BEST PRACTICES

Dave Yost
Ohio Auditor of State

October 2017

Vigilance, planning help to avoid becoming cyberattack victim

With increasing regularity, governments of all sizes are being targeted by cybercriminals who want access to the rich data sets that they maintain. The sophistication with which these hackers infiltrate emails, computers and networks has grown rapidly, and the number of successful attacks is growing as well.

It has been estimated that by 2019, cybercrime will reach $2 trillion a year in losses. In 2016, more than 29 million records were exposed. In 2015, Ohio ranked 10th in the nation for cybercrime, according to the 2015 FBI cybercrime report. In 2016, Ohio had climbed to 9th in the nation for cybercrime.

There have been some well-publicized cases in Ohio over the past couple of years. On Jan. 31, 2017, Licking County information technology employees realized a ransomware virus had been installed on a county computer. The attack forced the county to shut down its computers and phone systems; ultimately, 1,000 computers had to be reformatted. The cybercriminals demanded

Continued on next page

► **Visit www.ohioauditor.gov/Cybersecurity.html for all of the office's publications, trainings and tips on cybersecurity.**

Continued from page 1

a ransom to unlock the computers and release the data that had been hijacked. Rather than pay, the county was able to rebuild its systems because data were backed up the previous day. However, the impact of the attack on the central Ohio county lasted an entire week.

In May of 2016, a virus encrypted Columbiana County's court data, crippling the court for a short time. Because the county did not have a recent backup of its data, it eventually agreed to pay the $2,500 demand. A month earlier, a similar ransomware attack hit Vernon Township in Clinton County. Fortunately, no ransom was paid because the township's data had been backed up.

Criminals, whether stealing jewels or data, look for weaknesses in protection. In the cyberworld, part of the weakness involves evolving technology and hacker sophistication while another part is human error and vulnerabilities.

In addition to training, experts offer the following tips to avoid being hacked (or minimize the damage caused by a cybercriminal):

- Scan systems regularly – Free software for both anti-virus and anti-malware
- Keep your operating system up to date
- Update software and browsers
- Use a dedicated computer for financial transactions
- Use strong, long passwords
- Do not list your email address online
- Use encryption if possible/encrypt hard drives
- Have backups in place and regularly test them
- Work with your IT department and limit privileges

Protecting your systems

Best Practices

Know the three rules of computing

1. If you didn't go looking for it, don't install it
2. If you installed it, update it
3. If you no longer need it (or, if it's become too big of a security risk) get rid of it

Perform a self-assessment

1. Identify most valuable assets by thinking like a hacker
2. Conduct an internal phishing campaign
3. Educate employees (KnowBe4.com/ Kevin Mitnik)
4. Ask IT to review NIST and CIS Controls for compliance
   - » https://www.nist.gov/cyberframework
   - » https://www.cisecurity.org/controls/

Preparedness Checklist

To do:

1. Create a response plan and team: This should include the office holder or head of the organization, IT, Legal, Finance and Public Relations at a minimum
2. Establish clear action items
3. Identify key contacts
4. Know your reporting guidelines in the event of a breach
5. Encrypt sensitive data
6. Map locations of critical data
7. Restrict access
8. Follow a retention policy
9. Purge old employee accounts

If attacked

1. If a ransomware page pops up, immediately unplug that computer from the network/WiFi NOT from power
2. Stop additional loss and contact Information Technology (IT) immediately
3. Have IT change security access and passwords if possible
4. Contact proper law enforcement
5. Start documenting times/dates/people, etc.
6. Take note of date/time for notification and reporting requirements
7. Wait for law enforcement/forensic experts to arrive
8. Handle media requests for information

If you've been hacked, DON'T ...

- Pretend it isn't happening
- Try to fix or look at computers and networks
- Turn off computers unless IT has directed you to do so
- Attempt to make backup copies of computers
- Connect USB/storage devices or any other machine
- Run antivirus or malware software
- Turn on a machine or network if turned off

Protecting your systems

Should you pay a ransom?

It depends ...

- Do you have a recent backup? If you do, you may not have to pay
- What is the time loss if you wait for IT to restore via backup and can you afford to wait?
- Are you prepared to lose everything if you pay and it is not restored?
- Is there already a key you can use to unlock data? ›› nomoreransom.org
- Have you talked with your attorney?

What is bitcoin?

- Digital currency started in 2009 also known as cryptocurrency
- Currency used in the black market
- No names used, only numeric "addresses" known as the blockchain
- You can buy bitcoin from exchanges or people via marketplaces
- You can pay by cash, credit, debit card, wire transfer or even with other cryptocurrency
- There are several exchanges that are used for safely obtaining bitcoin
- Coinbase is the most trusted currently because it is U.S. operated and bound by our legal system

