Tech Safety + Older Adults

ncall

Tech Safety + Older Adults

October 2020

Funded by:
U.S. Department of Justice, Office on Violence Against Women (OVW)

This toolkit was produced by the National Clearinghouse on Abuse in Later Life under award #2016-TA-AX-K077, awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this toolkit are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The Office on Violence Against Women Abuse in Later Life Program

The U.S. Department of Justice, Office on Violence Against Women (OVW) is committed to raising awareness and supporting training and services to address incidents of domestic violence, dating violence, sexual assault, and stalking. Through the Enhanced Training and Services to End Abuse in Later in Life Program, OVW provides grantees with an opportunity to work collaboratively with their project partners to improve the response to older victims and hold offenders accountable through professional training, victim services, and a coordinated community response. For more information about the OVW Abuse in Later Life Program, visit www.justice.gov/ovw/grant-programs.

National Clearinghouse on Abuse in Later Life (NCALL), an initiative of the End Domestic Abuse Wisconsin

The National Clearinghouse on Abuse in Later Life (NCALL) is an initiative of End Domestic Abuse Wisconsin. NCALL's mission is to engage communities to foster a collaborative, inclusive, survivor-centered response to abuse in later life. Our vision is that one day society respects older adults, and communities work collaboratively to ensure their dignity and safety.

And we strive to operate from this set of values:

- Survivor-Informed
    - We respect the autonomy of older survivors.
    - We center the voices of older survivors in our work.
- Equitable & Just
    - We recognize the differential impact of institutional oppressions on older survivors from marginalized communities.
    - We promote responses that meaningfully include all older survivors in creating more just and equitable systems.
- Collaborative
    - We believe collaboration can be an effective response to the complexities of abuse in later life cases.
    - We advocate for individuals, organizations, communities, and systems to work together to address abuse in later life.

National Clearinghouse on Abuse in Later Life,
an End Domestic Abuse Wisconsin initiative
1400 E. Washington Ave., Suite 227
Madison, Wisconsin 53703
Phone: (608) 255-0539 | TTY: (608) 255-3560
www.ncall.us | www.endabusewi.org

Table of Contents

Introduction

Project History

In 2014, the National Clearinghouse on Abuse in Later Life (NCALL), with contributions from Disability Rights Wisconsin and the Safety Net Project of the National Network to End Domestic Violence, released a series of handouts aimed at helping older adults identify ways to safeguard themselves from those who misuse technology to control, harass, stalk, and/or threaten them. In 2020, NCALL updated and expanded those resources to create this toolkit.

How to Use this Toolkit

At the conclusion of this toolkit the reader will find the section, Frequently Used Tech Terms, which offers a broad overview of commonly used technology terms and concepts, including many of the key terms used throughout this resource. The first time a term is used in the toolkit, it is ***bolded and italicized*** and linked to its definition. If the reader is using this toolkit online, they can access the definition of any term or concept by clicking on the term to view it in the Frequently Used Tech Terms section. The reader can return to where they left off in the resource by clicking the specific ***Return*** link at the end of the term's definition. If the reader is using a printed copy of this toolkit, they can turn to the end of the toolkit.

Technology and Abuse in Later Life

The Dynamics of Abuse in Later Life

Abuse in later life is the willful abuse, neglect, or financial exploitation of an older adult that is perpetrated by someone in an ongoing relationship of trust with the victim. Abusers may be, for example, a spouse, partner, family member, or caregiver. The term applies to victims who are age 50 and older.

As is true with interpersonal violence involving younger victims, power and control dynamics are often present in abuse in later life cases. It is common to find that perpetrators use many of the same abuser tactics found in domestic violence and sexual assault cases involving younger victims, like intimidation and stalking, to prevent older victims from seeking help or reporting their abuse. It should also be recognized that there are a number of unique tactics of abuse used against older victims. Perpetrators of abuse in later life are often found to target vulnerabilities, neglect, isolate, and psychologically or emotionally abuse their victims.

Persons depicted in this resource are models and used for illustrative purposes only.

Technology and Abuse in Later Life

Technology is an invaluable resource to aid older survivors in finding safety, stay connected to friends and family like never before, and find support and resources around abuse in later life. In this increasingly digital age, however, technology can be misused, and pose serious risks to safety for survivors. Technologies that abusers misuse include, but are not limited to: phones, ***emails***, ***text messaging***, ***instant messaging***, computers, ***apps***, ***spyware/stalkerware*** or other computer monitoring tools, ***TTY/TDD*** (text telephones), relay services and other ***assistive technology***, ***GPS*** and other location tracking services, cameras, and a variety of other surveillance devices.

The following pages provide an overview of ways abusers might misuse technologies to cause harm to their victims. In addition to the tactics listed, many offenders justify or minimize the abuse and deny that these behaviors are abusive. Perpetrators may normalize the control and abuse by making comments like “this is for their own safety” or “they’re just too old to understand.”

Tactics of Abuse

Coercion and Threats

- Makes threats via email, instant and text messages, and ***social media***.
- Forces victim to participate in illegal ***online*** activities.
- Posts ***non-consensual intimate images*** of victim online.

- Abuses victim for not responding to emails, calls, or texts quickly enough.
- Threatens to out them online to family and friends.
- Threatens to take the tech away.

Emotional and Psychological Abuse

- Impersonates victim online. For example: creating a social media account using the victim's name without their consent.
- Ridicules or puts down victim using technology.
- Manipulates technology to confuse or scare victim. For example: changing settings, making a computer talk/make sounds, etc.
- Sends the victim (***sexts***) intimate or sexually explicit photos or videos without their consent.
- Sends victim disturbing or offensive information or ***website*** links.

Financial Exploitation

- Tracks or manipulates victim's financial accounts online.
- Denies victim's access to online accounts.
- Uses technology to defraud victim of assets, titles, or properties.
- Forces victim to make unwanted online purchases.

Intimidating, Monitoring, and Stalking

- Monitors victim's activities, online or ***offline,*** using technology. For example: using spyware/stalkerware to track computer activity or hiding a cell phone in the victim's car to listen to them and/or to track their location via GPS.
- Secretly changes victim's files or ***device*** settings.
- Constantly contacts victim using technology. For example: calling or texting repeatedly or sending unwanted messages.
- Uses Internet connected devices such as Alexa and Google Home to scare, monitor, and harass.
- Has emails/messages forwarded to their devices.
- Changes passwords to accounts.

