Cyber Security and Internet Safety

front porch

A Toolkit and Resource Guide of the Piers Project (version 2019)

An initiative of the Front Porch Center for Innovation and Wellbeing

Additionally sponsored by

California Lutheran Homes

Front Porch, a not-for-profit human serving organization featuring innovative communities and programs that meet the changing needs of individuals as they age, received a generous monetary gift on behalf of the family of former retirement community resident, Ellie Piers.

Ellie Piers

The gift benefits the Front Porch Center for Innovation and Wellbeing's (FPCIW's) ongoing mission of using technology to enhance wellbeing among older adults. Piers lived at Carlsbad By The Sea, a Front Porch retirement community in Carlsbad, CA. Her contribution allowed the CIW to confront the issue of elder security through information technologies to develop initiatives related to senior online security in the Greater San Diego Area, but accessible also to communities far and wide across the Internet.

Piers had a curious mind and adventurous spirit when it came to technology, and believed technology could help elders live well and securely. She embraced the opportunity to leverage technology to stay in touch with friends and family, but was mindful and aware of security issues that came along with its use. Having a keen sense of the vulnerability that came with using technology, Piers had a habit of asking thorough questions before venturing onto the web that helped guide her toward the goal of each "web surfing" episode. In celebrating Piers' spirit in helping others, FPCIW has developed the **Piers Project** to address elder security and raising its awareness through:

- Piloting emerging technologies related to senior safety and developing content relative to online security for older adults;
- Outreach to Greater San Diego Area organizations that have expertise in the area to establish a cooperative for leveraging contributions in order to create an increased impact on the issue of senior online security;
- Exploring mediums for raising awareness for technologies that can improve the lives of older adults in the Greater San Diego Area; and
- Creating an online and social media campaign that would pay tribute to Piers' gift and interest in making a difference in this important area of wellbeing for seniors.

This toolkit, created by FPCIW, has been additionally sponsored by the California Lutheran Homes Foundation to bring this resource to more communities and languages. Our toolkit serves as a guide for individuals to better understand some of the risks in the online world, and to help proactively and confidently avoid them while enjoying the benefits of the internet.

Table of Contents

I. Cyber Security & Seniors as Fraud Targets | page 5

II. Who to Believe? Identify the Imposters! | page 6

- Healthcare Scams
- Tax-Related Fraud
- Lottery Fraud
- Investment Fraud

IV. Emails| page 9

- Phishing
- Hacking
- Spam
- Nigerian Letters

V. Protecting Your Finances| page 13

- Shopping Online
- Online Banking

VI. Malware | page 16

- Malware, Ransomware, and Viruses
- Vaccine and Anti-Malware Programs

VII. Password Safety | page 19

VIII. Smart Assistants, Smart Homes and Wi-Fi | page 21

IX. Social Media and Fake News | page 22

X. Cyber Fraud Response Procedure | page 25

XI. Reporting Agencies | page 26

XII. Resources | page 28

XIII. References | page 30

Did you know...

- In 2016, **67% of Americans** 65 and over were using the Internet[1].
- **Only 1 in 24 cases of elder abuse** are reported[2].
- In 2017, older adults lost **$1.7 billion to financial abuse**[3].
- **45% of financial abuse** begins through the use of the Internet[4].
- **59% of people** say they are unsure whether what they see in the media is true[5].

Technology today has become an integral tool for how we live our daily lives. We talk to our loved ones over the internet, do our banking and shopping online, socialize on platforms such as Facebook and Twitter, and research our favorite topics. There are so many great benefits of the internet, but how do we take advantage of the vast digital universe while doing so safely?

As active members of a digital society, it's important that we practice good internet hygiene. We need to be aware of the unseemly tactics that some people will use to exploit our personal information that could lead to personal, social, and/or financial damage. Like any useful skill, it is important to take preventative measures that can help reduce risks allowing you to utilize the benefits of the internet with comfort, safety and peace of mind: our power and control come from knowledge and sharing our experiences.

This toolkit is designed to be a resource guide about safe computing for older adults. The lessons in this toolkit are all based upon three simple, yet important rules on successful and safe online experiences.

1) **QUESTION** the content you see on the Internet,
2) **CHECK** for validity and authenticity, and
3) **ASK** your friends, neighbors or colleagues for help and to educate others around you.

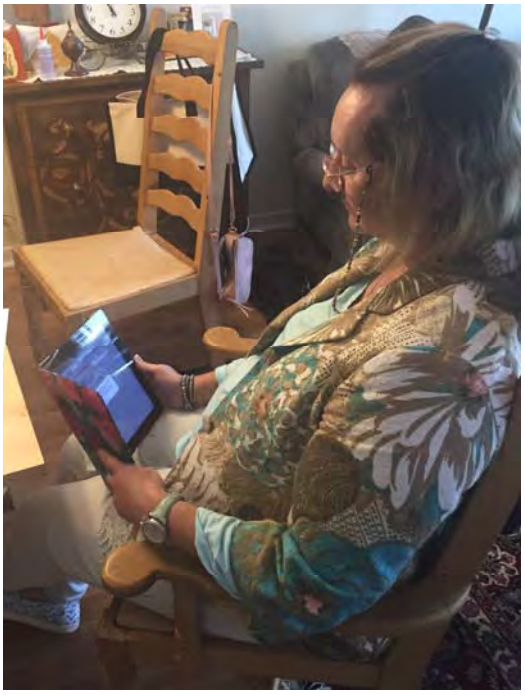
Cyber Security & Seniors as Fraud Targets

Cyber security refers to general internet safety, and focuses on the protection of information that is either stored in computers or accessible through the internet. Fraud that utilizes various modes of technology, including computers and the internet, are undergoing continual advancement.

Anyone who uses the internet can be targeted by cyber criminals, but why are older adults most commonly targeted? Older adults are more likely to be financially secure, less likely to report a fraud, or may not know how or where to report the incident. Older adults may also financially invest larger funds in products that falsely promise enhanced memory, longevity, or physical health.

Older adults tend to under-report crimes out of shame or fear, perpetuating the financial abuse to claim additional victims[9]. If you have been the victim of cyber crime in the past, it may be helpful to know **that you are not alone** and that many people have encountered the same challenges.

It is crucial that all populations, who may not be familiar enough with using consumer technologies, learn techniques of actively avoiding cyber fraud. The goal of the Piers Project Toolkit is to help prevent the online mistreatment of older adults and empower them to gain the great benefits of information technologies while practicing safe online behavior.



Who to Believe? Identify the Imposters!

