CYBERGENERATIONS

SELF-PACED GUIDE

REVISED APRIL 2022

CyberGenerations

CyberPatriot – the National Youth Cyber Education Program - was created by AFA to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.

CyberGenerations – the Senior Citizens' Cyber Safety Initiative – is designed to teach individuals how to protect themselves safely and confidently against the cyber threats found online and on mobile devices.
More information about the CyberPatriot program can be found at: www.uscyberpatriot.org

Welcome to CyberGenerations!

CyberGenerations – the Senior Citizens' Cyber Safety Initiative –is designed to teach basic cybersecurity topics and to provide self-help resources for seniors who have been victims of a cyberattack.

By obtaining this guide, you are committing yourself to be a smarter and safer user of internet-connected devices, such as cell phones and computers.

Thank you for your participation in the program. We hope you find the information to be not only practical, but also enjoyable.

Sincerely,

Rachel Zimmerman
CyberPatriot National Commissioner
Air & Space Forces Association

This page is intentionally blank.

Table of Contents

Introduction to Cybersecurity

Welcome to CyberGenerations! This is your guide to cyber safety! Through this self-paced guide, you will learn about the many do's and don'ts of being safe and secure while online.

Before you get started, please take 2-3 minutes to complete the pre-program survey in the link below. Your honest feedback is extremely important in measuring the value and success of the CyberGenerations program, and for implementing improvements to the program content as needed. We greatly appreciate your participation.

CyberGenerations Survey (via Google Forms): http://bit.ly/2Sk9Z5S

You can also test your cybersecurity knowledge on AT&T's Cyber Aware site:

AT&T Cyber Aware Quiz: How Cybersecure Are You?

https://about.att.com/pages/cyberaware/ni/blog/cybersecure_quiz

What is Cybersecurity?

Cybersecurity is the protection of internet-connected systems – including hardware, software, and data – from cyberattacks.[1]

It is important to be aware of the potential threats of cybercrime because it affects us all. According to one report, cybercrime is one of the toughest challenges that the world is facing today, and it is set to cost the world over $10 trillion by 2025.[2]

Why is it important to be safe online?

We rely on computers, mobile devices, and the internet for many things in our day-to-day lives. A lot of our data is stored online or on computers. Even if you don't use computers regularly, or at all, it is still possible that your data is at risk.
To explain this better, let's look at some myths about the internet:

- ***Myth 1*** *– If you didn't put your information online, you are untraceable and therefore safe from intrusions.*
  Truth: Publicly available government records, court records, or records of any organization or committee that you are a member of are all viable sources of personal information.
- ***Myth 2*** *– Information you post online is only shared with your family and friends.*

Truth: The internet is a mysterious place, and you never know where your information will ultimately end up. Even if you are being careful and deleting data that exposes personal information, there's always a chance that your personal information has been copied and stored in a location where it can be accessed by criminals.[3]

Personally Identifiable Information (PII)

Personally Identifiable Information, or PII, is any data that can be used to identify a particular person.[4]

- First Name or Last Name
- Social Security Number
- Driver's License or State ID Card #
- Passport Number
- Credit Card Number
- Security Question Answers
- Passwords
- 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.

Did you know? The Equifax data breach in 2017 exposed the Social Security Numbers of 146 million people and the names and birthdates of 147 million people.[5]

Physical Threats to PII

Before we dive deeper into cybersecurity threats from our online activities, we must discuss some offline threats which are just as dangerous.

- ***Dumpster Diving:*** In terms of cybersecurity, dumpster diving is a practice of salvaging information that could be used to carry out a cyberattack. It's not just limited to searching through the trash for obvious clues like passwords or PINs. Attackers can also use information like phone lists, calendars, or address book pages to carry out malicious activities.[6]

- ***Shoulder Surfing:*** Shoulder surfing refers to the act of acquiring personal or private information through direct observation. Shoulder surfing involves 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.[7]

Securing Mobile Devices

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
- Laptops
- Tablets
- Digital Cameras
- Pagers
- Smart watches (e.g., Apple Watch)
- Flash drives

Because these devices can store and share data, it's important to keep them protected from cyberattacks. Here are some tips on how to do that:[8]

- 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're 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.

If you lose a device (for example, your smartphone), there is a way to locate it:

<u>Android Device:</u>
If you've added a Google Account to your device, Find My Device is automatically turned on. To use Find My Device, your lost device must:

- Be turned on
- Be signed into a Google Account
- Be connected to mobile data or Wi-Fi
- Be visible on Google Play
- Have location turned on
- Have *Find My Device* turned on

1. Go to android.com/find and sign into your Google Account.
2. The lost device gets a notification.
3. On the map, you'll get info about where the device is.
4. Pick what you want to do. If needed, first click Enable lock & erase.
    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.

Apple Device:
Find the approximate location of your iOS device (Apple Watch, AirPods, iPhone, MacBook) by using Find My iPhone on iCloud.com. You can locate your device if:

- Find My iPhone is set up on the iOS device you want to locate.
- Apple Watch is paired with an iPhone.

1. The iOS device is online. Click 'All Devices.' In the list, the dot next to the device indicates its status: Green Dot = Online | Gray Dot = Offline.
2. If the device is online and can be located, its approximate location appears on the map.
3. If device can't be located, the last known location is displayed for up to 24 hours. Select "Notify me when found" to get an email when it comes online. [9]

Web Browser Safety

A ***web browser*** is a software application used for retrieving, presenting, and navigating information resources on the World Wide Web.[10]

The 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: [11]


Microsoft Edge https://www.microsoft.com/en-us/edge


Google Chrome https://www.google.com/chrome/

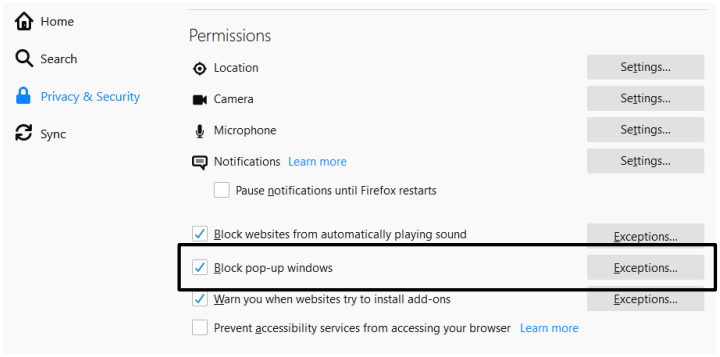

Mozilla Firefox https://www.mozilla.org/en-US/firefox/

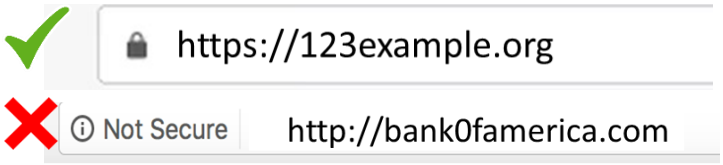

Opera https://www.opera.com (has built-in VPN)


Safari (macOS) https://support.apple.com/downloads/safari


Did you know? Google has 90.46% of the search engine market share worldwide and it receives over 63,000 searches per second on any given day.[12]

Web Browser Safety Tips





- 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, 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. [13]

Browser Symbols and what they mean:

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

Password Management

Imagine the following scenario:

Susan was very active online. She especially liked the convenience of online shopping and managing her bank account from home. Susan had used the same password for her personal accounts for many years because it was too much of a hassle to remember multiple passwords. She was convinced that one password was perfect for her online activity.
One day Susan attempted to log in to her personal email account, but found that she couldn't log in. This seemed odd to Susan, so she tried to log into her online bank account using the same password. Susan was relieved to find out she was able to get into her online checking account but soon realized she had a mysterious withdrawal for $500. What happened?!

After speaking to her bank over the phone, it was confirmed that the bank's customer database was breached earlier in the day. They had sent an email warning customers of the compromise, but of course Susan wasn't able to see the warning. Susan soon realized that whoever had access to her bank account information had also changed her email password. Susan thought this only happened to other people. What should she do?

In this Password Management section, you will learn the importance of setting strong passwords and the steps you can take to make your log in credentials more secure.

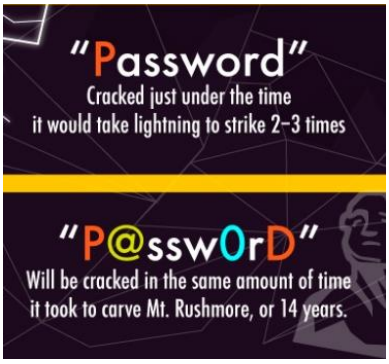
Did you know? For every incident of violent crime, approximately three incidents of internet crime were committed against seniors.

Creating Strong Passwords

Passwords help protect our personal information on the internet, and they are often the only thing standing between cyber criminals and our sensitive data. A strong password is not only important, but necessary. The examples below are not strong passwords because they use personal information that could be guessed by others.

Bad/Weak Password Ideas	Examples
Birthdays	Marchtenth, March10, 03101958
Names (yours, pets, spouses, etc.)	Shawn, Rachel, Kitty
Dictionary Words	Password, Monkey123
Phone #/SSN/Sequential Numbers	5555551234, 123456789

Password length should always be at least 10 characters. The longer a password is, the harder it is to crack.



Additionally, adding complex characters can help strengthen a password. Passwords should always include:

- UPPERCASE letters
- Lowercase letters
- Numbers
- Symbols (#$%^&?)

The more of these you can include in a password, the stronger the password will be.

NOTE: The example graphic is used to show variety of symbols and letters. Do not use any form of "Password" as your password.

Did you know? There are tools you can use to check the strength of your password or passphrase. Check yours today at https://nordpass.com/secure-password/[14]

Passwords for Mobile Devices

AT&T Cyber-Aware Tip:
Mobile devices (like cell phones) need password protection too! There are multiple ways to unlock a device (depending on what device it is), including passcode, fingerprint, pattern-based lock, or facial recognition. Use a long passcode number or a passphrase to strengthen the security. Short codes are easier to break. The pattern-based lock is less secure because scammers can trace the trail your fingers leave on the screen.