Isolation

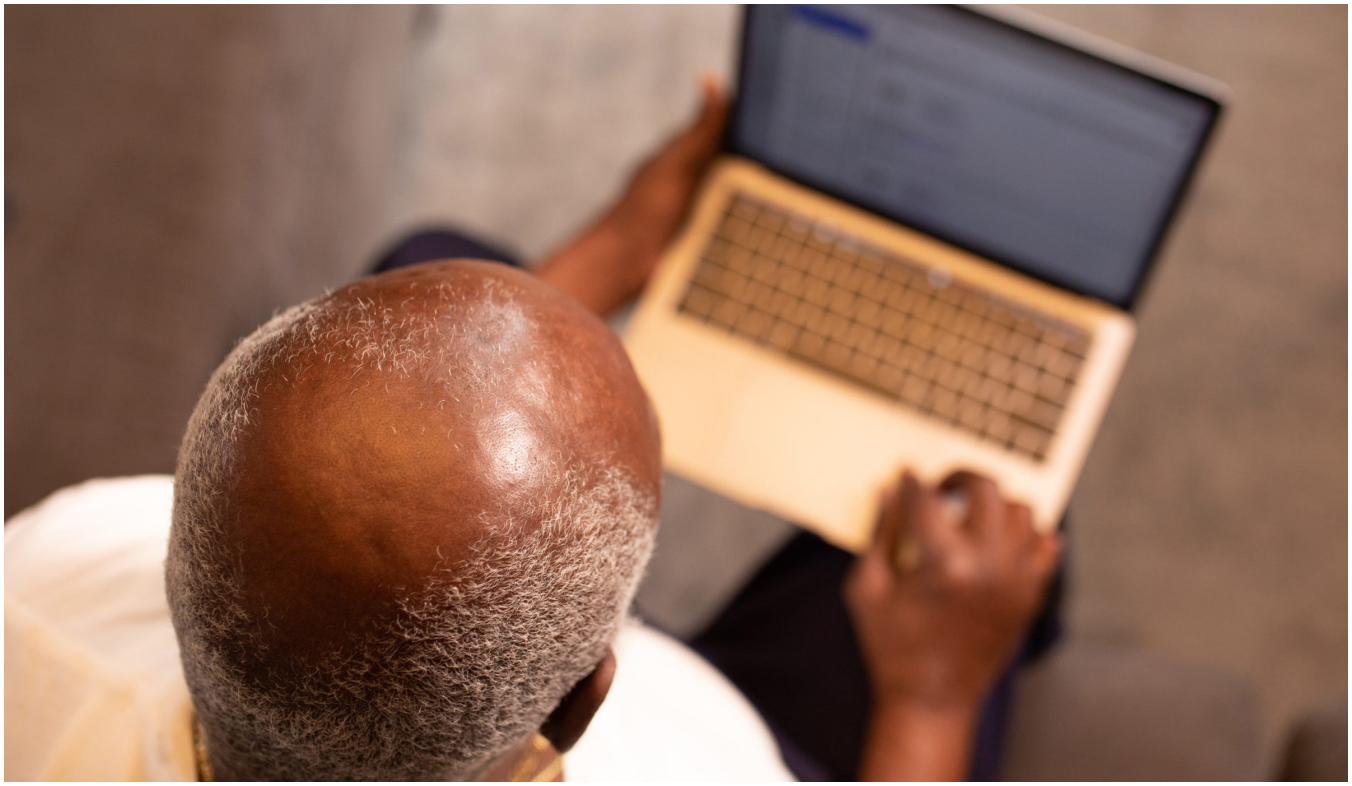
- Cuts off or limits victim's technology use and access.
- Controls what the victim does and who they may contact online.
- Uses technology to discredit victim.

Targeting Vulnerabilities and Neglecting

- Compromises safety and independence of victim by withholding, removing, or damaging technology or assistive devices. For example: altering an electronic device's settings so that it doesn't function properly.
- Uses "safety" of victim as an excuse for controlling or limiting access to technology.

Using Family and Trusted Others

- Misleads others (children, grandchildren, friends, caregivers) about victim's wellbeing. For example: sending emails from the victim's account to suggest that everything is fine or intercepting the victim's email to keep them from telling friends or family about the abuse or from seeking help.
- Misleads victim to distrust others. For example: telling the victim that a caregiver is making electronic withdrawals from their financial account.



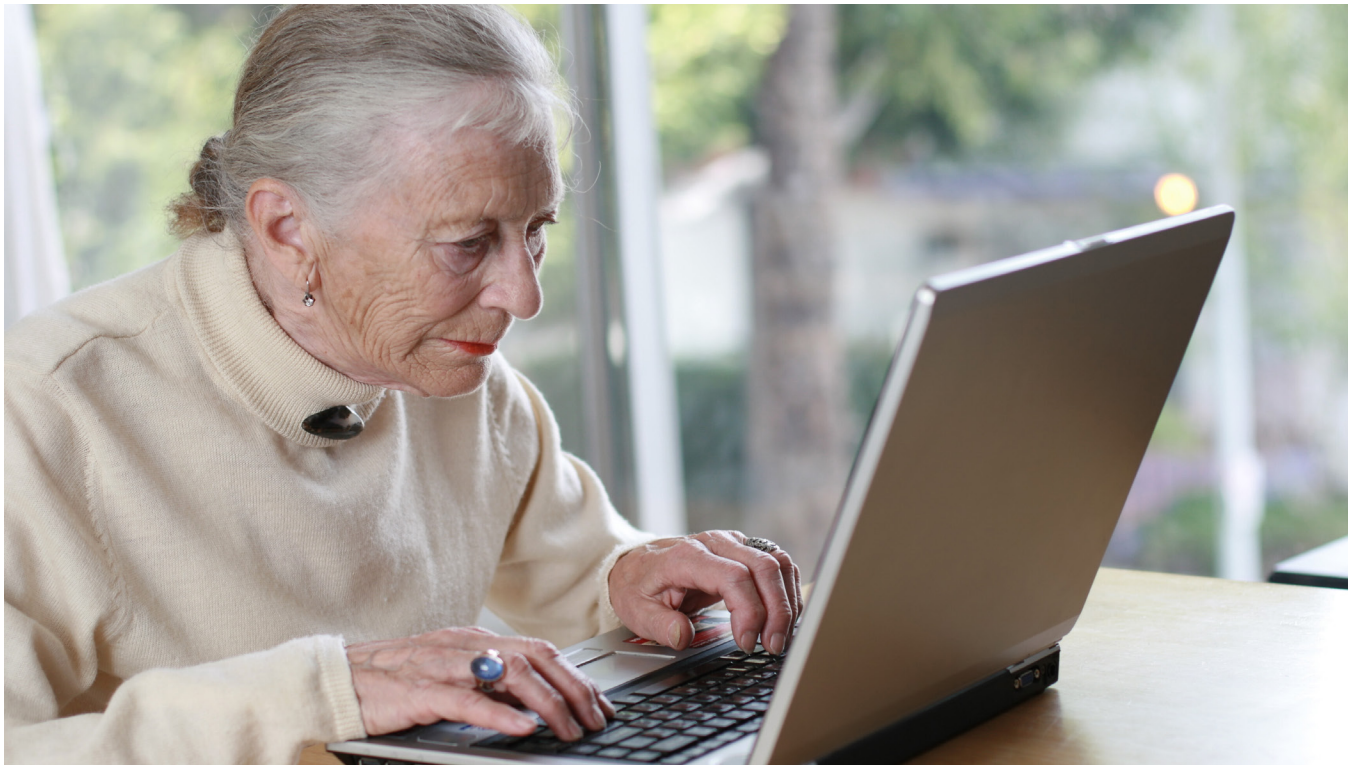
- Discredits victim through electronic communication with family.
- Manipulates victim's family and trusted others to monitor online activities or get information such as account numbers or passwords. For example: convincing others that the victim is unfit to care for themselves and therefore needs online supervision.

