Place: Romers Catering, Main Room
Date: 10/8/2019

Members present: Renee Whittington, Margie Jacobs, Ron Rindler, Carol Bruns, Frank Urwin, John Yoder, Lisa Niekamp Urwin, Jason Romer, Josh Schmackers, Kim Baumer, Janet Jacobs, Sharon Rindler, Eydie Kremer, Michelle Bruns

Josh Schmackers called the meeting to order. **Minutes** from the September 16th meeting were approved following a motion from Frank Urwin & a second by Kim Baumer.

Treasures Report (submitted)
Checking account: $343.66
Main account: $36,174.18

Our newest member is **Grace and Serenity Wellness Studio**, a massage therapy studio located on Kremer Hoying Rd and owned by Madison Buschur. Kim mentioned that Troy Steinbrunner, owner of S S Auto has inquired about membership and may be joining as well!

Information for the **Combined Drive** has been sent; several people at the meeting commented on receiving their forms in the mail. The deadline to return the forms and payment is October 31st. We will plan to present checks to recipients once all dollars are counted and checks prepared. This is likely to happen at the December meeting.

Kim gave an update on the **Holiday Open House** – the event is scheduled for November 8 – 10th. The committee is on target for giving away $5500 in cash and prizes again this year. We have many new businesses supporting the Open House and remaining open to shoppers. We will send a direct mail piece to all St Henry and Burkettsville residents advertising the event. The mail piece will have a tear off tab that people can bring to the Open House for a registration chance. We will again have posters around town promoting the event and a newspaper advertisement displaying individually purchased block ads inviting people to shop their particular business and/or shop the community. Lisa reminded everyone that we will have postings on social media and she encourages all of us to *like* or *share* the information to help spread the word!

Lisa announced that October is **National Cyber Prevention** month. She shared a company newsletter with facts and data to help protect your operating systems and a learning opportunity with experts talking about ……

St Henry Village Map – Josh Schmackers has been working with Mitch Kremer from Messenger Press on a new village map. Jason Romer suggested that we list businesses by 'type of business' which makes it convenient for out-of-towners to find a business based on need. There seems to be no existing document for making simple revisions therefore a new product is being created. Ideally, we would like to list all St Henry Businesses in the brochure; but, we will possibly map only the businesses who are Chamber Members... Jason also suggested having a digital copy to post on our Website and Facebook page. Josh will work with Mitch to keep this project moving forward.

Ron Rindler shared information about the Mercer, Auglaize, Van Wert Youth Mentoring program, formerly known as Big Brothers Big Sisters of Mercer, Auglaize, & Van Wert Counties. Again this year Ron is performing in the *Dancing with the Big Stars* fundraising event. Ron is partnered with Chamber member Becca Wenning, owner of Brides and Beyond. They have been working countless

hours on a routine to dance on the November 2nd event. While they are working toward the top spot on the dance floor, their greater goal is to raise money to support the programs that help our local kids. Frank Urwin made a motion to donate $500 to MAV Youth Mentoring; the motion was seconded by Janet Jacobs and passed by unanimous vote. Ron agreed to perform the routine with Becca at the November meeting!

Josh thanked **Rindler Truss** for sponsoring the Stress Relief.

Pot of Gold winner – Kim Baumer from Homestretch Sportswear. $28.00

Motion to adjourn the meeting from John Yoder & second by Frank Urwin

Minutes taken and prepared by

Sharon Rindler

Secretary

MAV YOUTH MENTORING

For the past 30 years, the organization has operated as Big Brothers Big Sisters of Mercer, Auglaize, and Van Wert Counties. In 2019, they disaffiliated from Big Brothers Big Sisters of America and became M.A.V. Youth Mentoring. They are the same mentoring program serving Mercer, Auglaize, and Van Wert Counties, with the same dedicated staff and board of directors. Their need to disaffiliate came as a result of increased fees and demands on resources from the national office and with added restrictions on the mentoring model. They felt it was no longer in the best interest of our community to be a BBBS agency. They are pleased to keep all money 100% local. They are also excited about the possibility of expanding programs to include other types of mentoring that work with our community's needs.

