



CYBER Safety Tips

KEEPING YOU, YOUR FAMILY & THE COUNTY SAFE

Presented by Summit County OIT

THE OFFICE OF INFORMATION TECHNOLOGY

County of Summit - Stephen Byrne, CIO

IT Support - (330) 643-2013

In Office x2013

ServiceNow Self Service Portal

<http://snow.summitoh.net>

- ▶ Primary Presenter:
Matthew McVey
- ▶ Deputy Director of IT – Security
- ▶ Email: mmcvey@summitoh.net
- ▶ Phone: (330) 643-5039



Best Practices and Scope

- ▶ Focus will be primarily on current trends and the potential and known threats related to them
- ▶ What you can do to protect yourself and your family
- ▶ Best practices for using social media platforms and current “trends”
- ▶ How you can “spot” or predict future threats and trends to be ahead of the game
- ▶ Preparing vs. Scaring
 - ▶ There is a fine line here, and we are trying to prepare you and educate you on situations, behavior and patterns to look for Not scare the daylights out of you

Where there is an opportunity to run a scam... it will happen

- ▶ Bad actors (hackers, scammers) will use tried and true methods to develop their social engineering schemes
 - ▶ Exploiting using many different techniques

Exploitation of Technological Vulnerabilities

- ▶ Keep your devices up to date with security patches, operating system upgrades etc.
- ▶ Most of the time the Operating System like Windows, Mac, iOS, Android will notify you that there is an update available
 - ▶ Best to check on your own periodically
- ▶ There is a difference between UPDATES, and UPGRADES.....
 - ▶ A major difference – be aware

Exploitation of Sociological Vulnerabilities

- ▶ As mentioned, where a scam can be created, it will be
 - Bad Actors will create phishing email campaigns and fake call centers to solicit donations for anything that is going on in the news
- ▶ COVID19
- ▶ Economic Relief
- ▶ Student Loans
- ▶ Disaster Situations –terrible events of that day in September 2001
- ▶ And so on.....

Exploitation of Psychological Vulnerabilities

- ▶ Bad actors will also take advantage of “The Human Condition”
- ▶ Playing on emotions, financial situations, create fear and urgency
 - ▶ Emails – you have won....
 - ▶ This is not just based in email phishing campaigns
 - ▶ Game Downloads, Social Media Apps, Dating Apps etc. This is how they harvest data and interest to target at a more personal level – BOTS come into play here, and can assist with direct target attacks such as acting as an imposter CEO or company decision maker, or even government official

Social Media – Danger Will Robinson

- ▶ Not just a separate “app” or website any longer – has been integrated into our lives whether we like it or not
- ▶ Facebook
- ▶ Instagram (owned by Facebook)
- ▶ WhatsApp (also owned by Facebook)

Anyone seeing a pattern here?

CHECK YOUR PRIVACY AND SECURITY SETTINGS in EACH APP they do not carry over

Search engine indexing

Content Availability – which Audience – Facebook defaults to EVERYONE can view EVERYTHING. Same holds true for the others.


Be mindful of WHAT you share and WHEN you share it

Facebook Contributions Continued

- ▶ Regardless of how they claim to be “socially responsible” and have independent “fact finders” working tirelessly for them checking posts etc..... The fact is they have their own agenda
- ▶ Everything you say or do, can and will be used against you – sound familiar?
- ▶ Social media of all flavors is a double-edged sword

Facebook ads push new Ov3r_Stealer password-stealing malware
Mr. Kevin Hodges Just shared this with me this morning.....



- 
- ▶ A new password-stealing malware named Ov3r_Stealer is spreading through fake job advertisements on Facebook, aiming to steal account credentials and cryptocurrency.
 - ▶ The fake job ads are for management positions and lead users to a Discord URL where a PowerShell script downloads the malware payload from a GitHub repository.
 - ▶ Analysts at Trustwave who discovered the malware campaign note that although none of its tactics are novel, it remains a severe threat to many potential victims, given Facebook's popularity as a social media platform.