Managing Passwords

In the scenario at the start of this section, Susan used the same passwords for all her accounts because it was too difficult to remember a new password for each new account. Susan also paid the price when all her accounts were hacked at the same time!

If you create different passwords for each account, a breach in one system does not endanger your other online accounts. And keeping track of all these passwords does not have to be difficult. Base passwords and password management systems are useful tools for helping to manage passwords.

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:

Account	Base Password	Site	New Password
Gmail	Coconut!23$	GMA	Coconut!23$GMA
Facebook	Coconut!23$	FAC	Coconut!23$FAC

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]

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.

Account examples:

- Email
- Social Media
- Banking/Finance
- Healthcare
- Shopping
- Personal Info

Some of the most popular password management systems are:

LastPass dashlane 1Password

These password managers can also be accessed as mobile apps.

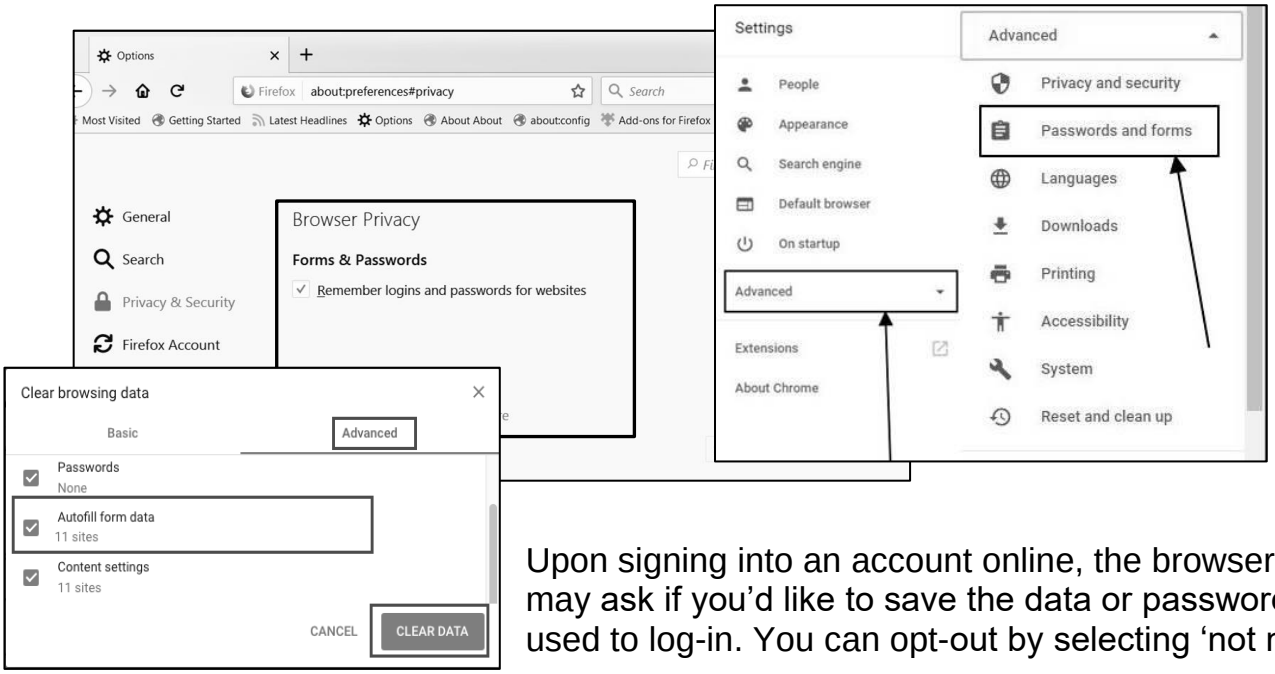
Changing passwords

Most people only change their passwords when it's required, or when they're a victim of a data breach. While it's smart to change your passwords after a breach, there's no harm in changing them sooner.

The recommended time for changing your password is once every 90 days. If 90 days is too often to change your passwords, ***make sure to change your passwords at least once every 6-12 months***. And with password management system, there's no excuse for forgetting your new passwords!

Autofill and Saved 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.



Upon signing into an account online, the browser may ask if you'd like to save the data or password used to log-in. You can opt-out by selecting 'not now.'

If you accidentally save a password or autofill information to the browser, you can delete the saved records by clearing the browsing data. This is usually found under the browser's 'history' menu.

Did you know? 63% of network intrusions are the result of compromised user passwords and usernames.

Two-Factor Authentication

Many websites today use two-factor authentication when a person is trying to sign-in.

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. [15]

For example, after inputting your password, the site may also send a text to your phone with a code or PIN that must be entered to gain access to your account.

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.

Some websites use two-step authentication as their standard log-in procedure, but other sites allow you to opt-in or opt-out of two-step authentication. It is recommended that you opt-in. This can be done in most account settings.

Biometrics

Biometrics are measurable behavioral traits or physical characteristics used to access computer hardware, software, and equipment through identity recognition. The following are examples of biometrics:

- Facial Recognition
- Fingerprints
- Voice recognition
- Retinal Scan
- Digital Signatures

The most popular ones we use with our electronical devices, including our Smartphones, are facial recognition and fingerprints. Biometrics is useful because you don’t need to remember a password or PINs to unlock or gain access to your devices. Although Biometrics is convenient and safe, if you are expecting any facial or finger surgeries, Bio metrics may not be the best security option.

Compromised Account: What to Do

If you receive notification that your account has been compromised (a log in from a suspicious location, data breach at company, etc.), follow the steps below:

- Immediately change the password for that account.
    - Many sites have a ‘SEARCH’ box or ‘Contact Us’ option.
    - Look for the option to CHANGE PASSWORD.
- Contact the service (Gmail, Yahoo, etc.) for support and/or to report an account breach.
    - Many site settings are located on the top right corner of the webpage.
    - Most sites have options to contact the company by email and by phone. Remember, legitimate company employees will NEVER ask you for your password or other sensitive personal information.
- Check other accounts to ensure they have not been compromised.
    - If the sites have been breached, change passwords for the different accounts and contact the services directly.

Section Review: Password Management

Review Checklist

- ✓ Use unique password for every account
- ✓ Use 10+ mixed characters for strong password
- ✓ Use a passphrase that’s easy to remember but hard to hack
- ✓ Monitor your accounts frequently
- ✓ Consider using a password management system to help remember passwords in a safe way
- ✓ Change your passwords every 6-12 months
- ✓ Use Two-Factor Authentication

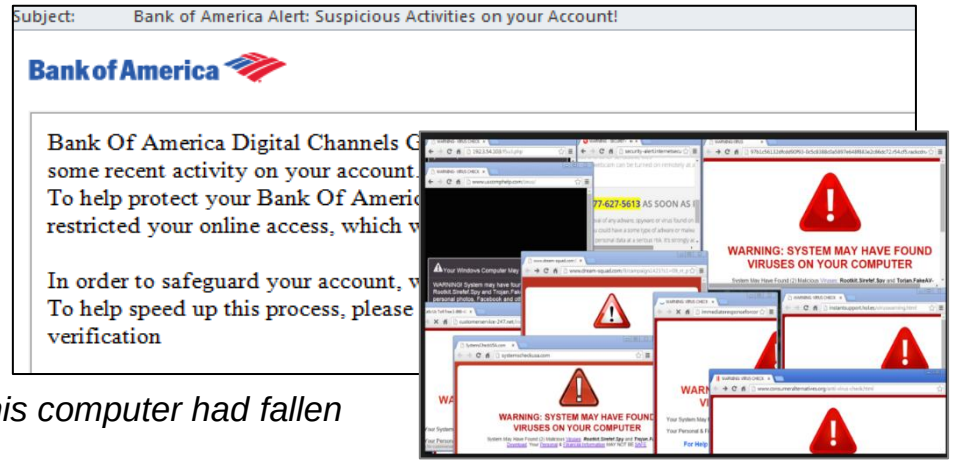
Reflection Questions

- How often should you change your passwords?
- Have any of your accounts been compromised in the past four years?
- Your close friend asks to have your password to send an email from your personal email account. How do you respond?
- What are the three types of characters you should have in every password?
- Ideally, how long should your passwords be?
- How do you remember/store your passwords?
- What do you think are the most common passwords?
- Why should you not use the same PIN and password for all your accounts?
- What are the advantages of two-factor authentication?
- Do you write down your passwords? Why or why not?
- What are the pros and cons of using a password management service?

Common Internet Threats

Imagine the following scenario:

Allen received an email from his credit card company asking him to confirm his account. He hadn't used his online account much and wasn't even sure if he remembered the login password. He recently saw in the news that security settings for online accounts are becoming more mainstream and he didn't want to put himself in danger.



Thinking the email looked legitimate, Allen followed the directions on the email and clicked the link to confirm his account settings…

Soon after, Allen began getting pop-ups on his computer… He realized his computer had fallen victim to Malware.

In this section you will learn about the various threats seen on the internet, including malware, spoof emails, calls and texts, and the different kinds of social engineering. More importantly, you will learn easy-to-remember tips on how to avoid these common threats.

Malware

Malicious software, also known as ***malware,*** is any software intentionally designed to cause damage to a computer or computer network. Malware can take many shapes, from viruses that infect your devices to spyware that tracks your online activities. Malware is the leading cause of compromised information, so it's important to recognize when your computer might be infected.

AT&T Cyber-Aware Tip:
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 [16]

Types of Malware

Different types of malware have different effects on your computer system. Let's take a closer look at the various types:

Virus

Viruses spread from machine to machine through email attachments, malicious websites, spoofed links, file downloads, or shared files like "free" movies.

Worm

Worms can infect and spread without human assistance. They scan networks, find weaknesses, then attack the system.

Trojan Horse

Trojan horses are programs with hidden malicious functions. They look like something you want (e.g., file/attachment) but have malicious content.

