STAYING SAFE ON THE INTERNET

Sherry Garvin, Partner, Fortium Partners
May 13, 2024

DISCLAIMER:

THIS PRESENTATION IS NOT INTENDED FOR MARKETING FORTIUM PARTNERS, LP SERVICES AND SHOULD NOT BE CONSIDERED PROFESSIONAL CONSULTING ADVICE TO YOU ON BEHALF OF FORTIUM PARTNERS, LP

AGENDA

WHAT'S IN

- PROTECT YOUR IDENTITY AND INFORMATION
- IMPROVE YOUR SECURITY AWARENESS
- SECURE YOUR DEVICES AND HOME NETWORKS

WHAT'S NOT

- EVERY POSSIBLE CYBER THREAT SCENARIO
- DELUSIONAL HOPE OF ELIMINATING ALL CYBER THREATS
- DETAILS ABOUT SPECIFIC TECHNOLOGY SOLUTIONS

WHY DO YOU USE THE INTERNET?

- Email communications
- Manage bank accounts and finances; pay bills
- E-commerce: purchase products, services, etc.
- Manage club membership and activities
- Research using internet browsers to access online resources
- Social media
- Maps, travel routes, public transportation

HAVE FUN AND MAKE GOOD CHOICES

INFORMATION

- Where is your information stored: on your device and/or in the cloud?
- What's most important to keep and have access to?
- Who else has access to it?

DEVICES/NETWORKS

- What device(s) do you typically use?
- Who else uses those devices?
- How are the devices updated and configured?
- What networks do you use?
- Who else is using the network?

EMAIL

- Avoid using Internet Service Provider (ISP) email accounts (e.g. astound.net, mygrande.net, etc.)
- Use/create email accounts using MS Office (outlook.com), Google (gmail.com), or Apple (icloud.com)
- Use a strong password and multifactor authentication where possible
- Learn to recognize spoofing and phishing
- **STOP AND THINK BEFORE YOU CLICK!**
- **ASK YOURSELF**
  - Urgency
  - Relevancy
  - Expected
- **HOVER**

PASSWORDS

- DON’T REUSE THEM!
- Don’t “Remember” or “Save for Later” on the login screen
- Make them complicated (strong)
  - Use lengthy phrases substituting numbers and special characters for letters
  - 8-12 characters
  - Generate them using a password management application 
- Change them if you suspect they have been compromised

WHY USE A PASSWORD MANAGEMENT TOOL?

- Store account and password information in an encrypted “vault” on your device and synched in the cloud
- Generate complex passwords and store PINs, codes, and other information needed to access accounts
- Safely share account record information with other family members
- Use biometrics or a complex master password to open application
- Copy/paste from the password application to login on the online site
- Consider Keeper, 1Password, Dashlane (some have free versions)

KEEPER 1Password DASHLANE

MULTIFACTOR OR 2-FACTOR AUTHENTICATION

- Something you **know** and something you **have**
  - "Know" your password
  - "Have" a one-time code sent to you phone via text OR authenticator application
- Use whenever possible! Especially when banking or financial transactions are involved.
- SMS (texts) have the potential of being initiated by a threat actor and are less secure than using an authenticator application but many banks and credit card companies only offer SMS solutions.
- Example of "man in the middle" attack.

THREAT ACTOR METHODS

SPOOFING:

- **Threat actor sends a message purporting to be someone you may know or trust.**
- **The “from” address may or may not appear to be the person’s real email address.**
- **Threat actor may use realistic logos and the message may be familiar or believable based on your past interactions with that person or company.**
- **Hover over “FROM” email address. Does that appear to be legitimate?**