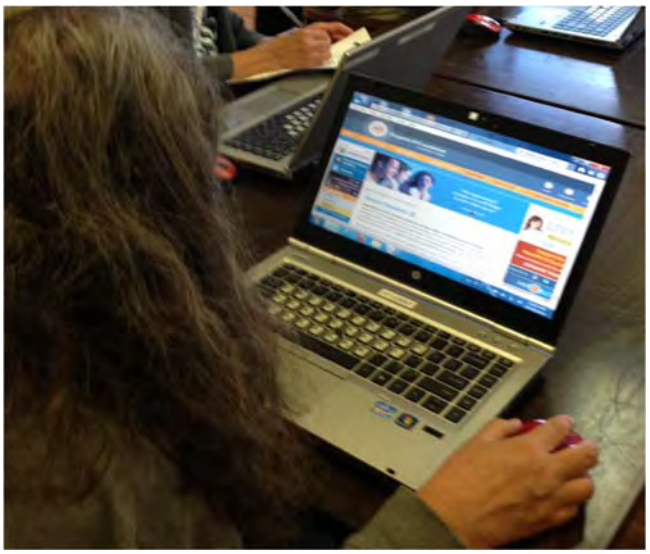
One of the many benefits of the internet is the convenience of managing many aspects of our lives, whether it be for health, taxes, or finances. We can easily find needed information and connect quickly with the right people when we need assistance. When using the internet, it is important to be able to identify and sift through scams and imposters.

Identity theft occurs when an individual obtains or uses your personal identification information without your authorization or consent. This information can then be used to order/purchase items, receive Social Security benefits, steal your personal finances, or commit other crimes. Being a victim of identity theft may result in damaging consequences. Some instances may include an illegally copied passport, diminished credit, or Medicare/ Medicaid fraud. Following is a list of common scams to be aware of and what you can do to take preventative action to proceed with safety:

Health Care Scams. These types of scams come in different forms, including falsely-presented television ads, exploiting newly established law requirements which may pertain to individuals receiving additional health care cards, or callers who promise significant discounts on health insurance.

1) **QUESTION** the content you see on the Internet,
2) **CHECK** for validity and authenticity, and
3) **ASK** your friends, neighbors or colleagues for help and to educate others around you.

Other scams consist of impersonation-related fraud, where individuals may claim that they are government officials in need of your Medicare number, so they can send an updated beneficiary card.



Here's what you can do!

- ✓ **Stay up to date on current events**. Scammers often plan to execute their attacks during periods of time where Medicare and other health programs undergo changes and are discussed widely in the media[6]. Be ready and cautious during Medicare open season. As part of the Social Security Number Removal Initiative (SSNRI), starting in April 2018, the Centers for Medicare and Medicaid Services have begun issuing and mailing new Medicare cards to replace old cards with social security numbers.
- ✓ **Research to confirm if statements are true**. Prior to sharing your private information, contact Medicare (1-800-MEDICARE) to be on the safe side. Know that Medicare will never call you, so if you get a phone call do not give out any of your personal information.

Tax-related Fraud. W-2 phishing scams have recently become a point of concern in cyber security. Scammers are finding ways to send fake emails that look like they've come from a CEO or other executive asking for W-2 tax information from employees. The cyber criminals then take the W-2 information and file fraudulent tax returns and steal people's identity[7].

Here's what you can do!

- ✓ **Pick up the phone**. If you receive any emails requesting W-2 tax information, call your company to verify the request before sending any information.
- ✓ **File your taxes early**. By filing as quickly as possible, you can beat cyber criminals to the punch before they are able to file a fraudulent claim.
- ✓ **Check your credit report regularly.** You can check your credit with a free once-a-year credit report from AnnualCreditReport.com and freeze any accounts that have suspicious activity.

Lottery Fraud. This type of illegal activity includes false claims stating that you have been selected as the winner of a lottery, in addition to financial requests to pay initial processing fees. Lottery fraud through email uses names of legitimate lottery organizations or other legitimate corporations. Take it slow, do some research, and if it sounds too good to be true, it probably is.

Investment Fraud. These inquiries concern investments in new and/or existing funds. You may be asked to invest in anything from mining, oil, gas, or a new technology company. "Prime Bank" fraud is a typical scenario. Promoters claim that the funds from investors will be used to purchase and trade a "Prime Bank" instrument issued or guaranteed by an official organization such as the U.S. Federal Reserve. They also often claim that investment opportunities of this format are solely through exclusive invitations and limited to a select group of customers[8]. Moreover, offshore investments should be critically examined, requiring additional due diligence, as a result of domestic regulations and oversight.

Here's what you can do!

- ✓ **Don't judge a company by its cover.** Some websites may look appealing and legitimate, but that does not always mean that they're trustworthy.
- ✓ **Inquire about the terms and conditions agreement.** It is advised to carefully review this agreement, as individuals often ignore the significant details.
- ✓ **Do not believe the promise of large sums of money.** This is a common tactic to bait e-mail recipients.

Emails

Email is a major mode of communication on the internet, but how can you know which ones are safe to open and which ones to discard? What are some clues to look out for? Below are some terms to know as well as what you can do recognize potential threats in your inbox.

Phishing. When a scammer uses fraudulent emails or texts to get you to share valuable personal information it is called “phishing”. Similar to “fishing”, scammers try to bait victims with a link or fake website that is disguised as a legitimate secure website. This is how they collect passwords, social security numbers, bank account information, etc.

Spam. This is categorized as unsolicited, bulk e-mails that can be used to commit a diverse range of online fraud. Most spam is harmless and are just annoying advertisements, but some can access computers and servers without authorization while transmitting viruses. This form of fraud can also illegally obtain and sell your private information.

Hacking. An individual who remotely accesses a computer or personal account without authorization is a hacker. Any form of hacking to exploit weaknesses in a computer system or computer network is considered illegal and criminal activity.

Nigerian Letter Fraud / 419 Fraud. This scam, also known as Advance Fee Fraud, requests your personal or bank-related information via e-mail, claiming that the sender is a foreign government official or a foreigner in need of financial assistance. The recipient is encouraged to send information to the author, such as a blank letterhead stationery, with their bank name(s) and account number(s), and other private information that can also be accessed through a fax number (provided within the letter)[9]. Be skeptical of foreign government emails. They typically ask for assistance by requesting a large deposit of money into a bank that is located outside of your country. These types of scammers typically make urgent appeals and ask for your immediate financial assistance. Also, be skeptical of US Government emails and beware of messages from, for example, someone who claims to be from the Social Security Administration Office, requesting your social security number. Think twice! Ordinarily, these types of organizations would not ask for your personal information through the Internet.

Taking a Closer Look

Phishing scams are not restricted to just Nigerian sources: be suspicious of any emails that seek assistance in moving large sums of money, including those that appear to come from a friend or family member in a questionable emergency.

Hi David,

I'm writing this message with tears in my eyes. I traveled to London for a short vacation and, unfortunitely, I was mugged at gunpoint last night in a park near my hotel. They got all my cash, credit cards, and mobile phone, all taken away.