Diminishing Self-Efficacy and Autonomy

- Makes all of the decisions about technology.
- Takes advantage of victim's lack of knowledge of technology.
- Makes victim feel stupid and incapable of understanding technology.
- Uses age of victim as an excuse for controlling or limiting access to technology.
- Withholds access to victim's online healthcare and telemedicine information.

To learn more about the dynamics of abuse in later life, visit: https://www.ncall.us/abuse-in-later-life/.

If you feel you are being harmed or that someone is taking advantage of you, support is available. To talk to someone confidentially, call or visit the National Domestic Violence Hotline at 1-800-799-7233 or TTY 1-800-787-3224.



Tech Tips for Older Adults: Tech Safety

Technology can help maintain or enhance one's quality of life. Email and ***social networking sites***, for example, provide a way for people to stay connected, while websites and ***forums*** offer convenient access to a wide array of information, products, support, and services. There also are a number of technologies aimed at increasing personal independence and safety such as ***smartphones***, ***smartwatches***, assistive technology, home security systems, and medical alerts. Unfortunately, technology is also misused by some people to harm others. This section provides a general overview of computer, cell phone, and ***Internet*** safety. For information about online privacy considerations and specific technology safety planning strategies, please visit the National Network to End Domestic Violence Technology Safety page.

Spying on You

Does it seem like someone knows too much about your activity or your whereabouts? That person could be monitoring your computer or device, (e.g., cell phone, ***tablet***) accessing your online accounts, and even gathering information about you, both online and offline.

Physical access to your computer is not needed for someone to install spyware/ stalkerware. Spyware/ stalkerware can be sent via email as an image, *attachment*, or link, and can be installed without your knowledge when opened. For smaller devices like a cell phone or tablet a person typically needs physical access to install spyware/stalkerware.

If someone knows what you are doing online or has access to your online accounts, it is possible that they have hacked into your computer or device, learned the passwords to your accounts, or installed spyware to your computer or device. Once spyware/stalkerware is on your computer or device, another person is able to see all activities on the

device, including messages sent and received (email, ***IM***, chat), documents accessed, websites visited, web searches, and programs downloaded, etc. Some programs may even allow the person to turn on the computer's camera or microphone to eavesdrop or actually control the device itself.

But there are other ways that someone can monitor you. For example, your whereabouts can be tracked if you check-in on Facebook, a friend or family member tags you in a photo, or through a smartwatch or ***OnStar***. These can all give someone more information than what you wanted to share. It is important to be mindful about all of the ways your information and location can be shared and can be used to spy on you.

Safety Strategies

Knowing about the features and functions of common technologies can go a long way in keeping you and your computer or device safe. The safety tips outlined below offer some practical ways to use your computer, cell phone, and the Internet more safely.

SAFETY TIP: Before installing apps on your computer, device, or cell phone, take a moment to read user reviews, terms of service, and learn how the apps may use your personal information.

Computer/Device

- Install and enable a ***firewall*** to prevent unauthorized access of your computer or device.
- Install ***anti-spyware*** and ***anti-virus*** software and set your computer or device to update automatically. Run this before you click on your internet browser.
- If you suspect there is spyware/stalkerware on your computer or device, try using a safer computer, such as one at a public library or community center, to look up and browse for things you do not want monitored. Switching all your computer or device activity could alert the person monitoring you that things have changed and may increase the violence. It is important to make sure to sign out of any website you logged into before walking away from a public computer.
- To learn more about spyware/stalkerware, please see the Spyware/Stalkerware Handouts from the Safety Net Project at NNEDV.

Cell Phone/Smartphone

- Lock your phone with a unique passcode.
- Install and run anti-spyware/stalkerware and anti-virus software if your phone has that capability.
- Check your phone's settings to ensure that other devices are not connected to the phone.
- Review the location and privacy settings of both your phone and its apps' permissions to be sure you know what information is being shared about you.
- Turn off the ***Bluetooth*** when it is not in use. When you leave Bluetooth on, your phone is constantly open to other devices to connect to it, leaving it vulnerable to hackers. Hackers can take control of a phone via Bluetooth and even steal data from it.
- Turn off or limit the location feature on the apps you use. Check regularly to ensure that your preferences don't change during ***software*** updates.
- Global Position Systems (GPS), a technology feature on most cell phones, can precisely pinpoint a person's location at all times. Turn off the GPS and limit it to ***E911*** emergency services only.
- Consider logging out of certain accounts if you are able so that others can't access them if they are using your phone. Keep in mind that depending on the type of phone you have, you might not be able to log out of some

accounts, such as email accounts, but may instead need to remove the entire account from your phone. In this case, make your decision based on your own privacy and safety risk. While it may be inconvenient to access the account through the browser instead of the app, it may be safer.

