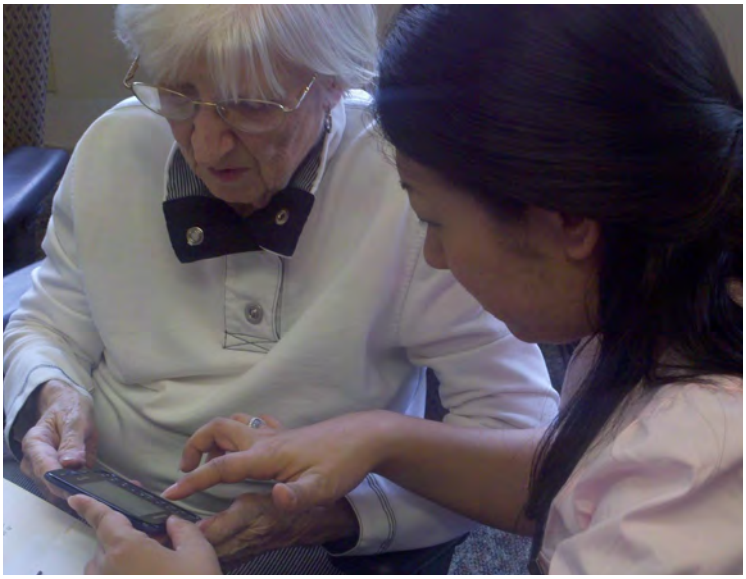


Cyber Safety Toolkit

An Internet Resource Guide of the Piers Project

An initiative of the Front Porch Center for Innovation and Wellbeing

front porch

CENTER FOR INNOVATION AND WELLBEING

front porch | CENTER FOR INNOVATION AND WELLBEING

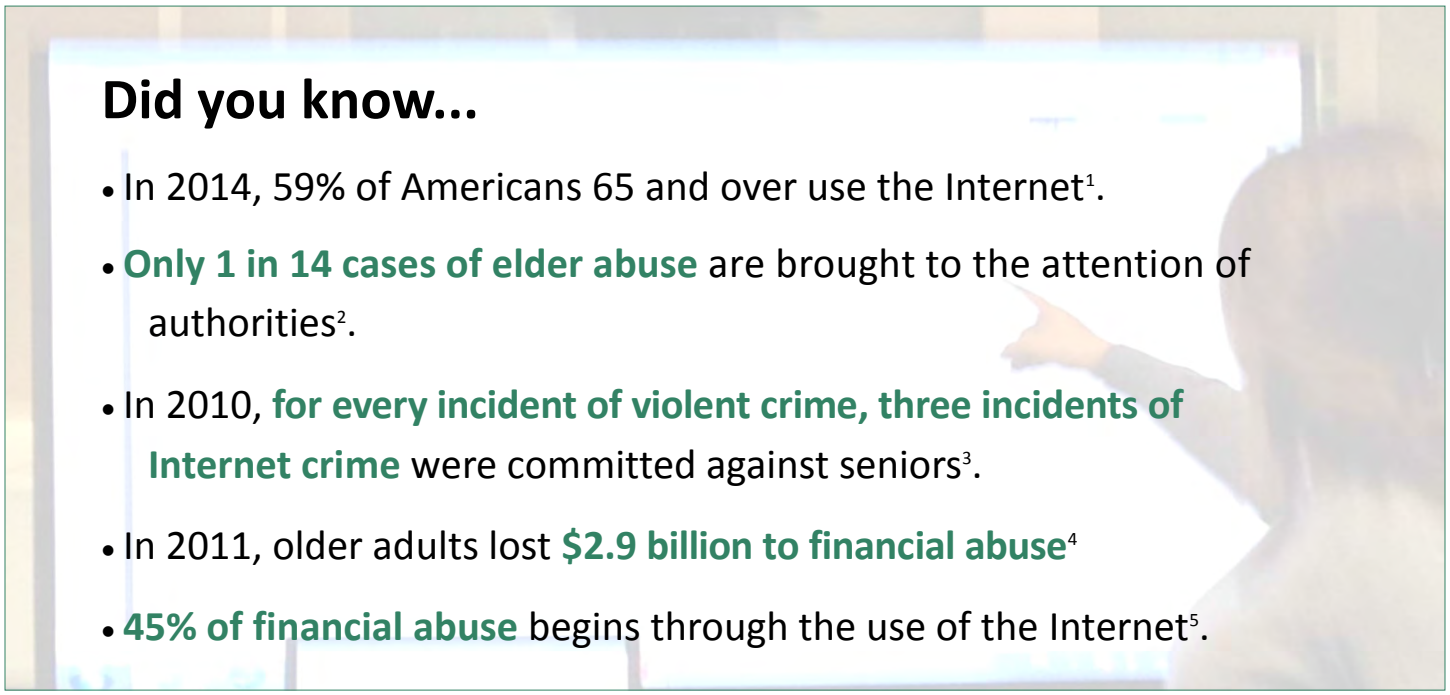
Our Mission: Exploring innovative uses of technology to empower individuals to live well, especially in their later years.