As a youth mentoring program, they will continue to make meaningful, monitored matches between adults and children, ages 5 through 18 in the communities across the three county area. They will continue to develop positive relationships that have a direct and lasting effect on the lives of young people.

The expenses that they incur are: salaries, insurance for youth and mentors, program materials/supplies, background check, afterschool snacks, utilities, accounting fees and audits.

Vision: To help all children reach success in life.

Mission: Provide all children facing difficulties a positive, professionally-supported one-on-one relationship that improves their lives, forever.

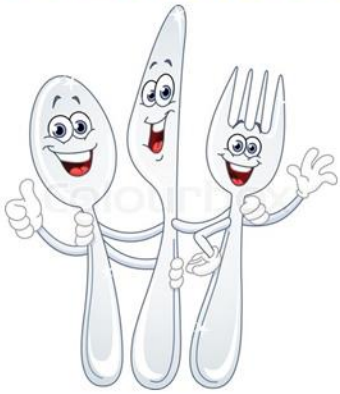
Last year in St. Henry they ran an after school program that involved over 20 youth and mentors from St. Henry. However this year they decided to switch from an after school program to a lunch club program. Last year, transportation was an issue and some kids were not able to stay after school. So a Lunch Club Program has been introduced eliminating the need for transportation. So far, 9 kids are enrolled in the program. They are currently looking for 5 more Mentors (community members willing to eat lunch with the kiddos.)

M.A.V. YOUTH MENTORING
Making a difference, together.

Mentors Needed for the Lunch Club Program at St. Henry Elementary

LUNCH CLUB PROGRAM
BE A MENTOR. BE THE DIFFERENCE.

Each one of us can make a DIFFERENCE!



Contact Nancy Eberle at
MAV Youth Mentoring
(formerly Big Brothers Big Sisters)
for more information or to enroll
419-584-2447 or
nancy@mavyouthmentoring.com

The Lunch Club Program is designed to match a student from St. Henry with an adult who truly cares about and will encourage his or her success. This is done through one-on-one interactions at school during the lunch period.

What does it take to become a Lunch Club Mentor?

- **You commit to spending 45 min. twice a month with an elementary student for the length of the school year.**
- **Complete an application, background check, and orientation led by MAV YM Staff.**
- **You get to be a positive adult role model to a child in your community by just talking and spending time with a child during their lunch period.**

Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, and More Profitably"

Security Update

How to spot a phishing e-mail

A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular website or to click and download a virus. Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate e-mail. So, how can you tell a phishing e-mail from a legitimate one? Here are a few telltale signs… First, hover over the URL in the e-mail (but DON'T CLICK!) to see the ACTUAL website you'll be directed to. If there's a mismatched or suspicious URL, delete the e-mail immediately. In fact, it's a good practice to just go to the site direct (typing it into your browser) rather than clicking on the link to get to a particular site. Another telltale sign is poor grammar and spelling errors. Another warning sign is that the e-mail is asking you to "verify" or "validate" your login or asking for personal information. Why would your bank need you to verify your account number? They should already have that information. And finally, if the offer seems too good to be true, it probably is.

October 2019

We implement enterprise level solutions that are industry standards without breaking the bank account.