Adware

Adware programs are designed to display unwanted ads on a computer. Sometimes they redirect the user to advertising websites and secretly collect data about their online activity.

Spyware

Spyware collects information about the user without their knowledge or consent, sometimes by tracking keystrokes and online activities.

Ransomware

Ransomware locks the user out of their computer, steals their data, encrypts it, and then demands a ransom to get it back. Now, Hackers are asking victims to pay ransom in cryptocurrency because it is not traceable, nor is it insured. No matter what the criminal demands, don't send anything and don't reply to the email or click on any links!

Rogue Security Software

Rogue security software comes disguised as legitimate software, but usually displays bothersome pop-up messages and prompts the victim to pay money to fix made-up issues.

Browser Hijackers

Browser hijackers change browser settings without your permission. They inject unwanted ads into the user's browser or replace the user's home page with the hijacker page. They may contain spyware to steal sensitive information.

Zombie

A zombie is a type of software application that performs malicious tasks and allows an attacker to remotely take control over an affected computer.[17]

How Malware Spreads

Malware can spread from one device to another by any of the following means:

- **The Internet:** Visiting infected websites can expose your device to various malware. Once your device is infected, it becomes a repository and can infect other computers easily.
- **Online Media Downloads:** Downloading media like movies, TV shows, or music from questionable online sources for free is not only illegal but can be potentially dangerous for your devices.
- **Downloading Free Software:** If you are downloading software for free (Freeware and Shareware), there's a good chance that you are also downloading undesirable programs along with the software. Sometimes they might try to add extensions and at other times they might install unwanted programs on your computer.
- **Using Removable Media:** Malware can spread from one computer to another very easily through removable media like DVDs or USB thumb drives. Make sure that your anti-virus software is up and running before you use any such removable media.
- **Email Attachments:** If you receive unsolicited emails with suspicious attachments, you should never download such attachments as they can infect your computer with malware. With over half the world's population using email in 2018, it's no wonder that this is one of the most popular methods used by people with malicious intent. [18]

Social Engineering

Social engineering is a new name for an old con-artist trick. In this scam, a fraudster tries to gain your confidence by convincing you they are someone they are not, or someone whom you can trust, in order to get personal information from you.
These con artists can approach you by phone, email, text or social media. Here are some of their usual tricks:

- Claim to be a friend or family member in trouble.
- Pretend to be a company threatening to shut down an account or service.
- Pretend to be a company with a great discount offer or verifying account information.
- Claim to be a collection agent working on behalf of a government agency or company.[19]

To better identify if you're the target of social engineering, let's look at the different methods used to trick victims:

Phishing

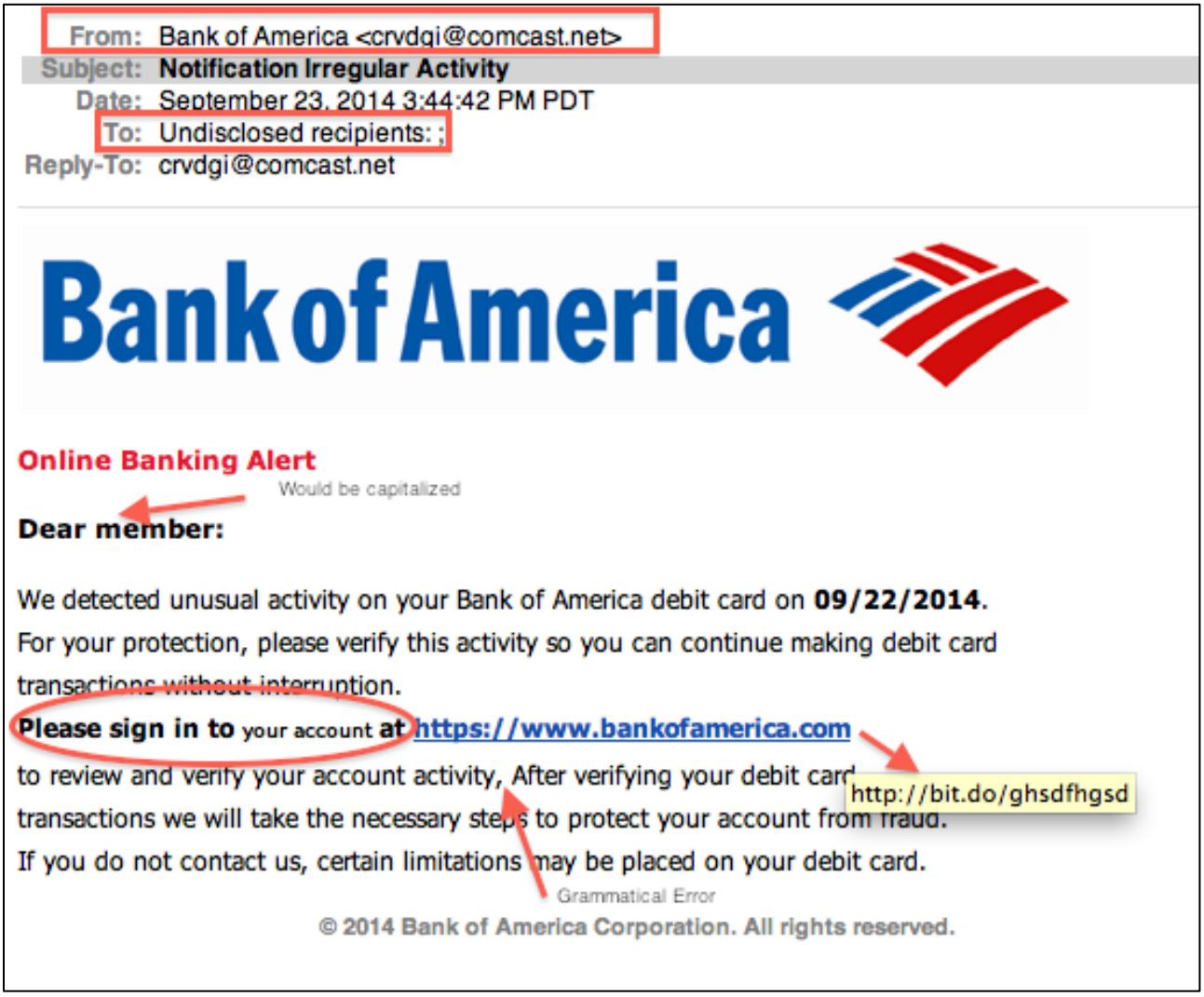
Phishing is when scammers use fake emails to “fish” for information. These messages can look real, but link to fake websites. The website may also look like a trusted, well-known company, but it’s all a trick to get your information – such as Social Security number or bank and credit card account numbers.

A more aggressive fake email may invade your computer with malware as soon as you open the email.

Check these warning signs when you are not sure of an email:

- Use common sense. Read emails carefully and make sure you know the sender.
- Only open emails and attachments or links from a sender you know and trust.
- Go directly to a company’s published website if asked to fill out information. Do not use a link provided in an email.
- Double check the message: Look for false “from” and “subject” lines, spelling errors and grammar mistakes.
- Ensure that a website is secure by checking to see whether there is an “s” after the http in the address (https://) and a lock icon at the bottom of the screen – both are indicators that the site is secure. Never enter payment information on a site that isn't secure.
- Be vigilant. Monitor your bank and credit card statements for any suspicious charges or transfers.[20]

The next page shows an example of a phishing email:



If you wonder whether an email is legitimate, contact the company named in the email by using a phone number or email you found through a trusted source. Most companies do not ask customers for information through email. To report a fraud attempt:

- Report spam emails to Federal Trade Commission (FTC) at https://reportfraud.ftc.gov and to the organization impersonated in the email.
- You can also report phishing by forwarding the suspected email to phishing-report@us-cert.gov.
- Within your email there is typically an option to 'Report as Spam.' By clicking this option, the email is safely removed from your account and the email provider is made aware of the attempt.

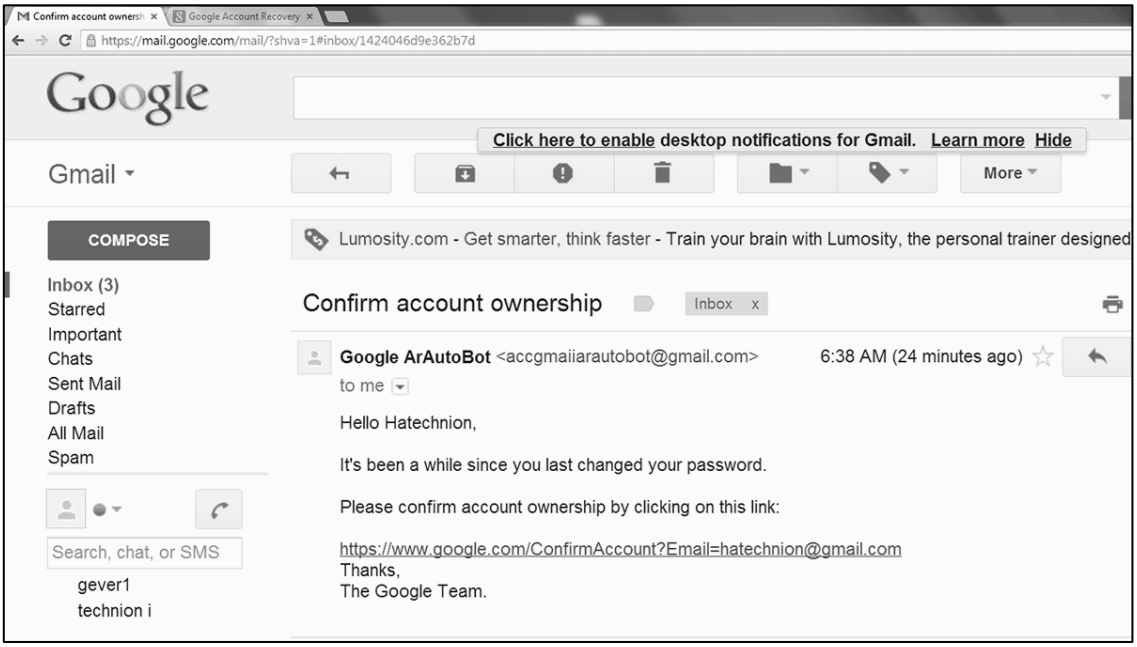
Did you know? 91% of cyberattacks begin with email phishing. 30% of phishing emails are opened and 12% of targeted victims then click on the infected links.[21]

Spear Phishing

Spear Phishing is a more targeted type of phishing in which the attackers disguise themselves as trustworthy friends or entities to acquire sensitive information.