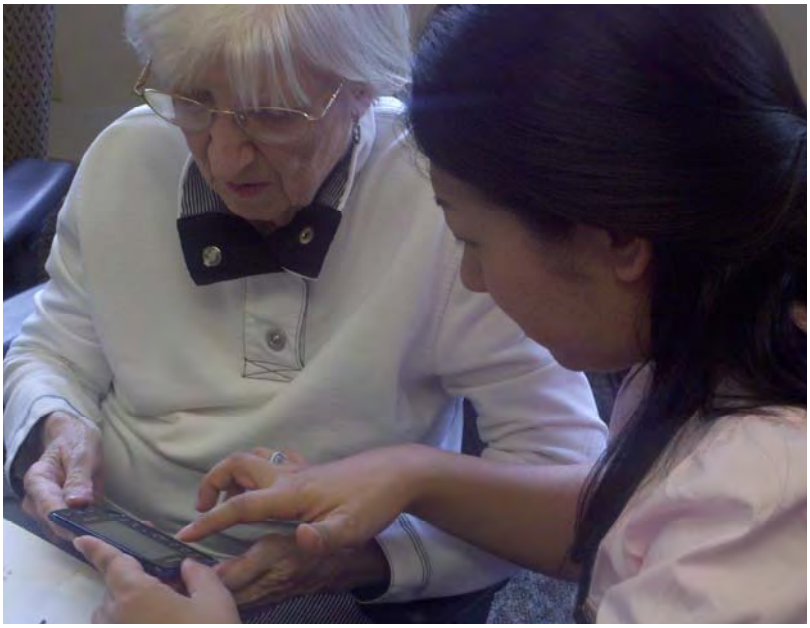
I have gone to the embassy and police station but their not helping me. My flight leaves in less than 8hrs from now and I cant pay my hotel bills. The hotel manager won't let me leave until I settle the bills. Well I really need your financial assitance! I need a loan of $1500 from you to return back home.

Won't you help me out? please I am freaking out.

Casey

In this example, we should find it strange that an emergency request is coming through email from this supposed family member. Look for other clues that may not make sense, and be aware of the possibility that someone else has hijacked this familiar person's email address. Always CHECK for validity, and call a mutual family member or friend to confirm.

Here's what you can do!



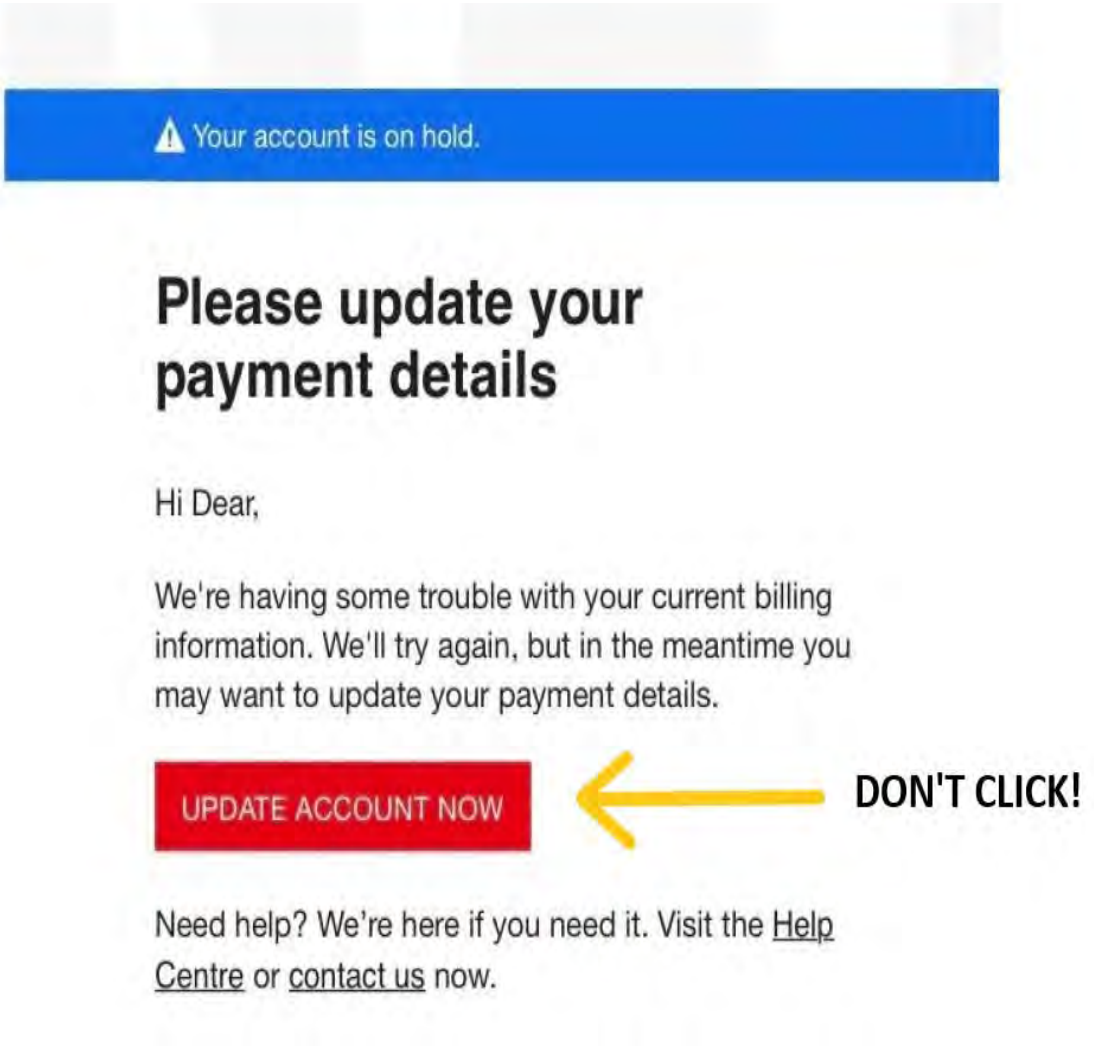
- ✓ **Pay attention to spelling and grammar in the email**. Check the spelling of the URLs, email addresses, and the content of the email. Phishing emails commonly have subtle spelling errors you can look for. When you see the sender name, take another look past it to check the email address the message is coming from. Additionally, if you hover your mouse pointer over links, you may find that it leads to a suspicious site instead of the website it promises to lead you to.
- ✓ **Don't open emails from unknown sources.** If an email, text or social media message is coming from an unfamiliar person, delete or disregard it. Practice the same caution with emails that state that you need to claim money, gifts, or vacation offers: it is likely that the message will direct you to another website where you can be prone to receiving malware or viruses. When in doubt, throw it out!
- ✓ **Be suspicious of links in emails or text messages**. If you receive an email from someone you know, but the only content in the email is a link, do not click on the link. This is a common sign that the person who sent the email to you might have been hacked. In a situation like this, contact the person by phone or other method and delete the email.
- ✓ **Never give your bank account or personal information over email**. Know that legitimate companies like banks and insurance companies will never ask for your personal information via email. Go instead to the secure website and log into your account for messages and notifications.