Tomorrow's Technology Today
An IT Pro Alliance Company

www.TomTechToday.com
419-678-4600

3 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

1. IT ALL STARTS WITH EDUCATION. One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target of hackers and scammers.

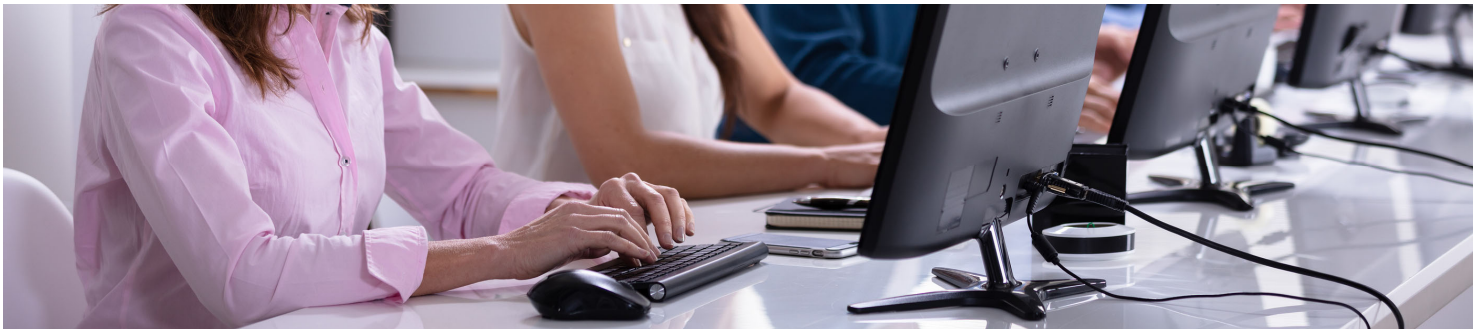
You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer your questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to ***hold this training regularly.*** Threats evolve, and you need to stay ahead of the curve. Keep IT security on the minds of your employees. When they forget about it, that's when the risk is highest.

2. SAY NO TO UNSECURED, PUBLIC WIFI. This is a big problem for businesses with remote employees, employees who work from home or employees who use

Continued on pg.2

Continued from pg.1



company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely.

This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social media that you're going to be out of town for a week. You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft *even easier.*

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi *at all.* And place a bigger focus on endpoint security – make sure your equipment has up-to-date software, malware protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3. PROTECT ALL OF YOUR DATA. Your employees should never save personal or business data on portable/ external hard drives, USB drives or even as printed material – and then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they *will* search the drive for sensitive data, such as financial or customer information that they can use or sell.

If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary. Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security.

"It's all about understanding the threats and taking a proactive approach to security."

While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business.

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now, call 419-678-4600.

Own IT. IT's up to you.

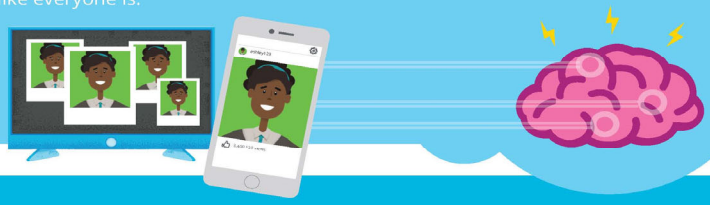
OWN IT. SECURE IT. PROTECT IT. OCTOBER 2019 National Cybersecurity Awareness Month #BeCyberSmart

Who wants to know?

There's more than **three billion** people on the internet, and not all of them are who they say they are. Keep your your friends list small, and **never** friend anyone you don't know in real life.

The internet never forgets

With archive sites, screencaps and the quick spread of information on social media, the internet never forgets a mistake. You may dance like nobody's watching, but post like everyone is.

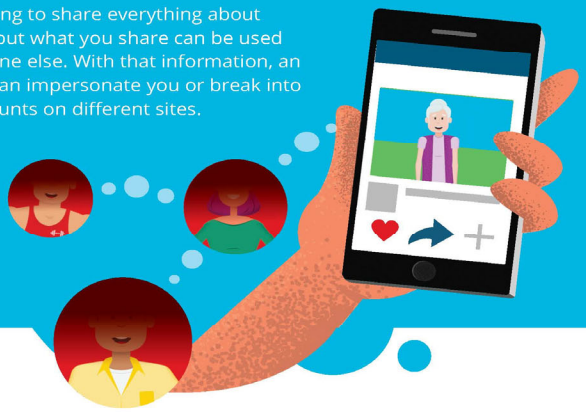


Take it slow

Attackers will often goad people into making quick decisions, hoping to take advantage of your mistakes. **Think fast, but type slow,** and they can't touch you.

