



**Cyber**Generations

# The Senior Citizens' Cyber Safety Initiative

## Self-Paced Guide



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)

© Air Force Association







# Table of Contents

<b>Introduction: Cybersecurity 101</b>	<b>4-11</b>
What is Cybersecurity?	5
Why is it important to be safe online?	6
Physical Threats	7
What are mobile devices?	8
Browser Safety	9-10
Personally Identifiable Information	11
<b>Module 1: Password Management</b>	<b>12-25</b>
Introduction Scenario	13-14
What You Will Learn	15
Password: What is it and why is it important?	16
How safe is your password?	17
Don't Use the same Password	18
Password Facts	19
Password Creation Guidelines	20
Password Management Systems	21
Two-Factor Authentication	22
Notified your account has been compromised?	23
Review Checklist	24
Reflection and Discussion	25
<b>Module 2: Common Internet Threats</b>	<b>26-47</b>
Introduction Scenario	27
What You Will Learn	28
Malware	29
Types of Malware	30-32
How does Malware spread	33
Social Engineering	34
Phishing	35
Spear Phishing	36
Vishing	37
Smishing	38
The Anatomy of Ransomware	39
Proactive Cyber Tips	40
How to avoid common internet threats – Anti-Malware	41
How to avoid common internet threats – VPN	42
How to avoid common internet threats – Security Updates	43
Connection Options	44
Signs of Malware Infection	45
Review Checklist	46
Reflection and Discussion	47



# Table of Contents

<b>Module 3: Internet Scams and Fraud</b>	<b>48-66</b>
Introduction Scenario	49
What You Will Learn	50
Scam Awareness	51
IRS Scam	52
Send Money Scam	53
Foreign Lottery Scam	54
Survey Scam	55
Money Making Scam	56
Computer Security Scam	57
When is it safe to share your information?	58
Dating Scam	59
Charity Scam	60
Identity Theft	61
Online Shopping Tips	62
Think Before You Click	63-64
Review Checklist	65
Reflection and Discussion	66
 <b>Module 4: Social Media Safety</b>	 <b>67-78</b>
Introduction Scenario	68-69
What You Will Learn	70
Social Media Breakdown	71
Safety Tips	72
Privacy Settings	73
Common Social Media Scams – Sham Profile	74
Common Social Media Scams – Clickbait	75
Common Social Media Scams – Sick Baby Scam	76
Social Media Etiquette	77
Review Checklist	78
Reflection and Discussion	79
 <b>Resources</b>	 <b>80-84</b>
Government Resources	81-82
Aging Division Services by State	83-86
 <b>Notes Pages</b>	 <b>87-90</b>



**CyberGenerations**

# Introduction

## Cybersecurity 101



## What is Cybersecurity?

All the tools we use and actions we take to keep computers, networks, and information safe and available for those who need them, and unavailable for those who should not.

It is important to be aware of the potential threat of cyber crimes because it affects all of us. According to a report, cyber crime is one of the toughest challenges that the world is facing today and it's set to cost us up to \$6 trillion dollars annually by 2021.

Source: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>





## Why is it important to be safe online?

We rely on computers, mobile devices, and the internet for a lot of 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 take a 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.**

Publicly available government records, court records, records of any organization or committee that you are a member of – these are all viable sources of personal information.

### **Myth 2 – The other common myth is that if you post anything online, it's only shared with your family and friends.**

The internet is a mysterious place sometimes and you never know where your information will end up. Even if you are being careful and deleting data which exposes personal information, there's always a chance that your personally identifiable information has been copied and stored somewhere and can be accessed by criminals.

Source: <https://www.atg.wa.gov/internet-safety-seniors>



Globally, one third of all scams are now targeting mobile transactions with 81 million cybercrime attacks on Financial Institutions in the first half of 2018, 27 million of which targeted the mobile channel. So, these risks apply to both - computers and smart phones.

Source: <https://www.pymnts.com/news/security-and-risk/2018/cybercriminals-global-banking-mobile-fraud-attacks/>



## Physical Threats

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

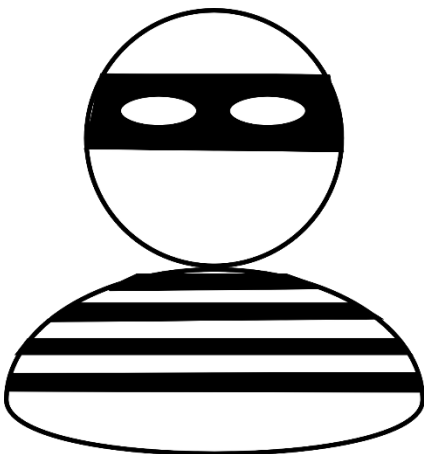
### Dumpster Diving



In terms of cybersecurity, dumpster diving is a practice used to salvage information that could be used to carry out a cyber attack. It's not just limited to searching through the trash for obvious clues like passwords or PINs. Attackers can also use information like phone list, calendar, or address book pages to carry out malicious activities.

Source: <https://searchsecurity.techtarget.com/definition/dumpster-diving>

### 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 pervasive in crowded places where a person uses a computer, smartphone or ATM.

Source: <https://www.techopedia.com/definition/4103/shoulder-surfing>

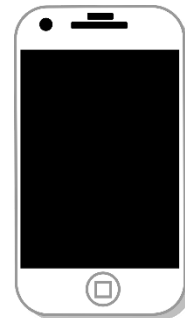
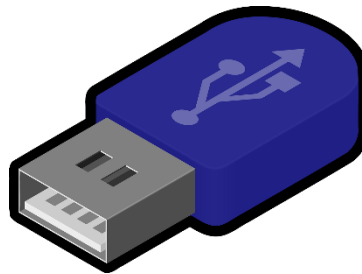




## Securing Mobile Devices

### What are mobile devices?

Portable or handheld devices that have data or can connect to another device that has data.



### Risks

- Easily stolen and lost
- Often not encrypted
- Targets of virus infections
- Can be compromised via wireless
- Apps collect information



### Fixes

- Guard your devices
- Set a strong password
- Use anti-malware and updates
- Avoid using open networks





## Browser Safety

- **Use pop-up blockers**
- **Use automatic updates**
- **Look for a “S” after http in the web address**
- **Look for a padlock in the address bar**



Most browsers have built-in security features to help you stay secure. However, you must make sure the features are up-to-date and turned on for them to work properly.

Browsers can block pop-up ads and extra programs or scripts that you don't know you're downloading.

They will also check a site before you visit it to see if it might be a scam or infected with malicious software.

Browsers can also scan a URL for known spoofs. That's why reporting spoofs to a company is important.



## Ask: "IS THIS A SAFE SITE?"



### Use a secure website:

- Look for an "s" after "http" in the web address
- Look for a 'padlock' in the browser address bar
- Look for a green background or green text



<https://login.microsoftonline.com/>

### Check for correct spelling, beware of spoofs:



<http://bank0famerica.com>

### Use a free site checker:

GetLinkInfo.com





## GetLinkInfo.com

<http://uscyberpatriot.org/>

Get Link Info

Enter any URL, for example: <http://tinyurl.com/2unsh>, <http://bit.ly/1dNVPaw>

#### Link Information

 Title	AFA CyberPatriot Website
 Description	(none)
 URL	<a href="http://uscyberpatriot.org/">http://uscyberpatriot.org/</a> more info  Safe
 Effective URL	<a href="http://uscyberpatriot.org/">http://uscyberpatriot.org/</a> more info  Safe
 Redirections	(none)
 Frames	1. <a href="https://www.youtube.com/embed/sBnONfiV2ck">https://www.youtube.com/embed/sBnONfiV2ck</a> more info  Safe
 External Links	<a href="#">View (31 safe, 0 unsafe)</a>
 Safe Browsing	This site is malware-free and safe to visit. <a href="#">Advisory provided by Google</a>



## Personally Identifiable Information PII

Personally Identifiable Information, or PII, is any data that could potentially be used to identify a particular person.



- First Name or Initial and Last Name
- SSN
- Driver's license or State ID card #
- Passport number
- Credit Card number
- Security Question Answers
- Passwords
- Fingerprints
- Medical information
- Health Insurance information

Source - <https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html>

### Why is it important to safeguard your PII?

Nowadays, we hear the term “data breach” tossed around a lot. That’s because data breaches at big and small companies have become an everyday affair, unfortunately. If an organization suffers a data breach, an important concern is whether the attackers have gained access to the personal data of the customers that do business with the concerned company. Exposed PII can be sold on the dark web and used to commit identity theft, putting breach victims at risk.



The Equifax data breach in 2017 exposed the Social Security Numbers of 146 million people and the Names and DOBs of 147 million people.