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 maintaining brain health, enhancing social connectedness, promoting engagement and growth while also giving individuals autonomy over their own health and wellness, preventing emergencies and increasing supportive resources to both formal and informal caregivers.

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

Table of Contents



Did you know...

- In 2014, 59% of Americans 65 and over use the Internet[1].
- **Only 1 in 14 cases of elder abuse** are brought to the attention of authorities[2].
- In 2010, **for every incident of violent crime, three incidents of Internet crime** were committed against seniors[3].
- In 2011, older adults lost **$2.9 billion to financial abuse**[4]
- **45% of financial abuse** begins through the use of the Internet[5].

The Internet comes with many advantages, as you are able to communicate with loved ones, share priceless moments with friends, and research your favorite topics (just to name a few), while in the comfort and convenience of your home. However, it is important to stay educated on how to protect yourself and your privacy online through training in cyber security.

Common cyber fraud schemes consist of online financial fraud (e.g. through credit cards, investments, tax returns, etc.), identity theft, social media fraud, and malware distribution. It is crucial that vulnerable populations, who may not be familiar enough with developing technologies, learn techniques of actively avoiding cyber fraud. With the goal of helping seniors gain the great benefits of information technologies, and to help initiate their participation in a digital society while practicing safe online behavior, the Front Porch Center for Innovation and Wellbeing (FPCIW) is working with a wide array of community-based organizations, government agencies, innovators, technology companies, and universities to identify and prevent the online mistreatment of older adults.

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 steps toward successful and safe online experiences.

1) **QUESTION** the content you see on the Internet,

2) **CHECK** for validity and authenticity, and

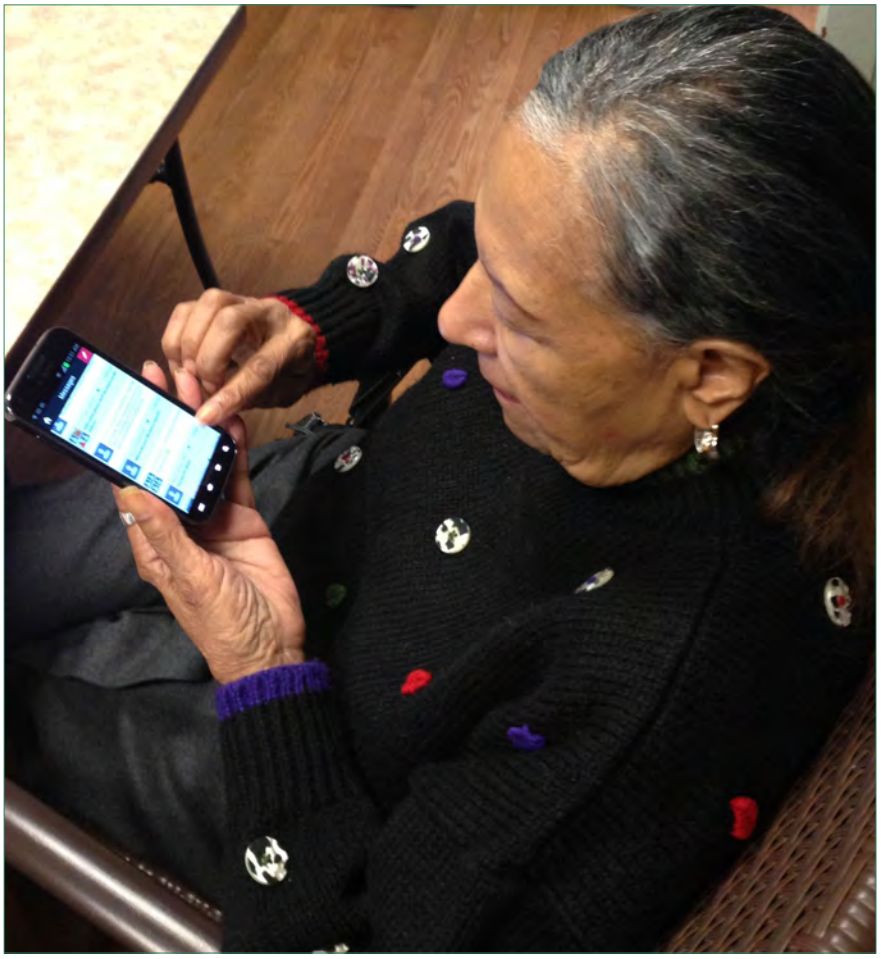
3) **ASK** your friends, neighbors or colleagues for help and to educate others around you.