- To learn more about cellphone privacy tips visit the 12 Cell Phone Safety and Privacy Tips handout from the Safety Net Project at NNEDV.

HTTP:// vs. HTTPS://

http:// = your data can be shared

https:// = your data can not be shared

SAFETY TIP: Download the HTTPS Everywhere extension to make your browsing more secure. https://www.eff.org/.

Internet

- Update your ***web browser***. An out-of-date browser can leave your computer vulnerable to ***malware***.
- Don't give out personal information simply because a website requests it. Consider why the site may need your full name, address, phone number, and/or date of birth.
- Be aware that free wireless networks are not secure. Avoid making any online financial transactions, logging into personal accounts or doing anything sensitive in nature online until you are certain you are on a secure network.
- Browse securely. Websites that use the standard ***HTTP*** protocol transmit and receive data in an unsecured manner. With ***HTTPS***, data is encrypted so that it cannot be read by anyone except the recipient. If you see HTTPS in the ***URL*** address bar, you are on a secure webpage and your browsing and data will be secure.
- Anytime you have to enter personal or financial information on a website, make sure the web address starts with https://.
- Browse privately. Some web browsers offer a ***privacy mode***, which, when enabled, prevents a user's web search history from being stored and later accessed by another. It is important to remember that when you're finished browsing, you must close the browser to erase your history.

Email addresses and Usernames

- Don't use identifying information in your email addresses and usernames. Including your name, birthdate or location will make it that much easier for someone to obtain details about you and your whereabouts.

Passwords

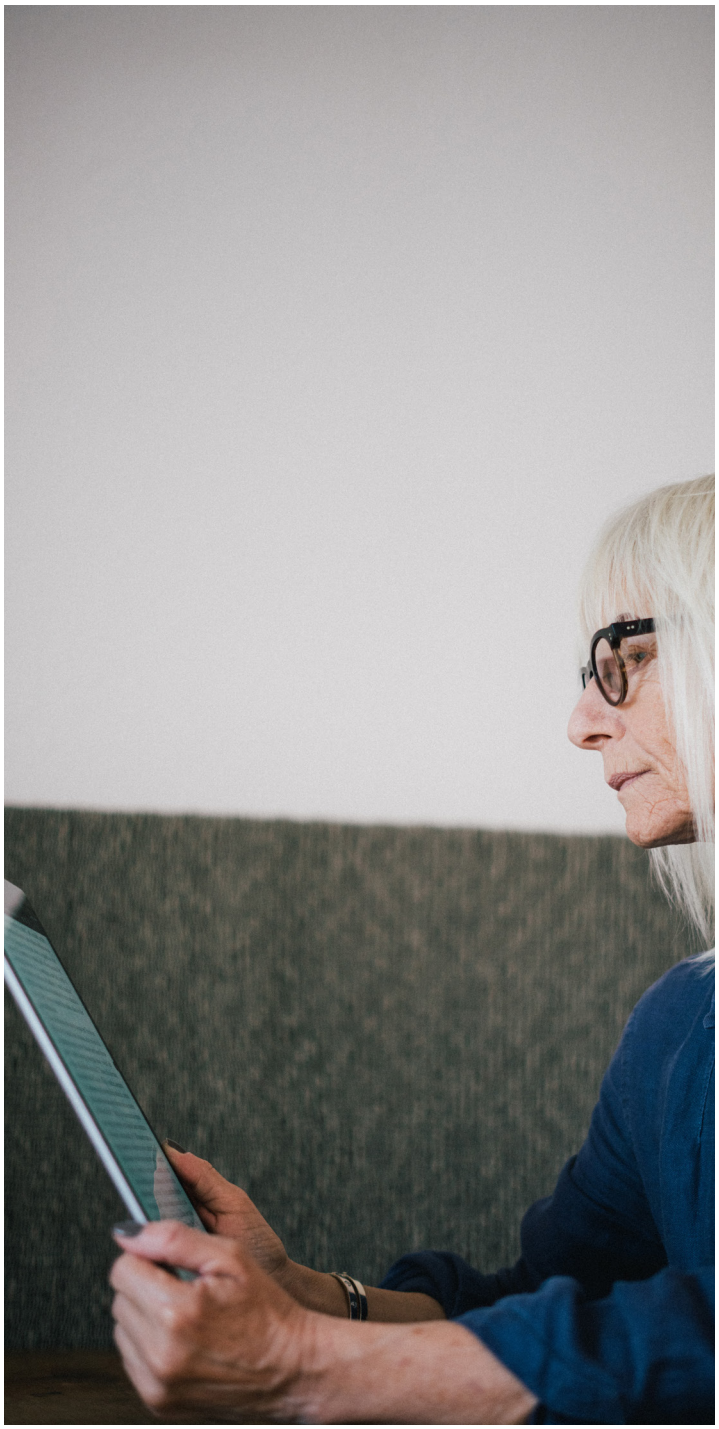
- Change all vendor default passwords.
- Use a strong password for all of your accounts. Strong passwords are at least 8 characters long, (12 or 15 characters is even better!) contain a combination of upper- and lower-case letters, numbers, and symbols.
- Don't create passwords that contain your user name, real name, family member's name, pet's name, or complete words.
- Don't use the same password for every account. Come up with a system that's easy to remember but will enable you to have a different password for each account.

SAFETY TIP: Test the strength of your password by visiting: www.howsecureismypassword.net.

- Don't share your password. There's no valid reason for a third party to contact you for your password. Even within our personal relationships, we deserve privacy, respect, and trust. No one should demand your password or access to any of your accounts.
- Don't reuse any of your previous passwords, even if you haven't used them in years.
- When using a public computer to access your online accounts, don't save passwords or use "keep me signed in" or "remember me" options. Doing so may enable the next person that uses the computer to access your accounts.
- If you suspect that someone has the password to any of your accounts, use a safer computer or device and change your password. Be sure that the new password is unique and not a variation of your old password.
- When in doubt use a password manager to help you maintain your passwords and keep them secure. To learn more about password managers, check out this article on CNET.