Source: <https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07>



**CyberGenerations**

# Module 1

## Password Management



# Password Management

*Susan was very active online. She especially liked the convenience of online shopping and managing her bank card from home. Susan had used the same single password for her personal accounts for many years - she didn't want to have to use more than one password, it was too much hassle. She was convinced that one password was perfect for her online activity.*

*One day Susan attempted to log into her personal email, but found that she wasn't able to log in. This seemed odd to Susan so she tried to log into her online bank account to see if maybe she typed her password incorrectly. 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 had 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 could she do?*







# Password Management



*Sadly, this scenario is more common than you may think....*

## **How Safe is Your Password?**

Page 17 will tell you how to check to see if your password is strong and secure.

Cyber criminals impact our lives daily. **Cyber Crime Facts** on Page 19 illustrates the potential dangers behind our computers.

## **Password Creation Guidelines**

Page 20 will give you step-by-step password guidelines.

Maybe you find it too difficult to remember all of your passwords and you are ready to learn about **Password Management Systems** on Page 21.

You may have noticed that some of your accounts ask if you would like to utilize **Two Factor Authentication** but you aren't sure what that entails. Page 22 will show you the benefits and the ease of use of that option.

Lastly, in **Compromised Accounts** on Page 23, we share how to secure your accounts after a security breach.



# Password Management



## What you will learn in this section:

- ✓ How safe is your password?
- ✓ Password Creation Guidelines
- ✓ Password Management Systems
- ✓ Two-Factor Authentication
- ✓ Steps to take after an account breach



*Data compromises may include names, emails, physical addresses, personal bank details, ethnicity data, and phone numbers*

*Seniors lose an estimated \$36.5 billion each year due to fraud and financial exploitation*

*For every incident of violent crime, approximately three incidents of internet crime were committed against seniors*

Source: <https://www.bloomberg.com/news/features/2018-05-03/america-s-elderly-are-losing-37-billion-a-year-to-fraud>



# Password Management

## Password: What is it and why is it important?

Passwords help protect our personal information on the internet and they are often the only things standing between cyber criminals and our sensitive data. A strong password is not only important, but absolutely necessary.

Bad Password Ideas	Examples
Birthdays	Marchtenth, 0310, 03108, March10
Names – Yours, Pets, Parents, Spouse or Friend	Shawn, Rachel, Freckles, Kitty
Dictionary Words	Password, Security, Profile, Word
Phone Numbers, Social Security Number, Sequential Numbers	2223339999, 1111111111, 769231111, 123456
Names of Movies, TV shows, Famous Songs, Dialogues	Titanic, HeyJude, Casablanca



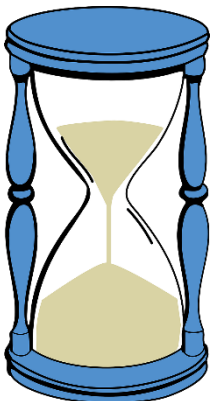
## How Safe is Your Password?



# of Characters	Example	Maximum time to crack:
6	abc123	3 minutes
7	abc1234	5 hours
8	abc12345	3 weeks
9	abc123456	5 years
10	abc1234567	526 years

**Keyboard characters can make the difference between 'hacked' and secure:**

- UPPER case letters
- lower case letters
- numbers
- symbols



cyberpass	56 seconds
CyberPass	8 hours
CyberPass!	6 years
Cyb3rP@ss!	19 years
<b>Cyb3r#P@ss!</b>	<b>530 years</b>

Check to see if your password is secure: <https://howsecureismypassword.net>



## Don't Use the Same Password for All Your Accounts.

- If you create different passwords for each account, a breach in one system does not mean a breach in all of your accounts.
- Multiple passwords can be hard to remember. This is a good, simple trick: Start with a base password and then add an abbreviation to the beginning or end which will remind you what account it is for.



Example:

[base password]

[site]

[new]

Gmail:

[Ronald!23\$]

[GMA]

Ronald!23\$GMA

Facebook:

[Ronald!23\$]

[FAC]

Ronald!23\$FAC



**A 2016 Pew Research Center survey had these answers in response to password behavior for adults 55 and older...**



**SOUND FAMILIAR?**





## P@ssw#rd Creation Guidelines



### **LENGTH = STRENGTH**

10+ CHARACTERS FOR EVERY PASSWORD



### **MAKE IT COMPLEX – But easy to remember**

Always use at least 3 of the following characters:

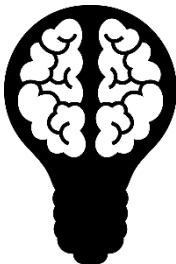
- UPPER CASE LETTERS
- lower case letters
- SYMBOLS (\*%\$#@!)
- NUMBERS



### **UNIQUE, NOT *YOU***

DO NOT USE PERSONAL INFO

- FAMILY/PET NAMES
- BIRTHDAYS



### **USE A 'PASSPHRASE'**

SHORT PHRASE, EASY TO REMEMBER

Where's the beef?

Wh d@ b33f?

Password is now: Whd@b33f?



### **CHANGE CAN BE GOOD**

Change your password every 6-12 months



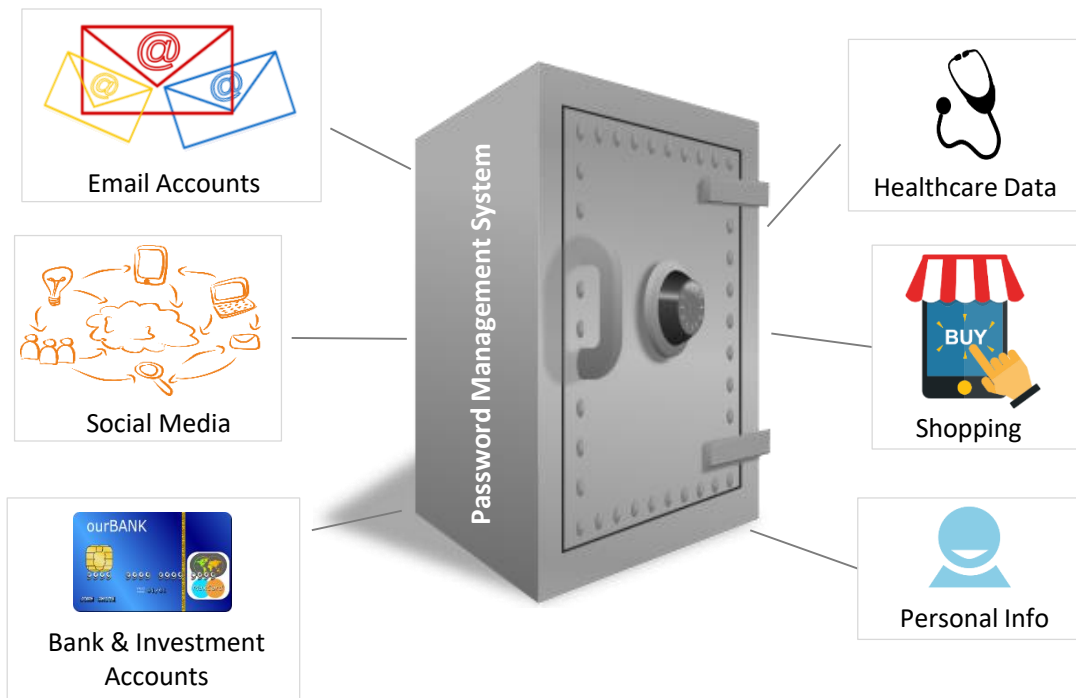
### **Don't Double Dip**

Use different passwords for different accounts



## Password Management Systems

Software application that stores and manages passwords that a user has for various online accounts.



PROS	CONS
Convenience	One password gives access to ALL your passwords
Safer than writing down passwords	Management programs on your desktop do not allow for mobile access
Generates a random password for each of your accounts	Cloud may not be secure and easily compromised

### Did You Know?

63% network intrusions are the result of compromised user passwords and usernames.

Source: <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref>



## Two-Factor Authentication Option for Your Accounts



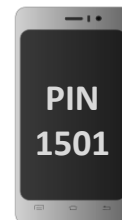
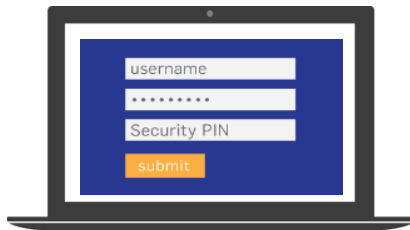
Opt in for a second level of security for your personal accounts



Generated unique access code/PIN  
Sent as text message to your cell phone  
Some services provide hardware token or other device



Two types of credentials entered before given access to an account



### Quick Tip:

You can use the Anti-Theft feature that's available with certain anti-virus software to ensure that you can track your phone in case you lose it.