The attacker first gathers information about the target and then uses that information to send fraudulent emails. They might pose as a business that you trust, like a store that you recently shopped at. They might offer you a big discount on a product, or they might ask you to reset your password or verify payment information.

Here is an example of a spear phishing email:



Much like phishing attempts, you should report all spear phishing emails.

Vishing

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

How to be prepared for a vishing attempt:

- Be suspicious of all unknown callers and don't trust Caller ID.
- Ask questions: If someone is asking for personal information, ask them to identify who they work for and then check to see if they are legitimate.
- Call the company back with a telephone number from your records or a number that is verified as legitimate.
- Interrupt to make sure it's not a ***robocall*** or recorded message.

AT&T Cyber-Aware Tip:
If you receive an unwanted robocall:

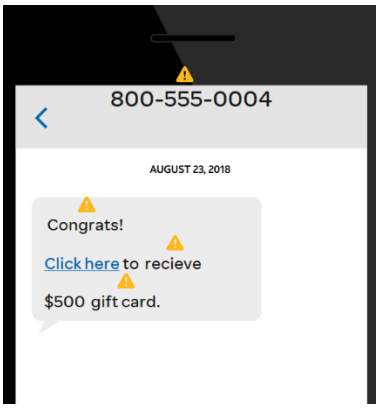
- Don’t try to outwit the con man by deliberately giving out wrong information. Just hang up.
- Add your number to the National Do Not Call list at www.donotcall.gov.
- Beware of spoofing attempts whereby the caller tries to disguise their identity by using numbers that appear to be legitimate.[22]

Smishing

SMiShing is a text message that leads you to a fake website that imitates a real company. That site will ask for personal information – username, password or credit card information. It’s called SMiShing because texts are SMS or "short message system" messages.

AT&T Cyber-Aware Tip:
Here’s how to help protect yourself for SMiShing:

- Only open and reply to text messages from numbers you know and trust.
- Don’t text back someone asking for personal information.
- Don’t click on links included in a text message.
- You can report spam texts to your carrier by forwarding it to the number 7726 (SPAM), free of charge.



Protection Against Common Internet Threats

As you’ve learned, threats are everywhere. In addition to the threat-specific avoidance practices mentioned throughout this section, there are a few other things you can do to protect yourself and your computer from common internet threats.

Antivirus Software

Antivirus is software designed to detect and destroy computer viruses. It is important to remember that the terms “anti-malware” and “antivirus” are often used interchangeably, even though malware and virus are two distinct concepts. Most antimalware solutions use anti-virus as a blanket term, though the software can detect and fix a wide range of malware

issues. They do this because consumers are generally more familiar with the term antivirus.

Antivirus software can be free, or you can purchase a subscription service:
Recommended free services:

- AVG Free https://www.avg.com/en-us/free-antivirus-download
- Bitdefender Free https://www.bitdefender.com/solutions/free.html
- Avast https://www.avast.com/en-us/index#pc

Recommended subscription services:

- Symantec https://www.symantec.com/
- McAfee https://www.mcafee.com/en-us/index.html
- AVG https://www.avg.com/

Regardless of which program you choose, only download from a trusted source. Beware of spoofed URLs! Additionally, only install and run one antivirus program on your devices. Multiple programs can cause problems and conflict with each other, as well as slow down your machine.

Not sure if you already have antivirus installed on your computer? You can check!

Windows Operating System

Click the Start button → Type in Control Panel → System and Maintenance → Review your computer's status and resolve issues → click drop-down button next to Security to expand section → Virus Protection (It should say "On").

If your version of Windows does not have these options, simply utilize the Search Box and type in 'antivirus'.

macOS

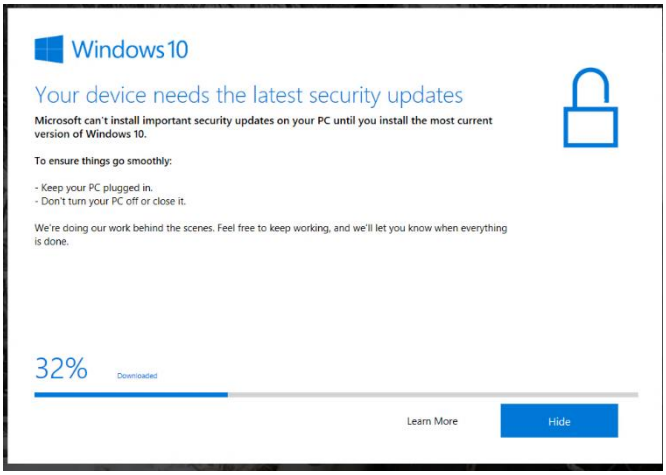
Built-in anti-malware protection on Mac OSX and macOS automatically regulates virus protection.

Security Updates

Your operating system will periodically remind you of important security updates necessary to safeguard your computer. Make sure to schedule these updates at your earliest convenience. Hackers take advantage of security flaws and specifically attack those users who have been left vulnerable because they ignored the security update.

Windows Operation System

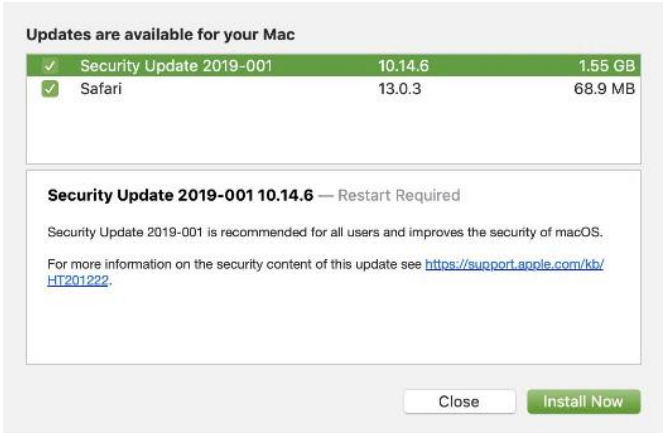
All updates in Windows 10 are automatic. They cannot be turned off, but you can postpone them. Check for available updates manually:



- Click on the Windows button on the left and open Settings.
- Click on Update and Security.
- Go to Windows Update.
- Click on Check for Updates.

MacOS

Periodically, Apple releases updates to your macOS software (which can include updates to apps that come with your Mac and important security updates). To install updates manually on your Mac, do one of the following:



Choose Apple menu > System Preferences, then click Software Update.

Virtual Private Network (VPN)

A ***Virtual Private Network (VPN)*** redirects your internet traffic and helps hide your location when you visit different websites on the internet. It also encrypts any data you send across the internet, making it indecipherable to anyone who intercepts your traffic. [23]

You can subscribe to a legitimate VPN service and pay a monthly fee for the use of the VPN app. You can also purchase a VPN connection through your cell phone or internet provider.

Make sure to do proper research and then choose a VPN service that's reputable and reliable. If you use Opera as your web-browser, it has a built in VPN. To set-up:

- In Opera, go to Settings.
- In the sidebar, click Advanced, then click Privacy & security.
- Under VPN, click Enable VPN.

Some recommended VPNs include **NordVPN**, **ExpressVPN**, and **IVPN**. These are paid services but are easy to use and have effective results. [24]
Some free options include:[25]

- ProtonVPN https://protonvpn.com/free-vpn
- TunnelBear https://www.tunnelbear.com/
- Windscribe https://windscribe.com/

Public Internet Connectivity

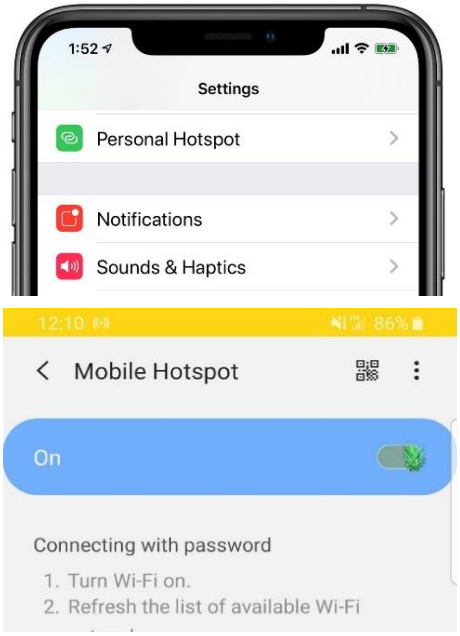
Being connected to the internet 24/7 is convenient, but it's not always safe. Public Wi-Fi is not a secure network. Any information you share (or access) can be tapped into while on a public network, and anyone near you can intercept the connection.

AT&T Cyber-Aware Tip:
If you use public Wi-Fi, here are some tips to protect yourself:

- Make sure you connect to the right Wi-Fi network. Double-check the name of the Wi-Fi network. Watch out for other networks with alternate spellings or added numbers.
- Be wary of networks without passwords. Many hotspots require a password. This does not ensure security, but it does add a layer of security and most criminals do not put password-protection on their fake networks.
- Don't do sensitive activities on public Wi-Fi networks. Avoid online shopping, banking or other activities involving sensitive data while connected to an open network. Don't give the bad guys the opportunity. to steal anything valuable, like your Social Security number or credit card information.
- Don't download or upload on public Wi-Fi networks. If you can, wait to share documents or download content when you are on your own safe and secured network.
- Consider using a virtual private network (VPN). [26]

Personal hotspots (or mobile hotspots) are an alternative option to public Wi-Fi. Hotspots provide data-tethering functionality from a cellular-enabled device, allowing you to share its data connection to another device via Wi-Fi. It is a great way to work from a laptop without having to worry about finding a Wi-Fi connection. However, keep in mind that:

- The cost of cellular data may be expensive, depending on your service provider.
- Personal hotspots might not be included in your cell phone plan.
- Hotspots must be manually turned on and off – beware of the charges!