Source - <https://www.bleepingcomputer.com/news/security/facebook-ads-push-new-ov3r-stealer-password-stealing-malware/>

Bad Actor Common Mistakes

- ▶ Most of the time we can spot the bad emails by terrible grammar, usually caused by cultural barriers etc.
- ▶ Looks like a child composed the email
- ▶ Links and email addresses that are similar are ridiculously long, spoof a legit website like www.microsoft.com , those are ZERO's instead of the letter "o" and it is a scam website
- ▶ Watch out for .ru , .cz , .ch and so on at the very end of an email address or website – not picking on anyone just stating a summary of statistical facts of the origin for most of these

Bad Actor Career Advancement Opportunities

- ▶ Bad actors have a chance now to become an “A” List actor with the help of AI
 - ▶ AI is the next coolest thing, and also the next biggest threat
 - ▶ Image and link creation – copyright infringement
 - ▶ Pulling Actual websites and images to trick you into a malicious connection
- AND IT looks identical – Same concepts, always inspect the link
- Deep Fakes – images and videos – progression of AI engines and sites is unprecedented. ChatGPT is growing at an astounding rate

QR Codes are cool But.....

- ▶ They can also be used to embed content, just like an email link to a malicious website or file download
- ▶ All around us, Just pull out your phone and point your camera.....
 - ▶ Be mindful, these are graphical representations of many different things
 - ▶ Can be a website, can be a picture, a document, a malicious file etc.
 - ▶ Consider the source – a lot of restaurants now are eliminating their physical menus altogether and having you scan a QR code embedded or taped to the table instead – just adds to the stellar customer service of today's age 😊

Placements all over

- ▶ I PROMISE THIS ONE IS SAFE if you would like to try it out



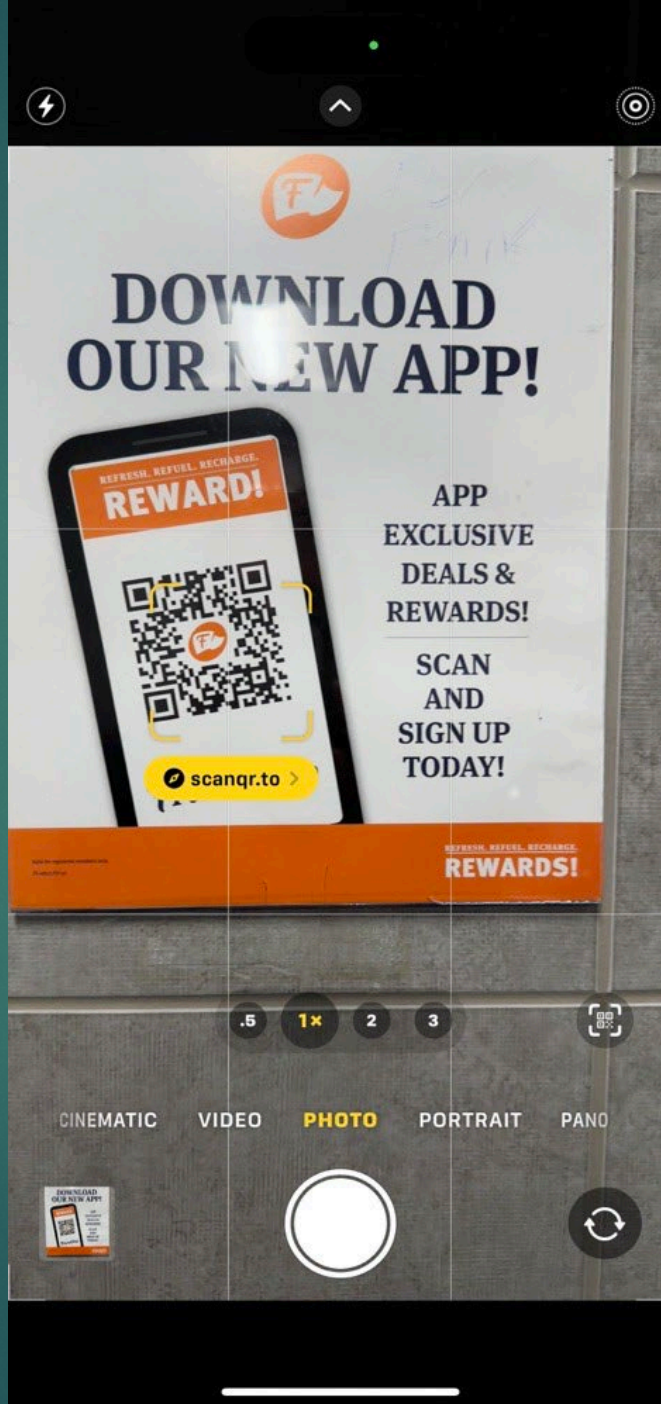
DOWNLOAD OUR NEW APP!