1) **QUESTION** the content you see on the Internet,
2) **CHECK** for validity and authenticity, and
3) **ASK** your friends, neighbors or colleagues for help and to educate others around you.

Taking a Closer Look

Scammers will often use familiar company names in their emails to make you feel like you can trust clicking on an embedded link. Take a look at the email below. This is a real life example of a "phishing" email that police reported in Ohio in December 2018 that *appears* to be from Netflix.

If you are unsure if it is safe to click on a link embedded in a company's email, the safest practice is to open a new browser window, go directly to the company's website, and log into your account. If there are important notifications or messages regarding your account, they will usually be there within your account on the secure website.



Protecting Your Finances

There are many benefits to using the Internet for managing your finances: convenient online shopping, scheduling and paying your bills, and instant transfers of funds. Solicited online financial fraud comes in different forms, and the most common type of fraud involves the usage of credit cards or bank account information, which are often exploited for purchases, investments, or tax-related complications. These schemes may obtain such information through fraudulent websites or e-mail messages.

Shopping Online. Fraudulent activity may include the utilization of a debit/credit card. It may be achieved through the theft of the actual card, or by illegally obtaining the cardholder's account and personal information, including the card number, the card's security number, and the cardholder's name and address.

Here's what you can do!

- ✓ **Use alternate payment services when possible.** Instead of making a payment directly to a site, use alternate payment services such as PayPal, Amazon, and Google Check Out that use extra levels of security[10]. When possible, you can also check out as a "guest" and choose not to save your card in an account.
- ✓ **Watch your statements**. Keep an organized list of your active credit cards and check your bank statements regularly. Contact your card issuer immediately if you notice anything that looks wrong or unfamiliar.
- ✓ **Use credit cards when possible.** Credit cards are generally safer to use than debit cards because they allow buyers to seek credit from the issuer if the product isn't delivered or what was ordered[11].
- ✓ **Enable the strongest authentication tools.** You can protect your online shopping accounts by enabling the strongest authentication tools possible such as biometrics, security keys, or a unique one time code through an app on your mobile device[11].

Taking a Closer Look

Check for a padlock icon. When you access a website and a small padlock icon appears on the address bar, this indicates that the website uses a *higher* degree of security to transmit data. Although this icon represents some protection, it does not necessarily guarantee complete security!

Check the address of the link. Links that externally appear legitimate may not be authentic, so read the link very carefully. For instance, the link may read “bankofamericacard.com” or “B-of-America”—containing the word “bank” or “America,” which helps make it appear legitimate, yet it is not a link for the true company’s website.

Check out the Federal Trade Commission website **www.ftc.gov** for more online consumer tips and advice!

Online Banking. When you are safely connected to your secure banking website or app, it is safe for you to do your banking online. Look for the same security signs as when you do your online shopping (green padlock, "https", and correct spelling of URL). Below are a few more tips to banking safely online.

Here's what you can do!

- ✓ **Use your personal Wi-Fi to do online banking**. Do not use free or public Wi-Fi to do anything that involves sensitive information.
- ✓ **Check your statements regularly**. Make sure that all purchases you see look familiar. If you see any suspicious activity in your account contact your bank immediately.
- ✓ **Before leaving your banking site or app, be sure to log out.** You may even want to close out of your browser completely after logging out.
- ✓ **Inquire about your bank's insurance policies**. In the case that a cyber criminal does acquire your banking information, it is good to know ahead of time what your bank's policies and procedures are for reimbursing you if fraudulent activity occurs. How long do you have to report a claim and how much will your bank cover?

1) **QUESTION** the content you see on the Internet,
2) **CHECK** for validity and authenticity, and
3) **ASK** your friends, neighbors or colleagues for help and to educate others around you.

Malware

How do you know what is safe to click and what is not? You want to be able to receive messages that are genuinely intended for you from trustworthy sources, so there are some important things to know.

Clickbait refers to content on the internet with the purpose of attracting attention and get visitors to click a link to a particular web page. Some headlines or ads you see may genuinely take you to an interesting article or an online store you might want to shop at. However, sites that use many clickbait headlines are more likely to contain malware.

Malware. Malware is short for "malicious software" which is a program intended to harm or disable computer systems. It is important to also use caution with your mobile devices as they are not free from malware and virus attacks. According to wikipedia.org, "Malware may be stealthy, intended to steal information, or spy on computer users for an extended period without their knowledge." Malware has several categories of software:

Ransomware. A combination of the terms '*ransom*' and '*software*', Ransomware refers to any malware that can remotely freeze your computer and retrieve stored information or even prompt a request for financial compensation, in order to return the stolen funds. Individuals who distribute these malwares may falsely identify themselves as authoritative figures, such as the police. These harmful attacks of ransomware may also target smartphones and tablet devices.

Viruses. Viruses among individuals are similar to viruses in computers. Technologically speaking, they use computers as the hosts for their own survival. In doing so, viruses may continue to multiply and modify themselves within your computer to achieve their mission, further disseminating the malware to others during this attack.

Vaccine programs. Vaccines, also known as "anti-virus software", function as either preventative or counter attacking tools against malwares. Confirm that your computer has at least one actively-operating anti-virus program (or Windows FireWall) to help prevent malware attacks. These programs may be especially necessary if your computer has been recently experiencing significant reductions in processing speed.

There are numerous vaccine programs available, with varying vaccine functions and price options. Some common brands include:

- Avast
- AVG
- Bitdefender Antivirus
- Kaspersky Anti-Virus
- McAfee AntiVirus
- Norton Security

Anti-Malware Program. Windows FireWall functions as the most basic form of protection against malwares, which is also built into the Microsoft Windows program. However, for Apple Mac users, it is important to confirm that software updates are enabled from the Apple Menu. Additionally, Apple users must allow regularly scheduled update checks in the "System Preferences" option. Browser extensions like uBlock Origin can block ads that track your activity and install malware.

Taking a Closer Look

Here are some red flags to look out for with your computer:

- Computer freezes or slows down
- Unusual sounds or beeping noises
- Continuous pop-up notifications
- Unwanted pictures
- Disappearing data

Regularly check for updates with your antivirus software—then complete a comprehensive scan as confirmation[12]. And don't forget to renew your annual subscription to keep your software updated against new attacks.

Here's what you can do!

- ✓ **Close out**. If a pop up ad or website looks sketchy, simply close out of it by clicking the upper right box with the "X". If your browser or antivirus program questions a website's safety, don't go to that website[11].
- ✓ **Don't download** anything unless you are completely aware of what it is and that it is coming from a safe source.
- ✓ **Ads and pop up windows** can often times look like a system diagnostic warming or claim that you have won a prize. Do not click on these. Close out of them immediately and run your normal antivirus scan on your computer or device. Below are examples of some common pop-up windows to avoid.

