TECH CAREGIVERS

CyberPatriot - AFA's National Youth Cyber Education Program

CyberPatriot's Tech Caregiver Program Training Course

In 2020, CyberPatriot and AT&T joined forces to create CyberGenerations, a program designed to help older individuals who need assistance understanding the safety risks of using mobile devices and computers. CyberGenerations offers a self-paced guide for interested seniors to review at their own convenience. Workshop resources are also available for those communities looking to hold a larger scale event on the topic of cybersecurity.

AT&T Cyber Aware
AT&T is dedicated to empowering Tech Caregivers with the tools necessary to have conversations and provide information about online safety. It can be overwhelming when considering where to begin with conversations about online privacy and security. But even the most basic security tips can still have a huge impact on preventing many scams, security breaches and thefts.

To help start those conversations, AT&T has created guides on how to talk to your loved-ones and friends about protecting themselves from internet threats. You will see examples of these throughout this training course.

The Importance of Tech Caregivers
As the world becomes increasingly dependent on technology, we must consider the importance of protecting and empowering those who may not possess the cyber skills to protect and empower themselves.

Tech Caregivers are people who provide cyber security support to those adults who are often vulnerable to cyber threats due to a lack of technological experience and knowledge. While many older Americans are tech savvy, others find some online activities and security measures to be confusing or intimidating. Tech Caregivers are trained to help individuals gain the confidence necessary to safely operate online by teaching basic security measures in a way that is easy to understand.

Becoming a Tech Caregiver
Through completion of a Tech Caregiver training course, which uses a combination of resources and guides provided by CyberPatriot and AT&T, participants may become a certified Tech Caregiver and start giving back to the senior citizens in their communities.

The general course outline can be found on the next page. At the end of the course, participants must complete a brief test. Those with passing grades will be issued a Tech Caregiver certificate.

Tech Caregiver Training Course Outline

Introduction to Cybersecurity

Cybersecurity: Definition and Importance

Cybersecurity is the protection of internet-connected systems – including hardware, software, and data – from cyberattacks.

Understanding the importance of cybersecurity is critical because:

- Cybercrime affects us all.
  - Cybercrime is one of the toughest challenges that the world is facing today.
  - Cybercrime is set to cost the world up to $6 trillion by 2021.
- We rely on computers, mobile devices, and the internet in our daily lives.
  - Even if you we don't use computers or phones regularly, a lot of our personal data is stored online or on computers and is at risk for being compromised.
- Poor understanding of cybersecurity can lead to your personal information being stolen.

Personally Identifiable Information

Personally Identifiable Information (PII) is any data that can be used to identify a particular person.

Examples of PII include, but are not limited to:

- First Name or Last Name
- Social Security Number
- Driver's License or State ID Card #
- Passport Number
- Credit Card Number
- Date of Birth
- Passwords / Security Answers
- Fingerprints
- Health Insurance Information
- Medical Records

If a company suffers a data breach, an important concern is whether or not the attackers have gained access to the personal data of the customers that do business with that company. Exposed PII can be sold on the dark web and used to commit identity theft, putting breach victims at risk.

That is why it's important to protect your PII and limit how often you share it, and who you share it with.

Data breaches are not the only way PII can be exploited. There are also physical ways in which a person can steal your information:

> *Dumpster diving:* The physical act of digging through garbage and discarded documents in search of passwords, account numbers, PIN numbers, or any other information that can be used to carry out a malicious cyberattacks or cybertheft.
>
> *Shoulder surfing:* The act of acquiring personal or private information through direct observation, such as looking over a person's shoulder to obtain vital information while the victim is unaware. This is most common in crowded places where a person uses a computer, smartphone, or ATM.

Basic Cybersecurity Practices for Web Browsers and Mobile Devices

Web Browser Safety

A ***web browser*** is a software application used for retrieving, presenting, and navigating information resources on the World Wide Web.

The web browser is the primary apparatus through which viruses enter the computer, but it can also be the first line of defense against computer viruses. The following internet browsers are recommended for safe browsing.

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Safari (macOS)
- Opera

When using a web browser, it is important to know these safety tips to help stay protected:

- Use pop-up blockers. Pop-up rules can be changed in a browser's "Settings" or "Options" menu.
- Look for the "S" after http in the web address (URL), indicating the website is secure.
- Look for a padlock in the address bar. The padlock indicates secure mode.
- Make sure automatic updates are turned on and working efficiently.
- Beware of using the autofill and built-in password management feature in your browser. Autofill fills in the fields on a form automatically, according to the information that the user has previously used.

Most web browsers will warn you if a website is not safe. Here are some common web browser safety symbols and what their meanings:

Connection to site is not secure

Information OR connection to site is not secure

Connection is secure

Warning OR connection to site is not secure

Connection to site is not private / not secure

Mobile Device Safety

Mobile devices are portable or handheld devices that have data or can connect to another device that has data. Common examples of mobile devices include:

- Smartphones (iPhone, Android, etc.)
- Smart Watches (Apple Watch, etc.)
- Laptops
- Tablets
- E-Readers
- Flash Drives

Because these devices can store and share data, it's important to keep them protected from cyberattacks. Tips on how to keep mobile devices secure include:

- Keep security software updated.
- Delete apps that you are no longer using.
- Disable Wi-Fi and Bluetooth when not in use, especially in public places.
- Make sure to use strong passwords to lock your devices.
- Think through what personal information you are allowing your apps to access.
- If an app appears sketchy, read the reviews and scan the privacy policy before installing it on your device.

- Log out of social media apps once you are done using them.

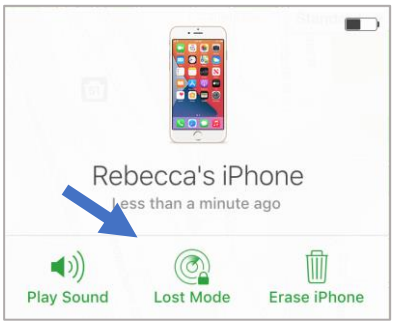
A big problem with mobile devices is that because they are portable, they are sometimes lost, misplaced, or stolen. If you lose a device (for example, a smartphone) there is a way to locate it, and more importantly, secure it while it's out of your possession.

How to turn on 'Find My' settings for iPhone or iPad

1. On your iPhone or iPad open the Settings app.
2. Tap your name.
3. Tap Find My.
4. Tap Find My [device], then turn on Find My [device].
5. To see your device even when it's offline, turn on Enable Offline Finding. To have the location of your device sent to Apple when the battery is low, turn on Send Last Location.
6. If you want to be able to find your lost device on a map, make sure that Location Services is turned on. To do this, go to Settings > Privacy > Location Services, and turn on location services.