Be careful about using SMS verification. Hackers can easily intercept your text messages and might also go as far as to use your personal information and move your number to a new SIM card.



## Notified your account has been compromised?

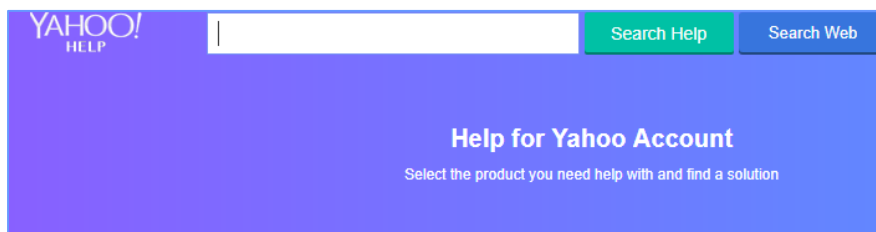
### ☐ Immediately change the password for that account

- Many sites have a 'SEARCH' box or 'Contact Us' option
- Look for the option to CHANGE PASSWORD

A screenshot of a web form titled "Change Your Password". The form has three input fields: "Original Password:", "Password:", and "Confirm Password:". At the bottom right of the form are two buttons: "Update »" and "Cancel".

### ☐ 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



## Review Checklist



- ☐ Unique password for every account
- ☐ 10+ mixed characters for strong password
- ☐ Passphrase, easy to remember, hard to steal
- ☐ Monitor your accounts frequently
- ☐ Password management system can help to remember passwords in a safe way
- ☐ Consider Two-Factor Authentication
- ☐ Change your passwords every 6-12 months
- ☐ Use different passwords for different accounts



## Reflection & Discussion Questions

- How often do 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?
- Be honest, do you write down your passwords? Why or why not?
- What are the pros and cons of using a password management service?





**CyberGenerations**

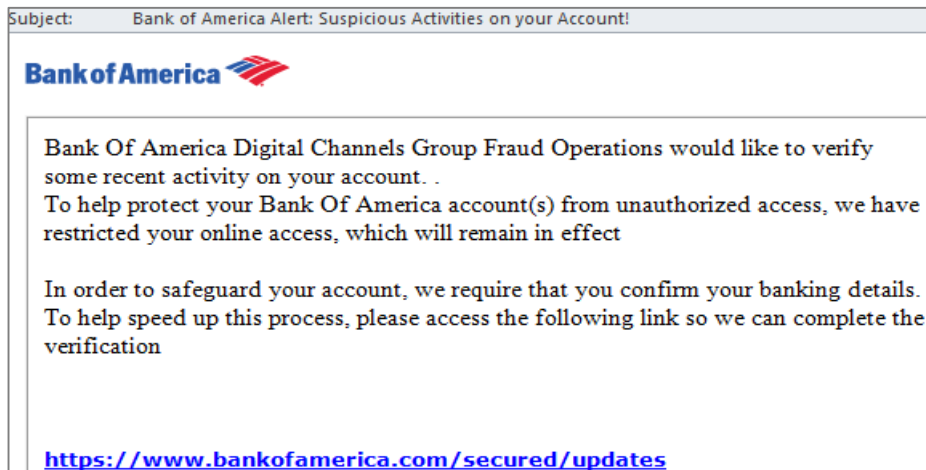
## Module 2

### Common Internet Threats

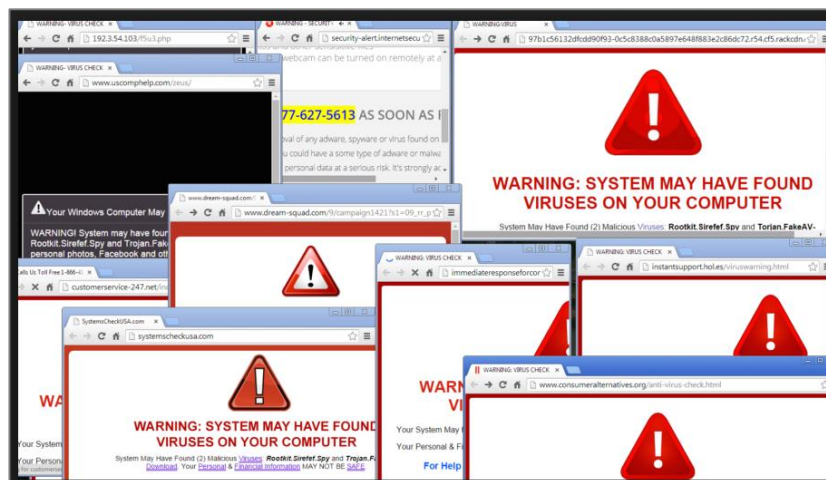


# Common Internet Threats

*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...*



*And he realized, his computer had been **hacked**.*



# Common Internet Threats



## What you will learn in this section:

- ✓ Types of malware
- ✓ How malware spreads
- ✓ How to identify spoof emails, calls and text messages
- ✓ Methods of Social Engineering
- ✓ Easy-to-remember cyber tips
- ✓ How to avoid these common threats

How do you know if you already have anti-virus software on your computer?



### **Windows**

Start button -> click Control Panel -> System and Security -> Review your computer's status -> click button next to Security to expand section -> Virus Protection

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

### **MAC**

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



# Common Internet Threats

**Malware is the #1 cause of online compromised information, but what is malware and how can it affect our personal accounts?**



Malware is software designed and written to:

- Steal information
- Spy on users
- Gain control of computers

Malware is a stealth imposter that takes many forms in unpredictable ways. **Types of Malware** on [pages 30-32](#) will identify the different kinds of malware that may be lurking in your cyber space.

Not sure about the different ways in which you can fall victim to malware? Social Engineering methods on [pages 34-38](#) will help you figure it out.

Nowadays it isn't uncommon for you or someone you know to have their files taken hostage and held for money. **The Anatomy of Ransomware** on [page 39](#) will teach you all you need to know to prevent a hostage situation.

**Proactive Cyber Tips** on [page 40](#) will give you a dependable go-to list to ensure your cyber domain remains secure.

**How to avoid these common threats** on [pages 41-43](#) provide some basic advice to help secure your computer.

Also, Check out the **Signs of Malware infection** on [page 45](#)



## Types of Malware



### VIRUS

Spreads from machine to machine through:

- Email attachments
  - Malicious websites
  - Spoofed links
  - Downloads
  - Shared files like “free” movies.
- 



### WORM

- Can infect and spread without human assistance.
  - Scans networks, finds weaknesses, and attacks systems.
- 



### TROJAN HORSE

- Named after the Greek mythology legend.
- Program with a hidden malicious function.
- File or attachment may look like something you want but it has malicious content.



## Types of Malware



### ADWARE

- Programs designed to display unwanted ads on your computer.
  - Redirect you to advertising websites.
  - Secretly collect data on your online activities.
- 



### SPYWARE

- Collects information about you without your knowledge or consent.
  - Logs your keystrokes and activities.
- 



### RANSOMWARE

- Can lock you out of your computer.
- Steals your data, encrypts it, and then demands a ransom.





## Types of Malware

### ROGUE SECURITY SOFTWARE



- Comes disguised as legitimate software like anti-virus.
  - Usually displays bothersome pop-up messages persistently.
  - Prompts the victim to pay money to fix the made-up issue.
- 

### BROWSER HIJACKERS



- Changes your browser settings without your permission.
  - Injects unwanted ads into the user's browser.
  - Replaces the user's home page with the hijacker page.
  - May contain spyware to steal sensitive information.
- 

### ZOMBIE



- Makes it possible for someone else to control your computer. from anywhere in the world.
- Malicious goal is to install the zombie software on as many computers as possible.

Source: <https://networkbees.com/2017/02/14/types-of-malware/>



## How Does Malware Spread?

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 device.



### 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 want to 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 emails in 2018, it's no wonder that this is one of the most popular methods used by people with malicious intent.

Source: [https://www.radicati.com/wp/wp-content/uploads/2018/01/Email\\_Statistics\\_Report\\_2018-2022\\_Executive\\_Summary.pdf](https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report_2018-2022_Executive_Summary.pdf)



## Social Engineering



Manipulating people into giving up personal information is called Social Engineering. For example, pretending to be your friend online, or giving a false reason for needing the information.

There are a few main methods social engineers might use to extract information from you:

- Phishing
- Spear Phishing
- Vishing
- Smishing



91% of cyber attacks begin with email phishing. 30% of phishing emails are actually opened and 12% of targeted victims then click on the infected links.