Password Safety

We should treat personal information like money—*we should value and protect it.* Password safety is crucial because it can provide access to personally valuable information—think of passwords as the keys to your house. A significant aspect of protecting ourselves is to create passwords that are difficult for others to figure out.

Creating a Strong Password.

- ✓ Make it long. More than 6 characters is ideal.
- ✓ Don't' use the same password for every account.
- ✓ Use a good mix of letters, numbers and symbols.
- ✓ Don't use personal information such as a child's name, birthdate, age, or address.
- ✓ Change your password on a regular basis. Experts suggest changing it at least every 6 months.

Password Managers. Password management programs help you use one password for multiple accounts. They auto-fill your login information for the websites you have pre-registered. Consider researching the pros and cons of each program to find out which best suits you. Some examples of free programs with optional paid services include:

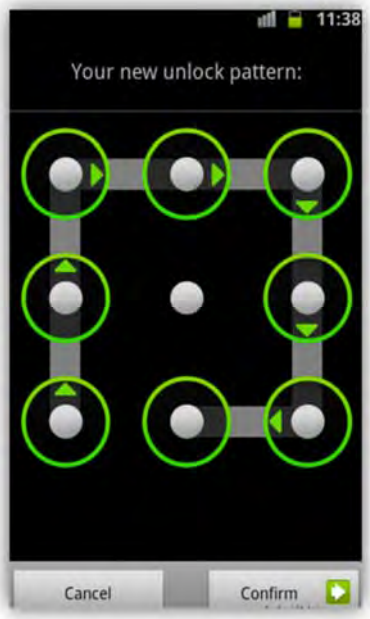
- LastPass
- Keeper
- Dashlane

Is your password on this list?

Hackers get into our accounts by guessing our passwords, so don't make it easy for someone to figure it out. Be sure you're not using any of the passwords below: these are among the top 25 most commonly-used—and therefore hackable—passwords of 2018.*

RANK	PASSWORD
1	123456
2	password
3	123456789
4	12345678
5	12345
6	111111
7	1234567
8	sunshine
9	qwerty
10	iloveyou
11	princess
12	admin
13	welcome
14	666666
15	abc123
16	football
17	123123
18	monkey
19	654321
20	!@#$%^&*
21	charlie
22	aa123456
23	donald
24	password1
25	qwerty123

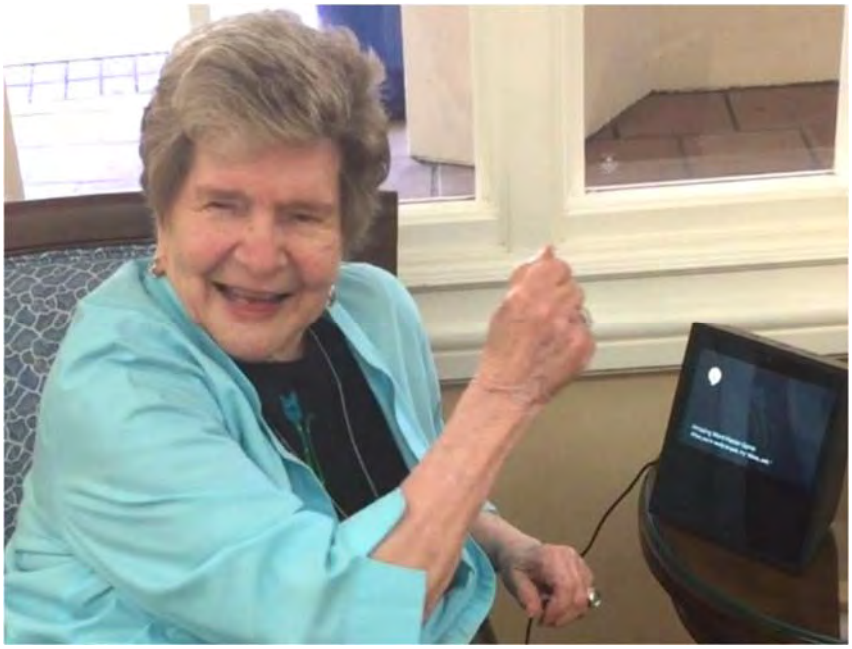
**SplashData, 2018*



Be sure to lock your devices, whether it's a computer, laptop, tablet, or smartphone. Your device allows you to set a password, so that only you can use the device.

Two-Factor Authentication. Enabling two-factor authentication (2FA) adds an extra level of security to help deter people who might try to access your accounts. This means that even if someone were to figure out your password, they would still need your physical phone to access your account. Here is what makes it two-factor: something you know (your password) and something you have in your possession (your cell phone)[13]. Authentication tools can come in the form of biometrics, security keys, or a unique one-time code through an app on your mobile device[14].

Smart Assistants, Smart Homes and Wi-Fi

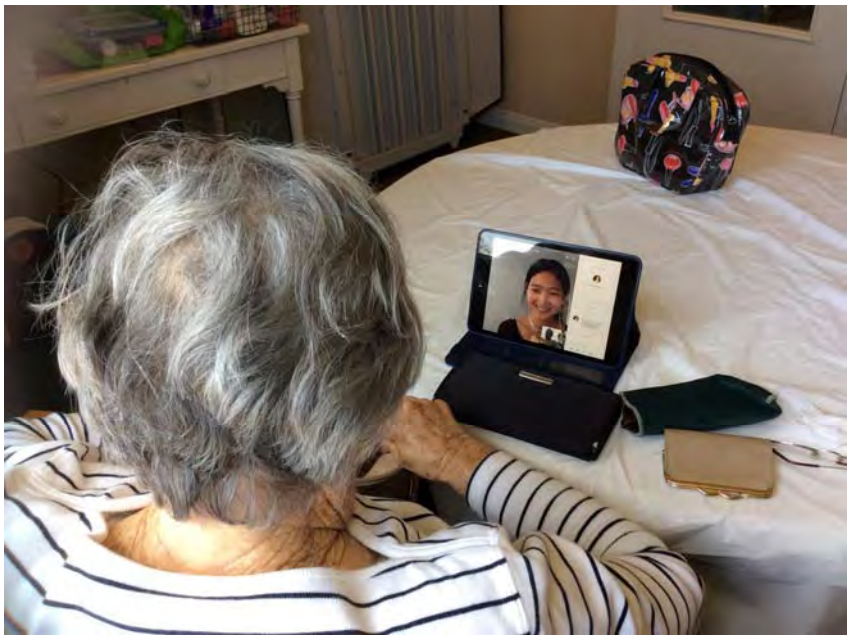


With Voice Assistants like the Amazon Alexa becoming more common place in the home, it is important to be aware of safety measures you can take to protect your privacy. **IoT** (also known as "The Internet of Things") refers to the networking capability that allows information to be sent and received from objects and devices[15]. This includes any smart home devices, appliances, speakers, toys, wearables, etc. A common question is "Is Alexa recording all of my conversations?" The Amazon website states that the answer is no. It explains that the devices are designed to detect only the "wake word" (Alexa) which it identifies through acoustic patterns that match the wake word, so no other audio is stored or sent to "the cloud"[16]. Just keep in mind that when using any internet-connected device, there is an inherent risk that a person with malicious intent can gain access to some information. However, as always, remember not to share or store any sensitive or private information on the internet.