APP
EXCLUSIVE
DEALS &
REWARDS!

SCAN
AND
SIGN UP
TODAY!

REFRESH. REFUEL. RECHARGE.
REWARDS!



QR Codes Continued

- ▶ The previous example is designed to take you to the app store to download their app.
- ▶ The first picture is of the marketing materials as it hangs on the wall
- ▶ The second is screenshot of my camera, where my phone displays the website that the QR code will connect me to IF I tap on it.
- ▶ After tapping on it, it takes you through a couple websites (of course for tracking and marketing purposes) and then tries to open up the respective app store to download.
- ▶ As mentioned previously, QR codes can be a representation for many different types of actions

Telephone Scams

- ▶ Register your phone numbers at www.donotcall.gov
 - ▶ ANY REPUTABLE business, will HONOR the do not call database
 - ▶ It's sad to say but any phone call you get anymore from a "call center" such as a credit card, bank etc. has a 99.99999% likelihood of a scam
 - ▶ Watch out for emails that look legit, NO OBVIOUS suspicious links, but want you to call a phone number.....
 - ▶ Always have the company verify their identity – it's a two way street
 - ▶ Don't give up the farm.... If it looks like a scam.... Smells like a scam...
Well, you get the picture
- Use an app like RoboKiller, or other spam filtering (subscription but worth it)

Safeguarding Accounts like email etc.

- ▶ Turn on 2 Step authentication for all of your email and online accounts that support this security function
- ▶ Use a third-party authenticator such as Microsoft Authenticator, Authy, Google Authenticator, there is no shortage
- ▶ Allows you to verify login and devices by sending a code to an alternative email address or device or an authenticator app
 - ▶ Gmail – go into user dashboard/account settings
 - ▶ Other email account settings for this can be accessed in a similar fashion i.e. Yahoo, Outlook personal accounts (yes Hotmail is still around too)

Make sure to enable 2 factor authentication especially on accounts that are tied into your mobile devices.

For example, if you have an iphone make sure this is enabled for the email account you use for iCloud and App store etc (same account)

On Android devices the main email account you set your phone up with (the account that is tied into the Google Play Store) needs to have 2 step authentication enabled as well.

There are so many topics....

- ▶ We don't have enough time to discuss all of the topics and arenas of cybersecurity do's and don'ts BUT I welcome you to reach out to me with any further questions that you may have about today's presentation or any other related questions you may have.
- ▶ I know that many of you may have questions that you don't know quite who to ask or where to find unbiased or unsolicited answers and advice.
- ▶ I don't know everything, but I will do my best to answer your questions completely or provide you with the resources or contacts that you are looking for

Email me or message via Microsoft Teams

mmcvey@summitoh.net

Put 2024 L&L in the subject line of your email

Summary

- ▶ We all play a role in network security and preventing data leaks and cyber attacks. Security awareness and critical thinking are key.
- ▶ Visit training.knowbe4.com and login using your email address for material related to this webinar, as well as further courses and content to learn more about Cybersecurity
- ▶ If you have any questions regarding this presentation or would like more info please feel free to contact me via Microsoft Teams or via email at mmcvey@summitoh.net
Put 2024 L&L in the subject line of your email
- ▶ If you have any immediate security concerns please contact the OIT Support Desk @ (330) 643-2013 or submit the help forms for incidents or requests at <https://snow.summitoh.net>

Links discussed and participant requested information

- ▶ <https://training.knowbe4.com> Login for our County Training platform and optional additional Cybersecurity training and knowledge base
- ▶ www.protonvpn.com VPN Client as discussed for all device platforms (will not be accessible if connecting from inside county network) Will need to be downloaded from home or on another network for your personal devices
- ▶ <https://www.robokiller.com/> Spam call filtering app for iPhone and Android – monthly subscription fee
- ▶ Facebook Privacy Settings – great video – need to perform this from a FULL computer and not your phone. Once settings are changed, they will be applied to the Facebook app on your mobile device because it is the same ACCOUNT
<https://www.youtube.com/watch?v=KBdFF2Bm5jg>