AHA! AT HOME IN ALEXANDRIA

Tuesday Tech Talk - October 30, 2018
Guarding Your Privacy Online

GENERAL ONLINE SAFETY MEASURES

- Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with.
- Install a password manager - Consider using a master password system like LastPass, DashLane, Keepass or 1Password to enhance your password security. These programs store all of your passwords in an encrypted vault that can only be opened by a master password you create and only you know. Free versions allow you to set that one master password and then it creates long, hard passwords for each site you visit (that requires a password). Pay versions offer more options like digital wallet, secure notes, etc.
- If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.
- Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. AHA volunteers can help with this.
- Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.
- Encrypt your data to keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.
- Keep Passwords Private - Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your

password. Substitute numbers for some words or letters. For example, “I want to see the Pacific Ocean” could become 1W2CtPo.

- Secure Your Social Security Number - Keep a close hold on your Social Security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN, ask:
    - why they need it
    - how it will be used
    - how they will protect it
    - what happens if you don’t share the number

  The decision to share is yours. A business may not provide you with a service or benefit if you don’t provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

- Use Security Software – Your computer may have Windows Defender or other anti-virus/spying/malware software. If not, these and a firewall are necessary. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs. AHA volunteers can help you with this.
- Avoid Phishing Emails - Phishing is when someone poses as a legitimate business to trick consumers into divulging information. Don’t open files, click on links, or download programs sent by strangers **or a company sending something you weren’t expecting**. Opening a file could expose your system to a computer virus or spyware that captures your passwords or other information you type. **Make the call if you’re not sure.** Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email. Check any links’ safety with www.sitecheck.sucuri.net or www.urlvoid.com. First, hover over the suspicious link and the full address will appear in the bottom corner of your browser; right-click to access the drop-down menu, and select Copy Link. Now paste the URL into your link checker to get a report. Foolproof? No. A good hint if there's a problem? Yes.
- Report phishing emails and texts - Forward phishing emails to spam@uce.gov – and to the organization impersonated in the email. You can also help others if you:

    - File a report with the Federal Trade Commission at FTC.gov/complaint.
    - Visit Identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.
    - You can also report phishing email to reportphishing@apwg.org. The Anti-Phishing Working Group – which includes ISPs, security vendors, financial institutions and law enforcement agencies – uses these reports to fight phishing.

- Be Wise About Wi-Fi - Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected. Most public wifi systems are not protected if you don't have to login in with a password.
- Lock Up Your Laptop - Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.
- Turn on two-factor authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised. As an extra precaution, you may want to choose more than one type of second authentication (e.g. a PIN) in case your primary method (such as a phone) is unavailable.
- Back up your files to an external hard drive or cloud storage. Back up your files regularly to protect yourself against viruses or a ransomware attack.
- Turn on Automatic Updates - According to security professionals surveyed last year by Google, the most critical step you can take to boost security is to keep your operating system and other software up to date. Make sure you have auto-updates turned on across the board.
    - Windows: Search Windows Updates/View Update History to see when last updated. Go to Advanced Options to set update parameters.
- Use Screen Locks on Every Device - Set a password or PIN for every laptop, smartphone, and tablet you own. Any lost device without a screen lock is an unprotected gateway for thieves, who may be able to access your email and banking and social accounts, changing passwords and taking control of your digital life. Use a screen lock that's at least six characters long. And avoid easy-to-guess passwords, such as a birthdate or your phone number.