How to locate iPhone or iPad if lost or stolen

1. In a web browser, sign-in to www.icloud.com/find using your Apple ID and password.
2. Click All Devices. Select the device you want to locate. The name of the device appears in the center of the toolbar.
    a. *If the device can be located:* it appears on the map so you can see where it is.**
    b. *If the device cannot be located:* you see Offline under the device's name. The last known location is displayed for up to 24 hours. Select "Notify me when found" to get an email when it is located again.**



** If you are concerned about somebody accessing the information on your phone, put your phone in Lost Mode. Lost Mode lets you lock your device so that others cannot access your personal information. It also allows you to display a custom message on your device screen. For example, you may want to indicate that the device is lost or how to contact you.

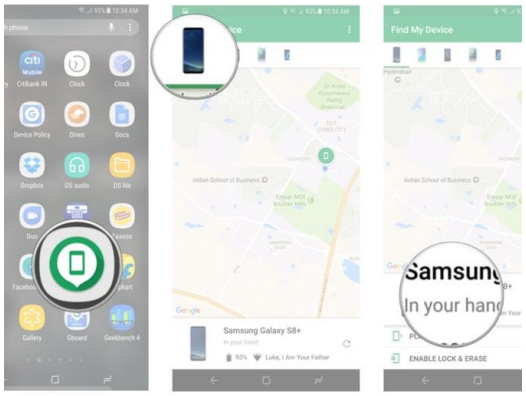
How to enable 'Find My Device' for Android

Find My Device should be installed out of the box on most recent phones, but you can manually download it from the Play Store.

1. Open Play Store from your home screen or app drawer.
2. Search for Find My Device.
3. Tap the three dots next to the first search result and select Install.
4. After installation, sign-in to Find My Device from your Google account.

How to locate Android if lost or stolen

1. In a web browser, sign-in to the Find My Device website (www.google.com/android/find) using the Google account that was used to set up the device.
2. Check if your device is visible.
3. If visible, choose what action to take:
    a. Play sound: Rings your device at full volume for 5 minutes, even if it's set to silent or vibrate.
    b. Lock: Locks your device with your PIN, pattern, or password.
    c. Erase: Permanently deletes all data on your device.



Tech Caregiver Q&A

Possible questions to participants

- *How often do you browse the internet?*
- *What do you use the internet for?*
- *Do you own a smart phone or tablet?*
- *Have you ever had your data stolen?*

Possible questions from participants

- *Why does cybersecurity matter?*
- *What web browser should I use?*
- *How do I know if a website is safe?*
- *What happens if I lose my phone?*

Lesson 1: Passwords

Passwords: Definition and Importance

Passwords are secret words or phrases that must be used to gain admission to something. Passwords are strings of characters, words, or phrases that are used to verify the identity of the user. In some cases, passwords can also be a biometric (fingerprint or facial recognition) that grants the user access to the secured information.

Passwords are important to keep personal information and data private, secure and to prevent cyber theft and its consequences. Passwords are often the only thing standing between cyber criminals and access to sensitive/personal data.

Understanding the importance of passwords is critical because:

- Passwords are the first line of defense.
    - A strong password prevents hackers from stealing your personal information.
    - If you do not choose a strong password, a cyber breach can allow hackers to access your banking information, social media accounts, medical records, or other sensitive information.
    - Weak passwords can lead to identity theft.

Password Creation: Strengths and Strategies

Most passwords are required to be a minimum length and must contain a variety of character types, as specified by the specific system for which you are creating the password. The system will not accept the password if it does not meet the specified criteria.

Strengths

Strong passwords are more difficult to guess by hackers, and less likely to be cracked with code cracking software. Strong passwords have:

- A variety of different characters
  - Letters (both lowercase and UPPERCASE)
  - Numbers (1, 2, 3, 4, etc.)
  - Symbols (&, @, $, %, !, ?)
- Length
  - Passwords should be at the very least 8 characters, but 10+ characters is recommended
- Complexity
  - Something that is easy for you to remember but difficult for others to guess

Good Password Examples

L3mon@d3
123Green456#
IamGr00t!!!
Viking@84
J@n$m1tH

Bad Password Examples

password
123456
abc123
letmein
JohnSmith

Strategies

When creating passwords, it can sometimes be difficult to come up with unique and complex that others will not guess, but that you can easily remember. It might be tempting to use the same password for all your accounts but doing so means that a breach in one account could lead to a breach in all accounts. Luckily, there are several methods you can use to create unique and secure passwords that are easily remembered.

1. **Biometrics:** Some passwords are not words at all, but rather biometric recognition. ***Biometric recognition*** is an information system that allows the identification of a person based on some of their main physiological and behavioral characteristics, such as facial features or fingerprints. Mobile devices are using facial and fingerprint recognition as an alternative to access the device. This is an easy way to keep your device secure. If the device cannot recognize you by your biometric, it will ask for a passcode or password.

2. **Base Passwords:** To help keep track of various passwords, start with a base password and then add an abbreviation to the beginning or end that will remind you what account it is for. For example:

Example	[base password]	[site]	New Password
Gmail	[Coconut!35$]	[GMA]	Coconut!35$GMA
Facebook	[Coconut!35$]	[FAC]	Coconut!35$FAC

3. **Passphrases:** We often use the term ‘password,’ but a passphrase is really what we should be using. A ***passphrase*** is a password composed of a sentence or a combination of words. Adding complex characters like symbols or numbers to a passphrase make it more secure – and to help you remember it, you can use a phrase that has some significance or meaning to you.

Where’s the Beef [phrase]	➡	**WhrsD@B33f?** [passphrase]

4. **Two-factor Authentication (2FA): *Two-factor authentication*** is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

   Two Factor Authentication requires the user to have two out of three types of credentials before being able to access an account:

   - Something you know, such as a personal identification number (PIN), password or a pattern
   - Something you have, such as an ATM card, phone, or fob
   - Something you are, such as a biometric like a fingerprint or voice print

   Example: You want to purchase a cooking app on your iPad. You go to the App Store, find the app and select purchase. Apple asks you to enter your password. You enter it successfully, but Apple also ask you to enter a code that was sent to your iPhone to verify you are the person that entered your Apple password to purchase the cooking app.

   Some websites use two-factor authentication as their standard log-in procedure, but other sites allow you to opt-in or opt-out of two-factor authentication. It is recommended that you opt-in. This can be done in most account settings. If you are concerned about having extra security beyond your password, two-factor authentication is recommended.

Managing Passwords

Despite the various strategies that help us create and remember passwords, it can still be overwhelming trying to remember passwords and usernames for the many accounts (social media, banking, healthcare, online retail, email, etc.) that you access throughout the year. Forgetting passwords can be frustrating, but there are tools available for helping us manage our passwords, some better than others. Read on to learn more about which tools to use and which to avoid when possible.

Autofill and Saves Passwords

Most web browsers have their own systems for storing passwords and other personal information typically used when filling out online forms. While it is convenient to have that information stored directly in the browser, it is not necessarily safe.

It is important to ***turn off your browser's 'remember password and autofill information'*** *settings*. This is typically done from the browser's settings, under a 'privacy' or 'passwords and forms' section.