<u>Microphone "Off" Button and Unplugging</u>

Voice First devices come with a mute button so that when it is activated, even if you say the wake word, the device will not respond. If you absolutely want to ensure that a device is not listening or recording at all, you can unplug the device or remove the batteries.

WiFi Router Protection. Wireless routers offer a lot of freedom for laptops and mobile devices. Yet when you purchase a new WiFi router, it often comes with a preset configuration that someone can possibly look up or guess. Make sure to change its password and rename the wireless network so that the internet source you are using for your smart devices is secure[11].



Social Media and Fake News

Social media networks have become very popular over the past several years. While they allow you to connect to your friends and family anytime and anywhere, it would be much safer if you exercised caution in what is shared with others in these platforms.

Here's what you can do!

- ✓ **Don't accept friend requests from people you don't know**. You may receive messages by unknown users who offer free gifts or tickets as a baiting technique to either click on their links or to meet them in person. Also be aware of embedded posts in the newsfeeds that advertise products or services. Never click on suspicious links even if they appear to come from a friend or company you know.
- ✓ **Be aware of how much information you are sharing**. Your online social media profiles can share a significant amount of information about you. This can include where you live, your birth date, your preferences, your family, and much more. Be careful with what you post—this information is intended for your friends but scammers may also see it depending on your privacy settings.
- ✓ **Try alternatives to Facebook Messenger or email**. Encrypted apps like Signal, Whatsapp and ProntonMail provide extra security.

- ✓ **Check your privacy settings**. On social media platforms such as Facebook, you can manage who can see your profile information, what you post, your activity, who can post on your timeline and who can tag you in pictures. It is wise to set these privacy settings with high restrictions so that you can review what pictures and posts you are tagged in before others can see them on your profile.

Taking a Closer Look

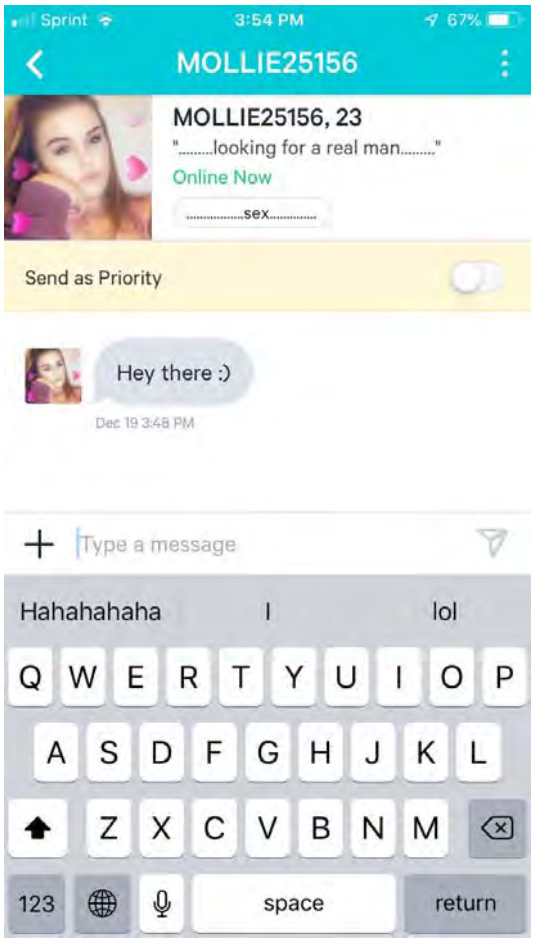
Like the "Like"? A button that looks like the "Like" button on Facebook, or a video screenshot that immediately grabs your attention, with a misleading image, may involuntarily redirect you to unwanted shopping websites or even cause the onset of viruses and malware.

It is important to be able to distinguish between the appearance of an authentic "Like" button that is located under a Facebook post, and a deceptive button which may initially look similar. "Clickbaiting" makes users curious and tempted to click a particular link, picture, video, or article. While some of these deceptive stories or advertisements just simply take you to another website, some can be harmful. However, by falling victim to this trick of liking an item, you may unknowingly propagate the same fraudulent video/image with the fake "Like" button, potentially victimizing your online friends, too.

Take a look at this reference link to the National Cyber Security Alliance—Stay Safe Online initiative to manage your privacy settings over multiple platforms. **https://bit.ly/2BYiFVh**

Online Dating Sites. Online dating can be a great tool for meeting new people with similar interests, as long as you are cautious and observant about what you decide to share with others. Be aware that there are many fake profiles on dating apps with people who will try to get you to click a link that will lead you to compromising sites.

Here's what you can do!



- ✓ **Look for red flags in their profile**. When connecting with someone on social media or on dating apps, know that a name with a long series of numbers after it can be a sign of a fake profile. Does the headline and text seem to imply that they are just looking for something physical?
- ✓ **Don't click on any links they may send**. After several message exchanges and feeling like you're getting to know someone, you may feel comfortable sharing your phone number to set up a meeting. But if there is no substance to the conversation and they simply send you a link, it may lead to a website full of malware and viruses—avoid clicking on such links and move on.

Fake News. In today's news and media, it can be difficult to decipher what is real and what is fake. Now more than ever, people have greater access to information; however, the truth is not always clear since anyone is able to put anything on the internet and claim it is true. So how do you determine what is a reliable source of news?