Tech Tips for Older Adults: Online Privacy & Safety

Internet privacy and safety is a concern for many people. A good general rule is that nothing online is private. For example, when you post a photo on Facebook to share with your family and friends, the photo may be seen by countless other people even if that is not your intent. Once information is online, others can share it, talk about it, and even change it with or without your knowledge.



Another important point is that it is becoming increasingly improbable to remain completely anonymous online. Personal information from photos, emails and social media posts, behavioral data generated from web searches, and the use of apps all feed our individual ***digital footprints***. However, there are steps you can take to prevent sensitive and personal information from making its rounds on the Internet.

This section will provide an overview of the importance of online privacy and offer some strategies

for maintaining your privacy and safety online. For additional information, please refer to the National Network to End Domestic Violence Technology Safety page.

Why Does It Matter?

Information posted by us or others may seem harmless or non-identifying by itself. However, in combination, it's both amazing and scary what we can learn about someone just with the available information online. Perhaps, for example, you've chosen to list your current city on your Facebook account, but did not include that identifying information in the profiles of your other social media accounts. Now suppose that you've shared your day's plans on Twitter or posted your beach vacation photos on Instagram. If you use the same profile photo for these different social media accounts, a simple photo search–even if those

accounts use entirely different profile and username information–can link all those accounts to one individual. This linked information quickly decreases your online anonymity and increases your vulnerability to anyone who wishes to do you harm.

Social media presents new challenges. Snapchat, for example, is set up automatically to show your location on a map to all of your contacts that use the app. This must be turned off from within the app.

If you have ever volunteered for a community organization, had your work included in an art show, or been on a community team, then your name and personal details, such as affiliated groups and location, might be posted online.

What Are You Sharing Online?

When we post information online, we share our lives with family and friends. However, depending on where we are sharing that information and what privacy settings are being used, this information could be accessible to more people than we intend. Information we share offline may also end up online.

Web Activity

When you surf the web, your browsing activity may be recorded. A ***cookie*** keeps track of where and what you've visited online. This information can help improve your web experience (e.g., remembering your location for weather reports), but the data, when combined, can also create a revealing profile of your online activities. **SAFETY TIP:** Review your web browser settings. Browsers offer various ways to limit or delete cookies. Choose the browser and settings that best meet your privacy preferences. This is especially important if you are concerned about someone seeing your specific online activity or if you are using a public computer.

Online Accounts

Have you created social media accounts or signed up for online sites, such as email accounts, ***blogs***, instant messaging services, or ***photosharing sites***? When signing up, you may be asked for personally identifying information, like your name, age, gender, and city or town. The companies that collect this information may sell or share it so that it can become publicly available elsewhere. **SAFETY TIP:** Choose carefully what information you give out and

use other information that you will remember but isn't necessarily identifying to you (e.g., just your first name or a fake name). In addition, check your account privacy settings to ensure that you know what pieces of your profile information is publicly available and what you can control.

Permissions

When you download an app, you may be prompted to give it permission to access certain information on your cell phone or device such as your contacts, the device's location, or even details about how you use the app. This data may or may not be necessary for the app to function. **SAFETY TIP:** Read the permissions. Before you install an app, learn what information you'll be asked to share and consider whether the permissions make sense for the app.

Privacy Settings

Have you looked through all the privacy and security settings in the sites and apps you use and limited who can see your profile information? If your accounts are set to be available to the public, anyone who visits that site, including employers, neighbors, friends-of-friends, or strangers can see your personal information. **SAFETY TIP:** Review your privacy settings. Limit what others see, whether it's your status updates, photos, or profile information. Don't forget that it's more than just social networks that have privacy settings. Most online accounts, such as Amazon, Pinterest, Spotify, and Pandora, allow you to limit who can see your profile information.

Other Ways Your Information Gets on the Web

- When stores ask for your phone number, email address, or zip code when you buy something, that information is put into a database. The store might later sell your information to a data broker who posts it or sells it online. This personal information then shows up in an online people search. **SAFETY TIP:** Be aware of what you share. Find out how the store intends to use your information and know you can decline to offer your personal information.

If you have a driver's license and got a ticket, your name, address, and other personal information could be available online on a court or county website.

- Information about you can end up online when friends, community members, or relatives post information or photos that include you. Be aware of what others share. Ask others not to share photos of you or tag you in their posts.
- Even if you are cautious about not posting identifying information about yourself, a photo that shows a sign or landmark within your community could reveal your location. Photos taken on your smartphone also may unknowingly share your location with your exact GPS coordinates.

SAFETY TIP: Turn off the *geotagging* settings on your smartphone camera, photosharing, and social media apps (e.g., TikTok, Instagram, Facebook).

Archives

With the Internet and ***search engines***, everything online is indexed and searchable. Even sites where you think only members can see the content could be public or seen by others who aren't members, anywhere in the world. When websites are archived or ***cached***, people can access old content even if the site disappears or changes. This means that any information posted could be online for a long time–potentially forever.

How Can You Find What's on the Web About You?

- If you can find it, someone else can too. Search online for your personal information and photos. Some places to start: Google, Yahoo!, Classmates.com, YouTube, and Flickr.
- Look on sites for groups and places where you might have a connection: organizations where you worked or volunteered, clubs, faith community, etc.

What Can You Do To Remove Your Information?

Some sites will remove information at your request, but if the site is archived, your info may not really be gone. If your information is posted online, act quickly to have it removed. For a fee, some online privacy companies will remove your information from online search engines. Some of them will contact companies that are sharing personal information and opt-out on your behalf. (You can do this yourself.) Some companies will monitor the sites to ensure that your data doesn't come back. Other companies will simply bury your data by introducing false data to obscure your correct information. More at: National Network to End Domestic Violence Technology Safety resource, People Searches & Data Brokers.

Assistive Technology

What is Assistive Technology?

Assistive Technology (AT) is any device, equipment, item, product, or service used to increase, maintain, or improve accessibility. AT may include mobility devices such as walkers and wheelchairs or computer software, apps, and equipment to facilitate communication and enhance a person's daily living. Any popular technology (e.g., cell phone, text messaging, email, Internet chat, and Instant Messaging) also can be considered AT if it increases access and decreases or removes systemic barriers. AT also may be referred to as adaptive devices; however, adaptive devices really are a subset of AT.

Who Uses Assistive Technology?