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. Therefore, it is crucial to constantly stay abreast of the latest development in cyber security.

According to the FBI, older adults should invest close attention to fraud schemes for the following reasons[6]:

- Older adults are more likely to be financially secure. This may indicated that these individuals own their house, possess retirement funds, and/or have reputable credit history.
- Older adults are less likely to report a fraud, for they may not know how or where to report the incident, and they may not even be aware that the circumstance is considered fraudulent.
- Older adults may financially invest larger funds in products that falsely promise enhanced cognitive function, longevity, or physical health.



However, when an elderly victim does report a crime, he or she may not remember all the details of the fraudulent event, due to normative effects of memory loss from aging.

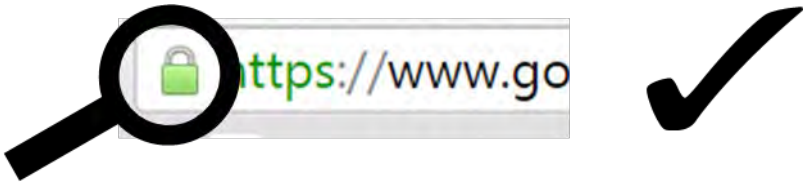
Common Cyber Fraud Schemes

There are many benefits to using the Internet for managing your finances: convenient online shopping, easy-to-retrieve online bank statements, and instant transfers of funds. Solicited online financial fraud comes in different forms, which can make it difficult to distinguish from other non-fraudulent events. 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 frauds may obtain such information through fraudulent websites or e-mail messages. Following is a brief overview of popular financial frauds:

Credit Card Fraud. Fraudulent activity may also 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. Presently, the latter type is more common.

Click with Care

Look 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!



Keep an organized list of your active credit cards. It is important to contact your card issuer immediately if you notice any suspicious activities in your mailed or online statements.

Check the address of the link. For example, 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 the valid link for the actual website.

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

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 a well-known 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[7]. Moreover, offshore investments should be critically examined, requiring additional due diligence, as a result of domestic regulations and oversight.

Click with Care

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.

Do not believe the promise of large sums of money for your cooperation! This is a common tactic to bait e-mail recipients.

Inquire about the terms and conditions agreement. It is advised to carefully review this agreement, as individuals often ignore the significant details.

IRS or Tax-related Fraud. Requests to pay taxes and/or payments through untrustworthy websites. If you have filed a report with your local police department due to tax refund fraud, they may require you to complete an IRS Identity Theft Affidavit (IRS Form 14039), which is reported to the Internal Revenue Service, further assisting the investigation process. This affidavit permits the IRS to share the fraudulent tax return, filed under the victim's name, with your local and state law enforcement agency.

Click with Care

Avoid revealing your personal information. It is not safe to include your account information, social security number, or bank account details in e-mail messages, especially when replying to e-mails from unreliable or unfamiliar sources.

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 e-mail knowingly uses names of legitimate lottery organizations or other legitimate corporations.