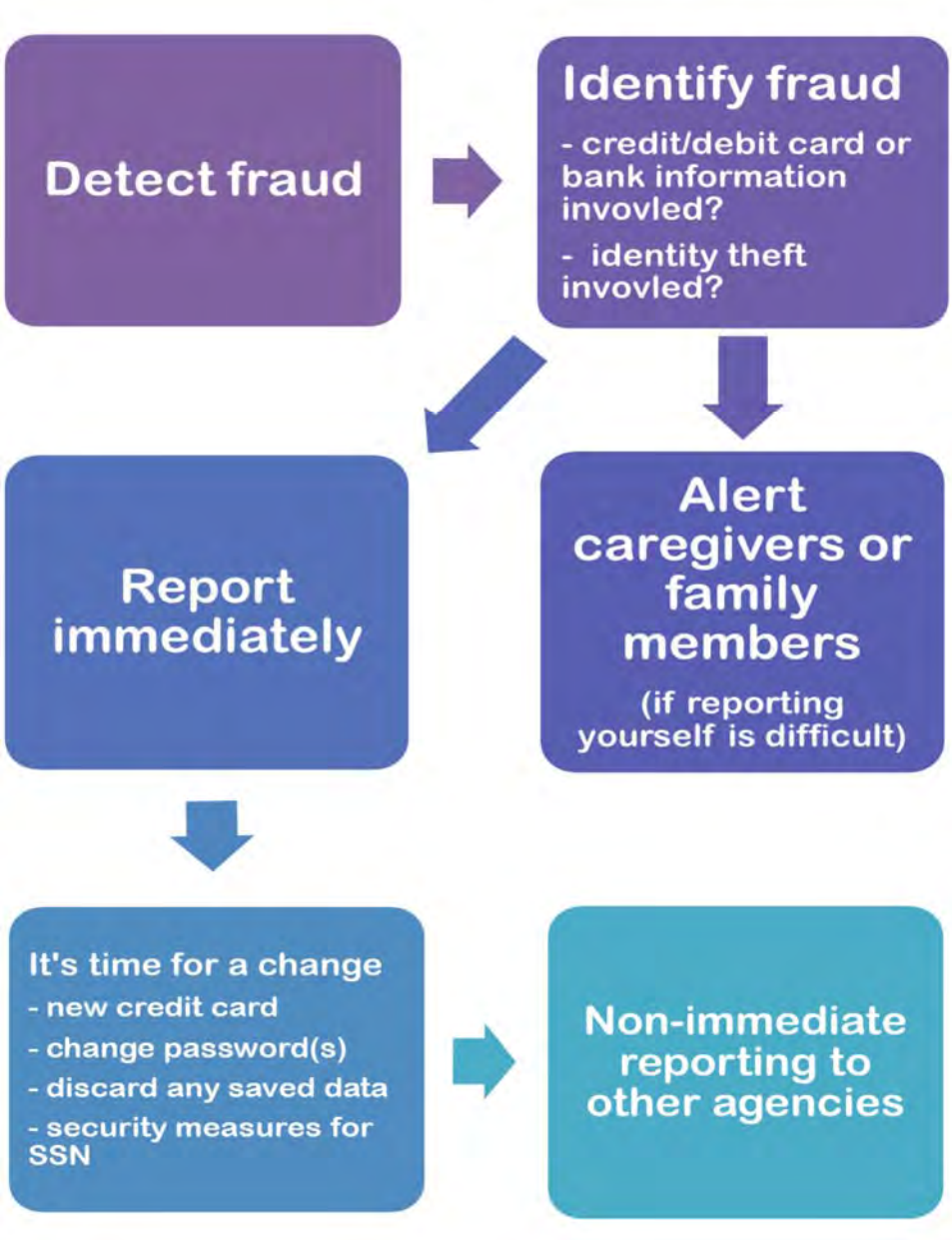
Here's what you can do!

- ✓ **Consider the source.** When you're on a website, gather information about the site itself. Looking at the "About Us" section, who runs the site? Why have they created the site? Who is paying for the site and do they favor a sponsor? Where did the information come from? There are different levels of credibility that you can find just by looking at the end of a website URL. If a site ends in **.gov**, this often means it is a government website and generally goes through several reviews and quality assurance checks before being posted.

If a site ends in .edu, this identifies a site as coming from a school or university which usually adheres to academic standards for posted materials.

- ✓ **Cross reference**. If you were to go on several different, well-known, reputable news sources, despite the biases the sources may have, are there commonalities in the facts? Does it sound outlandish, or like a joke? Are other sources verifying that the information is true?
- ✓ **Do some research**. Check the date to see if the information is relevant to current events. Ask an expert when possible or consult fact-checking sites.

Cyber Fraud Response Procedure



Reporting Agencies

Fraud Type	Agency & Contact
Reporting Scams in General (Recommended)	**Local law enforcement agency** The police are obligated to assist you and refer you to other appropriate agencies.
Reporting Scams in General (Recommended)	**Federal Trade Commission** Phone: 1-877-382-4357 (TTY/TTD: 1-866-653-4261)
Internet Crime and Fraud (Recommended)	**Internet Crime Complaint Center** (IC3) comes from a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Report any crimes or frauds based on the internet. http://www.ic3.gov/default.aspx
Reporting Health Care Scams	**Call the Federal Trade Commission (FTC)** at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261 OR visit: ftc.gov/complaint
Medicare Fraud	**Department of Health and Human Services** Phone: 1-800-633-4227 Report Medicare and Medicaid fraud, waste, and abuse. Phone: 1-877-808-2468 **Senior Medicare Patrol** www.smpresource.org **Office of the Inspector General** 1-800-447-8477 or email spoof@oig.hhs.gov
Identity Theft Crime	**Identity Theft Resource Center** Phone: 1- 888-400-5530 http://www.idtheftcenter.org/knowledge-base/
Health-related Issues for Spanish Speakers	**Su Familia: The National Hispanic Family Health Helpline** Monday through Friday 9 am to 6 pm (EST) Phone: 1-866-Su-Familia (1-866-783-2645)
IRS and Tax-related Fraud	**IRS's Identity Protection Specialized Unit** Phone: 1-800-908-4490 **Internal Revenue Service** If you or someone you know has received an email from someone claiming to be the IRS asking for personal or financial information, forward the email to the Internal Revenue Service at phishing@irs.gov.

Fraud Type	Agency & Contact
IRS and Tax-related Fraud	**IRS's Identity Protection Specialized Unit** Phone: 1-800-908-4490 **Internal Revenue Service** If you or someone you know has received an email from someone claiming to be the IRS asking for personal or financial information, forward the email to the Internal Revenue Service at phishing@irs.gov.
Lottery Scam	**AARP Fraud Fight Call Center** Report any foreign lottery scams. Phone: 1-800 646-2283 **U.S. Postal Inspection Service** Report any lottery or mail scams. 1-877-876-2455
Social Security Fraud	**Social Security Administration** Phone: 1-800-269-0271 (TTY: 1-866-501-2101) 10:00 am to 4:00 pm (EST) http://oig.ssa.gov/report/
Passport Fraud	**Department of the State** Contact PassportVisaFraud@state.gov
Business Fraud	**Better Business Bureau** Report on their website. https://www.bbb.org/consumer-complaints/file-a-complaint/get-started
Reporting Phishing Emails	**Department of Homeland Security, U.S. Computer Emergency Readiness Team** Email: phishing-report@us-cert.gov Or file a report with the Federal Trade Commission at spam@uce.gov You can also forward phishing emails to spam@uce.gov
General Adult Abuse Reporting	**Adult Protective Services** under California Department of Social Services Everyone provides support for elder and dependent adults. Report suspected abuse including: physical abuse, sexual abuse, self-neglect, abandonment, financial abuse, psychological abuse and neglect by others. For information visit http://www.cdss.ca.gov/Adult-Protective-Services Number varies in each county in California: http://www.cdss.ca.gov/inforesources/County-APS-Offices

Resources

If you are interested in learning more or even teaching others on online security, this resource list may be of help.