Did you know? 54% of online adults report that they use insecure public Wi-Fi networks – with around one-in-five of them reporting that they use such networks to carry out sensitive activities such as online shopping or online banking. [27]

Section Review: Common Internet Threats

Review Checklist

- ✓ Malware comes in different forms and each form infects your device differently.
- ✓ If you receive a suspicious email, do not open the email, click links, or download attachments.
- ✓ Quickly scan emails to identify red flags such as typos, fishy email address, or requests for personal information.
- ✓ Do not respond to strange text messages.
- ✓ Contact companies to report spoof emails, false texts, or spam phone calls whenever you receive them.
- ✓ Never share personal information over the phone or through email unless you have initiated contact.
- ✓ Schedule your computer to conduct weekly security updates as well as a weekly antivirus scan.
- ✓ Reliable FREE software is available for the public. Do your research and when in doubt, at the very least, use pre-installed antimalware software that comes with your computer.

Reflection Questions

- Have you had malware on your computer? Can you identify what kind of malware it was? How were you able to fix the issue?
- Would you pay the ransom if your files were held hostage? Why or why not?
- Have you ever mistakenly clicked on a link within a suspicious email?
- What possible red flags should you look out for in a spoof email?
- What can you do if you are not sure of the authenticity of an email you received?
- Should you ever join a public Wi-Fi connection? When is it safe to do so? When is it not safe to do so?
- If a virus attacks your computer, what are the steps you can take to get rid of the infection?

Scams and Fraud

Imagine the following scenario:

You're sitting at home when the phone rings. You answer, and the person on the other end of the line says "Hello, my name is Angela from [cell phone provider]. Do you have a moment to talk about your current phone plan? I will just need your social security number to verify your account."

How do you know this is a legitimate call? Do you share your social security number?

Or consider this email that showed up in your inbox:
"Congratulations! You have won an all-expenses paid trip to Hawaii! Complete the form below to claim your free vacation!"

Why did you get selected for a free vacation? Who is the form being shared with? Scams like those mentioned above happen to normal people every day. In this section, you will learn about the various types of phone and online scams, including identity theft and how to prevent it. You will also learn some safety tips for online shopping.

Did you know? The Federal Trade Commission (FTC) can help with phone and email scams. Report scams to FTC at https://reportfraud.ftc.gov or call 877-382-435.

Scam Awareness

During scam attempts, bad guys like to pose as the companies and agencies listed on the next page. One of the most important tips to remember with any of these scams is that you are never obligated to share information if you feel uncomfortable.
If you question the authenticity of any call it is best to hang up and call the company back at the number on their website and verify the authenticity of the caller.

Financial/Investment Companies

- Target retirement and bank accounts
- Spoof emails requiring log-in
- Phone calls requesting PIN numbers or SSN

Government Agencies (IRS, FBI, SSA, etc.)

- Emails and phone calls requesting SSN or demanding payment

Insurance Companies

- Target home, life, health, and car coverage
- False claims received through email
- Phone calls requesting personal information regarding an unfiled claim

Donation Organizations

- Typically, from little known charities or newly formed organizations
- Email requests for money donations
- Phone calls asking for monetary donations without an option to donate used items

Dating Sites

- Email requests for personal information regarding your account
- Phone calls introducing a new match or requesting more personal information

Online and Phone Surveys

- Scam emails with live links to complete an online survey, typically for a prize
- Phone surveys to win a trip or prize

IRS / Tax Scams

IRS-related scams are very common these days, especially during the tax season. Scam artists posing as IRS officials take advantage of taxpayers by playing on their fears. As people prepare their tax returns, those emotions are stronger, making them easier targets for scam artists.

Scammers have also expanded beyond the IRS and are claiming to be from other government agencies like the Social Security Administration. Regardless of their tactics, their goal is the same: to get you to send them money.[28]

Remember, if you get a suspicious email claiming to be from the IRS or any other government agency, do not open any attachments or click on any links. They may have malicious code that will infect your computer. **Forward the email to phishing@irs.gov and then delete the email.**

AT&T Cyber-Aware Tip:
If you receive a call that is an IRS scam:

- Do not believe them!
- Never give these scam artists bank account information, credit card numbers, your Social Security Number or any other sensitive personal information.

- The IRS and other agencies will usually contact you first by mail and give you a chance to resolve any issues. You can read more on the IRS website.
- While the IRS recently started using collection companies, these companies and the IRS will not threaten you with arrest. The IRS also does not accept gift cards – especially iTunes and Amazon – as payment.
- While the tax season is prime season for these scams, they may happen at any time of the year.
- For other government benefit scams, federal government agencies and federal employees also don't ask people to send money for prizes or unpaid loans. They will not ask you to wire money or add money to a prepaid debit card to pay for anything.[29]

Send-Money / Wire-Transfer Scam

A ***send-money or wire-transfer scam*** involves a call or email where an individual posing as a friend asks for money. The caller or emailer may act desperate for financial help because they are stranded out of the country, lost their wallet, or are injured. They then ask for money to be wired to a specific location.

To handle this scam via phone:

- Ask personal questions that only that real person would know the answer to.
- Verify that the person calling is out of the country (contact another relative, the caller's workplace, etc.).
- Never give credit card information or bank information over the phone.
- If you feel that the person is in serious trouble and needs immediate help, get as much information as possible regarding their location and the nature of the emergency. Then contact the proper authorities.

To handle this scam via email:

- Do not respond to the sender - instead, email the person using an email address you have on file.
- Try contacting another family member or friend to get contact information for the person requesting the money.
- Never send a wire transfer, credit card or bank account information without confirming that the request is legitimate.

Foreign Lottery Scam

In a ***foreign lottery scam***, the bad guy calls and says, “Congratulations, you won the Jamaican Lottery! [or some other big prize]. To claim it, all you need to do is to pay the fees or taxes on your winnings.” They’ll tell you they can help you do it easily over the phone, if you’ll just give them some of your financial information, a credit card number, or prepaid cash/gift cards.[30]

AT&T Cyber-Aware Tip:
If you receive a call that claims you won a foreign lottery or some other prize:

- Do not give them any information. Resisting that urge can help protect you from this and similar types of scams.
- Recognize that if they ask you to pay to get something you won – it’s a scam.
- Only answer calls from familiar phone numbers. If you don’t recognize the number, especially the area code, don’t answer.
- If you do answer, and realize it’s a possible scam, hang up. Then report the number to the FTC.[31]

Survey Scam

Survey scams usually come in the form of an email that prompts you to click on a suspicious link to complete a survey. You might also receive a phone call from companies conducting surveys to give out some grand prize, like a trip or a car. A survey scam email might read something like:

We want to thank you for being a loyal Google user. Today is your lucky day! You are one of the 10 randomly selected users who will receive a gift. Just complete this short and anonymous survey. But hurry! There are only a few gifts available today.

To handle a survey scam:

- Do not click on the suspicious links.
- Do not give out any personal or financial information.
- Report the spam email or phone call to the relevant authority.[32]

Money-Making Scam

A ***money-making scam*** is a get-rich-quick scam which promises that you can make some amount of money working from home with minimum effort. This type of scam usually prompts you to purchase a trial kit or training package for a fixed amount to be paid via PayPal or by check. The offer usually sounds too good to be true… and that’s because it is!

Signs of a money-making scam:

- You are asked to spend some money up front.
- The company is based overseas.
- Little to no contact information is provided for the company.

If you are unsure of the legitimacy of the offer, do a quick Google search. You might find that there's already information online about the illegitimacy of the suspicious company.[33]

Computer Security / Tech Support Scam

In ***tech support scams***, bogus tech support employees make calls claiming to be from trusted companies like Microsoft or Apple.

They tell you that they have detected a problem with your computer, and they need remote access to the device in order to help fix the issue. Once they have access to the computer, the hacker will either demand money to fix the made-up issue or they might install malware on the computer that helps them steal valuable personal data from the victim.

The on-screen pop-up or email version of this scam similarly warns you about security issues on your computer. It instructs you to dial a number for help or click a link to download antivirus software.

It might look like an error message from your operating system, or it might look like antivirus software. It may even use logos from trusted companies or websites.[34]

AT&T Cyber-Aware Tip:
If you think you are the victim of a tech support scam:

- Do not call the number or click on the link! By doing this, you may give the hacker access to your machine, you may download malware, or you may start a conversation you don't want to have.
- Do not assume that people contacting you are working for the company they say they are. Legitimate companies will not call you and tell you that you must pay for tech support. If a pop-up message appears in your web browser offering help, or saying a threat has been detected, it is likely a scam. (Note: this is different from a pop-up window from your security software. To confirm the warning, close your browser and contact your security service through a trusted email or phone number.)

- Don't share personal information. Do not share sensitive financial information like passwords, credit card, or bank account routing numbers over the phone. And do not supply a prepaid gift card as payment.
- **REMEMBER: Tech support will not contact you if you did not contact them first.**[35]

Did you know? This very CyberGenerations program was created when the CyberPatriot Commissioner received a phone call from his mother regarding the legitimacy of a phone call from “Microsoft.” As it turned out, that phone call was a tech support scam!

Dating Scam

Dating scams are unfortunately rampant, and they are particularly disturbing because the scammers perceive their victims as gullible and despondent and their ultimate intention is to take advantage of any vulnerability.

Scammers usually connect with their victims through some online dating site, posing as interested singles looking to make a genuine connection with a like-minded individual. They have an elaborate profile and backstory with pictures of real people. These con artists strike up romantic relationships with unsuspecting victims and then ask for money through emotional manipulation or by devising fake emergencies. Sometimes they might pretend to be Americans living abroad who need money to get back to the country and meet the victim.