Sharing is not caring

It's tempting to share everything about your life, but what you share can be used by someone else. With that information, an attacker can impersonate you or break into your accounts on different sites.



Don't reuse passwords

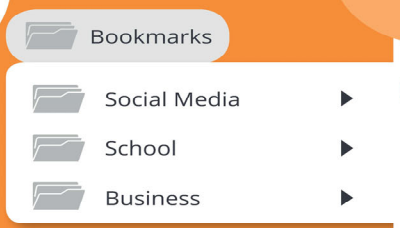
Passwords get cracked all the time, and each broken password is added to a hacker's database of passwords to use in the future. **Always use unique passwords.**

Link and you'll miss it

Links on websites and in emails can be spoofed, making you think you're going to a site you aren't. Instead, **use bookmarks** to ensure you're going right back to where you want to be.

Click here

http://filledwithviruses.com/haxyouraccounts/



Spot the scam

A product or service may look good on the site, but how do you know it's legitimate before you buy? Consumer watchdogs like the **Better Business Bureau** can help you check if a business is on the level — before you give them your credit card number.

Look for the S

These days, a legitimate shopping site is going to be using HTTPS rather than HTTP. (The S stands for "secure.") Look in the upper corner of the screen for the **HTTPS and the lock icon.**

Tomorrow's TECHNOLOGY Today

October is National Cybersecurity Awareness Month. Let's Celebrate!

Like getting your steps in or lifting from your knees, secure habits keep you safe and your online reputation healthy. This October is National Cybersecurity Awareness Month — a collaborative effort between government and organizations like ours to ensure everyone has the resources and knowledge they need to stay secure at work and at home.

In the coming weeks, we'll share a variety of resources to help you outsmart cyberthreats and protect you and your family from online attacks. We encourage you to read and share the information with your colleagues, friends and family.

When it comes to cybersecurity, knowledge is power. Join us this October in the fight against cybercrime!

Think before you click: staying safe on social media

There are more than four billion people on the internet today, and many of them use social media to communicate. But while social media can be fun and a great way to chat with friends, it can be risky as well. When people share personal information about themselves, they may become targets for scammers and identity thieves.

However, you can take a few simple precautions to keep yourself and your friends and family safe on social media. Here's how.

First, always use the strongest privacy settings you can. Check the Settings section of your social media profile and make sure what you're posting can only be seen by your friends.

Second, think about what you post before you post it. It's easy for people to misunderstand a joke or a fun meme, especially with billions of people out there who might see it. It's easy to avoid this, though. Think of your social media as your outfit: there are some things you wouldn't wear in public because people would laugh or think it wasn't a good choice.

Lisa Recommends: Scamming You Through Social Media

Many of us have received phishing email, either at work or home. These emails look legitimate, such as from your bank, your boss, or your favorite online store, but are really an attack, attempting to pressure or trick you into taking an action you should not take, such as opening an infected email attachment, sharing your password, or transferring money. The challenge is, the more savvy we become at spotting and stopping these email attacks, the more cyber criminals try other ways of contacting and scamming us.

Attempts to scam or fool you can happen over almost any form of communication you use—from Skype, WhatsApp, and Slack to Twitter, Facebook, Snapchat, Instagram, and even gaming apps. Communication over these platforms or channels can feel more informal or trustworthy, which is precisely why attackers are using them to fool others. In addition, with today's technologies, it has become much easier for any attacker anywhere in the world to pretend to be anything or anyone they want. It is important to remember that any communications that come your way might not be what they seem and that people are not always who they appear to be.

Key Takeaways

Here are the most common clues that a message you just received or a post you just read may be an attack:

Urgency: The message has a sense of urgency that demands "immediate action" before something bad happens, like threatening to close your account or send you to jail. The attacker wants to rush you into making a mistake.