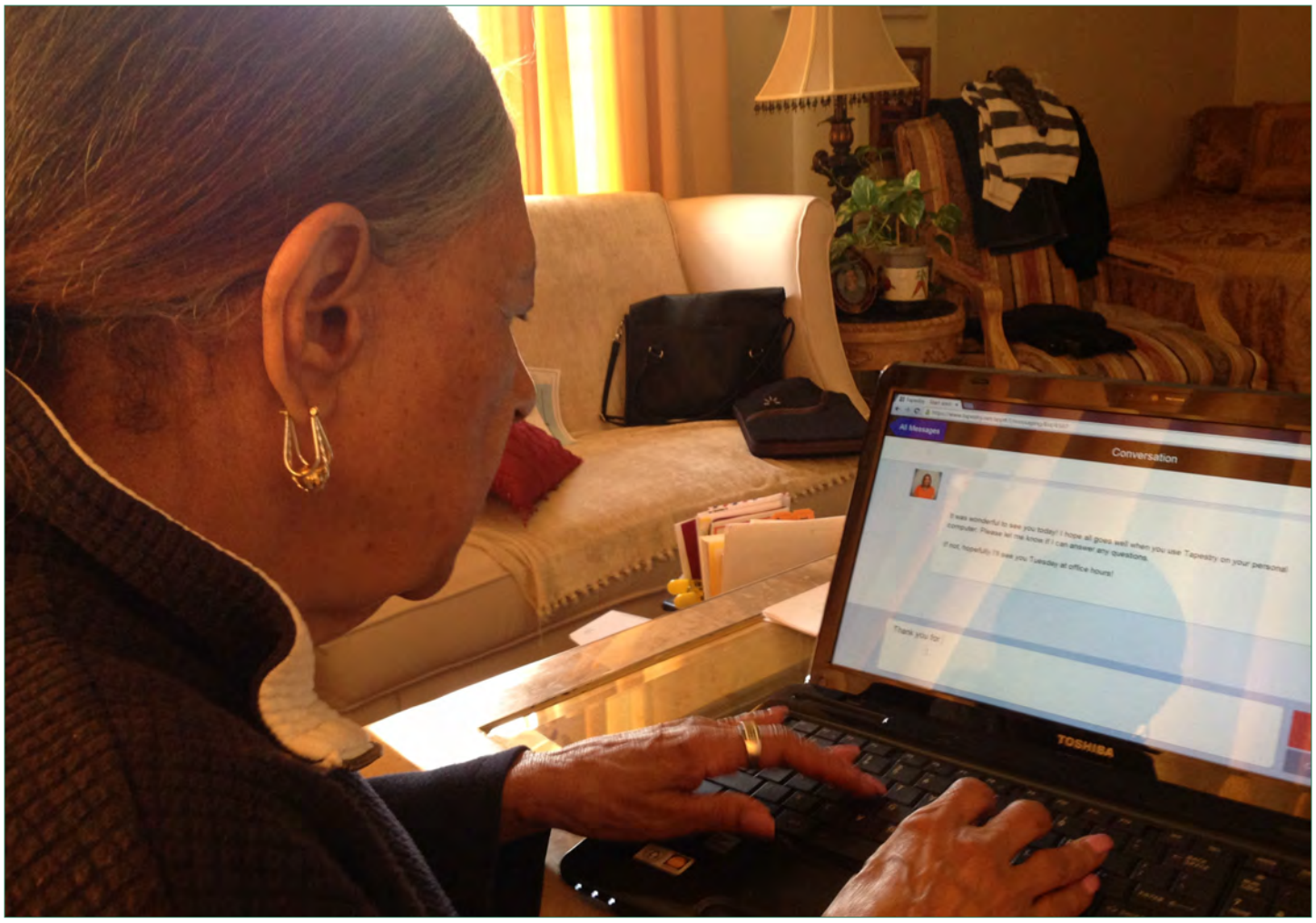
Online Shopping Fraud. When you shop online, be aware of what/who the product or service is targeting. Scammers do a lot of research on what they think older adults will likely be deceived by, including their general needs or areas of interest. If and when you do use a credit card, avoid the choice to save your card information on the company's files.

Click with Care

Purchase with care. Confirm that your purchasing activity matches a reliable source. You may be able to verify the company or seller's information, such as its phone number, website address, name(s), and address(es).

Use a credit card rather than your debit card. There is room for debate regarding fraudulent cases. However, debit cards are more susceptible to fraud, since they have direct access to the withdrawal of funds from your bank account. This situation makes it more difficult for debit card issuers to retrieve their stolen money.

Location, Location, Location! Exercise additional caution when purchasing items from websites that are based outside of your country.



Check with the Better Business Bureau **www.bbb.org** to retrieve information about a company.

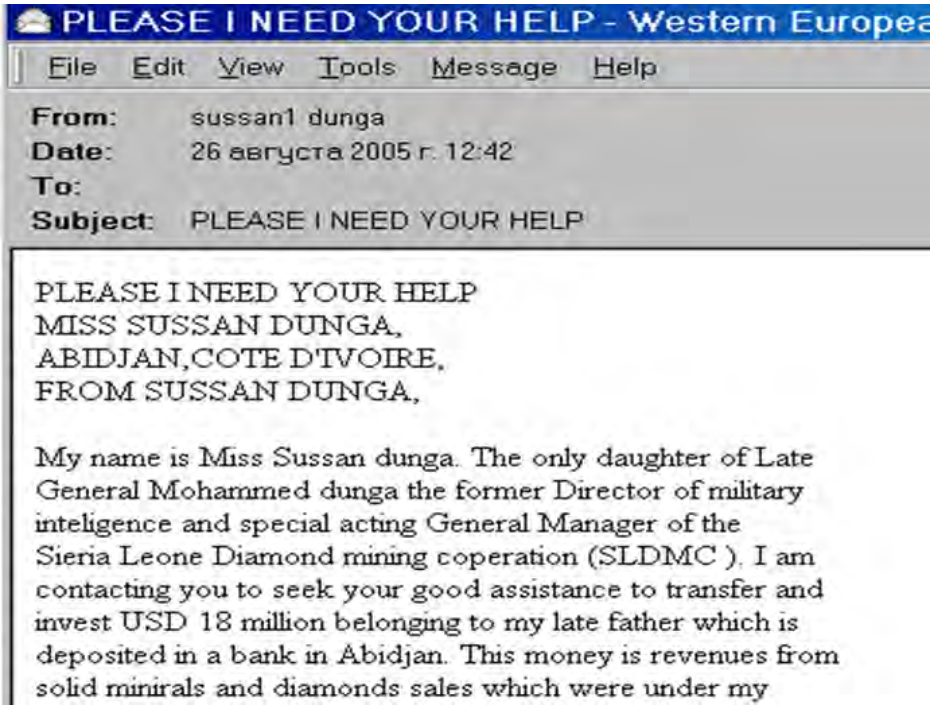
Phishing & Identity Theft

Identity theft refers to any crime where an individual obtains your personal identification information in an unauthorized manner and/or utilizes the information without your consent. This information may 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, and Medicare or Medicaid fraud. The following are some examples of identity theft:

Nigerian Letter Fraud / 419 Fraud. This scam 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)[8].