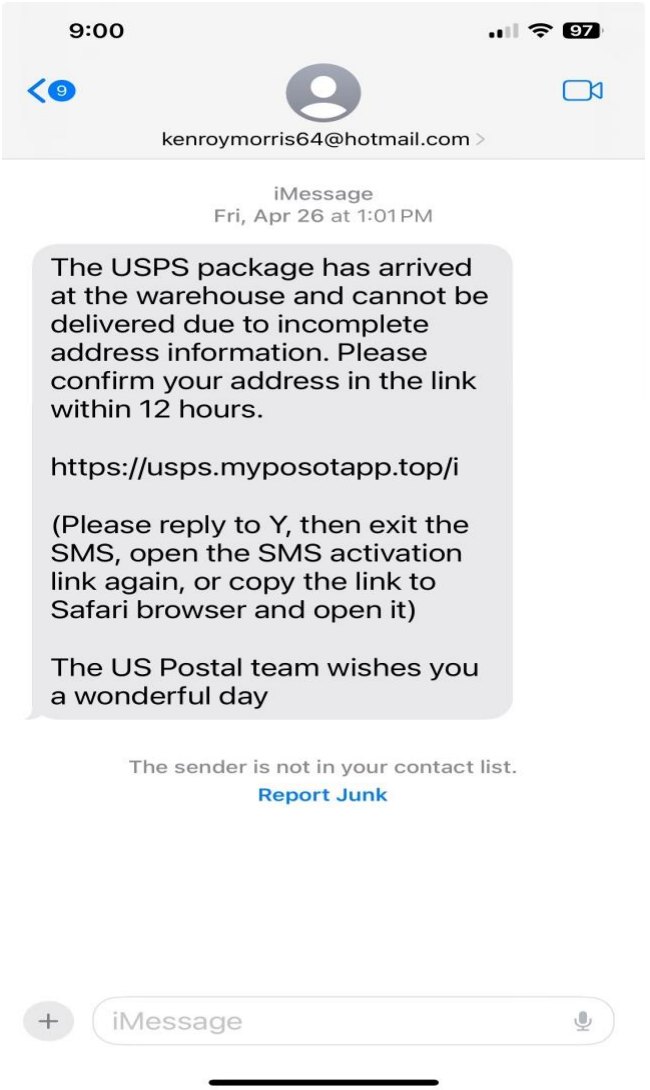
PHISHING:

- **Threat actor sends email seeking action or information.**
- **May spoof a known identity’s real name and/or real email address.**
- **Asks you to click on a link, take an action, or respond with information.**
- **Should I be receiving an email from this person with this type of request?**

EXAMPLES

EMAIL

TEXT



STOP AND THINK

- ✓ **Is this request or a response to the email really urgent?**
- ✓ **Is it from a legitimate source? Hover over “FROM” email address. Does that appear to be legitimate?**
- ✓ **Should I be receiving an email or text from this person with this type of request?**
- ✓ **If it is supposedly a friend or family asking to click on a link, attachment or take an action, reach out to contact outside of email (call or text them) to confirm legitimacy.**
- ✓ **Avoid clicking on links or opening unexpected attachments particularly when communication is branded with a social networking site logo.**

PHONE CALLS, CREDIT CARDS, AND PAYMENTS

- Don’t answer the phone if the number coming in is not in your contacts, even if there is an individual’s name showing up.
- Legitimate callers will leave a message.
- If you answer the phone and it is a recorded message asking you questions to answer with your voice, hang up
- Bankers, financial or technology service providers will not call to ask you for your account information, passwords, etc.
- If someone does call you requesting information, **end the call and call back** using a phone number shown on your account.
- If you receive a text from your credit card about fraudulent charges, you can respond Y or N as to whether they are legitimate but don’t click on any other links. Then call the number on your credit card.
- Recommend using credit cards rather than debit cards.
- Zelle and ApplePay are more secure electronic payment options.
- NEVER allow someone you don’t know to “remote in” to your computer.

A FEW NOTES ABOUT MAIL, PACKAGE DELIVERY AND ELECTRONIC SIGNATURE SERVICES

- Opt-in for “all electronic” communication for banking, credit card and financial services statements and correspondence.
- Ensure physical/email addresses and phone numbers are accurate on online accounts.
- What’s most important to keep and have physical access to?
- Who else should have access to it?