Password Management Systems

A ***password management system*** is a software application that stores and manages a user's passwords for various online accounts. A user can store account log-in information for all their accounts in one place, therefore only having to remember one main password (also referred to as a 'master' password).

There are many password management systems to choose from, each varying in price and capability. The CyberPatriot Program Office recommends these free options:

1Password

Dashlane

LastPass…

Changing Passwords

Changing Password is vital to cybersecurity. Hackers will often target passwords or logins to steal your credentials. In any of the following situations, it is recommended that you **change your password immediately:**

- Trouble logging in or password does not work
- Information missing on your computer
- Unusually slow speeds on your internet device
- Alerts from anti-virus software
- Alert from company of compromised accounts or data breach
- Loss of control of your computer
- Notifications indicating unauthorized access

Under normal circumstances where your accounts are still secure, passwords should still be changed every so often… but how often is enough? Frequency of changing passwords is a personal choice, and the range varies – cybersecurity experts recommend a minimum of 90 days (on the most secure end of the spectrum), but others recommend changing it once every 6-12 months.

The Do's and Don'ts of Passwords

Now that you understand the importance of passwords, here is a quick recap of the do's and don't of passwords.

Password Do's

- Do use various numbers, symbols and phrases to increase strength of password.
- Do protect files, documents, and devices with passwords.
- Do use passphrases to help make the password easier to remember without making it easier for others to guess.
- Do change your passwords every 12 months.
- Do report suspicious account activity and change your password immediately.
- Do use two-factor authentication.
- Do use password management systems.

Password Don'ts

- Do not use personal information (birthday, name, phone number) as passwords.
- Do not share passwords or confidential information with anyone.
- Do not write down a password on paper and then leave the paper where somebody can easily find it.
- Do not select the option to "Remember My Password." Many times this option is unsecured.
- Do not use the same passwords and security questions for multiple accounts.
- Do not leave your password unchanged if your account has been compromised.

Tech Caregiver Q&A

Possible questions to participants

- *What devices should have a password?*
- *Why is having a strong password important?*
- *If you have been hacked, what do you need to do?*
- *Was this section helpful? If not, why?*

Possible questions from participants

- *Where do I report suspicious activity?*
- *I don't use the Internet, why are passwords important for me?*
- *Can I have the same password for two accounts?*
- *Where can I get a password manager for all my devices?*

Lesson 2: Common Internet Threats

The internet is an extremely useful tool, but it also a source of many dangerous cyber threats that can create lots of headaches in your life. Understanding the various types of internet threats – what they are, how to recognize them, and how to protect yourself – is key in being able to safely use internet-connected devices.

Malware: Definition and Examples

Malware (also known as malicious software) is any piece of installed intrusive software intentionally designed to cause damage to a computer or computer network.

Malware typically covert, can make computers and applications inoperable, make data unattainable, and can infect others that you have communicated with via the internet. Malware infects the host by entering devices through downloads, attachments, including images, or audio/video files, etc.

Malware is the leading cause of compromised information, so it is important to when your computer might be infected, and what type of malware is causing the infection. Symptoms of malware on your device include:

- Sluggish or choppy performance
- A barrage of unwanted pop-up ads
- New and unfamiliar toolbar icons
- Unauthorized account access or signs of fraud

There are many different types of malware. The most common types are listed below:

Viruses	A malicious program designed to alter how computers operates and can spread from one computer to another.
Worms	A self-contained application and can transfer or copy itself from one computer to another.
Adware	Displays ads or pop up advertisements. Adware can control your web browser and monitor your search activity. It can even redirect you to harmful websites.
Spyware	Designed to infect your computer device to collect data about the user and forward it to a third-party without the user's consent. It is often used to profit from stolen data.
Ransomware	Inhibits users from accessing their computer system, including personal files, and demands ransom payment to regain access. It can also be used to bribe people for payment.
Rogue Security Software	Also known as scareware, are applications that mimic antivirus programs, but is malware designed to alert the user to infections and to purchase a product to get rid of the threat.
Browser Hijackers	A malware program that changes a web browser setting without permission from the user.

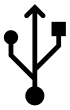
Zombie	A virus that gains access to computer devices, including smart phones, and takes control remotely.

How malware spreads

Internet: Malware can spread through surfing the web and downloading or sharing infected websites or software. Browsing through the internet can expose your device to unsolicited contact and infected websites.

Online media downloads: Movies, commercials, and video clips from social media sites. Social networks are a favorite target of scammers because just by attaching a worm, the scammer can infect just about anyone who visits the site.

Free software: often contains a variety of malware or hidden programs like spyware. If it seems too good to be true, it probably is.



Removeable media: Thumb drives or flash drives, CDs, and DVDs can all contain malware. By sharing these devices with another computer they can corrupt the entire device and can spread to many other computers.

Email attachments: Attachments like links, files, documents, videos, etc. can all contain malware. Cybercriminals can even use emails that look like they come from someone you know.

Signs a device is infected with malware:

- Trouble logging in or passwords do not work
- Information missing on your computer
- Unusually slow speeds on your internet device
- Alerts from anti-virus software
- Pop up ads that require personal information
- Loss of control of your computer (self-reboots, freezing, system errors)
- Unsecure and fake URLs that resemble real website addresses

Social Engineering: Definition and Awareness

Social Engineering involves influencing, tricking, or manipulating users to divulge sensitive information or other private data.

Social engineering should not be confused with social media or social networking. Social engineering involves using deception and psychological manipulation that includes phishing, vishing, smishing, and pharming to gain control over computer systems and the information stored in them. Social engineering can be implemented using computers, email, phone or even direct contact.

Awareness:
Do not open any emails from unknown or untrusted sources.

If you receive an unusual email or notification in social media, like a duplicate friend request, from a family member or friend, contact them immediately.

Do not give or verify any sensitive information to strangers. Do not accept any offers from strangers without doing some research, especially if the offer seems too good to be true.

Phishing: Definition and Examples

Phishing is the attempt to acquire confidential information like credit card numbers, passwords, usernames, etc. that comes from what seems to be a reliable and trustworthy source but is actually from a deceptive actor.