Click with Care

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.



PLEASE I NEED YOUR HELP - Western Europea

File Edit View Tools Message Help

From: sussan1 dunga
Date: 26 августа 2005 г. 12:42
To:
Subject: PLEASE I NEED YOUR HELP

PLEASE I NEED YOUR HELP
MISS SUSSAN DUNGA,
ABIDJAN,COTE D'IVOIRE,
FROM SUSSAN DUNGA,

My name is Miss Sussan dunga. The only daughter of Late General Mohammed dunga the former Director of military inteligence and special acting General Manager of the Sieria Leone Diamond mining coperation (SLDMC). I am contacting you to seek your good assistance to transfer and invest USD 18 million belonging to my late father which is deposited in a bank in Abidjan. This money is revenues from solid minirals and diamonds sales which were under my

Be skeptical of US Government emails. 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

Health Care Scams. These types of scams come in different forms, including falsely presented television ads, proposing newly established law requirements, which may pertain to individuals receiving additional health care cards, in addition to callers that state their offer of significant discounts on health insurance. Other scams consist of impersonation-related fraud, where individuals may claim that they are government officials in need of your Medicare number, so that they can send an updated beneficiary card. It is important to always remain cautious and knowledgeable of current events, as 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[9].

Hacking. This form of illegal activity is comprised of an individual remotely accessing a computer or personal accounts, in order to retrieve sensitive information.

Click with Care

Research to confirm if statements made are actually true. Prior to sharing your private information, contact Medicare (1-800-MEDICARE) to be on the safe side. Distribute your knowledge by informing your friends, relatives, etc.[10]

Avoid exposing any personal information over an e-mail. Examples of sensitive information include: your social security number, government-based benefit information, insurance details, passport number, and any credit card or bank information.

Social Media Fraud

Social media networks have recently 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.

Facebook. Facebook is an interactive tool that allows individuals to connect to the world. Here are some tips for you to keep in mind when using this social media website:

Click with Care

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, yet it does not possess the same functions or intentions. "Click-baiting" makes users curious and tempted to click a particular link, picture, video, or article. However, by falling victim to this crime, you may also post the same fraudulent video/image with the fake "Like" button, potentially victimizing your online friends, too.

Free gifts and offers in disguise. 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 imbedded posts in the newsfeeds that advertise products or services.

How much is too much information? The answer may depend, varying among locations and individual circumstances. However, when you share information regarding your home location, your preferences, your family, and your birth date, it is important to confirm that this type of exchange is safe. For example, if you will be vacationing soon, it is advised to post about your trip (if you want, of course) after you return, so that others are not informed of an empty house.

Be careful with sharing too much personal information on social media. You may be contacted by scammers who know what you like and where you reside. For instance, they may attempt to entice you by offering free, yet non-existent, gifts and tickets. It is crucial to consistently check your privacy settings before you post anything, while also being cautious of accepting unfamiliar or questionable 'friend' requests online.

Be skeptical of what others "like" or material that others post on social media websites. Videos and images that look suspicious and provocative can be filled with hidden website links, which can redirect you to other websites that possess malware and viruses.

Online Dating Sites. Companionship becomes increasingly important as we age. 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. Scams are widespread throughout online dating platforms.

Utilizing the dating website's message option is the safest way to respond, due to the system feature that allows you to 'Block User' or 'Report User,' if you encounter an individual online that appears suspicious or makes you feel uncomfortable. However, it is not advised to respond by using your personal e-mail address. In a similar manner to creating an online dating profile, avoid revealing your home address, phone number, and other personal information during message exchanges.

Click with Care

Avoid creating a username that is too similar to your own name. Steer clear from creating a username that could possibly reveal your location, such as *'JuliefromSD'*, which reveals an individual's name and (most likely) her location to the public. Also, it is noteworthy to remember that provocative or controversial usernames could potentially attract unwanted attention from others.

Malware

Malware, which is short for "malicious software", is a program intended to harm or disable computer systems. According to www.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*') 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 tablets devices.