AT can be any technology, item, or service that is used to increase safety and accessibility for people who:

- Are Deaf or hard-of-hearing
- Are blind or have low vision
- Have physical/motor disabilities
- Have cognitive/intellectual and developmental disabilities
- Have mental health concerns or psychiatric disabilities
- Have multiple or invisible disabilities.

AT also has been found to be useful for individuals without disabilities due to its focus on making access universal (e.g., a person pushing a baby stroller up a ramp versus navigating steps to enter a building).

Examples of Assistive Technology

Assistive Technologies for Individuals Who Are Deaf or Are Hard-of-Hearing

- Flashing lights for doorbells, ringing phones, fire alarms (e.g., when a doorbell rings, a strobe light flashes above the door).
- Personal Assistive Listening Devices (e.g., hearing aids or other amplifications devices)
- Amplified telephones
- Video Phones (specific phone equipment that allows users to communicate visually by seeing each other communicate, which is especially useful for Deaf individuals who communicate through American Sign Language, a visual, not verbally-based language).

- TTY/TDD (Text Telephone) – allows people to type messages back and forth to one another instead of talking and listening. TTYs are becoming obsolete with the rapid advancement of other technologies. TTY is now available in most social media apps.
- Telecommunications Relay Service (TRS) – telephone service that allows persons with hearing or speech disabilities to place and receive telephone calls. TRS uses operators to facilitate telephone calls between people with hearing and speech disabilities and other individuals.
- TTY Relay – operator voices what person types on TTY and types what the person voices on phone.
- Internet Protocol (IP) Relay Service – text-based form of TRS that is accessed using a computer and the Internet rather than a TTY and a telephone.
- Video Relay Services (VRS) – a form of Telecommunications Relay Service (TRS) that enables persons with hearing disabilities who use American Sign Language (ASL) to communicate with voice telephone users through video equipment rather than through typed text.
- Video Remote Interpreting (VRI) – combines video conferencing technology with a live remote (off-site) sign language interpreter to allow two individuals in the same room to communicate. (e.g., use a Video Phone, Skype, Zoom, etc.).
- Voice Carry-Over (VCO) Devices – enable Deaf and hard of hearing individuals to use their speech on the telephone. The VCO user speaks directly to the other person, and when the person speaks back, the relay operator types a text response that is displayed on a TTY or VCO device.
- Captioned Telephone Service – the telephone converts spoken words into text for the user to read. Users can speak and then simultaneously listen and read what the other person says.
- IP Captioned Telephone Service – combines two other forms of TRS, Captioned Telephone Service and IP Relay, allowing consumers to use a computer or similar device, rather than a specialized captioned telephone, to make captioned telephone calls.
- Service animals – known also as “hearing” animals that alert a person when a sound occurs.

Assistive Technologies for Individuals Who Have Speech Disabilities

- Hearing Carry Over (HCO) Devices – a type of TRS that allows a person with a speech disability, but who wants to use their own hearing, to listen to the called party and type their part of the conversation on a TTY.
- Speech-to-Speech (STS) Relay Service – enables persons with a speech disability to make telephone calls using their own voice (or an assistive voice device). Communications Assistants (CAs) relay the conversation back and forth between the person with the speech disability and the other party to the call.
- Speech Synthesizers – individuals type/paste words in and computer "speaks" what you want is typed.
- Computer, tablet, and smartphone apps and software that speak words or phrases aloud to assist with communication needs.

Assistive Technologies for Individuals Who Are Blind or Have Low Vision

- Large print
- Full page magnifier
- Screen magnifiers/software
- Screen readers – converts files into audio (MP3 or WAV files), converts into Braille, or prints to Braille printer/embosser.
- Scanners – scans documents and converts printed words to electronic text file or Braille, reads aloud, or converts to large print on computer.
- Braille PDAs and Note takers – Braille keyboard for inputting information and refreshable Braille dots for reading.
- Telebraille or Braillephone Relay – allows users with TeleBraille or Braillephone TTYs to communicate with listener via Relay Operator or directly to another TTY.
- GPS Orientation Devices – plot routes and download maps in speech or Braille.
- Service animals – guide animals that assist people to navigate their environment.
- Computer, tablet, and smartphone apps and software that allows content to be read aloud. This feature is built into Safari and Edge web browsers.

Photo courtesy of The Center for Volunteer Caregiving, Cary, NC
National Aging and Disability Transportation Center

Assistive Technologies for Individuals with Physical, Motor, or Communication Disabilities

- Devices for Daily Living, Communicating, and Working
  - Mobility aids (e.g., walkers, canes)
  - Home modifications (e.g., grab bars, safety rails, Dycem (non-slip material), doorway threshold ramps, adapted seating, wedges for positioning), lever door handles (versus doorknobs that require more fine motor skills), hand-held shower.
  - Daily aids (e.g., zipper pulls, book holders, page turners, pencil grips, switches, reachers/ grabbers, foam adapter handles).
  - Service animals that assist an individual by providing support or performing tasks related to the person's disability.
- Electronic Aids for Daily Living, Communicating, and Working
  - Mobility aids (e.g., scooters, wheelchairs)
  - Augmentative or Alternative Communication: (e.g., voice recognition software, voice synthesizers, voice amplifier, artificial larynx, pocket-sized communicators, communication board software).
  - Environmental Controls (e.g., adaptive switches, hands-free controller for lights, appliances, blinds, phone, fan, etc.).

Where to Find Out More About Assistive Technology

Association of Tech Act Projects (ATAP) strives to collaborate with Assistive Technology programs and persons with disabilities and others at the state and national level to increase the availability and utilization of accessible information technology (IT) and assistive technology devices and services (AT) for all individuals with disabilities in the United States and territories. https://www.ataporg.org/

Eldercare Locator offers information about the benefits of assistive technology for older adults, including how to find out if assistive technology is right for an individual and how to get help paying for it. https://eldercare.acl.gov/Public/Index.aspx

National Council of Independent Living is the national organization made up of hundreds of community-based centers for independent living. These centers, known as CILs, provide services and advocacy by and for people with all types of disabilities, including assistive technology. Many CILs have a "loan closet" for individuals to try out various assistive technology devices that could enhance their safety and accessibility. http://www.ncil.org

Where to Find Out More About Creating Access for People with Disabilities and Deaf People

Vera Institute of Justice, Center on Victimization and Safety provides resources to assist in creating and implementing accessible resources that address the needs of all people, including people with disabilities and Deaf people. https://www.vera.org/centers/victimization-and-safety

Assistive Technology and Abuse in Later Life

Along with the many benefits of assistive technology come the great number of risks to older adults when those technologies are deliberately misused by an abuser. This section provides a general overview of the ways abusers might misuse assistive technologies to cause harm to their victims.