Pressure: The message pressures you to bypass or ignore policies or procedures at work.

Curiosity: The message invokes a strong sense of curiosity or promises something that is too good to be true. No, you did not just win the lottery.

Sensitive: The message includes a request for highly sensitive information, such as your credit card number or password, or any information that you're just not comfortable sharing.

Official: The message says it comes from an official organization, but has poor grammar or spelling. Most government organizations will not use social media for official communications directly with you. If you are not sure if the message is legitimate, call the organization back, but use a trusted phone number, such as one from their website.

Impersonation: You receive a message from a friend or co-worker, but the tone or wording just does not sound like them. If you are suspicious, call the sender on the phone to verify they sent the message. It is easy for a cyber attacker to create messages that appear to be from someone you know. In some cases, they can take over one of your friend's accounts and then pretend to be your friend and reach out to you. Be particularly aware of text messages, Twitter, and other short message formats, where it is more difficult to get a sense of the sender's personality.

You are the best defense against scams, cons, and attacks like these. If a post or message seems odd or suspicious, simply ignore or delete it. If it is from someone you personally know, call the person on the phone to confirm if they really sent it.

Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.

Shiny New Gadget Of The Month:

The Philips Somneo Sleep & Wake-Up Light

Research suggests that when you wake up naturally (that is, you aren't jolted awake by an alarm or radio), you feel more refreshed and energized during the day.

The Philips Somneo Sleep & Wake-Up Light puts this research to the test. It's designed to simulate a natural sunrise right in your bedroom. You can set it to your specific needs, and it will slowly and steadily brighten when you need to wake up. It can also simulate a sunset for the opposite effect when you're going to bed! You can even use the light as a reading lamp — and it has a built-in radio, too!

The Philips Somneo Sleep & Wake-Up Light is a versatile device, perfect for anyone who wants to get a better night's sleep. Find it at Amazon and many other electronic retailers.

The Power Of Punctuality

Personally, I am not a fan of people who are always late. Sometimes, things happen that we have no control over, such as car accidents, traffic jams and unexpected family emergencies, to name a few. I am not addressing those situations.

What I am addressing is how punctuality can do wonders for your success.

Have you ever thought about what being punctual says about you? It shows you are in control, disciplined, able to keep track of things, trustworthy, reliable and respectful of another person's time. Being late demonstrates none of those things. In fact, being late shows you are unreliable, disorganized, disinterested and inconsiderate. When you look at it from that perspective, you would never want yourself described that way.

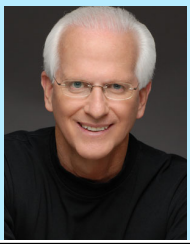
Do you want to hire someone who is unreliable? Not me. How about disorganized? A disorganized person will make mistakes — and mistakes cost money. Let's take a closer look at *disinterested*. One of the definitions of *disinterested* is having or feeling no interest in something, unconcerned, uncaring and unenthusiastic. That sounds like someone you NEVER want to have on your team. Then that leaves us with inconsiderate, defined as thoughtlessly causing hurt or inconvenience to others, unthinking, selfish, impolite and rude.

Associates, bosses and customers have NO fondness for lateness. I heard one person express it this way: "If you are chronically late, you are chronically rude." If you are looking to be promoted to a leadership position, it will be difficult to prove yourself reliable when people are having to wait for you to show up. Punctuality is a product of discipline, proper planning and respect for others. In simple terms, preparedness and punctuality are two of the most important qualities of a leader.

When you are late, you are saying, "My time is more valuable than yours." That is not a great way to start anything. The celebrated writer Charles Dickens once said, "I could have never done what I have done without the habits of punctuality, order and discipline." I feel that by being punctual, you are paying a courteous compliment to those you are about to see or serve; it's a respectful gesture of how you value their time.

Chronic lateness sets a tone about accountability. If you want a culture in which people are accountable to customers, associates and even to themselves, then make punctuality a priority. Start all meetings on time regardless of who is missing. The word will get out, and people will start showing up on time.