Source: <https://bigdata-madesimple.com/77-facts-about-cyber-crimes-one-should-know-in-2018-infographic/>



## Phishing

*Fraud attempts by random attackers against a wide number of users.*

The diagram shows a screenshot of a phishing email in a web browser window. The email header and body are annotated with letters A through E, which are linked to labels on the left:

- Spoof email address** points to the 'From' field: **aw-confirm@ebay.com** (A)
- Generic greeting** points to the salutation: **Dear eBay User,** (B)
- Typos/grammatical errors** and **Nonsense content** point to the body text: **During our regular update and verification of the accounts,** (C)
- Executable attachment or link to a website** points to the URL: **<https://scqi.ebay.com/VerifyInformation>** (E)

Other visible text in the email includes:

- To:** Customer
- Cc:**
- Subject:** Ebay Account Verification
- As a result, your access to bid or buy on eBay has been restricted. To start using your eBay account fully, please update and verify your information by clicking below:** (D)
- Regards, eBay**
- \*\*\*Please Do Not Reply To This E-Mail As You Will Not Receive A Response\*\*\***

### REPORT THE ATTEMPT:

- Forward spam emails to [spam@uce.gov](mailto:spam@uce.gov) (Federal Trade Commission) and to the organization impersonated in the email
- You can also report phishing to [reportphishing@apwg.org](mailto:reportphishing@apwg.org) which is the Anti-Phishing Working Group
- In 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



## Spear Phishing

*Fraud attempts by random attackers against a wide number of users.*

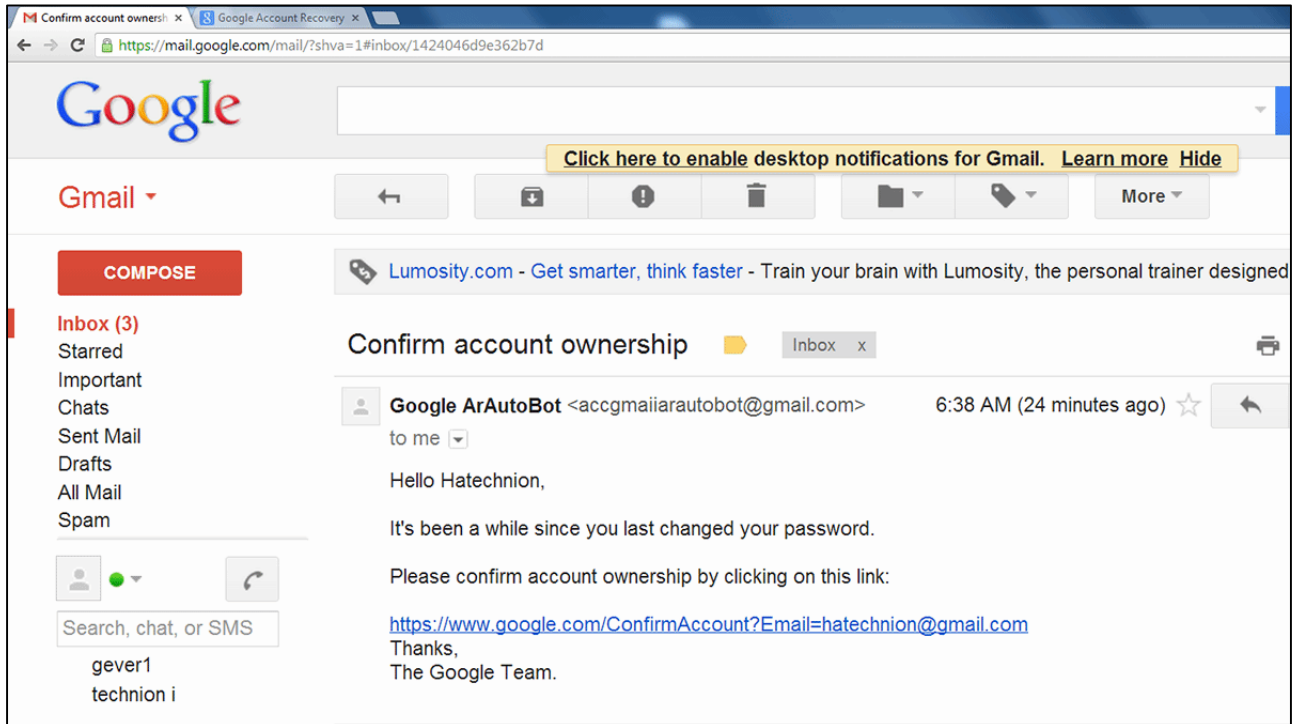


Image Source: searchsecurity.techtarget.com

Spear Phishing is a more targeted type of Phishing. Spear phishing emails are more personalized, and it usually targets a select group or individual. The attacker first gathers information about the target and then uses that information to send fraudulent emails. The attackers might pose as a business that you trust, like a store that you recently shopped at. They will either offer a great deal or a discount, or they can ask you to reset your password or tell you that your account has been locked.



## VISHING

*Voice Phishing: Attempts by thieves to gain confidential information over the phone*



*I just need a few details to ensure you don't experience disruption of service...may I have your social security number and date of birth?*

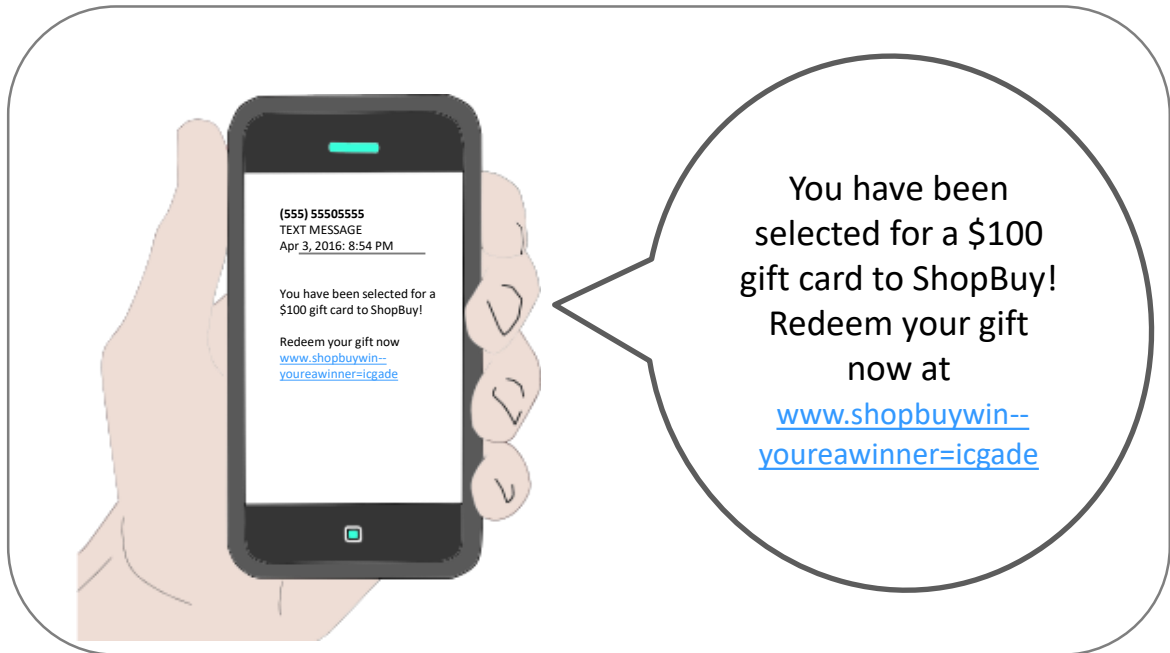
### BE PREPARED:

- Be suspicious of all unknown callers
- Don't trust Caller ID – when unsure let unknown or unexpected calls go to voicemail
- Ask questions: If someone is trying to sell you something or asking for personal information, ask them to identify who they work for and then check to see if they are legitimate (you may need to call them back)
- Interrupt to make sure it's not a robo-call or recorded message. This is an easy way for scammers to get personal information or "permission" by having you answer YES to a question
- Call the company back with a telephone number from your records or a number that is verified as legitimate



## SMISHING

*Phishing attempts sent by SMS (text message)*



### REFUSE THE ATTEMPT:

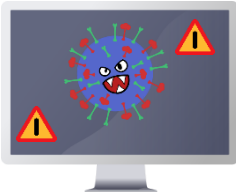
- Do not reply to unknown numbers
- Report spam text to your phone carrier by forwarding the original message to 7726 (SPAM) from all carriers
- Delete the text
- Review your cell phone bill for unauthorized charges
- Change your general phone settings to block unknown numbers



## The Anatomy of Ransomware



User opens an email with a suspicious attachment.