- Check Your Data-Breach Status - Wondering whether your personal data has been stolen and posted for sale on the web? At www.haveibeenpwned.com, you can check your email addresses and user names against lists from 120 known breaches at companies including Adobe, LinkedIn, and Snapchat. (You'll need to register to check the full database.) If your name pops up, change the password for the compromised account and any other site where—tut, tut—you were using the same password. (Bonus tip: Pros pronounce “pwned” as “poned,” not “pawned.”)
- Use Temporary Email Addresses - You’re often asked for an email address to access a website or to sign up for a loyalty card, even if you want to use the service just once. Comply and you may be in for years of marketing come-ons. “Everyone wants your email address these days,” says Nathan White, senior legislative manager at Access Now, a digital-rights organization. But you don’t have to provide a real one. White recommends www.10minutemail.com, where you can get a functional email address for 10 minutes (or 20, if you need it), just long enough for you to log on to a site. When the time is up, the email address self-destructs—and 10minutemail.com doesn’t retain any personal data.
- Cover Your Laptop Webcam - Malicious actors have repeatedly proven that they can turn on a laptop’s camera without the user’s knowledge. The simplest solution? Do what Facebook CEO Mark Zuckerberg and FBI director James Comey do—put a piece of tape or a Post-it note over it. Hackers haven’t yet cracked the adhesive code.
- Use the HTTPS Everywhere Browser Extension - When you see “https” and a green padlock alongside a URL in your browser’s address bar, it means that the data is encrypted as it travels back and forth between the website and your computer. (The “s” stands for “secure.”) Some sites that support https use it inconsistently. Add the HTTPS Everywhere browser extension, which you can download from the Electronic Frontier Foundation, and your connections will be encrypted anytime you connect to a website that supports https. It works with the Chrome, Firefox, and Opera browsers.
- Use separate browsers for high-stakes and low-stakes websites. If you use Google Chrome for general internet browsing and Opera/Firefox solely for purchases and banking, then anyone intruding through your general browsing will not “see” the activities on the other browser.
- Recognize “click bait” and don’t take the bait. If you see a story that interests you, go to Google and search for it through a reputable site.
- See Who Shared Your Private Data - Sometimes you need to register for a website with your real email address, say, if you plan to log in repeatedly to make purchases. Here’s a neat hack for ferreting out which companies are sharing your data with email lists, if you have a Gmail account: Type “+” before the @ symbol and add the website’s name. Email addressed to

YourName+Websitename.com@gmail.com will go to the regular inbox for YourName@gmail.com. But now it will carry an extra crumb of data, and if you get spam from a company you've never heard of, you'll know whom to blame.

- Websites popups may ask whether to "show notifications" – do not allow – block.
- Back up your data on a regular schedule – should you ever be hacked or your computer fail, you'll have key data/photos/etc. back up on an external hard drive or in "the cloud" via Google Drive or Dropbox.

On Your Phone

- LOCK YOUR PHONE – set up a pin or password under settings. It's a tiny inconvenience that you will appreciate if you you're your phone or its stolen. You
- Remove old Wifi connection options:
    - Samsung – Connections/wi-fi/advanced/manage networks – delete old wifi options
    - IPhone/Ipad – go into General Settings/Reset Network Settings and delete all at once.
- Watch Your Bills - Many wireless plans are based on a flat rate, so make sure your bill is consistent from month to month. If it's not, take a closer look at your account.
- Turn Off Location Tracking in Apps - Many mobile apps can extract your whereabouts from your phone. In the case of a restaurant-recommendation service or Uber, that makes sense. But there's no reason to share your location data with many other companies that won't use the information to provide you with any obvious benefits. You can selectively decide whether individual apps can access that data. On iPhones, go to Settings, then Privacy, then Location Services. Now scroll down to any app to control if and when it can access your location. You can do the same on any Android phone running a recent version of the operating system (6.0 Marshmallow or later). Go to Settings, then Application Manager, and tap on the specific app you want to adjust. Next, tap on Permissions to access the location setting.
- Be mindful of every app you install - Each time you install an app, it will ask you for permissions to your phone's features or data, like your contacts, photos, camera, or even the phone dialer itself. Be mindful of apps that you install, as a single rogue app can punch a hole in your privacy protections.
- Use your phone's data for better security – If you need a secure network, you should use your phone's data -- such as 4G or LTE -- or use your phone as a hotspot for your computer. It's far better to use your phone's data plan for anything important than using insecure public Wi-Fi. You can usually find your hotspot option in iPhone's settings or Android's notification tray. Check your plan to ensure availability.