Monitoring or Intercepting Communications

- Accessing entire, verbatim conversations by printing or retrieving the history from a device's memory.
- Monitoring all computer/tablet/device activity through spyware or other monitoring software.

Misusing Communication Devices to Impersonate the Victim

- Impersonating the victim and misleading those close to the victim. For example: contacting an agency through a TTY or a relay system, pretending to be the victim, and requesting a protection order or other charges be dropped.

Misusing Communication Devices to Harass the Victim

- Threatening or taunting the victim through technology. For example: calling or texting repeatedly or sending unwanted messages.

Breaking or Tampering with Assistive Technology Devices

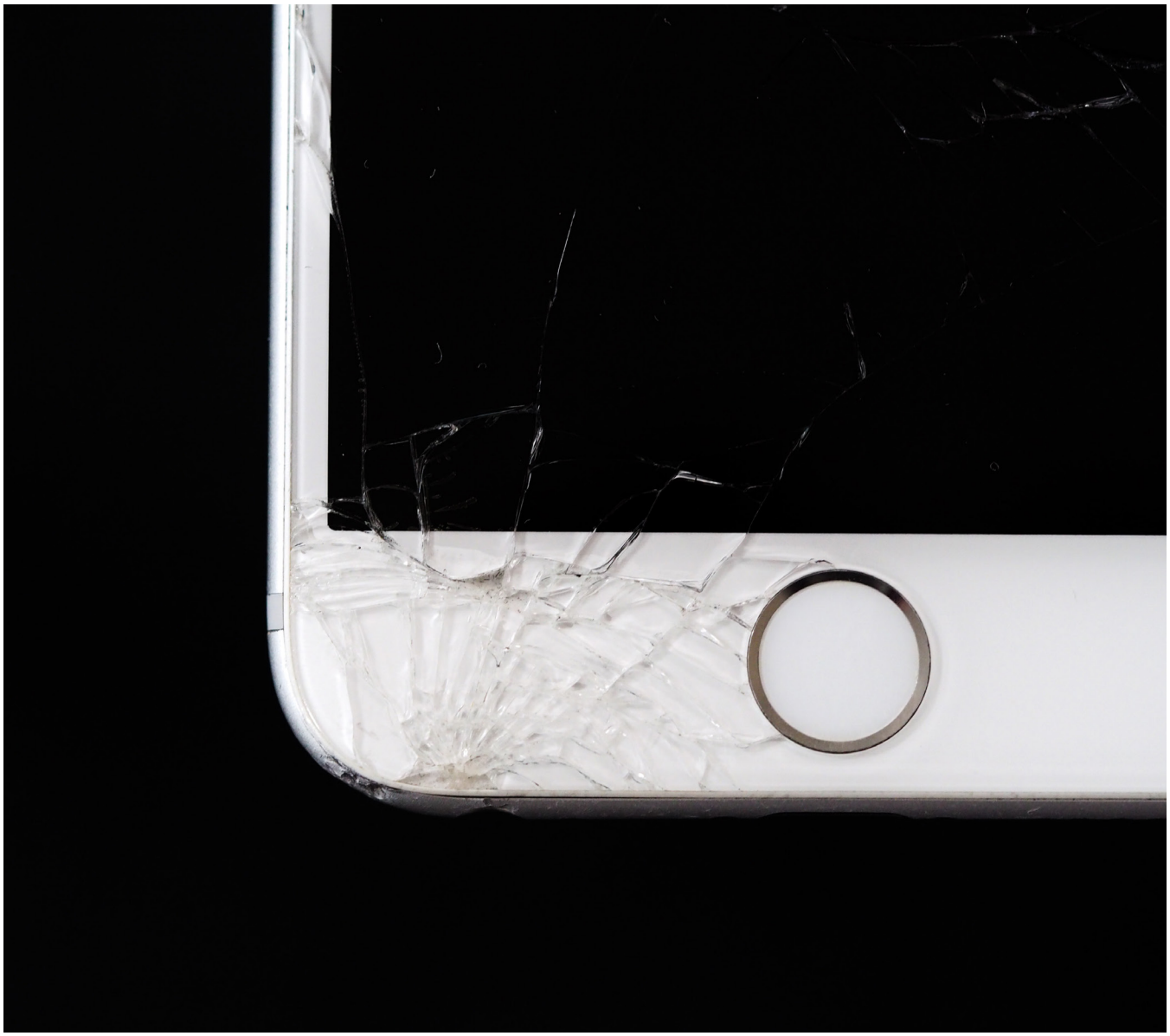
- Disabling or breaking the assistive technology to control the victim. For example: altering an electronic device's settings so that it doesn't function properly or destroying a wheelchair to limit the victim's mobility.

Denying Access to Assistive Technology Devices

- Isolating the victim by limiting, withholding, or removing assistive devices so that they are not accessible.

Injuring the Victim to Prevent Use of the Assistive Technology Device

- Physically harming the victim so that they can't use the technology. For example: purposely breaking the victim's fingers so that they cannot use a touchscreen.



Tech Scams

The Federal Bureau of Investigation (FBI) has identified more than 30 commonly encountered scams in the United States[1], many of which involve technology. These crimes may often be perpetrated by strangers, but many of the tactics are also used by a trusted person–an intimate partner, family member, or a caregiver–since these individuals have easy access to a victim's personal information.