Being on time may seem a bit trivial to some people, but it's a good idea to start making accountability part of your corporate culture. Shakespeare once stated: "Better three hours too soon, than a minute late." There truly is power in being punctual.



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

Do you know anyone we can help?

We ***LOVE*** our clients and we want more like you! If you know of any business owners that could benefit from one or more of our services, we would appreciate an introduction. I promise we will treat them with kid gloves! You can just drop us an introduction email:

sales@ttecht.com

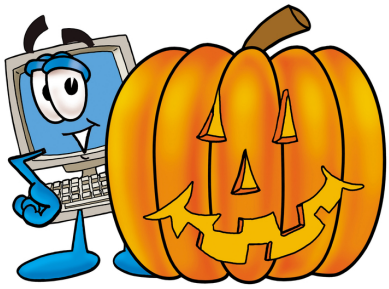
Technology Today

October 2019

"Insider Tips To Make Your Business Run Faster, Easier, and More Profitably"

Tomorrow's Technology Today
501 North Eastern Avenue
PO Box 432
Saint Henry, OH 45883

Inside this Issue:



These Are The Biggest Privacy Threats You Face Online Today

Webcam Access – While it's rare, there are known exploits that allow others to access your webcam (such as malicious software or software security flaws). Putting electrical tape over your webcam isn't a bad idea, but more webcams are coming with kill switches and shutters for peace of mind.

Phishing Scams – Don't ever expect these to go away. People still fall for them. NEVER click links in e-mails from anyone you don't know (and even if you do know them, verify that they sent you a link — e-mail addresses can be spoofed).

Web Browser Plug-ins – Vet every browser plug-in and extension you install. Many extensions collect your browsing history and sell it. Read the terms of service before you click install (a good rule of thumb for software in general).

Ad Tracking – Web ads (and web ad providers, such as Facebook and Google) are notorious for tracking users. They want to know what you like so they can cater ads directly to you in the hopes that you'll click the ad, which gives them ad revenue. It's one of the many reasons why people use ad blockers.

Device Tracking – If you have a smartphone, chances are it's being used to track your every move. Again, it comes back to delivering ads that are relevant to you so you'll click on them. For companies like Facebook and Google, users are the product. *Inc., 7/19/2019*

"All that work to tell you about stuff you could look up on Wikipedia?!"

Capitalize On This Strategy To Improve Your Bottom Line

Want to boost your bottom line? The answer may be in cashless payments. It's all about taking your current systems and updating them to current trends.

Outside of the U.S., particularly in Europe and much of Asia, cashless payments are king. More people are relying on smartphones as payment processing tools (both in the consumer and business worlds). Of course, you don't want to rely on cashless — you want to be able to accept any money your customers are spending, whether it's cash, card or electronic.

Look at your point-of-sale system — is it ready for cashless? If not, look into it, research your options, ask around and see what option makes sense for your business (and bottom line). *Small Business Trends, 6/26/2019*

How To Plan Ahead for Cyber Threats, Crisis, and Disasters

Keynote Presentation by FBI—Cleveland Division

Speaker- G. Ryan Macfarlane,

FBI Supervisory Special Agent

Topic- Cyber Threats: The Current State Of Play

Presenters include:

Allen County Bomb Squad,

Shawnee Twp. Fire Dept.,

Midwest Shooting Center,

Mental Health & Recovery Services Board,

Swartz Contracting & Emergency Services

MR IQ #K V#

Thursday, November 14, 2019

8:30 AM - 2 :00 PM

Place: Howard Johnson Hotel

1920 Roschman Ave.

Lima, Ohio 45804

LUNCH INCLUDED

$10 / person at registration

Register at: https://bit.ly/TTechTDCMS

Certificate of Continuing Professional Education Units available upon request

Lima / Allen County CHAMBER of Commerce

Tomorrow's TECHNOLOGY Today

2nd Annual Disaster & Crisis Management Symposium