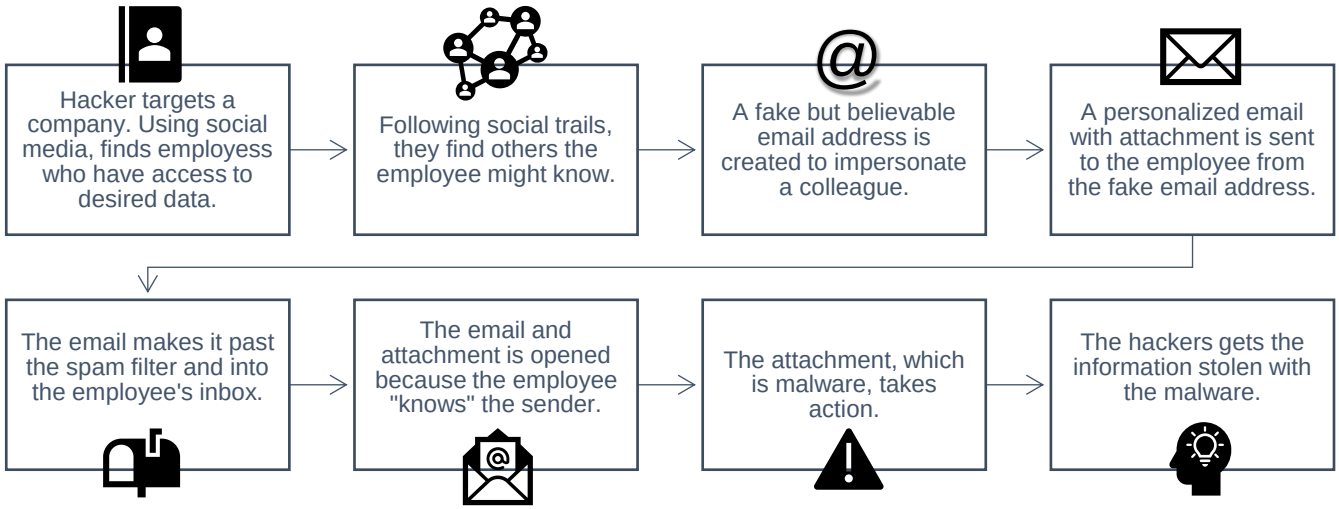
Phishing is probably the most frequently used social engineering technique.

Phishing attempts can be phone calls form hackers posing from a government agency or a debt collector. They can be in the form of an email from your bank claiming to reset your password by clicking on a link, or catfishing, which is often found on dating sites where predatorial impersonators pretend to be someone they are not and lure victims to get money.

Examples of actual phishing attempts in subject lines of emails:

- *Last Reminder You Must Update Your Apple Account Information!*
- *Help Desk Notice*
- *iTunes Access Disabled*
- *IRS Service Important Update*
- *Spear Phishing Attack Articles*

Spear Phishing is similar to phishing, but it involves what the victim thinks is a known or trusted source. Examples can be a friend, family member, colleague or even the IT Department at your work or school. Individuals and companies can be vulnerable to spear phishing. A visual example of spear phishing at a company is depicted below:



Vishing (voice phishing) is the attempt by phishers to gain confidential information over the phone.

Phishers uses phone calls rather than emails to compromise identities, steal money or a combination of both. Many involve fake caller ID profiles called Caller ID spoofing which can give some legitimacy to where the call is coming from. For example, the scammers can use a 202-area code from Washington, DC, and identify themselves as someone from the IRS. The scammers will often use scare tactics preying on people by saying if a tax error is not paid immediately the victim will suffer consequences like going to jail, notification to employer, or will be fined thousands of dollars. Some other popular vishing includes extended car warranties, fake charities, or illegitimate loan offers.

If you think a call might be a vishing attempt, do not answer. If you've already answered, hang up the call and do not engage with the person on the other end.

Smishing is a phishing attempt sent via text or SMS message in an attempt to scam recipients.

Smishing can be tricky because often people think if they are receiving a text, it is typically from someone you know or gave your phone number to, resulting in people letting their guard down a bit compared to the other methods of phishing.

Here's what you should do if you feel that you are a victim of smishing:

1. Never reply to a text message from a stranger.
2. Do not click on links via text. Even if the link comes from someone you know, call them first to verify if the link is legitimate.
3. Don't forward the text to anyone.
4. Even if the text is sent as an alert, emergency or an award from someone you don't know, do not open. Simply delete the text.

Protection from Internet Threats

Antivirus Software

Antivirus software helps protect computer devices from malware and criminal activity. It also protects files, software and hardware on desktops, laptops, tablets and Smart Phones.

The software searches for threats or suspicious behavior and will alert the user if any potential threats are found. Updates are necessary and depending on the type of antivirus software you are using, some updates are done automatically and others manually. As you can see from the picture above, there are plenty of antivirus programs to choose from; some are free while others are subscribed and have a yearly cost.

Free Versions of Antivirus	Paid Versions of Antivirus
AVG Free	Symantec
Bitdefender Free	McAfee
Avast	AVG

Make sure when downloading the antivirus software that the source is authentic, including the URL. Some devices come with antivirus software already installed or with a temporary trial period. If so, do not install additional antivirus software. You can check your Operating System on Windows by going to Control Panel. Macs already have built-in antivirus software.

Virtual Private Network (VPN)

Virtual private networks (VPNs) are private networks that use encryptions to transmit data across the Internet. By using a VPN to connect to the internet the user(s) can browse the web securely and privately.

VPNs provide the user(s) with its own IP address which is hidden to the public and protects your information via encryption while you are online. VPNs can be used with smart phones, desktop computers, laptops, and some tablets. Again, some are free and some must be paid for.

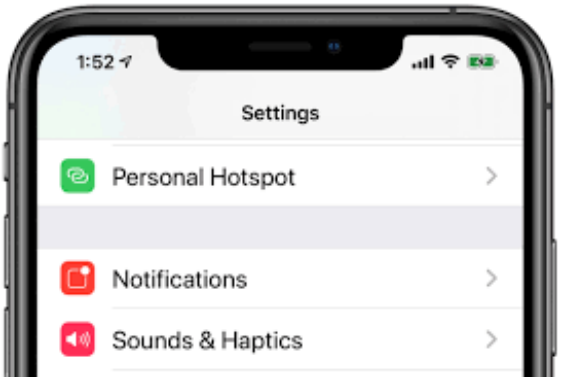
Free VPNs	Paid VPNs
ProtonVPN	NordVPN
TunnelBear	ExpressVPN
Windscribe	IVPN

When it comes to cyber safety, VPNs are far more superior than using public Wi-Fi. Most public Wi-Fi networks are NOT secure, and many hackers lurk in popular public places that offer public Wi-Fi to start criminal activity. These places include malls, hotels, airports, cafes, convention centers, stadiums and arenas, airports, etc.

If you absolutely must use public Wi-Fi, here are some safety precautions to keep in mind:

- ✓ Check your Wi-Fi settings and connections before getting on the internet.
- ✓ Choose networks that require a password over those that do not.
- ✓ Do NOT search or use apps that contain your confidential information. This includes apps and websites used for checking your banking information, medical records, or credit card balances.
- ✓ Refrain from online shopping on public networks, as your credit card information could be at risk.

Personal Hotspots



Personal hotspots provide data-tethering functionality from a cellular-enabled device, allowing you to share its data connection to another device via Wi-Fi, Bluetooth or USB. It's a great way to work mobile with a laptop and not have to worry about finding a Wi-Fi hotspot to work from.

NOTE: Check your data plan before purchasing a personal hotspot. If you aren't careful, using a hotspot might use up a lot of your cellular data and lead to expense charges from your services provider.