- UPS, USPS, and FEDEX notifications are frequently (and successfully) spoofed.
- If you expect a package and are receiving a notification, go to the delivery service web site and manually enter tracking number.
- Docusign and other electronic signature sites are frequently spoofed. If you can’t tell where it is sourced or who is requesting it ignore it.

SOCIAL MEDIA

- Social media is a trolling ground for threat actors. They use the information they find here to crack passwords, launch spoofing emails and texts, and make robocalls. They also put links to ransomware on social media.
- **Think carefully before posting anything on a social media account!**
- Don’t post while traveling – wait until you get back.
- If it sounds too good to be true, it probably is.
- Enable multifactor authentication, wherever available.
- Be vigilant of connection requests, even established connections to family or friends in your network.
- Exercise caution when clicking on links sent by email, especially shortened URLS when on a social networking site. Instead, go to a new tab and type in the name of the site into the address bar; don’t cut and paste the URL.
- Maintain familiarity with privacy filters and rules to know how your content is being shared. Set privacy filters to highest levels (e.g. functional only).

ANTIVIRUS AND OTHER PROTECTIONS

Spam filtering

- Depends on browser, email service
- Check junk folders and mark as junk if they come to regular inbox

Antivirus

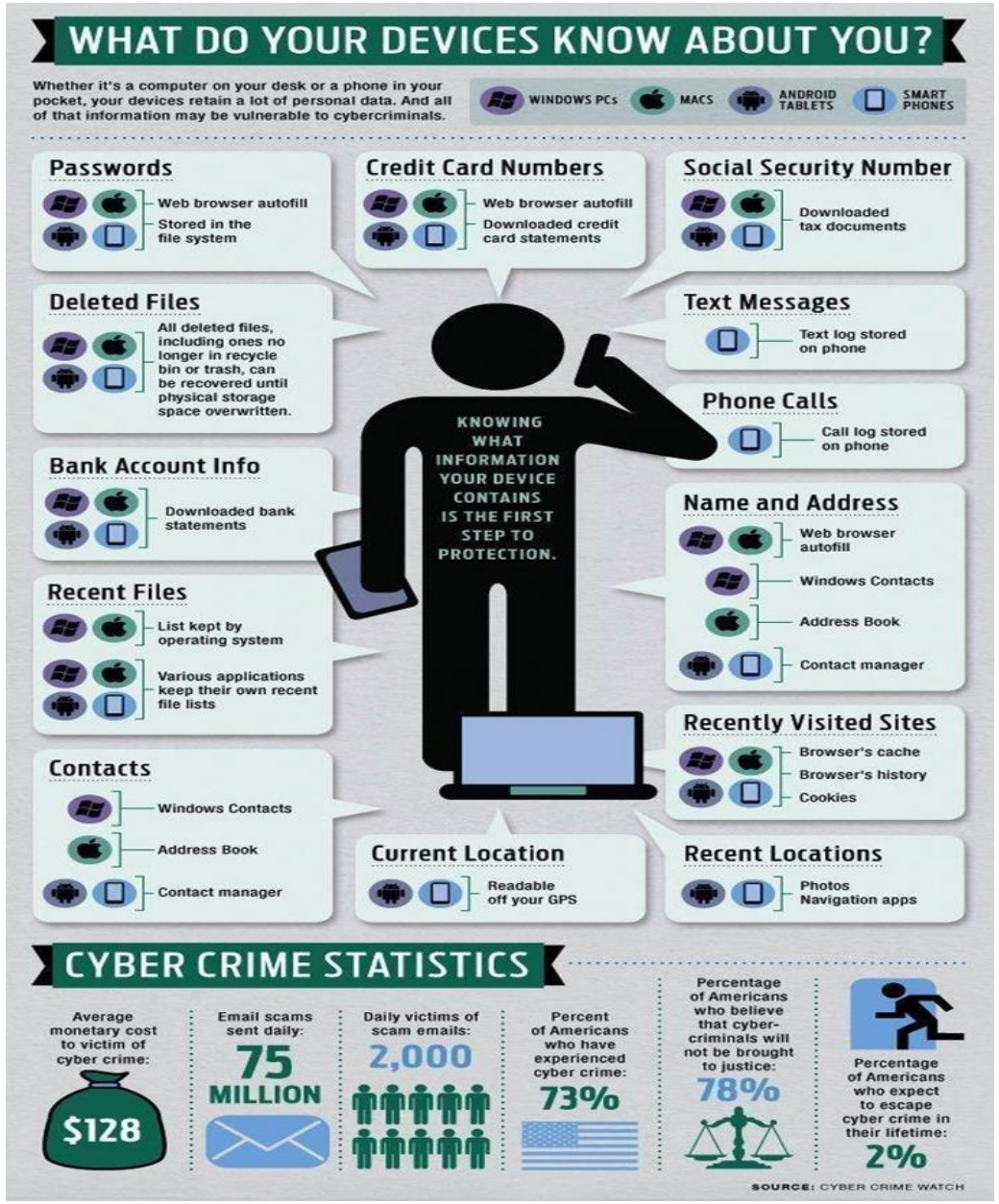
- Often comes with operating system (e.g. Microsoft Defender)
- Can be purchased separately – suggest avoiding Kapersky products

