OHIO AUDITOR OF STATE
KEITH FABER

Auditor of State Keith Faber's fraud investigation team has spent an extensive amount of time exploring cybercrimes that have affected Ohio communities. Some of the language used to describe cybercrime can be confusing. What's even more challenging is knowing what to do.

Below are some definitions of cybercrimes and the recommendations for communities on how to avoid them.

Ransomware – Considered the biggest threat in the information security industry today. Ransomware is a malware that is installed on your computer by clicking on links in emails. Ransomware holds your computer hostage by locking your screen or encrypting your files until you pay a specified amount of money for a key that will unlock your system. It is usually infected from macros in Microsoft office documents delivered via email. From December 2015 to May 2016, half of all ransomware attacks were in the United States, according to Microsoft.

Phishing - The practice of luring unsuspecting Internet users to a fake website by using authentic-looking email with the real organization's logo. The emails are loaded with viruses that launch when opened and typically include methods to trick you into providing your passwords or other financial or personal information. These usually look like emails from a bank, and once
you "log in" they have your account information and can then gain access to your account to transfer money. Usually these types of emails are sent out in the thousands.

Spear-phishing - Spear-phishing is a more targeted form of phishing. Emails are designed to appear to come from someone the recipient knows and trusts, usually a colleague, and can include a subject line or content that is specifically tailored to the victim's work. For high dollar victims, attackers may study their social networking accounts to gain further intelligence and
then choose the names of trusted people in their circle to impersonate or a topic of interest to lure the victim and gain their trust. (Don't friend people you do not know personally on Facebook, LinkedIn etc.)

Whaling – Spear-phishing targeted to high profile targets such as executive officers or elected officials within a business or government organization.

How can I avoid becoming a victim?

- Regularly backup the data on your system. If your system is infected, you can restore your system and avoid having to pay any fee to release your computer or its data. You should also secure your backup either offsite or with a cloud backup provider.
- Use strong passwords and never write them down on a sticky note and attach it to your computer or screen. A strong password is long and uses symbols, numbers and upper/lowercase letters. Consider an easy-to-remember phrase such as IlikeMondays! for your password.
- Use anti-virus software, anti-malware, and pop-up blockers. Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Ensure application patches for the operating system, software, and firmware are up to date, including Adobe Flash, Java, Web browsers, etc.
- Do not place your personal email addresses on your website. If you need an email address listed then set up a catchall account such as contact@agency.com.
- Only download software — especially no charge software — from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.
- Scrutinize links contained in emails and do not open attachments included in unsolicited emails. Hover over links and verify the destination matches the link. When in doubt, go to the site rather than clicking the link (e.g. go to the official UPS site and type in the tracking number rather than clicking the link in an email.)
- Use a phishing filter with your web browsers. Many web browsers have them built in or offer them as plug-ins. If your web browser doesn't do this for you, do it yourself.
- Disable macro scripts from files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- Avoid using an account with Admin privileges. Always use an account with "User Privileged" access. This helps prevent some, but not all, malware from installing.
- Remember that most companies, banks, agencies, etc. don't request personal information via email.
- Consider calling people instead of simply using emails. Emails are convenient, but they're also a convenient tool for criminals. When you call, be sure to use a phone number you've looked up or are familiar with, because cyber criminals will include fake phone numbers in phishing emails.

Should I pay the ransom?

There is no standard answer for this, but most cyber security professionals will lean towards not paying. In paying a ransom you open yourself up to bigger ransoms later, and there is no guarantee you will get the key to unlock your system. That being said, some entities pay because they need access to their files immediately and cannot wait on IT to perform a restore (such as a Sheriff's Office or Police Department).

What to do if you are a victim or suspect an email is a phishing email?

- Do not click on any link in the email.
- If you have an IT department, make them aware immediately in case others in your agency have also been sent the same email.
- Contact your local law enforcement if you have become a victim and actually sent money. They will know who to direct you to (such as the FBI, Secret Service etc.)
- If you sent money, contact your bank immediately, sometimes they can stop the wire transfer and recover some or all of the funds.

How do I identify a phishing email?

- They use generic greetings or subject lines such as "Bank Customer" "Friend" or "Subscriber"
- They request highly sensitive personal information
- They are "Urgent" or have a deadline.
- The URL does not include the "S" in HTTPS://

What are the most frequently used companies in phishing emails?

- Facebook (asks for login)
- Banks (asks for login and account data)
- Logistics companies such as: UPS, FedEx, DHL and USPS. (asks for more postage to obtain your credit card information