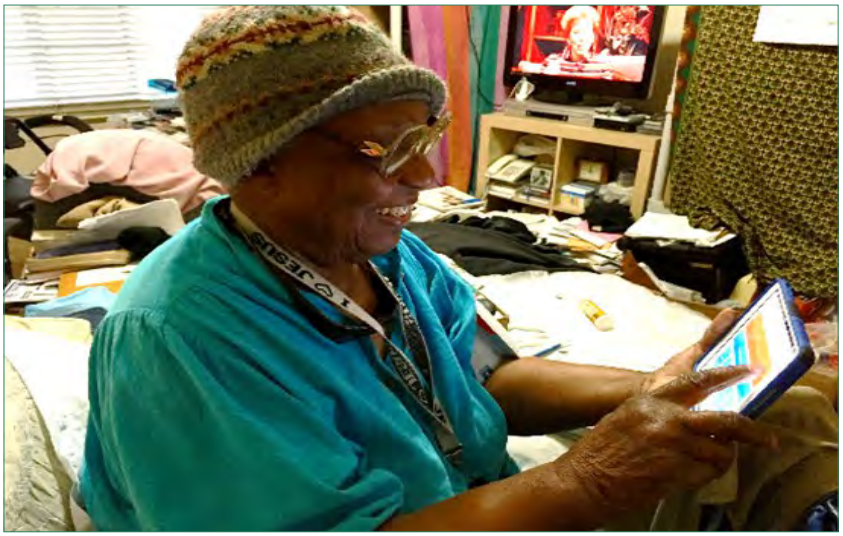
Viruses: Viruses among individuals are similar to viruses in computers. Technologically speaking, they use computers as the hosts for their own survival. In doing so, viruses may continue to multiply and modify themselves within your computer to achieve their mission, further disseminating all malware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

Spam: This is categorized as unsolicited, bulk e-mails that can be used to commit a diverse range of online fraud. Spam can access computers and servers without authorization, while also transmitting viruses. This form of fraud can also illegally obtain and sell your private information[12].

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 prices options). Some common companies include:

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



Click with Care

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

- Reduction in computer speed/Computer freeze
- Unusual sounds or beeping noises
- Continual pop-up notifications
- Unwanted pictures
- Disappearing data

Regularly check for updates regarding 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.

Built-in 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.

Use your devices with caution, too. Mobile devices, such as tablets (Android or iPad) and smartphones, are not free from malware and virus attacks—the same rules still apply. It is important to remain cautious when you are opening unfamiliar links from text messages or e-mails, while also avoiding any click-baiting attempts.

Click with Care

Be suspicious of links in e-mails or text messages. Did the e-mail or text message truly come from your friend, family member, school, work place, or subscribed newsletters? If the e-mail or text message states that you need to claim your 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.

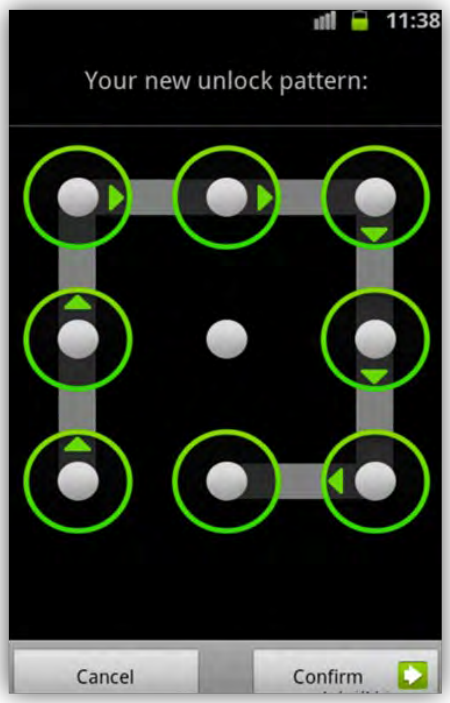
Password Safety

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.

Create strong passwords to prevent others from accessing the personal data in your devices. You may achieve this by creating passwords that are at least 8 characters long, in combination with numbers, letters, and symbols. Avoid using the same password for more than one account! Also, steer clear of including your full name, telephone number, home address, social security number, insurance policy number, physician information or any other type of sensitive detail.

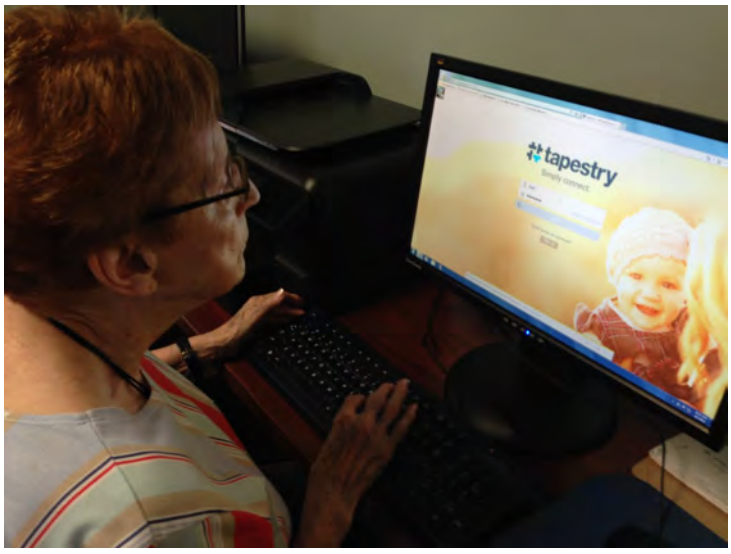
It is key to change your password on a regular basis. Using the same password for all your accounts is <u>not</u> recommended. If one account becomes hacked, the rest can be in danger, too.