Tech Caregiver Q&A

Possible questions to participants

- *What types of Phishing are there?*
- *Name three types of Malware?*
- *Can you scan a thumb or flash drive?*
- *What are three signs your computer might be infected?*
- *Was this section helpful? If not, why?*

Possible questions from participants

- *What is the best antivirus software to buy?*
- *How often should I update my antivirus software?*
- *Can pictures in text messages be infected with malware?*
- *What is the safest way to online shop?*

Lesson 3: Scams and Fraud

Scams Overview: Awareness and Recognition

Scams have always been a part of human existence. Cyber scams are no exception. Access to the internet, smartphones, and other mobile devices leaves us all vulnerable to cybercrimes in the intimacy of our own homes. We can be robbed without a person ever meeting us. It is vital to understand scams, especially for the elderly.

A ***scam*** is any fraudulent activity or scheme with the malicious intent to steal, cheat, or con money or goods from other people.

Cyber scams evolved with onset of the internet, and with more people connecting to more parts of our lives with the internet, the number of scams has increased, as has their sophistication. We must be vigilant and teach others how to do the same.

Scams are not always easy to recognize, but here are some things to look for to avoid a scam:

- It looks or sounds too good to be true (and most likely is). This includes free gift cards, unusually low prices, and winning a trip or money from a sweepstakes you never entered.
- You are contacted by a stranger and they are asking you for personal information.
- You are contacted by someone who says they are a friend or family member of someone you know.
- You are asked to pay immediately for an unknown debt or bill, or asked to transfer money.
- You are asked to pay a debt in an unusual manner, for example through iTunes vouchers, MoneyGram or Western Union.
- You are asked for password or PINs.
- The email or phone call comes from an abnormal source.
- There are multiple grammar and spelling mistakes in the email or advertisement.

The Elderly Population

According to research by the Stanford Center on Longevity and the Financial Industry Regulatory Authority's Investor Education Foundation, "those over the age of 65 are more likely to have lost money due to a financial scam than someone in their 40s." (Association of Certified Fraud Examiners)

The elderly are often targeted because their computer skill sets are average or below. Some are at a stage in their lives when their interface with technology simply does not keep up with the rapidly evolving technological world. Cybercriminals take advantage of this.

Examples of Common Scams

These are some of the most common scams targeting senior citizens.

Medicare Scam	Scammers disguised as Medicare representative solicit for information or offer fraudulent services.
Grandparent Scam	A person calls pretending to be a grandchild (after asking the grandparent to guess who is calling) and asks the grandparent to wire them money. Often times, they say they are in a bad situation and need help fast.
Funeral Scam	Criminals target obituaries and contact the families to extort money for fraudulent debt.
Prescription Drug Scam	Seniors search for cheaper prescription drugs due to high cost and are vulnerable to purchase counterfeit drugs on fake websites.
Investment Scam	Investment schemes take advantage of elderly people about to retire or are retired and pose as financial advisors to get access to their savings and retirement.
Mortgage Scams	Scammers will target and send elderly people communications offering reassessments on the value of their home for a fee.
Lottery / Sweepstakes Scam	Victims are typically contacted via phone or mail that they won a prize but need to pay a fee to obtain the money.
Anti-aging Product Scam	Scammers will target on the emotional and psychological desires of some elderly people to look younger so will sell worthless and even harmful products (sometimes endorsed by pictures of celebrities) to them.
Internet Scam	Senior citizens because they are not always updated with the latest technology terms, definitions and processes are vulnerable to Internet scams that involve Phishing emails, fake antivirus software and other commodities.
Charity/Door-to-Door Scam	Fake charities pretend to help an array of disadvantaged people such as cancer patients, starving children, or veterans in need. Whenever there's a natural disaster or ongoing humanitarian crisis, these scammers use high-pressure sales tactics to extract money

	from victims. Some scammers may also make false tax deduction claims and ask for personal information.
Dating / Romance Scam	Criminals posing as potential partners who prey on the lack of companionship and ask for money. This technique may be referred to as catfishing.
Tech Support Scam	Cyber thieves post as computer technicians to fix computer issues either they caused or can be fixed easily and charge hefty fees.
IRS / Government Scam	Fraudsters pose as government employees and make illegal threats of fines, imprisonments, or immediate payments to save your house or employer contact. The IRS is often used.

Identity Theft

Identity theft or identity fraud is criminal activity involving an imposter stealing personal information to form another identity of you. Typically, the personal information includes social security number, name, home address, etc. This is the information usually required to apply for a credit card, get a tax return, or access other accounts.

Identity theft can happen to anyone, but senior citizens and children under 18 are the most vulnerable. According to The Federal Trade Commission's 2017 Consumer Sentinel Network Report, these were the most common types of identity theft:

Credit Card Fraud	133,015 Reports
Employment or Tax Fraud	82,051 Reports
Phone or Utility Fraud	55,045 Reports
Bank Fraud	50,517 Reports
Loan and Lease Fraud	30,034 Reports
Government Documents Fraud	25,849 Reports

Signs of Identity Theft

- Your financial statements look strange or unauthorized withdrawals have occurred
- You get notifications from financial, social media or other accounts of unauthorized activity
- Your credit report has unfamiliar accounts or activity
- Your bills are missing or stop coming through mail or email
- Loss of services including utilities, phone, or cable
- You suddenly start receiving calls form debt collectors
- Your medical insurance shows either claims denied or bills you did not obtain
- You cannot file your taxes because someone else did in your name or you didn't get a refund
- There is a warrant for your arrest
- Merchants suddenly do not accept checks from you

Steps to take if you think your identity has been stolen

1. Immediately call the business or organization where the fraud has occurred
2. Notify your credit card companies, banks, and any other financial institutions

3. Report any identity theft to the Federal Trade Commission (FTC) https://reportfraud.ftc.gov/#/
4. File a report with your local police station
5. Notify all three major credit bureaus or agencies, get copies of current credit report, and ask them to place a fraud alert on your accounts

Experian	**Equifax**	**TransUnion**
Experian Freeze Center 1-888-397-3742 Experian Security Freeze PO Box 9554 Allen, TX 75013	Equifax Credit Report Services 1-800-685-1111 Equifax Information Services LLC PO Box 105788 Atlanta, GA 30348-5788	TransUnion Credit Freezes 1-888-909-8872 TransUnion LLC PO Box 2000 Chester, PA 19016

Additional Ways to Protect your Identity

- Review your financial statements monthly.
- Review your credit reports annually. For a free credit report, go to annualcreditreport.com.
- Be aware of skimmers at ATMs, Gas Station Pumps, or any place you insert your debit or credit card. Skimmers are placed over or around the card insertion box and collects your card's information.
- Shred any personal documents; dispose of medication bottles appropriately.
- Consider purchasing Identity Protection Services, especially if you have already been compromised. Here is a sample of a few:

LifeLock IDENTITY GUARD INTELIUS Identity Defense

Tech Caregiver Q&A

Possible questions to participants

- *Have you, or do you know someone who has been scammed?*
- *How do you respond to a scammer?*
- *Is it a good idea to try to find the scammer yourself?*
- *Should I discuss a suspicious activity with a friend?*
- *Was this section helpful? If not, why?*

Possible questions from participants

- *If I get scammed, do I lose everything or will I get reimbursed?*
- *What should I ask a company to see if they are a scam or not?*
- *Should I contact the Better Business Bureau?*
- *If I suspect a friend is being scammed, what should I do??*

Lesson 4: Social Media Safety and Awareness

Social Media: Definition and Examples

Social media is any internet-based platform where users can share, view, and create video, audio and text media in a social environment.

