchases than debit cards. Debit cards take money directly from your bank account, and if fraud has been committed, it can be far more difficult to get your money back.

Finally, there is new technology that enables you to pay without exposing your credit card number. Consider credit cards that generate a unique card number for every online purchase, or use well-known payment services, such as PayPal, which do not require you to disclose your credit card number to the vendor.

Your Computer/Mobile Device

In addition to shopping at legitimate websites, you want to ensure your computer or mobile device is secure. Cyber criminals will try to infect your devices so they can harvest your bank accounts, credit card information and passwords.

Take the following steps to keep your devices secured:

- If you have children in your house, consider having two devices: one for your kids and one for the adults. Kids are curious and interactive with technology. As a result, they are more likely to infect their own device. By using a separate computer or tablet just for online transactions, such as online banking and shopping, you reduce the chance of becoming infected. If separate devices are not an option, then have separate accounts on the shared computer and ensure your kids do not have administrative privileges.
- Only connect to wireless networks you manage, such as your home network, or networks you know you can trust when making financial transactions. Using public Wi-Fi networks, such as at your local coffee shop, may be great for reading the news, but not for accessing your bank account.
- Always install the latest updates and run up-to-date anti-virus software. This makes it much harder for a cyber-criminal to infect your device.



Our training room is getting a face lift!

The old EOC is now Telecom's training room and we have plans to personalize it! When entering the room, the immediate left wall will house posters of our training offerings. Further on that wall will be our logo stretched end to end.

The right wall will be Telecom orange with our signal wave graphic stretched floor to ceiling in the back right corner. Add in some updated tables + chairs, and we'll have a fresh new space to host trainings, meetings, and gatherings.



www.WarrenCountyTelecom.com | www.facebook.com/WarrenCountyTelecom | www.twitter.com/wcoh_telecom | www.youtube.com/warrencountytelecom

Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 adela.dingman@wcoh.net | Training 695-2802 allison.lyons@wcoh.net