Virus infects machine with 'Ransomware' – computer is locked and displays a message demanding payment to restore access.



### YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America Criminal Code of U.S.A. provides for a deprivation of liberty for two to ten years.

Following violations were detected:  
Your IP address was used to visit illegal movie websites.  
This computer lock is aimed to stop your illegal activity.



To unlock your computer you are obliged to pay a fine of \$250. You have 72 hours to pay the fine or you will be arrested.

You must pay the fine through Money2Go. Payment can be made at any Shop Rite or SnackStop locations.

If error occurs, email your social security number to [pay@fbi.com](mailto:pay@fbi.com).



Once the payment is made your computer may be unlocked...or it may stay locked. Payment is not a guarantee to regain access to your files.



Ransomware can be spread to any machine that is connected to the same network. Run a virus scan as soon as possible on your computer. Backup important files frequently to avoid disaster!





## Proactive Cyber Tips

Be aware of false anti-virus  
popups

Real anti-virus and malware  
popups will appear on your  
desktop and NOT in a browser

Use your computer's preinstalled antivirus and  
scheduled scans at least weekly

Benefits:

- Monitors your system
- Detects and deletes malware

Use popup blocker



Say no thank you to free  
Wi-Fi in public areas

Be weary of what you download:  
email attachments, plugins, software  
updates, music, movies, etc.

When on public computers  
avoid doing anything that  
requires you to log into  
personal bank accounts,  
retirement funds, etc.

Avoid clicking OK to get out of  
annoying pop-ups. Close  
browser if you cannot cancel.



## How to Avoid Common Internet Threats?



### Anti-malware Software

#### Examples of free reputable anti-virus programs:

- AVG
- Windows Defender
- Bitdefender
- Digital Defender

#### Examples of subscription services with free options:

- Symantec
- McAfee
- AVG



### Download Tips

- Download from a trusted source. Beware of spoofed URLs!
- Only install and run one anti-malware solution on machines. Multiple programs can cause problems and conflict with each other, as well as slow down your machine.
- Most computers have anti-malware pre-installed – use this to your advantage!
- Not sure how to download? Follow the download wizard that will walk you through the installation process step-by-step.

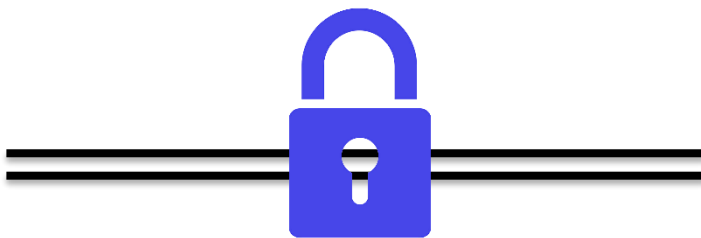


## How to Avoid Common Internet Threats?



### Virtual Private Network (VPN)

- A 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.
- You can subscribe to a legitimate VPN service and pay a monthly fee for the use of the VPN app.
- You can 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.



**Encrypted Connection**

Source: <https://www.cnet.com/news/vpn-protect-online-privacy-its-complicated/>



## How to Avoid Common Internet Threats?



### 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.



#### Example – How to update Windows 10?

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



## Connection Options

### The Truth About Public Wi-Fi

- Public Wi-Fi is not a secure network
- Any information you share or access can be tapped into
- Anyone near you can intercept the connection

*Beware of accessing any site using public Wi-Fi that requires you to share personal information: passwords, bank account information or other sensitive personal info.*

### When Using Public Wi-Fi

- Only visit trusted sites that do not require login credentials
- Save important tasks like paying bills or checking your credit card statements until you are home with a secure, password protected connection

VPN (Virtual Private Network) is a good choice if you will be using Wi-Fi outside of your home for long periods of time.

Personal Hot Spots are an option:

- Cost money to use per use (separate from your cell phone plan)
- Are as secure as your phone network (no added security)
- Never share your hotspot password with a stranger
- Hotspots must be manually turned on and off – beware of the charges!

**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.

Source: <https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf>



## Do you suspect that there's Malware on your computer? Look out for these signs:

- ✓ Your computer has slowed considerably and keeps getting stuck
- ✓ Unexpected pop-ups and suspicious messages are showing up on your computer screen
- ✓ Computer crashes unexpectedly while browsing the internet
- ✓ You see a blank or blue screen whenever you try to use your computer
- ✓ You get a message on your screen that says that your anti-virus protection has been disabled
- ✓ You suddenly notice that you are running low on disk space
- ✓ You find suspicious icons or files on your computer which appear out of nowhere



Source:

<https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/>  
<https://networkbees.com/2017/02/12/computer-viruses-signs-of-malware-infection/>



## Review Checklist



- ☐ Computer viruses can be transmitted by an unknowing user or behind the scenes on your computer.
- ☐ Ensure your computer conducts weekly scheduled updates for patches and updated software as well as a weekly anti-virus scan.
- ☐ If you receive a suspicious email, do not open the email, click links, or download attachments.
- ☐ Identify illegitimate portions of mysterious emails such as typos, unknown email address, or requests for personal information.
- ☐ Do not respond to strange text messages.
- ☐ Feel empowered to contact companies and organizations to report spoof emails, false texts or spam phone calls.
- ☐ Never share personal information over the phone or in email unless you have initiated contact.
- ☐ Reliable FREE software is available for the public. Do your research and when in doubt, at the very least, use preinstalled anti-virus and anti-malware software that comes with your computer.



## Reflection & Discussion Questions

- What do you think is the most harmful type of malware?
- Have you had a virus 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?
- On average, about how many spoof emails do you think you receive in a week? Have you ever mistakenly clicked on a link within a suspicious email?
- What red flags can you identify in a spoof email to ensure it is legitimate?
- 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 and when is it not safe?
- Why should you utilize your computer's preinstalled anti-virus software?
- How often should your computer download software updates?
- If a virus attacks your computer, what are the steps you can take to remedy the infection?





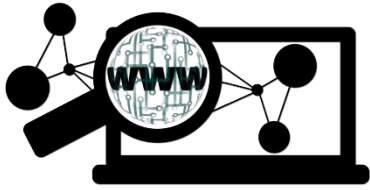
**CyberGenerations**

## Module 3

### Internet Scams and Fraud



# Internet Scams and Fraud



*"Hello, my name is Angela from PhoneUSA. Do you have a moment to talk about your current phone plan? I will just need your social security number to verify your account."*

*"Congratulations! You have won an all expenses paid trip to Hawaii! Press '1' to speak to a prize representative to claim your free vacation!"*

*These types of calls and emails may seem all too familiar to you...*

Your best defense is to be aware of the types of scams that are out there and be mindful of their approach methods. This information can be found in **Scam Awareness** on page 51.

For a detailed review of the different scams targeting senior citizens in the US, check out pages 52–57 and 59-60.

It's not always easy to identify a legitimate customer service call. Follow our tips on **When is it Safe to Share Your Information** on page 58 to ensure your safety.

**Online shopping** might be easy and convenient, but make sure that you follow the tips on page 62 before you buy anything online.

Temptation is everywhere online. **Think Before You Click** on pages 63-64 will demonstrate what links, pop-ups and information are safe to click, and how to differentiate between user-initiated and fraudulent actions.



## What you will learn in this section:

- ✓ Types of phone and online scams and examples of the types of fraudulent schemes
- ✓ Identity Theft and how to prevent it
- ✓ What information to share and not share over the phone and on the web
- ✓ Online shopping safety tips



Did you know that the Federal Trade Commission can help with phone and email scams?

<https://ftccomplaintassistant.gov>

call 877-382-4357

Forward spam email to: `s p a m @ u c e . g o v`



## Scam Awareness



### Financial/Investment Companies

- Retirement accounts
- Bank accounts
- Spoof emails requiring log-in
- Phone calls requesting PIN numbers or Social Security numbers (SSN)



### Government Agencies

- IRS, FBI, FTC etc.
- Spoof emails requiring payment or sending SSN
- Phone calls requesting SSN or demanding immediate payment



### Insurance Companies

- Home, Life, Health and Car coverage
- False email claims
- Phone calls requesting personal information regarding an unfiled claim



### Donation Organizations

- Previously used donation services
- Email requests for money donations
- Phone calls asking for monetary donations without an option to donate used items



### Dating Sites

- Free accounts or paid subscription service
- Email requests for personal information regarding your account
- Phone calls introducing a new love interest match or requesting more personal information



### Online and Phone Surveys

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



## IRS Scam

An IRS phishing scam is an unsolicited, fraudulent email that claims to come from the IRS. Some emails link to malicious websites that look real. The scammers' goal is to lure victims to give up their personal and financial information. If the thieves get what they're after, they use it to steal a victim's money and identity.