Social media encompasses many apps and websites and is enjoyed by people around the world of all ages, including the elderly population; however, it can also be a tool for cyber thieves to scam, exploit, compromise, and steal user's identity, money and/or personal information.

There are many different social media platforms that a person can join. Approximately 2.77 billion people used social media in 2019. Let's look at the platforms most commonly used by adults and seniors.

	**Facebook** is the largest social media site in the world with 2.6 billion users (as of 2019). User's typically post pictures, videos, text, links and share them with Facebook friends.
	**Twitter** is an online news and social networking site where people communicate in short messages called tweets. In 2019 there were over 330 million active Twitter accounts, which is about the same population as everyone in the United States. On average, about 500 million tweets are sent daily
	**Instagram** is a free social networking service built around sharing photos and videos. It is a mostly app-based platform.
	**YouTube** is the largest video-sharing social media site. People can post their own videos or watch videos posted by others. The company recently released YouTube TV where subscribers can access over 85 channels of media.
	**Pinterest** is a visual discovery engine for finding ideas like recipes, home and style inspiration, and more. Pinterest is unique because you can't share something on it unless an image is involved. Often identified as a social bookmarking site, it is entirely driven by visual images.
	**LinkedIn** is a social media site designed for professionals in a business audience. It has over 690 million members and is often a tool used to advertise professional skills, increase professional connections, and search/apply for jobs.

Here are a few more sites popular with senior citizens that you might encounter questions on from our workshop groups.

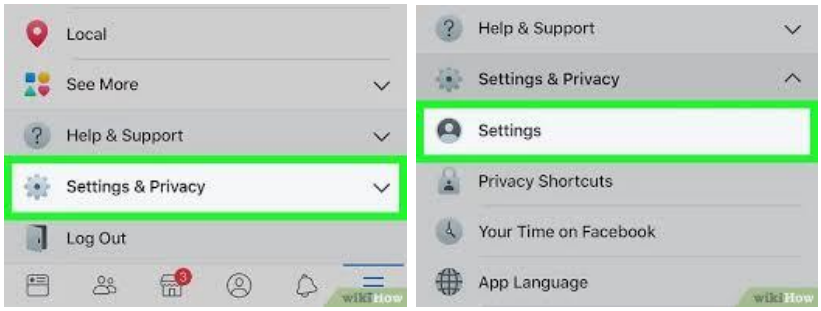
	**Skype** is a video chat and phone media used to connect with anyone around the world.
	**AARP (American Association of Retired Persons)** has information for the elderly ranging from relationships to investments. The organization assist seniors with information through their magazine but also through their website and Facebook account.

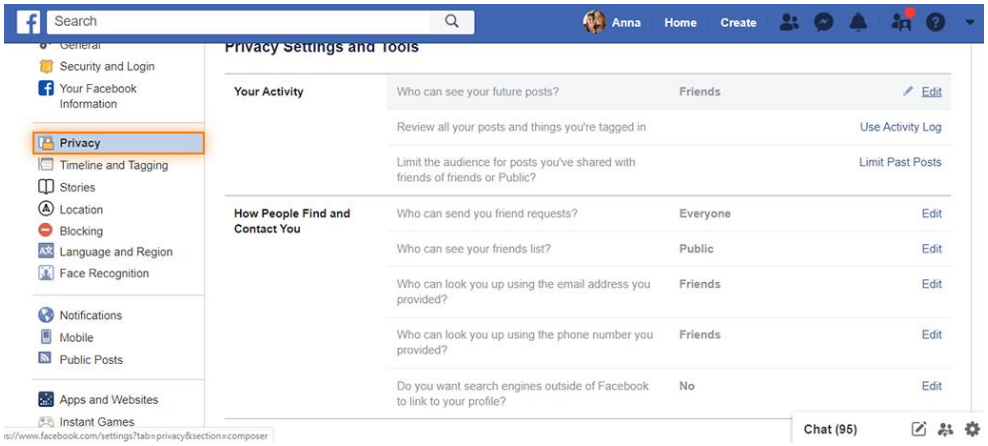
Social Media Privacy

Social media sites are a great way to stay connected to friends and family, and maybe even meet new people. However, social media sites are also home to many malicious actors and fake accounts whose intentions are bad.

Privacy settings allow you to limit the information other people can see and help keep your personal information protected. Since Facebook is one of the most popular social media sites, let's consider how a person would go about editing their privacy settings.

- Go to Settings & Privacy from the menu → select Settings select Privacy
- From Privacy Shortcuts select Check a few important settings
- Follow the steps by clicking next and complete the Privacy Checkup.





Most every social media platform allows you to customize your privacy settings. It is very important that you review the privacy settings periodically to understand if and how your information is being shared.

Tips for Social Media Safety

Create Anonymity	Consider creating a new email address that you use only for social media accounts. Do not use identifying features.
Create a strong password	Use complex and unique passwords for each different account.

Increase your privacy settings	Increase your protections and limit what information can be seen by strangers.
Avoid sharing your location	Turn off location settings and never share where you will be (especially if you are going out of town). If you want to share a picture of your vacation, wait until the trip is over and you've returned home.
Add friends carefully	Know who you are adding, and who is adding you. If you are unsure of the legitimacy of the request, send a private message to the individual before accepting.
Do not share personal information	This includes any Personally Identifiable Information (PII) discussed in previous lessons.
Post/Share/Link carefully	Nothing on the internet is completely safe. Never post anything about yourself or your family that you don't want to be made public.
Think before you click	If you don't know what the link is, don't click it. That's how hackers can break into your account.
Know what action to take	If you are being harassed or threatened online, make sure you save the communication or offensive post. Report it to the site and any person that may be involved.

Online Dating Sites

Dating sites are a good way for senior citizens to meet new people and find companionship. In fact, in 2018 nearly 12 percent of seniors between the ages of 55 to 64 used online dating sites or mobile apps.

Scammers understand seniors are looking for companionship, with some vulnerable to the recent loss of a spouse, can sometimes be lonely and have feelings of abandonment. Often online dating is a new concept to seniors, so the more information they have the safer they can be, especially when it comes to catfishing.

Catfishing *is an online deception used by scammers often on dating sites where the scammer creates a fake dating profile to lure other seekers into a potential relationship.*

The imposters are often seeking money or gifts that exploits the vulnerabilities of some seniors. Some seniors have lost their retirement savings and even property over catfishing**.** In 2019, the FBI reported that catfishing (of all ages) scams cost Americans over $475 million.