Malware protection

- Often comes with the operating system; allow and initiate security scans on a regular basis

Backup and recovery

- Cloud back up and synchronization frequency should align with usage.
- Make sure mobile device is being backed up to the cloud
- May back up to external drive but scan data first (photos, etc.)
- If hard drive/device fails or is encrypted, how do you expect to restore data.



SECURING YOUR DEVICE(S)

Phone, tablet or laptop:

- Use at least a 6-digit password and facial recognition, if available.
- Protections when phone is out of sight or someone can watch over you shoulder (Steve)
- Set the device to lock (requiring password or biometric) after 1-2 minutes.
- Default applications to not allow access to camera, sound recognition, and voice.
- Personal choice is to not listen for Siri.
- Frequently (daily-weekly) shut down and restart the device. Different than putting it in sleep mode!
- Keep your devices updated and patched! These are typically in response to identified vulnerabilities in the operating systems running on the device.

CONNECTING (SECURELY) TO THE NETWORK

At Home

- Change default passwords on routers and switches; make passwords lengthy and complicated – at least 16 characters.
- Store network passwords in your password management application.
- Use sub-networks to separate network traffic
    1) regular use for banking, bill pay, etc. (like an internal intercom)
    2) guest network for visitors or to “surf” the internet (like a phone number)
    3) Internet of Thing (IOT) device connection to the internet (cameras, oven, refrigerator, etc.) (robot intercom)

While Away

- Use a personal virtual private network (VPN) application when connecting to public, unsecured networks in hotels, restaurants/coffee shops, libraries, etc. This encrypts information that would typically be transmitted “in the clear”.
- Unfortunately, there are some banks, financial institutions and credit card company applications that won’t work when a VPN is turned on; the application or site is likely encrypting the interaction.

FILE DOWNLOAD AND PROTECTION

- Know where your stuff is: get familiar with the file manager that comes with your operating system. Organize in a logical way and be aware of who you may be sharing files with.
- If it were in a drawer, you would need to clean it out from time to time. It's in a virtual drawer, so clean it out from time to time.
- Don't send Personally Identifiable Information (PII) or payment card information via email. If you store pictures or this type of information, **at least** password protect the file.
- Use encrypted file vault and communication encryption options offered by your financial planner, bank, or other service to exchange information.

QUESTIONS?

214-562-5886

sherry.garvin@outlook.com