From: "Internal Revenue Service" <[irs@gov.com](mailto:irs@gov.com)>  
Date: February 25, 2008 10:08:31 PM EST  
Subject: **Tax Refund Notification**



After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of \$9950.55. Please submit the tax refund request and allow us 2-3 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. To access the form for your tax refund, please click [here](#)

**Note: For security reasons, we will record your ip-address, the date and time. Deliberate wrong inputs are criminally pursued and indicated.**

Regards Internal Revenue Service.

For those who receive such a phishing email, the IRS offers this advice:

- Don't reply to the message.
- Don't give out your personal or financial information.
- Forward the email to [phishing@irs.gov](mailto:phishing@irs.gov). Then delete it.
- Don't open any attachments or click on any links. They may have malicious code that will infect your computer.

Source: [www.irs.gov](http://www.irs.gov)



## Send Money Scam

### *Common Scam Scenario:*

- *You receive a call or email from a friend or family member asking for money*
- *The person is desperate for financial help because they are stranded out of the country, lost their wallet or are injured*
- *The caller or email asks for money to be wired to a specific location*



### **What You Can Do**

#### On a Phone Call

- Ask a personal question that only that person would know the answer to
- Verify the person calling is out of the country (contact another relative, the caller's workplace, etc. any way to identify if they may indeed need help)
- *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 health status and then contact the proper authorities

#### In an 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

You might receive a fraudulent email from some foreign lottery company notifying you that you have won a ridiculous amount of money. These emails usually look very professional with a subject line that congratulates you on winning and the body of the email usually requests personal information like your full name, date of birth, or phone number.

- Don't reply to this email
- Don't share your personal or financial information
- Do a quick google search to verify the authenticity of the company

**Remember – If you didn't enter a lottery yourself, there's no way that you will actually win one.**



Source: <https://www.moneycrashers.com/common-email-internet-scams/>

Image Source: [www.fightidentitytheft.com](http://www.fightidentitytheft.com)



## SurveyScam

These scams are very common, and they usually come in the form of an email which will prompt you to click on suspicious links 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.

- Don't click on the suspicious links
- Don't give out any personal or financial information
- Report the spam email or phone call to the relevant authority



### EXAMPLES:

**Congratulations! Your IP Address has been randomly selected to receive an iPhone X. Just complete this quick survey!**

**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.**

Source: <https://www.moneycrashers.com/common-email-internet-scams/>





## Money Making Scam

There are plenty of get-rich-quick scams out there which promise that you can make some amount of money working from home and with minimum effort.

They usually prompt you to purchase a trial kit or training package for a fixed amount to be paid over PayPal or by sending them a check. These offers usually sound too good to be true and that's because they are!



- These scams will inevitably ask you to spend some money – either to purchase training material or for an upfront fee to get into the program
- Many times, these companies are based overseas, and they don't provide any contact information
- Do a quick Google search. You might find out that there's already some information online about the illegitimacy of the suspicious company

Source - <https://www.moneycrashers.com/work-from-home-scams-list-fake-jobs/>



## Computer Security Scam

Bogus tech support employees make calls claiming to be from trusted companies like Microsoft or Apple.

They tell the victim that they have detected a problem with their computer and they need remote access to their 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 some malware on the computer that helps them steal valuable personal data from the victim.



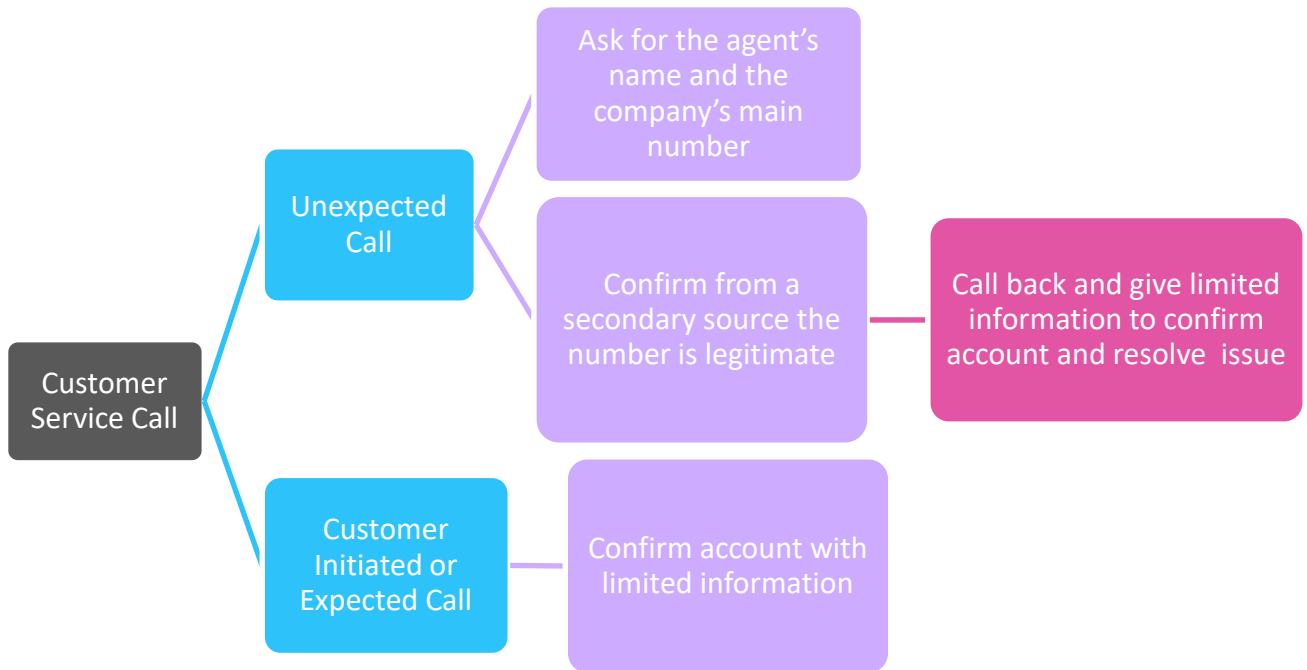
- Don't share any personal or financial information with such a caller.
- Don't give anyone remote access to your computer.
- If there's an actual problem, look up the customer service information on the product website.

**Remember that tech support will not contact you if you did not contact them first.**

Source: <https://staysafeonline.org/blog/3-internet-scams-targeting-seniors-avoid/>



## When is it Safe to Share Your Information?



### REMEMBER:

- 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 send you a hard copy bill to pay.
- Beware of “secure” online payment options (when in doubt, call the company directly).





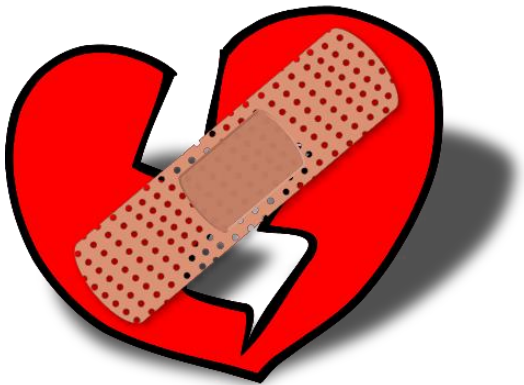
## Dating Scam

These scams are unfortunately rampant, and they are particularly disturbing because they take advantage of the victim's loneliness and trustworthiness.

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 usually have an elaborate profile and backstory with pictures of real people. These con artists strike up a romantic relationship with the unsuspecting victim and then ask for money using some kind of an emergency or emotional story.

Many times they pretend to be Americans living abroad who need money to get back to the country and meet the victim.



- Be cautious of people who claim to be madly in love with you even before they have met you in person.
- Beware of people who claim to be Americans working overseas, like soldiers.
- Even if you feel a strong connection, don't ever send money to someone you haven't met personally.

Source: <https://staysafeonline.org/blog/3-internet-scams-targeting-seniors-avoid/>



## Charity Scam

Charity scams are usually very sophisticated, and many people fall prey to them on a regular basis. Scammers take advantage of kind-hearted people and swindle them into “donating” to sham organizations.



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

They pretend to help an array of disadvantaged people like cancer patients or poor children or veterans in need. Some scammers may also make false tax deduction claims asking for personal information.

- **Do your research before donating to an organization.**
- **Delete unsolicited emails and stick to organizations you know and trust.**

Source: <https://www.investopedia.com/articles/personal-finance/073115/dont-donate-charity-scams-5-warning-signs.asp>



## Identity Theft



Identity thieves defraud people and the government by assuming the identities of unsuspecting victims and 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.