How to handle a dating scam:

- Be cautious of people who make grand promises of love and marriage even before meeting you in person.
- Beware of people who claim to be Americans working overseas.
- Even if you feel a strong connection, don’t ever send money to someone you haven’t met in person.[36]

Charity and Door-to Door Scams

Charity scams occur when scammers take advantage of kind-hearted people and swindle them into “donating” to sham organizations. These types of scams are usually very sophisticated, and many people fall prey to them on a regular basis. These scams pretend to help an array of disadvantaged people such as cancer patients, starving children, or veterans in need. Some scammers may also make false tax deduction claims and ask for personal information.

Whenever there's a natural disaster or ongoing humanitarian crisis, these scammers use high-pressure sales tactics to extract money from victims. [37]

AT&T Cyber-Aware Tip:
Door-to-Door Scams

Most salespeople knocking at your door are legitimate – they're just trying to sell a product or service. But there are some who are trying to scam you out of money or information with no actual product or service.[38]

These scammers may try to confuse you or pressure you to give them some kind of payment. Or they may just ask for information so they "can confirm with their boss that they actually talked with you" and use that information later as part of an ID theft scam. They may even carry a tablet or other device to try to access your personal information while you stand there.

Here are things you should look for to help you decide quickly if that door-to-door salesperson is legitimate or out to scam you.

- The salesperson should wear a visible badge that displays the company name listing them as an employee.
- Watch out for high-pressure sales tactics.
- Authorized door-to-door salespeople should carry general sales collateral. Ask the salesperson to leave you with written materials or a website you can visit later.
- If you feel uncomfortable, end the conversation and shut the door.

If you still question the salesperson's story, call the company they claimed to work for. Use a number on your bill or from a confirmed, secure source or website to find out if the offer is true. If not, you can alert the company of a possible door-to-door scam in your neighborhood.

Identity Theft

Identity thieves defraud people and the government by assuming the identities of unsuspecting victims in order to commit illegal activities. The increasing use of online tax filing services makes it even easier for scammers to steal your information and use it to make fraudulent tax claims.

Scammers may also use the stolen information to submit fraudulent billings to Medicare or Medicaid or to receive other social benefits. If you suspect that you are a victim of identity theft:

- Alert the organization where the theft occurred.
- Contact a credit reporting agency and ask them to place a fraud alert for your credit report.
- Report identity theft to the FTC.[39]

Identity theft can be costly in time, money and personal reputation. But there are steps you can take to help protect yourself:

AT&T Cyber-Aware Tip:
How to protect yourself from Identity Theft

- **DETER** identity thieves by safeguarding your information. Shred documents and don't share information.
- **DETECT** suspicious activity early by routinely monitoring accounts.
- **REVIEW** statements and your credit report.
- **DEFEND** against identity theft as soon as you suspect it. Immediately contact potentially impacted accounts, close accounts that were tampered with, and place a fraud alert on your credit reports. Be sure to also file a police report and report the incident to the FTC at www.IdentityTheft.gov. [40]

Did you know? Major nationwide consumer reporting companies like Equifax, Experian, and TransUnion are required to give you a free copy of your credit report each year if you ask for it. Visit www.AnnualCreditReport.com for more information.

Online Shopping

Almost everybody shops online these days. It's a convenient, hassle-free way to buy the things you want and need. But if you aren't careful, it can lead to more trouble than it's worth. When shopping online, consider the following:

- Use reputable retailers to avoid the risk of being sold counterfeit goods. If the price seems too good to be true, research the seller before buying.
- Don't believe all the reviews you read online. Reviews can be bought and sold, and phony reviews are everywhere. Be especially skeptical of reviews which seem generic.
- Be wary of shopping from shady websites. Some websites that offer too-good-to-be-true deals are trying to steal your information. Always verify the legitimacy of a website before providing PII.
- Be careful of additional fees which can increase the prices of the products considerably. Always check the additional fees that you are being charged which usually show up towards the end of the checkout process like shipping fee, handling fee, shipping insurance etc. If you think that the costs somehow don't add up, cancel the order right away.

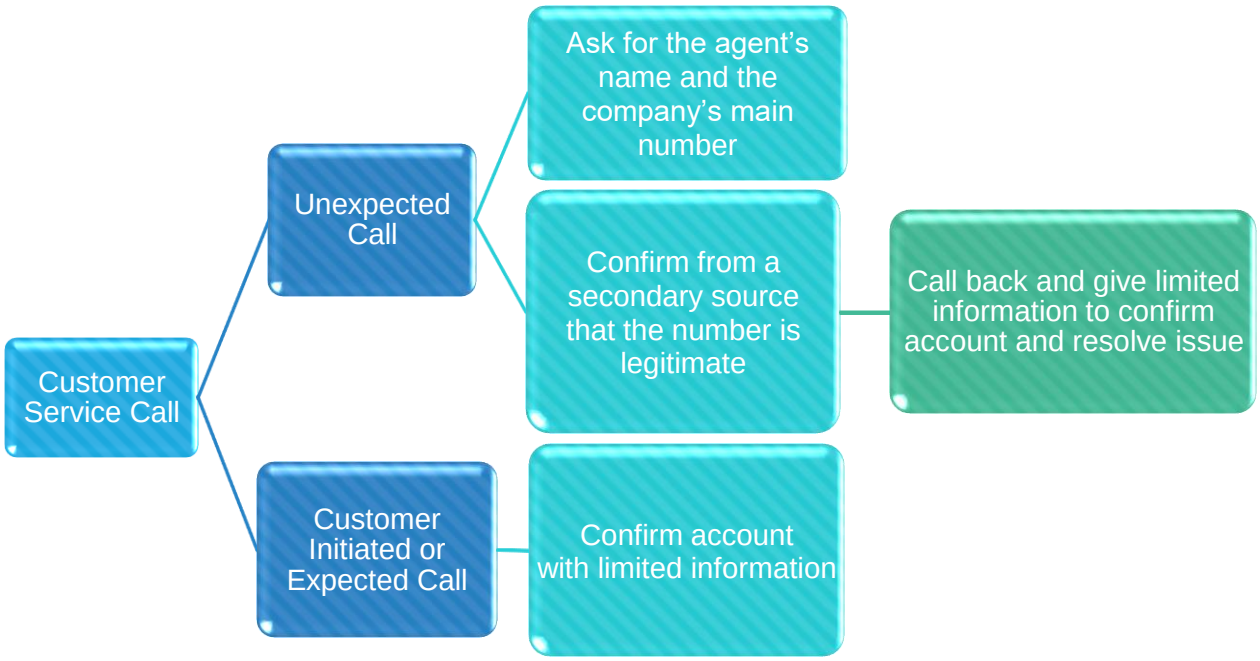
- Read the site's privacy policy before sharing sensitive information. Make sure to look out for policies pertaining to how the retailer plans on using your personal information.
- Beware of providing financial information while using an unprotected Wi-Fi connection. It is best to make any online financial transactions at home using a safe and secure internet connection.

Sharing information

With all these scams and internet threats, it can be difficult to know when sharing your information is safe. When trying to decide if you should share your information or not, remember the following:

- Companies will never use an automated system to request information from you or tell you that your account has been locked or disabled.
- Debt collectors will never require you to pay over the phone. Ask them to mail you a hard-copy bill.
- Beware of "secure" online payment options (when in doubt, call the company directly).

The flow-chart below depicts the process for determining if it's safe to share your information:



Section Review: Scams and Fraud

Review Checklist

- ✓ Phone and internet scams most commonly target uninformed customers.
- ✓ Phone scams can easily be avoided by not answering a phone call and allowing it to go to voicemail.
- ✓ Always verify a company phone number before returning a call.
- ✓ Never click on a pop-up or link unless you are sure of its authenticity.
- ✓ Always try to verify the authenticity and reputation of an online shopping website before making a purchase.

Reflection Questions

- What are the different types of phone and email scams?
- Have you ever shared PII over the phone or over email? What information did you worry the most about sharing?
- What government agencies are most often impersonated by spoof calls? How can you check to see if the call or email you received is real?
- What is the difference between a user-initiated call and a customer service agent call?
- What steps can you take to determine if a site is safe?

Social Media Safety & Awareness

Imagine the following scenario:

Hank enjoyed staying connected with his lifelong friends on Facebook. They had a 50-year high school reunion coming up, so he was using Facebook more to help with the event planning.

It had been so long that Hank couldn't remember all of the names of his classmates but tried his best to accept every friend request he received. His page was private for security reasons, but new 'old' friends were always welcome!

One afternoon, Hank noticed that he had a duplicate friend request from a pal he added years ago. Confused, Hank accepted the request.

Days later Hank's son called him to ask why he had created a second account on Facebook. Hank was confused. It seemed that someone had created a new account using Hank's photos and information. They even had details about his most recent trips and a post requesting money for charity!

Where did the duplicate account come from? And why was Hank the target?

Social media users fall victim to scams like this every day. While social media is a great way to stay connected with friends and family, it can be dangerous if not used properly. In this section, you will learn about the various social media sites, what they're used for, and how to stay safe and protect your information while using them.