Safety tips for Online Dating

- Perform an internet search of any dating prospect to see what additional information you can find out about that person
- Search for the person on other social media sites
- Proceed getting to know someone at a pace that is comfortable for you. If the person seems pushy or aggressive to meet or gather personal information, that could be a red flag.

- Communicate and get to know the person via email, text, video chat or phone masking phone number, For example, you can type *67 followed by the number you are calling to block your phone number on the caller ID
- When you finally meet an interest, meet him or her in a public setting only, let your friends know where you will be meeting them and give them information about your interest
- Do not respond to duplicate “Friend’s Request” on Facebook. Check with friend before accepting

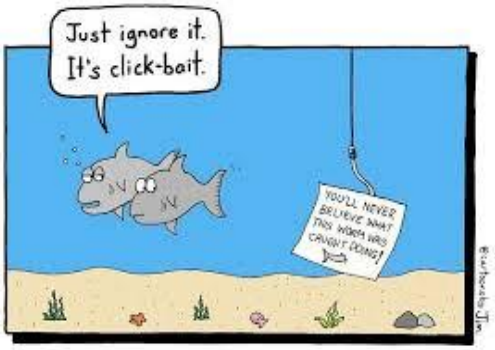
Social Media Scams

Dummy profiles

Dummy profiles are just what they sound like – fake profiles where a person claims to be somebody they are not. Dummy profiles are often used in catfishing. They can then impersonate a person whose information got stolen and reach out to you with some urgent financial emergency that requires you to make a wire transfer or they can lure you in with the promise of some brilliant business opportunity that will make you rich overnight.

Always be wary of online monetary requests from a friend or family member. Try contacting the friend in person before you proceed any further. Also, be careful about any friend request from a person who you are already friends with on that platform. Duplicate friend requests are a big red flag of dummy accounts.

Click-bait



Click-bait refers to a photo or headline which is tailored to grab your attention and prompt you to click through to learn more. Clicking on such links can redirect you to an altogether different website with malicious content, which can download dangerous malware onto your device.

Here are some examples:

- “Justin Bieber’s favorite keyboard shortcuts.”
- “Why using shortcut keys can save you hundreds of dollars a day.”
- “Keyboard shortcuts that won't make you look like an idiot.”
- “Is not using shortcut keys making your gain weight?”

Like-Jacking

Like-jacking occurs when criminals post false Facebook “like” buttons to webpages. Users who click the button do not “like” the page, but instead download malware. Mindlessly clicking a “like” button can lead to downloading software and/or spreading spam.

Sick Baby Hoax

In a ***sick baby hoax***, scammers use real pictures of sick and disabled children to manipulate people into donating money for emergency treatment. They then ask users to like and share such photos to raise awareness or money, thereby making the hoax spread faster.

Families are often distressed to find that photos of their sick child are being misused in this manner, but most of the time there is very little they can do to stop the circulation of the post. The problem is that the scenario is false, and the scammer takes the money. GoFundMe pages or other charitable venues are often used. A good segue into the next topic.

Charity Scam

A ***charity scam*** occurs when cyber thieves prey on the good will of people to help those in need by creating fake charitable or fundraising sites. The sites can be to donate items such as phones, money, or other items. The example in the CyberGenerations Self-Paced Guide mentions a scenario where the scammer says they are working with a charitable organization and request you to either place the order of phones on your account, or even go to the store and ship the phones to their address. The money for the order appears as an ACH pending transfer on your account, but when you order the phones, the money disappears.

So before purchasing, sending, or pulling out the plastic to donate, do some research to question the legitimacy of the charity. Here are some tips:

- Verify the charity: visit the charity's website, call the charity, or contact the Better Business Bureau (BBB).
- Do not open suspicious emails requesting donations. Do not click on any links. If a charity thanks you for donating last year, but you didn't, do not donate to the charity.
- If you suspect a charity is questionable contact the FCC Complaint Center.
- Do your research. There are charity watchdog groups called CharityWatch, CharityNavigator, and Wise Giving Alliance, which are all run by the BBB.
- If a charity is aggressive, pushy or demands money immediately, hang up.
- Be aware of payment method. If the charity request, gift cards, cash, or wire transfers, it may not be legitimate.

Social Media Etiquette

Social media etiquette is a set of guidelines and social tools used to maintain the reputations of individuals and the ethical interactions with others on the internet.

Social media etiquette is important for the following reasons:

1. To preserve your reputation. Refrain from derogatory remarks, profanity, or illegal activity.
2. To prevent saying something you will regret later.
3. To be a supporter among your friends and peers.
4. To help you to stay on task and focus on the issue at hand.
5. To set a good example for others, especially in a chatroom comment section.

Practicing good social media etiquette:

- **Don't Overshare:** Keep the personal information you share to a minimum.
    - Do not announce vacation details.
    - Do not share information about other people.
    - Do not share financial information or any sensitive data on social media.

- **Comment and Post Carefully:** Be careful with personal comments which may affect your relationships.
    - Consider how your comments may be perceived before posting them.
    - If you think that one of your friends might be interested in a post, send them a message rather than tagging them in the post.
    - When posting online, try not to flood people's feed. Post responsibly.
    - Don't get into arguments online. Respect the right of other people to express their opinion.
    - Don't use ALL CAPS. Using all caps may imply yelling and may be rude.

- **Cautiously Share Photos and Videos**
    - Do not repost someone's media without permission.
    - Ask before you post pictures you take of other people.

- **Be Wary of the Friends You Keep:** It's best to only accept friend requests from people you know.
    - Cyber criminals often send false friend requests to gain personal information.

Tech Caregiver Q&A

Possible questions to participants	**Possible questions from participants**
• *Why is social media etiquette important?* • *How can I see if a charity is legitimate?* • *What are some rules with online dating?* • *A friend of mine sent me another friend request. What should I do?* • *Was this section helpful? If not, why?*	• *What if other people don't practice good social media etiquette towards me?* • *Is it safe to have multiple social media accounts?* • *How much information about myself should I put in profile?* • *Is it safe to play games on an app or social media?*

Lesson 5: Cybersecurity Resources

There are resources in place to help assist those individuals who find that they have been a victim of identity theft or any other type of scam or cybersecurity breach.

Government Resources

The federal government offers a variety of recourses to help protect individuals who may have fallen victim to a cybercrime.