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

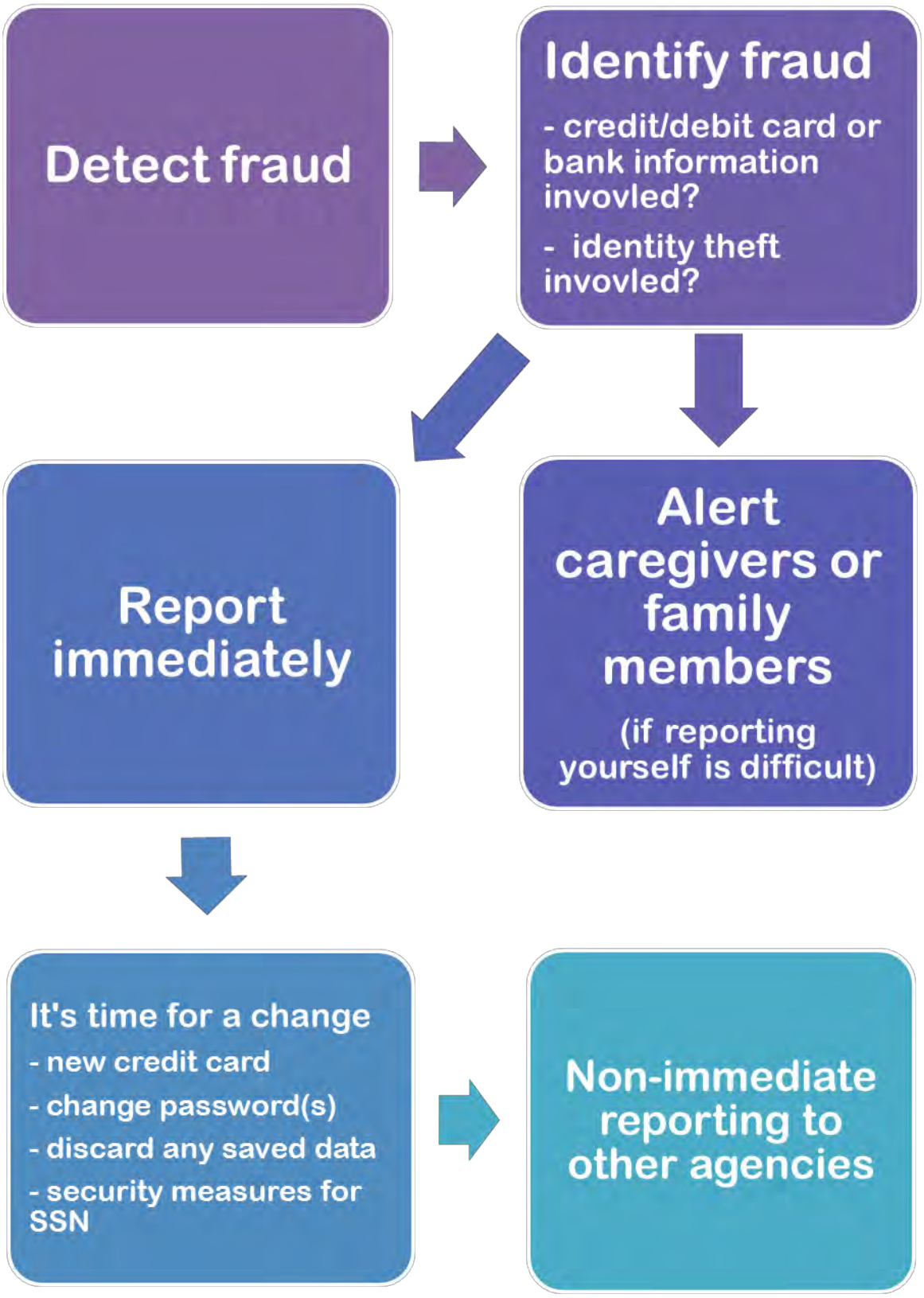


Practice the 3 keys to Cyber Security:

- **QUESTION** content you see online
- **CHECK** for validity
- **ASK** around



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 **Senior Medicare Patrol** Report Medicare and Medicaid fraud, waste, and abuse. Phone: 1-877-808-2468
Identity Theft Crime	**Identity Theft Resource Center** Phone: 1- 888-400-5530 http://www.idtheftcenter.org/index.php
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
Lottery Scam	**AARP Fraud Fight Call Center** Report any Jamaican lottery scams. Phone: 1-800 646-2283 **U.S. Postal Inspection Service** Report any lottery 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** Report on their website. http://travel.state.gov/content/passports/english/go/older-traveler.html
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
General Adult Abuse Reporting	**Adult Protective Services** under California Department of Social Services Everyone provide 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. Number varies in each county in California: http://www.cdss.ca.gov/agedblinddisabled/PG2300.htm

Resources

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

Name	Website
AARP (American Association of Retired Persons) provides the latest news on senior-targeting scams.	http://www.aarp.org/money/scams-fraud/ Check out AARP's campaign on fraud awareness: http://www.aarp.org/money/scams-fraud/fraud-watch-network/
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.	http://www.fbi.gov/?came_from=http%3a//www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment
ElderCare.gov connects you to community services for older adults, including legal and financial assistance services.	http://www.eldercare.gov/Eldercare.NET/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://origin.www.fhfaoig.gov/LearnMore/TipsConsumers
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
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	http://www.ic3.gov/crimeschemes.aspx

Name	Website
Federal Trade Commission provides information on identity theft.	http://www.consumer.ftc.gov/features/feature-0014-identity-theft
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 protecting yourself and your family.	https://www.staysafeonline.org/stay-safe-online/resources/
Wall Street Journal Guide on Identity Theft & Credit Card Fraud provides information on how to protect yourself from identity theft and credit card fraud.	http://guides.wsj.com/personal-finance/credit/how-to-protect-yourself-from-identity-theft/
Medicare.gov provides information on what to do to safeguard your personal information in medical settings.	http://www.medicare.gov/forms-help-and-resources/identity-theft/identity-theft.html

References

[1] Smith, Aaron. “Older Adults and Technology use.” *Pew Internet Center*, 3 Apr. 2014. Web. 4 Jan. 2016. http://www.pewinternet.org/files/2014/04/PIP_Seniors-and-Tech-Use_040314.pdf

[2] Bonnie, Richard J. and Wallace, Robert B. “Elder mistreatment: Abuse, neglect and exploitation in an aging America.” *The National Academies Press*, 2003. Web. 4 Jan. 2016. http://www.nap.edu/read/10406/chapter/1

[3] Bick, Jonathan. “Internet Crime and the Elderly: Enhanced penalties could prevent online targeting of senior citizens.” *New Jersey Law Journal*, 1 Aug 2011. Web. 4 Jan. 2016. http://www.bicklaw.com/publications/e-elderlaw.htm

[4] MetLife Mature Market Institute. “MetLife Study of Elder Financial Abuse: Crimes of occasion, desperation, and predation against America’s Elders.” N*ational Committee for the Prevention of Elder Abuse*, 2011. Web. 4 Jan. 2016. https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf

[5] 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

[6] The Federal Bureau of Investigation. “Fraud Target: Senior Citizens.” *Scams & Safety*, 2010. Web. 4 Jan. 2016. https://www.fbi.gov/scams-safety/fraud/seniors

[7] 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

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

[9] Federal Trade Commission. "Health Care Scams." *Stop Think Connect Resource Guide*, 2014. Web. 16 Dec. 2015. http://www.stcguide.com/resource-index/

[10] Federal Trade Commission. "Health Care Scams." *Pass It On*, 2014. Web. 4 Jan. 2016. http://www.consumer.ftc.gov/articles/pdf-0183-health-care-scams.pdf

[11] The Federal Bureau of Investigation. "Looking for Love? Beware of Online Dating Scams.” San Diego Division, 14 February 12, 2014. Web. October 22, 2015. https://www.fbi.gov/sandiego/press-releases/2013/looking-for-love-beware-of-online-dating-scams

[12] Kirchheimer, Sid. "Is Your Computer Infected." *AARP*, 9 Jan. 2012. Web. 16 Dec. 2015.

FPCIW would like to acknowledge the support of organizations of this project including AARP, the Elder Abuse Alliance, The San Diego Futures Foundation, OASIS and Serving Seniors. We would also like to recognize the contributions of Saemy Son, a student volunteer who supported the development of this toolkit.

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. The gift benefits the Front Porch Center for Innovation and Wellbeing's (CIW'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 allows the CIW to confront the issue of elder security by using adaptive technologies to develop initiatives related to senior online security, specifically in the Greater San Diego Area, but accessible also to communities far and wide across the Internet.

Ellie Piers

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 mindfully 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' intent to help others, the CIW is focusing on addressing 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, specifically in the Greater San Diego Area.
- 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, 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.