Source: <https://www.moneycrashers.com/what-to-do-suspect-identity-theft-victim/>  
<https://www.aging.senate.gov/imo/media/doc/217925%20Fraud%20Book%20Final.pdf>



## Online Shopping Safety Tips



### **Use reputable retailers to avoid the risk of being sold counterfeit goods**

- If a price seems too good to be true, research the seller before making a purchase.

### **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 jack up the prices of 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 connection or device**

- Best to make any online financial transaction at home using a safe and secure internet connection.



# Internet Scams and Fraud



## Think Before You Click



Ask: "Is this pop-up legitimate?"

### Anti-Virus/Anti-Malware:

- Your computer should have an anti-malware program running behind the scenes. You will never be asked to take an action for a virus or malware infection.
- Shut down your computer and delete your browsing history.
  - *Internet home page, History, delete history*



### Adobe, Flash, Java Updates:

- Go directly to the program site and download the most recent, up-to-date version.
- *Do not update your computer directly from the pop-up.*







## Think Before You Click



Ask: "Is this pop-up legitimate?"

### Email or Internet Pop-ups:

- Pop-ups initiated by an internet search or using your email account cannot always be trusted.
- Use a pop-up blocker.
- *Be suspicious of pop-ups if you are online, you can choose to not participate or fill in any pop-up for a site.*

Pop-up  
blocker  
enabled



### Dangerous Pop-ups:

- Pop-up windows that stay on your screen, even when you try to close them.
- Pop-ups from an anti-virus company you don't recognize.
- You are asked to make a payment to remove a virus.
- Request for remote access to your computer.



## Review Checklist



- ☐ Phone and internet scams most commonly target against 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.
- ☐ Pop-ups can show up on your desktop or when you are using the internet (shopping, searching, using email).
- ☐ 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 & Discussion 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 receive is real?
- You receive a phone call from your grandchild asking for money so they can get back home from a vacation gone terribly wrong. What steps should you take to ensure you aren't being scammed?
- 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?
- How can you know if a pop-up is secure? Are all pop-ups dangerous?



**CyberGenerations**

# Module 4

## Social Media Safety



# Social Media Safety

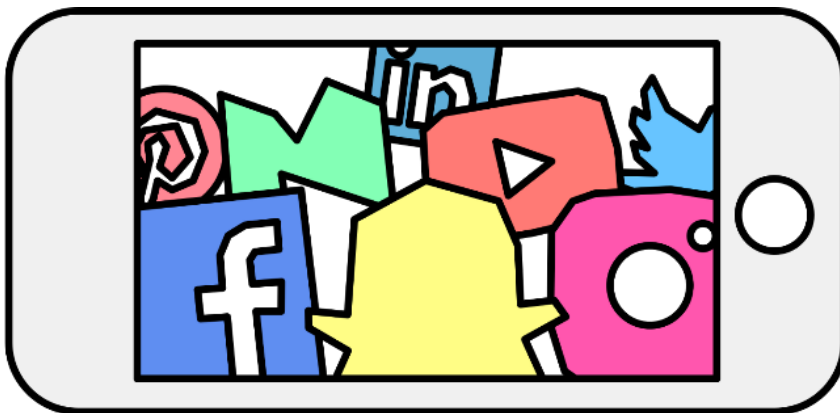
*Hank enjoyed keeping in touch with his lifelong friends on FriendBook. They had a 25 year high school reunion coming up and he was more active than usual on his social media page, organizing and planning all the details.*

*It had been so long that Hank couldn't remember all of his peers, 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. What harm could it do to accept the request again?*

*Days later Hank's son called him to ask why he had created a second page on FriendBook. Of course Hank had no idea what he was talking about. Apparently someone had created a brand new page using Hank's photos and information. They even had details about his most recent trips and a post requesting money for a charity!*

*Hank realized that the duplicate friend request was the culprit. He immediately blocked the new friend and changed all his safety settings to private. He will be more observant next time he receives a strange request.*





# Social Media Safety

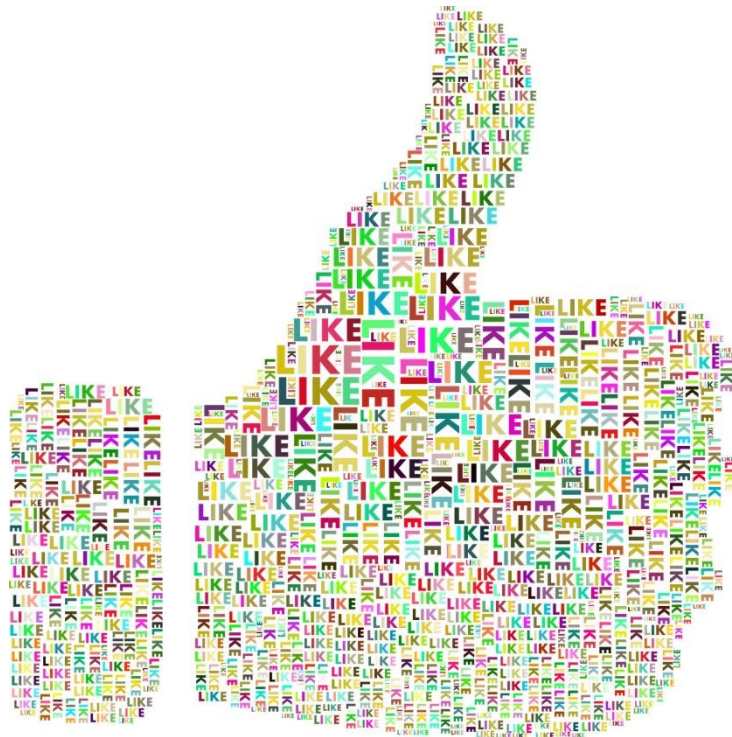
*Social media is a wonderful way to stay in touch with friends and family, but sharing your personal information can come at a cost...*

There are hundreds of social media sites. In **Social Media Breakdown** on [page 71](#) we will identify a few of the most popular sites and the most common types of activities associated with each one.

**Social Media Safety Tips** on [page 72](#) gives tips on how to secure your social media accounts and remain safe on such sites.

We discuss **Common Social Media Scams** on [pages 74-76](#), from clickbait to sick baby scams, all the pitfalls you should be wary of on social media sites.

Etiquette is just as important online as it is at the dinner table. **Social Media Etiquette** tips on [page 77](#) will show how to interact online while minding your cyber manners.





## What you will learn in this section:

- ✓ The most common social media sites and the activities associated with each
- ✓ Social media safety tips
- ✓ How to keep the information you share on social media sites safe by managing your privacy settings
- ✓ Social media scams
- ✓ Social media etiquette and how to mind your cyber manners when interacting online



According to a recent study, 62% of online adults aged 65 and older are using Facebook. The same study showed that a small percentage of online adults aged 65 and older are using Instagram (8%), LinkedIn (16%), and Twitter (10%).

Source: <https://www.spredfast.com/social-media-tips/social-media-demographics-current>





## Social Media Breakdown

*84% of U.S. adults have at least 1 social media account*



### Facebook

- Connect with friends and family
- Post status updates/comments and links on posts
- “Check-in” to locations
- Send private messages
- Join common interest groups
- Upload photos and videos
- Play games

### Twitter

- Broadcast short messages (“tweets”) in 280 characters or less
- Post pictures, links and videos
- Follow other users
- Direct messaging
- Used as a marketing tool

### YouTube

- Popular video-sharing website
- Watch user-generated content
- Lets users video-blog or vlog
- Upload your own videos and share videos you enjoy
- Subscribe to the channels you like

### Instagram

- Share photos and videos
- Add stories in the form of photos or videos which disappear after 24 hours
- Follow friends, brands, celebrities, and influencers
- Used as a marketing tool
- Edit photos

### LinkedIn

- Connects people through their careers and digital resumes
- Apply for jobs
- Announce job changes
- Endorse skills of coworkers

### Pinterest

- Digital pin board
- Post interesting visual content called ‘pins’
- Follow other users
- Message other users





## Social Media Safety Tips

**Be picky:** Only “accept” or “follow” friends you actually know in real life.

**Do not post your location:** Friends who “tag” you may also be giving out your location.

**Be careful with apps:** Games 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 reveal too much or say something you will regret. If you wouldn't say it to someone's face, you shouldn't post it.

**Don't over-share:** Just because a site asks for info, doesn't mean you have to give it. Most of the time, only a few of the requested bits of information are actually required to set up an account.

**Customize your privacy settings:** Do not use the default settings. They usually only provide the bare minimum in security. Be sure to update your settings regularly.

**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 e-mails to everyone in your contact list or even everyone you've ever sent an e-mail to.