Did you know? 42% of the world's population —3.2 billion people — use social media, and 34% of people that are 65+ years old use Facebook. This percentage is much higher than any other social media site. [41]

Social Media Sites

Facebook (the most popular among senior citizens)

- Connect with friends and family and send private messages
- Share updates/photos/videos and comment on other users' posts
- Join common interest groups
- Play games

Twitter

- Broadcast short messages (“tweets”) in 280 characters or less
- Post pictures, videos, and website links
- Follow other users
- Send private/direct messages
- Re-tweet other users’ posts, or tweet at companies and celebrities

Instagram

- Share photos and videos (with option to edit photos before posting)
- Add stories in the form of photos or videos which disappear after 24 hours
- Follow friends, brands, celebrities, and influencers
- Send private/direct messages
- Often used as a marketing tool

YouTube

- Video-sharing website
- Watch user-generated content
- Allows users to video-blog (also known as ‘vlogging’)
- Upload your own videos or share videos you enjoy
- Subscribe to the channels you like

Pinterest

- Digital pin board
- Often used for fashion, cooking, crafting, and home décor inspiration
- Post interesting visual content called ‘pins’
- Follow and/or message other users

LinkedIn

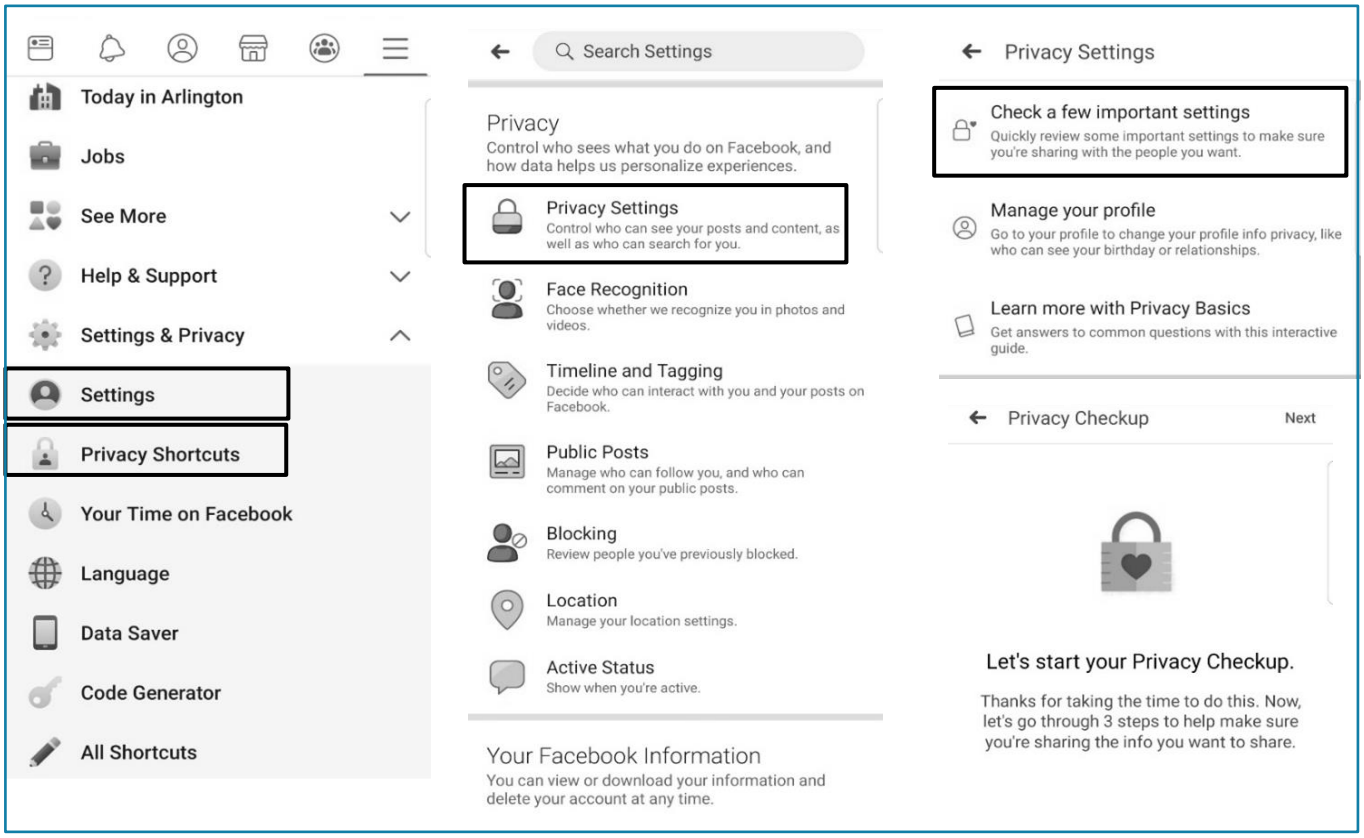
- Professional social media site
- Connects people through their careers and digital resumes
- Announce job changes
- Endorse skills of coworkers
- Upload resume and apply for jobs

Social Media Privacy & Safety

Privacy settings vary on different social media sites. Most privacy setting changes can be made from a site’s ‘settings’ or ‘privacy’ menu.

The popularity of Facebook has made it one of the most frequently used social media sites. Here’s how you can start a quick Privacy Checkup for your Facebook account on your smartphone:

Go to Settings and Privacy from the ≡ menu à select Settings → select Privacy Settings → select Check a few important settings → Follow the steps by clicking next and complete the Privacy Checkup.



While it's important to set your privacy settings to a more secure level than the default settings, there are also additional steps you should take to be as safe as possible while using social media:

- **Be picky:** Only accept or follow friends you know in real life.
- **Do not post your location:** Friends who tag you may also be giving out your location.
- **Be careful with apps:** Gaming apps like 'Candy Crush' may give away your location or other identifiable information. Never allow apps to store your log-in credentials.
- **Assume everything you post online is permanent:** Do not say something you will regret. If you wouldn't say it to someone's face, you shouldn't post it.
- **Do not over-share:** Just because a site asks for information, doesn't mean you have to give it. When signing up for an online account, fill in the required (*) fields and leave out the rest to protect your privacy.
- **Customize your privacy settings:** Do not use the default settings. They usually only provide the bare minimum in security. Update your settings to provide maximum protection, and review the settings regularly, as some site settings may change without user permission.

- **Be careful about who can access your contacts:** You don't want random sites to have access to your contacts. Some sites might use this information to send emails to everyone in your contact list.
- **If you get a suspicious message from one of your contacts, double check:** Scammers can break into someone's account or steal publicly available information to create a forged account that impersonates someone else. If you suspect that a message is fraudulent, find another way to contact your friend and verify the dubious claim.[42]

Online Dating Sites

We mentioned online dating scams in the previous section. Scammers can use general social media sites (Facebook, Instagram, Twitter) to trick people into online relationships, but they might also use dating-specific websites for older adults and seniors. The sites below are some of the more reliable dating sites, but you should still use caution while using them:

Here are some tips for using online dating sites:

- Once you have made the initial connection, search for the person online and see if you can find any additional information, or double check what you were already told.
- Search other social media platforms to verify the individual's identity.
- Don't be hasty about meeting in-person. Communicate through text messages, video chat, or use other digital methods to establish a connection first.
- Be careful about disclosing personal information like your address or telephone number.
- When you meet for the first time, meet in a public place like a restaurant or the movies. Do not invite them over to your place![43]

Social Media Scams

Just like phone and email scams, social media scams are common and can happen to anyone.

Dummy Profiles

Dummy profiles are just what they sound like: fake profiles claiming to be a person they are not. Hackers can easily steal the information of your loved ones and friends with whom you are connected on social media sites. They can then impersonate the 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.

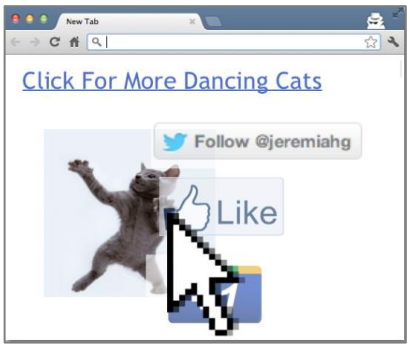
Did you know? Facebook pulled down more than 3 billion fake accounts from October 2018 to March 2019. The social network estimates about 5% of monthly active accounts are fake.[44]

Clickbait

Clickbait 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.

Examples of clickbait headlines include:

- *Do just this one thing and you will never have to go on a diet ever again…*
- *These yesteryear celebrities are practically unrecognizable now. #8 will shock you…*
- *This one practice can help you save thousands in utility bills…*



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.

Sick Baby Hoax

In ***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's very little they can do to stop the circulation of the post.

Some of these hoaxes can be detected by bad grammar and vagueness in the post, but others can be very detailed and appear convincingly authentic. If you suspect a sick baby hoax, report the post through the social media site![45]

Social Media Charity Scam

A new scam is taking advantage of people's desire to help others, expeically during the holiday season. In this scam, the bad guys use communication through social media to build trust and convince customers to do their dirty work.

Some say they are working with a charitable organization and ask you to provide reliable phones to less fortunate people who need them.

They say they have the money for the phones, they just need you to place the order on your account. They may even ask you to go to a store and ship the phones to their address.

The money for the order – up to $30,000 – appears as an ACH (pending) transfer on your account, but when you order the phones, the money disappears. The transfer never happens.

AT&T Cyber-Aware Tip:
If you receive such an inquiry:

- Do not reply and do not share personal or account information.
- Be wary of anyone asking you to order/ship phones to an unknown address.
- If you are interested to see if the request is legitimate, call the entity using a phone number found from a trusted source, such as their secure website or your bill. (Do not use a number or website provided by the possible scammer)
- Report the matter to the organization that supposedly contacted you.[46]

Social Media Etiquette

Just like table manners are important, social media etiquette is also important. It is easy to be a valuable contributor and to use the social media sites how they were intended to be used. Follow these main rules of social media use and you will be well-protected:

- **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.[47]

Section Review: Social Media Safety & Awareness

Review Checklist

- ✓ Know the function of social media sites before you join.
- ✓ Exercise caution when using online dating sites.
- ✓ Enable security settings to ensure your information is private and only shared with those you choose to share information with.
- ✓ When using social media be aware of social etiquette: Be careful what you share, think before posting information that is yours or someone else's and be mindful of who you 'friend' or 'follow.'
- ✓ Malware can easily be downloaded or spread by social media spammers. Verify a link source before you click.

- ✓ There are many scammers on social media sites. Be careful about what you share online and who you trust!