Name	Website
AARP (American Association of Retired Persons) provides the latest news on senior-targeting scams.	http://www.aarp.org/money/scams-fraud/ Trained volunteers in fraud counseling are available on their helpline at 1 (877) 908-3360.
CFTC (Commodity Futures Trading Commission) educate consumers on frauds in the U.S. futures markets.	http://www.cftc.gov/ConsumerProtection/Resources/index.htm
Consumer Financial Protection Bureau provides information about financial scams and deceptive financial products.	http://www.consumerfinance.gov/
FBI (Federal Bureau of Investigations) provides information on fraud schemes that use mass marketing to swindle consumers.	https://bit.ly/2rWBZOK
ElderCare.gov connects you to community services for older adults, including legal and financial assistance services.	https://eldercare.acl.gov/Public/Index.aspx
Federal Trade Commission provides information on new and ongoing fraud schemes, along with tips to help you protect yourself.	http://www.consumer.ftc.gov/scam-alerts Check out this online scam awareness campaign by FTC: http://www.consumer.ftc.gov/features/feature-0030-pass-it-on
Federal Housing Finance Agency includes tips to help consumers avoid housing related scams, such as mortgage rescue scams, bankruptcy scams, and reverse mortgage fraud.	https://www.fhfa.gov/
U.S. Bureau of Consular Affairs provides information for Americans who are victims of a crime overseas.	http://travel.state.gov/content/passports/english/go.html

Name	Website
Internet Crime Complaint Center comes from the partnership between the FBI and the National White Collar Crime Center and refers the criminal complaints to federal, state, local, or international law enforcement and/or regulatory	http://www.ic3.gov/crimeschemes.aspx
Oasis promotes continual learning for older adults and offers resources on cyber security.	https://bit.ly/2RrFnQh
Elder Justice Initiative provides information from the U.S. Department of Justice related to victims of elder abuse and financial exploitation and their families.	http://www.justice.gov/elderjustice/
Stay Safe Online by National Cyber Security Alliance provides tips and resources for	https://www.staysafeonline.org/stay-safe-online/resources/
GCF Global provides internet safety resources.	https://edu.gcfglobal.org/en/internetsafety/
Medicare.gov provides information on what to do to safeguard your personal information and	https://www.medicare.gov/forms-help-resources/help-fight-medicare-fraud

References

[1] Anderson, Monica and Andrew Perrin. “Technology Use Among Seniors.” *Pew Internet Center*, 17 May. 2017. Web. 31 Dec. 2018. http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/

[2] New York State Office of Children and Family Services “Under the Radar: The New York State Elder Abuse Prevalence Study.” *Self Reported Prevalence and Documented Case Surveys Final Report* 2011. Web. 31 Dec. 2018. https://ocfs.ny.gov/main/reports/Under%20the%20Radar%2005%2012%2011%20final%20report.pdf

[3] Office of Financial Protection for Older Adults “Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends.” *Consumer Financial Protection Bureau*, February 2019. Web. 12 March 2019. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_suspicious-activity-reports-elder-financial-exploitation_report.pdf

[4] Baig, Mehroz. “Elder Abuse and Technology.” *The Commonwealth Blog*, 6 Jun. 2013. Web. 4 Jan. 2016. http://www.commonwealthclub.org/blog/2013-06-06/elder-abuse-and-technology

[5] VanDeVelde, Amy. “Oasis YouTube video provides great guidance on how to navigate and trust what you hear on the news.” *Oasis Blog*, 14 March 2018. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/is-it-fake-news-find-out-how-to-know-for-sure-151661?utm_source=Center+0&utm_medium=email&utm_campaign=7585+March+2018+Discoveries&utm_term=620598

[6] Federal Trade Commission. "Health Care Scams." *Pass It On Resource Guide*, 2014. Web. 31 Dec. 2018. https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0183-health-care-scams.pdf

[7] Sjouwerman, Stu. “Scam Of The Week: New FBI and IRS Alerts Against W-2 Phishing.” *KnowB4 Security Awareness Training Blog*, 18 March. Web. 31 Dec. 2018. https://blog.knowbe4.com/scam-of-the-week-new-fbi-and-irs-alerts-against-w-2-phishing

[8] The Office of Investor Education and Advocacy (OIEA). “Investor Alert: Prime Bank Investments Are Scams.” U.S. Securities and Exchange Commission, 5 Feb. 2015. Web. 4 Jan. 2016. http://www.sec.gov/oiea/investor-alerts-bulletins/ia_primebankscam.html

[9] The Federal Bureau of Investigation. “Common Fraud Schemes.” *Scams & Safety*, 2010. Web. 4 Jan. 2016. https://www.fbi.gov/scams-safety/fraud

[10] AARP. “Prevention, Not Just Awareness, Key to Cyber Security.” Web. 31 Dec. 2018. https://states.aarp.org/prevention-awareness-cyber-security/

[11] Stay Safe Online. “Shopping Online.” *Online Safety Basics*. Web. 31 Dec. 2018. https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

[12] Kirchheimer, Sid. "Is Your Computer Infected." *AARP*, 9 Jan. 2012. Web. 31 Dec. 2018. https://www.aarp.org/money/scams-fraud/info-01-2012/computer-infected-scam-alert.html

[13] VanDeVelde, Amy. “Two factor authentication adds an essential layer of security.” *Oasis Blog*, 17 October 2017. Web. 31 Dec. 2018. https://www.oasisnet.org/Blog/want-more-protection-for-your-email-and-facebook-accounts-135523

[14] National Cyber Security Alliance. “Cheers to Safe Cybershopping!” *Stay Safe Online*. Web flyer. 31 Dec. 2018. https://staysafeonline.org/wp-content/uploads/2018/11/Online-shopping-tip-sheet-1118.pdf

https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230&pop-up=1

[15] “IOT.” *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

[16] Amazon.com. “Alexa and Alexa Device FAQS” Web. Feb. 2019. https://www.merriam-webster.com/dictionary/Internet%20of%20Things

Our Mission: Exploring innovative uses of technology to help individuals thrive, by enhancing wellbeing and independence, particularly as we age.

Our Vision: Technology innovation has an important role to play in enhancing each individual's ability to "live life my way" in the place he or she calls home. Our goal is to harness technology solutions that support and enhance wellbeing and help each of us thrive in mind, body and spirit.

Our Projects: Initiatives represent a diverse range of technologies and innovations that focus on key areas such as strengthening social connectedness, promoting meaningful engagement, growth and whole person wellness, advancing proactive/participatory control over health and wellbeing, expanding support for mobility, vision, hearing and cognitive abilities, preventing emergencies or serious events before they occur, empowering and supporting care circles, promoting healthy, safe, accessible, and sustainable environments.

For more information, please visit www.fpciw.org.

front porch | CENTER FOR INNOVATION AND WELLBEING