Iphone: Settings/Cellular/Personal Hotspot/turn on

Samsung: Settings/Connections/Mobile Hot Spot and Tethering/turn on

- Make sure mobile apps are updated. Security patches protect you.
- Want to know how much time you're spending online? Download App Usage and you can see how much time is spent on your device. The new iPhone 12 update includes a similar functionality.

Social Media

- Consider setting up a unique email just for social media accounts. This way any hack won't affect other aspects of our online presence.
- Use a different password for each social media account.
- Setup two-factor authentication on Facebook – Facebook/settings/security and login/two-factor authentication – this protects unauthorized logins since you would be notified when someone attempted to login from an unrecognized device.
- Setting up extra security – get alerts about unrecognized logins
- Go to Privacy/Privacy Settings and Tools to determine how much you want others to see. In Facebook:
    - Settings/Privacy/Your Activity and How People Find and Contact You
- Be selective with friend requests – don't accept if you don't know them or don't want them knowing more about you!
- Don't overshare. Post your photos *after* you're home from your trip, don't reveal home address or phone, etc. Remember, your friends can opt to "share" anything you post and you cannot control where that information goes.
- Close any social media accounts you are not using.
- Check what apps are connected to your social media. Do you use Facebook to sign in for other apps?
- Don't fall for fake news. Check the sources before you share.

Shopping

- **Check out as guest -** Nearly every online retailer will ask you to create an account before checkout. If you can check out as a "guest," you should. Using a guest account will keep a lot of your personal data off the company's servers and safe in the event of a hack.
- Every shopping site should have https:// and the lock symbol in the url to ensure the data is encrypted.

- If the site looks fishy, it's probably a scam. Shop known sites. Keep your receipts.
- Lose or misplace your credit card? Lock your credit card even if you think you just misplaced it. Better safe than sorry.
- Do not make purchases over public wifi. If you must, then make sure the wifi requires a password and has WPA2 AES encryption.
- Keep an eye on your bank account.
- Don't keep your pin with your credit card.
- If you get a phishing email from a retailer you don't know or use, don't fall for a great deal. And don't "unsubscribe" either. Mark the email as SPAM in your email client, which will remove it from your mailbox and block future emails.
- Surprisingly, major retailers like Amazon have dedicated mobile apps that are actually more secure than shopping on their website. But don't store your credit card information on your phone.
- Use credit card, not debit card, when shopping online. Credit cards allow you to dispute transactions more easily.

Internet of "Things"

- How connected do you need to be?

AND DON'T FORGET TO SECURE YOUR PAPERWORK *OFF-LINE*

1. Shred any documents that contain:

- Social Security number (even just last 4 digits)
- Birth date
- Credit card numbers
- Account numbers from financial institutions
- Medical insurance numbers

2. Shut Off the Flow of Credit Card Offers -These unsolicited mailings can be intercepted and filled out by identity thieves who have credit cards sent to their own addresses, then start piling up debt in your good name. You can put a stop to most of these offers by going to optoutprescreen.com or calling 888-567-8688. The service, run by the Consumer Credit Reporting Industry, will turn off the spigot permanently or for five years. You can always opt back in.

3. Stop ID Theft After a Death - Identity theft affects 2.5 million estates every year, according to the IRS. If a loved one has died, send a copy of the death certificate to the IRS (the funeral home may

help with that). Also, cancel any driver’s license, and notify credit agencies, banks, insurance firms, and financial institutions.

4. Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.

5. Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you are going to use your card at the doctor’s office.

6. Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.

7. Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don’t need them any longer.

8. Destroy the labels on prescription bottles before you throw them out. Don’t share your health plan information with anyone who offers free health services or products.

9. Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won’t be home for several days, request a vacation hold on your mail. When you order new checks, don’t have them mailed to your home, unless you have a secure mailbox with a lock.