Reflection Questions

- What social media account(s) do you use?
- Does social media help you keep in touch with friends and family more?
- Have you ever received malware from a social media post? If so, how did you handle it?
- Do you know how to set a privacy policy on a social media account?
- What should you keep in mind when you are posting a photo of someone else or reposting an already existing photograph?
- Should you accept all friend requests? Why or why not?
- Is it a good idea to share your upcoming vacation details on social media?
- What details about a strong password do you think would apply to your social media accounts? Do you think automatic login is ever a safe option?

Resources & Aging Services

Should you ever find that you are a victim of identity theft or any other type of scam, please use the following resources to help address the issue.

Government Resources

General Resources
Online Guide to government information/services → https://www.usa.gov
1-844-872-4681
Attorneys General (by State) →
http://www.naag.org/naag/attorneys-general/whos-my-ag
Elder Justice Initiative (Dept. of Justice) → **https://www.justice.gov/elderjustice**

Reporting phishing attempts and scams
Department of Homeland Security → phishing-report@us-cert.gov

Internal Revenue Service (IRS) → phishing@irs.gov

Federal Trade Commission → https://reportfraud.ftc.gov/#/ 1-877-438-4338

United States Senate Special Committee on Aging → 1-855-303-9470

Reporting Tax Fraud or Identity Theft
Identify Protection Specialized Unit of the IRS → 1-800-908-4490

Federal Trade Commission → https://www.identitytheft.gov/

Taxpayer Advocate → 1-877-777-4778

Social Security Administration → 1-800-772-1213

Medicare Fraud → 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 31 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. Information for divisions in each US State and Territory can be found in the table on the next page:

State	Website	Phone Number
Alabama	http://www.alabamaageline.gov/	1 (800) AGE-LINE 1 (800) 243-5463
Alaska	http://dhss.alaska.gov/dsds	1 (800) 478-9996
Arizona	https://des.az.gov/services/aging-and-adult/division-aging-and-adult-services	(602) 542-4446
Arkansas	http://www.daas.ar.gov/	(501) 682-2441
California	https://www.aging.ca.gov/	(916) 419-7500
Colorado	https://www.colorado.gov/pacific/cdhs/aging-and-disability-resources-colorado	(303) 866-5700
Connecticut	http://www.ct.gov/agingservices	(860) 424-5274
Delaware	http://dhss.delaware.gov/dsaapd/	1 (800) 223-9074
District of Columbia	https://dcoa.dc.gov/	(202) 724-5626
Florida	http://elderaffairs.state.fl.us/doea/arc.php	1 (800) 963-5337
Georgia	https://aging.georgia.gov/	1 (800) 436-7442
Hawaii	https://www.elderlyaffairs.com/	1 (800) 768-7700
Idaho	https://aging.idaho.gov/	(877) 471-2777
Illinois	https://www.illinois.gov/aging	1 (800) 252-8966
Indiana	https://www.in.gov/fssa/2329.htm	1-800 986-3505
Iowa	https://www.iowaaging.gov/	1 (800) 532-3213
Kansas	https://www.kdads.ks.gov/	(785) 296-4986
Kentucky	https://chfs.ky.gov/Pages/index.aspx	1 (800) 372-2973
Louisiana	http://www.dhh.louisiana.gov/index.cfm/subhome/12	1 (866) 758-5035
Maine	https://www1.maine.gov/dhhs/oads/	1 (888) 568-1112
Maryland	http://www.aging.maryland.gov	(410) 767-1100
Massachusetts	http://www.mass.gov/elders	1 (800) 243-4636
Michigan	http://www.michigan.gov/osa/	(517) 373-8230
Minnesota	http://www.mnaging.org/	1 (800) 882-6262
Mississippi	https://www.mdhs.ms.gov/	1 (800) 948-3090
Missouri	https://health.mo.gov/	(573) 443-5823
Montana	http://dphhs.mt.gov/seniors	1 (800) 332-2272
Nebraska	http://dhhs.ne.gov/pages/aging	(402) 471-3121
Nevada	http://adsd.nv.gov/	(775) 687-4210
New Hampshire	https://www.dhhs.nh.gov/dcbcs/beas/	1 (800) 275-3447
New Jersey	http://www.state.nj.us/humanservices/doas/home/	1 (877) 222-3737
New Mexico	http://www.nmaging.state.nm.us/	1 (800) 432-2080
New York	https://aging.ny.gov/	(844) 697-6321
North Carolina	https://www.ncdhhs.gov/divisions/daas	(919) 855-4800
North Dakota	http://www.nd.gov/dhs/	(701) 328-4601
Ohio	http://aging.ohio.gov/	1 (800) 266-4346

State	Website	Phone Number
Oklahoma	https://oklahoma.gov/okdhs.html	(405) 521-2281
Oregon	http://www.oregon.gov/DHS/seniors-disabilities	(503) 945-5600
Pennsylvania	http://www.aging.pa.gov	(717) 783-1550
Rhode Island	http://www.dea.ri.gov/	(401) 462-3000
South Carolina	https://aging.sc.gov/	1 (800) 868-9095
South Dakota	https://dhs.sd.gov/LTSS	(605) 773-5990
Tennessee	https://www.tn.gov/aging	(615) 741-2056
Texas	https://hhs.texas.gov/services/aging	(512) 424-6500
Utah	https://daas.utah.gov/	(801) 538-4171
Vermont	http://dail.vermont.gov/	(802) 241-2401
Virginia	https://www.vda.virginia.gov/	(804) 662-9333
Washington	https://www.dshs.wa.gov/altsa	1 (800) 865-7801
West Virginia	http://www.wvseniorservices.gov/	(877) 987-3646
Wisconsin	https://www.dhs.wisconsin.gov/aging/index.htm	(608) 266-2536
Wyoming	https://health.wyo.gov/aging/	(866) 571-0944
American Samoa	https://www.americansamoa.gov/territorial-administration-on-aging	(684) 633-1251
Guam	http://dhss.as/	(671) 735-7101
Northern Mariana Islands	https://resources.caregiver.com/listing/cnmi-aging-disability-54c2c0d952d07.html	(670) 664-2598
Puerto Rico	https://goo.gl/C55QRr	(787) 721-6121
US Virgin Islands	http://www.dhs.gov.vi/seniors/index.html	(340) 774-0930

Post-Program Survey

Congratulations! You've competed the CyberGenerations Self-Paced Guide! We hope you enjoyed it and feel better equipped to protect yourself from online threats. Please take 2-3 minutes to complete the post-program survey in the link below. Your honest feedback is extremely valuable in making continuous improvements to the program.

CyberGenerations Survey (via Google Forms):
http://bit.ly/2Sk9Z5S

Should you have any questions or comments regarding your experience with CyberGenerations, please contact the CyberPatriot staff at info@uscyberpatriot.org or call 877-885-5716.

Sources

[1] https://whatis.techtarget.com/definitions/C/page/21

[2] https://securityboulevard.com/2021/03/cybercrime-to-cost-over-10-trillion-by-2025/

[3] https://www.atg.wa.gov/internet-safety-seniors

[4] https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html

[5] https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07

[6] https://searchsecurity.techtarget.com/definition/dumpster-diving

[7] https://www.techopedia.com/definition/4103/shoulder-surfing

[8] https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/mobile-devices/

[9] https://support.apple.com/kb/PH2698?viewlocale=en_US&locale=en_AU

[10] https://thecyberwire.com/glossary.html

[11] https://thebestvpn.com/safe-internet-browsing/

[12] https://seotribunal.com/blog/google-stats-and-facts/

[13] https://thebestvpn.com/safe-internet-browsing/

[14] https://nordpass.com/secure-password

[15] https://www.groovypost.com/unplugged/two-factor-authentication-guide-secure-online-accounts/

[16] https://about.att.com/pages/cyberaware/ae/malware

[17] https://networkbees.com/2017/02/14/types-of-malware/

[18] https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf

[19] https://about.att.com/pages/cyberaware/ae/se

[20] https://www.braveriver.com/phishing-emails/

[21] https://bigdata-madesimple.com/77-facts-about-cyber-crimes-one-should-know-in-2018-infographic/

[22] about.att.com/pages/cyberaware/ae/robocall

[23] https://www.cnet.com/news/vpn-protect-online-privacy-its-complicated/

[24] https://onezero.medium.com/why-vpns-are-suddenly-everywhere-and-how-to-pick-the-best-one-22d4cfdeff6f

[25] https://www.techradar.com/vpn/best-free-vpn

[26] https://about.att.com/pages/cyberaware/ni/blog/safe_wifi

[27] https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

[28] http://www.irs.gov/

[29] https://about.att.com/pages/cyberaware/ar/irs_scam

[30] https://www.moneycrashers.com/common-email-internet-scams/

[31] https://about.att.com/pages/cyberaware/ar/lottery_scam

[32] https://www.moneycrashers.com/common-email-internet-scams/

[33] https://www.moneycrashers.com/work-from-home-scams-list-fake-jobs/

[34] https://staysafeonline.org/blog/3-internet-scams-targeting-seniors-avoid/

[35] https://about.att.com/pages/cyber-aware/alerts-reporting/tech_support_scam.html

[36] https://staysafeonline.org/blog/3-internet-scams-targeting-seniors-avoid/

[37] https://www.investopedia.com/articles/personal-finance/073115/dont-donate-charity-scams-5-warning-signs.asp

[38] https://about.att.com/pages/cyberaware/ni/blog/door_to_door

[39] https://www.aging.senate.gov/imo/media/doc/217925 Fraud Book Final.pdf

[40] https://about.att.com/pages/cyberaware/ae/idtheft

[41] https://khoros.com/resources/social-media-demographics-guide

[42] https://simpletexting.com/how-to-identify-a-text-scam/

[43] https://caringpeopleinc.com/blog/e-online-dating-seniors/

[44] https://www.cnet.com/news/facebook-took-down-more-than-3-billion-fake-accounts/

[45] https://www.zdnet.com/article/anti-scam-websites-beg-facebook-to-remove-sick-baby-hoaxes/

[46] https://about.att.com/pages/cyberaware/ar/social-media-charity-scam

[47] https://www.komando.com/social-media/is-facebook-friend-request-legit/559815/