**If you get a suspicious message from one of your contacts, double check:** Scammers can either break into someone's account or they can steal publicly available information to create a forged account impersonating someone else. If you suspect that a message is fraudulent, use some other method to contact your friend and verify the dubious claim.

Source <http://seniornet.org/blog/11-tips-for-social-networking-safety/>




## Privacy Settings

Securing your social media accounts is imperative to a safe online experience



**You can use Privacy Checkup to see your current privacy settings:**

1. Click  at the top of any page on Facebook (ex: your homepage).
2. Select Privacy Checkup.



**Make your tweets private or public:**

1. Go to your Privacy and safety settings.
2. In the Tweet privacy section, check the box next to Protect my Tweets.
3. Click the Save button at the bottom of the page and confirm with the account password to save changes.



**Change your account and privacy settings:**

1. Click the Me icon at the top of your LinkedIn homepage.
2. Select Settings & Privacy from the dropdown.



Various security options to keep your account private including safe mode and two factor authentication:

[help.pinterest.com](https://help.pinterest.com)



## Common Social Media Scams



### Dummy Profiles

Hackers can easily steal the information of your loved ones and friends to whom you are connected on any social media site. 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 very wary of any 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 particular platform. Duplicate friend requests are a big red flag.

**Did you Know?** Facebook deleted 583 million false accounts in the first three months of 2018!



Source: cnet.com



## Common Social Media Scams

### Clickbait

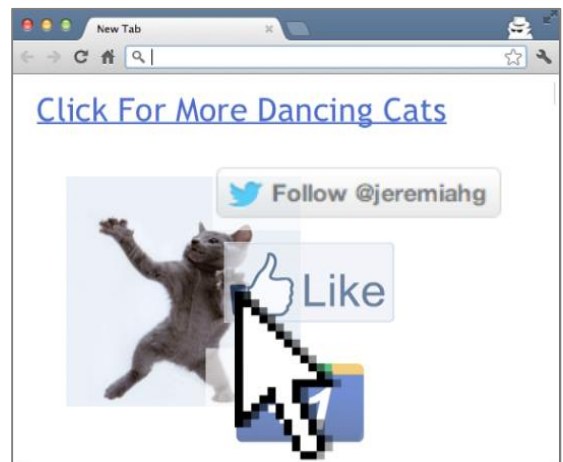
Clickbait usually refers to a photo or headline which is tailored to grab your attention and prompt you to click through to learn more.

Clicking on such links can redirect you to an altogether different website with malicious content, which can download dangerous malware onto your device.

### 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.

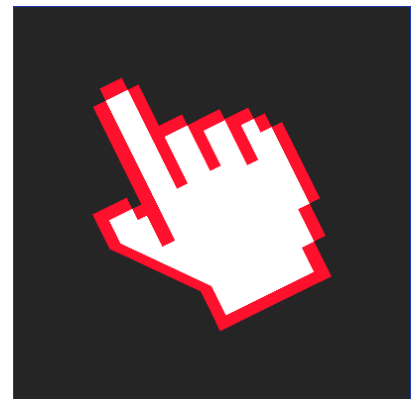


### Examples of Clickbait Headlines:

“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 . . .”





## Common Social Media Scams

### Sick Baby Scam

Scammers use the real pictures of sick and disabled children to manipulate people into donating to help save their lives or for emergency treatment.

People are often asked 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 family member 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.



#### Example:

This child's got a cancer. Facebook is ready to pay 3 cent for every share. we don't know is it true or not, but let's everybody share. maybe it's true and then... >SHARE< for this baby PLEASE SHARE, THANKS!

### Report it!

Is this photo about you or a friend?

Yes, this photo is about me or a friend:

- ☐ I don't like this photo of me
- ☐ It's harassing me
- ☐ It's harassing a friend

No, this photo is about something else:

- ☐ Spam or scam
- ☐ Nudity or pornography
- ☐ Graphic violence
- ☐ Hate speech or symbol
- ☐ Illegal drug use

Is this your intellectual property?

Continue

Cancel

Source: <https://www.zdnet.com/article/anti-scam-websites-beg-facebook-to-remove-sick-baby-hoaxes/>



## 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
- If someone tells you something in confidence, be careful about bringing up such topics online
- Don't get into arguments online. Respect the right of other people to express their opinion
- Don't use all caps. Using all caps usually means that you are yelling and is considered 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 invite and accept friend requests from people you know
- Cyber criminals use ways to gain your personal information by sending false friend requests



Source <http://blog.heritage-hall.org/2017/09/12/social-media-dos-and-donts-for-seniors/>



## Review Checklist



- ☐ Know the function of social media sites before you join.
- ☐ When using social media, enable security settings to ensure your information is private and only shared with those you choose to share information with.
- ☐ When participating in 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 & Discussion Questions

- Do you have a social media account? If yes, on which site?
- Do you feel that you keep in touch with friends and family more because of social media?
- Have you ever received malware from a social media post? If so, what did you do?
- What are the steps to set a privacy policy on a social media account? If you are not sure, where can you look for account settings?
- 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?
- You are planning on going on a cruise in the summer and are so excited you want everyone to know! Is it a good idea to share your trip 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?





**CyberGenerations**

# Resources

Government Resources &  
Aging Division Services



# Government Resources

## **Department of Homeland Security: U.S. Computer Emergency Readiness Team**

*Phishing and email scams*

Email: [phishing-report@us-cert.gov](mailto:phishing-report@us-cert.gov)

## **Elder Justice Initiative (Department of Justice)**

*Elder abuse, financial exploitation of seniors and their families*

[www.justice.gov/elderjustice/](http://www.justice.gov/elderjustice/)

Resources by State: <https://www.justice.gov/elderjustice/support/resources>

## **Federal Trade Commission**

*Identity theft, sweepstakes scam calls*

1-877-438-4338/ TTY TTD 1-866-653-4261

File a complaint:

<https://www.ftccomplaintassistant.gov>

Phishing attempts

[spam@uce.gov](mailto:spam@uce.gov)

## **Internal Revenue Service (IRS)**

*Tax refund fraud victims*

Identify Protection Specialized Unit

1-800-908-4490

Taxpayer Advocate

1-877-777-4778/TTY TTD 1-800-829-4059

*Received an email from the IRS?*

Email: [phishing@irs.gov](mailto:phishing@irs.gov)



# Government Resources

## **Medicare Fraud**

*For individuals that have been victim of Medicare fraud or suspect that it may be occurring*

1-800-MEDICARE (1-800-633-4227)

## **National Association of Attorneys General**

Find by state: <http://www.naag.org/naag/attorneys-general/whos-my-ag>

Email: [feedback@naag.org](mailto:feedback@naag.org)

## **Social Security Administration**

1-800-772-1213/ TTY TTD 1-800-325-0778

## **United States Senate Special Committee on Aging**

*Fraud Hotline*

1-855-303-9470

## **USA.gov for Seniors**

*Helps users access all government sites that provide services for Senior Citizens*

1-800-FED-INFO



# Aging Services Division by State (AL - KS)

## 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

## 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/adrc/>

1.877-471-2777

## 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



# Aging Services Division by State (KY – NY)

## Kentucky

<http://chfs.ky.gov/dail/>

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

<http://www.mdhs.state.ms.us/aging-adult-services/>

1.800-948-3090

## Missouri

<http://www.moaging.com>

(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/Programs/Seniors/Seniors/>

(775) 687-4210

## New Hampshire

<https://www.dhhs.nh.gov/dcbcs/beas/>

1.800-275-3447

## New Jersey

<http://www.state.nj.us/humanservices/das/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



# Aging Services Division by State (NC – WV)

## North Carolina

<https://www.ncdhhs.gov/divisions/daas>

(919) 855-4800

## North Dakota

<http://www.nd.gov/dhs/services/adultsaging/assistance.html>

(701) 328-4601

## Ohio

<http://aging.ohio.gov/>

1.800-266-4346

## Oklahoma

<http://www.okdhs.org/services/aging>

(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



# Aging Services Division by State (WI – WY)

## **Wisconsin**

<https://www.dhs.wisconsin.gov/aging/services>

(608) 266-2536

## **Wyoming**

<https://health.wyo.gov/aging/>

(866) 571-0944

## **Puerto Rico**

<https://goo.gl/C55QRr>

(787) 721-6121

## **Washington, D.C.**

<https://dcoa.dc.gov/>

(202) 724-5626



# Notes





# Notes



# Notes



# Notes

Thank you for participating in



For more information on how to participate in the Air Force Association's  
CyberPatriot National Youth Cyber Education Program, visit  
[www.uscyberpatriot.org](http://www.uscyberpatriot.org)