General Resources

Online Guide to government information/services	https://www.usa.gov	1-844-872-4681

Legal Assistance

Attorneys General (by state)	http://www.naag.org/naag/attorneys-general/whos-my-ag	
Elder Justice Initiative (Dept. of Justice)	www.justice.gov/elderjustice/	

Reporting phishing attempts and scams

Department of Homeland Security	Email: phishing-report@us-cert.gov	
Internal Revenue Service (IRS)	Email: phishing@irs.gov	
Federal Trade Commission (FTC)	Website: www.ftc.gov/complaint	1-877-438-4338
United States Senate Special Committee on Aging	Website: https://www.aging.senate.gov/fraud-hotline	1-855-303-9470

Reporting Tax Fraud or Identity Theft

Identity Protection Specialized Unit of the IRS	https://www.irs.gov/identity-theft-central	1-800-908-4490
Federal Trade Commission (FTC)	https://www.identitytheft.gov/	
Taxpayer Advocate	https://www.irs.gov/taxpayer-advocate	1-877-777-4778
Social Security Administration	https://www.ssa.gov/antifraudfacts/	1-800-772-1213
Medicare Fraud	https://www.medicare.gov/forms-help-resources	1-800-633-4227

Register Phone Number for Do Not Call List (Reduce telemarking calls)
Visit www.donotcall.gov or call 1-888-382-1222 from the phone number you want to register. You will get fewer telemarketing calls within 30 days of registering your number.

Aging Services Divisions

Aging Services Divisions provide and support a broad range of services and programs for older adults and their families. Each state (and sometimes individual counties within states) have their own aging services division. If an individual is looking for information about the Aging Services in their state or territory, they can do a Google search for "[state/territory] aging services division."

AT&T Customer Resources

AT&T is a proud supporter of CyberPatriot's CyberGenerations program. For their tips on outsmarting the bad guys and staying protected, visit ***AT&T's Cyber Aware*** website at https://about.att.com/pages/cyberaware.

Those individuals who are AT&T customers may want to consider downloading the AT&T Mobile Security and AT&T Call Protect apps on their mobile devices. These free mobile apps can help protect against fraudulent activity.

AT&T Call Protect:

- Automatic Fraud Blocking detects and blocks calls from likely fraudsters.
- Spam Risk Blocking blocks or sends to voicemail calls identified as Spam
- Nuisance Call Warnings provide a heads up on potential nuisance calls with warnings of telemarketers, account services and more.
- Unknown Callers sends callers not in your contact list to voicemail.
- Personal Block List lets you block specific unwanted calls. *
- Caller ID identifies unknown caller details. *
- Reverse Number Lookup† provides details when you enter a U.S. number. *

AT&T Mobile Security:

- Device Security helps protect your data from mobile threats.
- Breach Reports alert you to company data breaches.
- Secure Wi-Fi VPN helps protect your data over open (unencrypted) Wi-Fi. *
- Wi-Fi Alerts warn you if a Wi-Fi network may be dangerous to your privacy. *
- Personal ID Monitor notifies you if your personal information is found on the dark web. *
- Theft Alerts notify you if suspicious activity is detected. *
- Safe Browsing analyzes and warns you about suspicious websites. * 49

* Available with premium version – $3.99 per month for bundle of A&T Call Protect Plus and AT&T Mobile Security Plus together

Tech Caregiver Certification Quiz

Now that you have completed the Tech Caregiver Training Course, it is time to take the certification quiz. Upon successful completion of the quiz, you will be able to immediately download your Tech Caregiver Certification.

Click HERE to access the quiz (with instructions).

Appendix: Glossary of Cybersecurity Terms

Adware	an application software that displays advertisements based on codes to track and record user's activity
Antivirus Software	software used to scan and designed to help detect and prevent malware from infecting computer and computer systems
Biometrics	physical characteristics or personal behavioral traits measured and used to verify or identify an individual. Typically, facial and fingerprint recognition are used
Browser Hijackers	unsolicited software that can modify a user's web browser settings, typically resulting in unwanted browsers and advertisements
Catfishing	deception by fraudsters by creating false profiles or fake identities on social media sites. It is also a tactic used to gain a relationship, typically on dating websites, to extort the victim for money or gifts
charity scam	a scam in which cyber thieves prey on the good will of people to help those in need by creating fake charitable or fundraising sites
Click-bait	to a photo or headline which is tailored to grab your attention and prompt you to click through to learn more
Cybersecurity	the protection of internet-connected systems (including hardware, software, and data) from cyberattacks
Dummy profiles	fake profiles where a person claims to be somebody they are not
Dumpster diving	physical act of digging through garbage and discarded documents in search of passwords, account numbers, PIN numbers, or any other information that can be used to carry out a malicious cyberattacks or cybertheft.

Hardware	the machines, wiring, and other physical components of a computer or other electronic system
Identity theft	criminal activity involving an imposter stealing personal information to form another identity of you
Like-jacking	occurs when criminals post false Facebook “like” buttons to webpages
Malware	also known as malicious software) is any piece of installed intrusive software intentionally designed to cause damage to a computer or computer network
Mobile Device	portable or handheld device that have data or can connect to another device that has data (cell phone, tablet, flash drive, etc.)
Passphrase	a type of password that uses a series of phrases or words rather than a string of characters
Password	a string of characters used to authenticate a user’s identity to access a devices and information, while protecting personal information from cyber threats
Password Management System	software that stores and manages online credentials and passwords
Personal Hotspot	a mobile cellular network that converts data stream into a Wi-Fi signal that can be shared by several other devices
Personally Identifiable Information (PII)	any data that can be used to identify a particular person
Phishing	a type of social engineering used to collect confidential information and data via the Internet, often by email
Ransomware	a type of malware that prevents users to access their computer devices unless some form of ransom or payment is paid
Rogue Security Software	a type of malware that misleads consumers to think the product is antivirus software
Scam	any fraudulent activity or scheme with the malicious intent to steal, cheat, or con money or goods from other people
Shoulder surfing	the act of acquiring personal or private information through direct observation, such as looking over a person's shoulder to obtain vital information while the victim is unaware
sick baby hoax	a scam in which scammers use real pictures of sick and disabled children to manipulate people into donating money for emergency treatment

Smishing	a type of phishing where text or Short Message Service (SMS) are used to collect information from the user
Social Engineering	a tactic involving tricking or manipulating people into exposing their confidential information to cyber criminals
Social Media	Consist of websites and applications that allows people to create and share digital and text content; participate in social networking
Social Media Etiquette	is a set of guidelines and social tools used to maintain the reputations of individuals and the ethical interactions with others on the internet
Software	the programs and other operating information used by a computer
Spear Phishing	phishing disguised by a trustworthy person or a familiar entity
Spyware	Malware that covertly gathers data from user's and sells the data to third parties
Two-factor Authentication	Security measure that requires a user to offer at least two forms of identification to the authenticate access
Virtual Private Network (VPN)	a private network that use encryptions to transmit data over the Internet
Virus	a type of malware computer program installed on computer systems to replicate malicious code and alter programs and applications
Vishing	Also knows as voice phishing. A type of phishing attack that uses the phone and often victims of Voice over IP (VoIP) services
Web Browser	a software application used for retrieving, presenting, and navigating information resources on the World Wide Web
Worm	a type of malware that replicates itself and spreads throughout a computer without input from users by attaching to software programs
Zombie	Also known as Bots, is a computer that has been compromised by a hacker that is connected to a network that transmits spam and viruses to other computers