Don't be fooled by WiFi

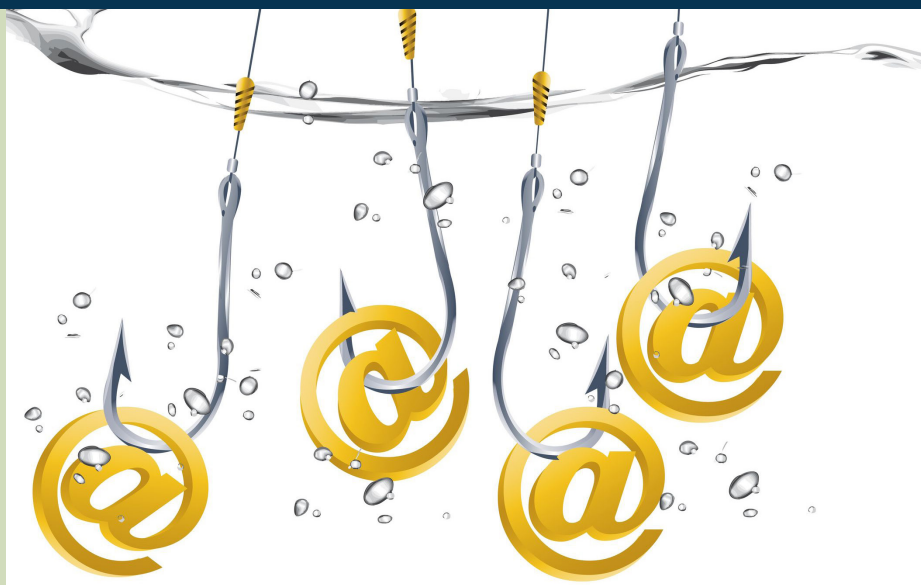
- Don't trust the WiFi just because your phone or computer automatically connects with it.
- Ask an employee for the WiFi network name. Some hackers will create duplicate WiFi names that are used to steal your information.
- Use a VPN to protect your information.
- If you must use WiFi, do not go to secure sites, like banking or others that use passwords. Wait until later.
- If possible, use your cell phone as a WiFi hotspot.
- Use two-factor authentication.

If victimized

United States Secret Service
- Electronic Crimes Task Force: www.secretservice.gov/investigation/#field
- Local Field Offices: www.secretservice.gov/contact/

Federal Bureau of Investigation
- Cyber Task Forces: www.fbi.gov/contact-us/field

Internet Crime Complaint Center
- www.ic3.gov



Cyber precautions

The need for vigilance against hackers is constant.

Auditor of State Dave Yost directed his IT department to conduct a small test to determine whether staff members would take the bait and open 'phishing' emails. The result: 19 percent were hooked.

Following the experiment, Auditor Yost contracted with an expert in battling cyberfraud and required all members of his staff to participate in extensive training to discern friendly email from the fraudulent. The training led to a major reduction in the number of times staff members opened problematic emails or attachments.

To help local governments avoid costly mistakes associated with cyberfraud, Auditor Yost began offering free cybersecurity training to local officials. The training is very similar to that provided to Yost's staff.

"Cyberfraud is a significant problem that is worsening," Auditor Yost said. "This training has proven to be effective in helping our staff be more discerning when it comes to opening emails, which is why I wanted to make it available to the local governments we serve. And with no cost, there's no reason why people shouldn't take advantage of it."

►Check our website for an upcoming cyberfraud webinar.

The training, which lasts about 60 minutes, is broken down into eight modules:

- Passwords
- Giving out personal information
- Online banking
- Protecting children online
- Protecting your identity
- Securing your computer and home network
- Spam viruses and more
- Opening email attachments

You can find the training by signing in to eServices in the Hinkle System or the Fiscal Integrity Act site on the Auditor of State's office website. (Did we mention that it's free?)

Protecting your systems

Clues to avoid being phished

- To whom is the email addressed?
- Look for grammar and spelling errors
- If a deal sounds too good to be true, it's probably not legitimate
- Is the email from somebody you deal with?
- Were you expecting the email?
- Does it include links? (Learn to hover over the link to see where it is redirecting you)
- Does the email ask for personal information that is different from typical information requests?
- Check domain names/email addresses before replying (Learn to hover the mouse over the sender's name to see if the email address is incognito)
- Does the email include a reason they can't be reached personally?
- Is it a high-pressure, deadline-sensitive email?

Social engineering

Hackers rely on human vulnerabilities to manipulate people by deception to divulge confidential information that is later used for fraudulent purposes. The methods of attack:

- Vishing (Use of voice/phone calls to obtain information, often through bogus offers of discounts or government scams)
- Smishing (Use of SMS text messaging to gain information, often including a link directing you to sign into something)
- Phishing (An attempt to obtain sensitive information through email by posing as a trustworthy source or someone you know. Often seek user names, passwords, credit card info., etc. These attacks are mass generated.)
- Spear Phishing (A targeted phishing attack)

Key definitions

Malware is a blanket term covering any form of intrusive software, such as:

- **Trojans**: A harmful type of software that looks legitimate. Users are usually tricked into loading and executing it on their systems.
- **Worms**: Similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage.
- **Spyware**: Malicious software that collects data without your consent. You likely installed it from an infected link or download.
- **Adware**: Software that display advertisements while you are online and collects data about you.
- **Bots**: "Bot" (as in "robot") is an automated process that interacts with other network services. They often automate tasks and provide information or services that would otherwise be conducted by a human being. Bots are used for a number of legit reasons as well as malicious ones.
- **Viruses:** Spread from one computer to another, leaving infections as they travel. They are inserted into your computer and become part of various programs.
- **Keyloggers**: A piece of software or hardware that logs every key you press on your keyboard. Used to capture messages, passwords, credit card numbers, and banking information.
- **Ransomware**: A form of malware that targets your critical data and systems for the purpose of extortion. The ransomware usually encrypts files and the cyber actor is the only one with the key to decrypt them. A timeframe is given and specific instructions are given to purchase the key, or risk loss or publication of data.

Share this

Up next

Stopping payroll fraud

To guard against payroll fraud and errors, a payroll system must restrict access to core information and include regular verification of changes.

Follow us

Ohio Auditor of State

@OhioAuditor

Dave Yost
Ohio Auditor of State

88 E. Broad St.
Columbus, Ohio 43215

Phone: 800-282-0370
Fax: 614-466-4490

www.ohioauditor.gov