1 https://www.fbi.gov/scams-and-safety/common-scams-and-crimes

Nearly one in five older adults has been the victim of financial abuse[2]. The FBI reports that every year, millions of older Americans fall victim to some type of financial fraud, including but not limited to romance, lottery, and sweepstakes scams. Technology is commonly used to carry out these schemes. Once successful, scammers are likely to keep a scheme going because of the prospect of significant financial gain.[3]

Vulnerability is often a risk factor for financial exploitation, leaving many who may already be facing financial hardship, who may be experiencing other types of abuse, or who may have medical or cognitive issues at greater risk for falling prey to scams.[4] Research suggests that older adults lose $36.48 billion each year to elder financial abuse.[5] On average, older victims lose $120,300 to scams.[6] However, people living in poverty are exploited at a higher rate than people with more assets.[7]

In addition to experiencing significant financial losses, the physical, emotional, and psychological toll of financial fraud on older victims is equally devasting. A 2015 report on elder financial abuse estimates that nearly 954,000 seniors skipped meals as a result of financial abuse.[8] The report also shared that of the seniors they surveyed who experienced financial fraud, many suffered from depression, anxiety, or loss of independence, and reported the following as a result:

- 1.8% lost their home or other major assets
- 4.2% reduced their nutritional intake for budgetary reasons
- 6.7% skipped medical care[9]

This section highlights some prevalent tech scams that target older adults in the U.S. and offers a number of tips and links to resources to help keep you or your loved one safe.

---

2 http://www.investorprotection.org/downloads/IPT_EIFFE_Medical_Survey_News_Release_03-22-16.pdf
3 https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud
4 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4242880/
5 http://documents.truelinkfinancial.com/True-Link-Report-On-Elder-Financial-Abuse-012815.pdf
6 https://www.aarp.org/content/dam/aarp/ppi/2016-02/banksafe-initiative-aarp-ppi.pdf
7 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4242880/
8 http://documents.truelinkfinancial.com/True-Link-Report-On-Elder-Financial-Abuse-012815.pdf
9 Ibid.

Scams

Computer tech support scams involve a person making telephone calls and claiming to be a computer technician associated with a well-known company. The person may also email a victim or place internet pop-up messages on a victim's computer to warn about non-existent computer problems. The scammers claim to have detected viruses, other malware, or hacking attempts on the victim's computer and pretend to be "tech support" asking the victim to give them remote access to their computer. Eventually, the scammer diagnoses a non-existent problem and asks the victim to pay large sums of money for unnecessary–or even harmful–services to resolve the issue.[10]

SAFETY TIPS:

- If you receive a phone call you didn't expect from someone who says there's a problem with your computer, hang up.
- If you get a pop-up window that warns of a security issue on your computer and tells you to call a phone number to get help, don't call the number.
- Real security warnings and messages will never ask you to call a phone number.
- If you think there may be a problem with your computer, update your computer's security software and run a scan.
- If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone.

The above safety tips are offered by the Federal Trade Commission.

10 https://www.justice.gov/elderjustice/senior-scam-alert

Grandparent scams involve a person calling or emailing an older adult, claiming to be their grandchild, and stating that they have gotten into a bad situation while in a foreign country. The person then asks for emergency funds to be wired immediately to them.

SAFETY TIPS:

- Don't let a caller rush you into making a decision.
- Consult another family member to verify the phone call or email.
- Never wire money based solely on a phone call or email.

For additional information and safety tips, visit the National Center on Elder Abuse's Grandparent Scam handout and AARP's Fraud Resource Center page on Grandparent Scams.

Lottery/Sweepstakes scams involve someone fraudulently identifying themselves as a lawyer, customs official, or lottery representative, and telling victims they have won money, vacations, or luxury items like cars or boats. "Winners" need only pay fees for shipping, insurance, customs duties, or taxes before they can claim their prizes. Victims are scammed into paying hundreds or thousands of dollars and receive nothing in return, and often are revictimized until they have no money left.[11]

SAFETY TIPS:

- If you are offered a prize or investment opportunity that sounds too good to be true, follow your instincts, it is not true.
- Don't believe any offers (lottery, prize claim, inheritance, etc.) that require a fee to be paid up front.
- To win the lottery you must play the lottery. Don't believe that you have won a lottery you never entered.
- It is illegal to play foreign lotteries from the United States.

The above information is offered by the U.S. Embassy in Jamaica.

Malware is a catch-all term for any type of malicious software designed to harm or exploit any programmable device, service, or network. This data can be taken from financial data, healthcare records, personal emails and passwords and more. Some examples of malware attacks can be to trick victims into providing personal data or stealing credit card data. (McAfee, 2020) https://www.mcafee.com/en-us/antivirus/malware.html

11 https://www.justice.gov/elderjustice/senior-scam-alert

Obituary scams consist of people trolling obituary notices looking for recent deaths that leave behind surviving partners. Often the scammer will then call the surviving partner and claim that their deceased partner owes thousands of dollars in unpaid debt, threatening financial ruin, eviction, and public shaming unless the debt is quickly paid. Often, a steeply discounted "settlement offer" is proposed if the debt is paid within a narrow time period. In other cases, the scammer uses personally-identifying information from the obituary to steal the deceased or surviving partner's identity.

SAFETY TIPS:

- Limit personal information in obituaries. Omit birthdate, address, mother's maiden name or any information that could be useful to scammers.
- Provide death certificate copies to the following: IRS, Equifax, Experian, TransUnion, and the department of motor vehicles, as well as banks, brokerages, and credit card and mortgage companies where the deceased held accounts.
- Never make a payment or give any information over the phone. Ask for their name, number, and company name so you can call them back.

The above safety tips are offered by Forbes magazine.

Online dating and romance scams consist of people creating fake profiles to build online relationships, eventually convincing the target to send money in the name of love. Some fraudsters even make wedding plans before disappearing with the money. Romance scams operating from abroad often use U.S.-based money mules to receive victim payments and transmit proceeds to perpetrators. Sometimes, perpetrators of romance scams convince victims to serve as money mules.

SAFETY TIPS:

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.
- Beware if the person attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- Take it slowly. Ask questions and look for inconsistent answers. Check the person's photo using your search engine's "search by image" feature. If the same picture shows up with a different name, that's a red flag.
- Never send money or gifts to a sweetheart you haven't met in person.
- Talk to someone about this new love interest. And pay attention if your friends or family are concerned.
- If you suspect a romance scam, cut off contact right away. Then, report to the scam to the FTC at ftc.gov/complaint. Notify the dating site where you met the scammer, too.

The above safety tips are offered by the Federal Bureau of Investigation and Federal Trade Commission.

Phone scams involve someone claiming to be a police officer, lawyer, IRS, Social Security, etc. over the phone and stating that the victim owes money. Tactics include threatening arrest, deportation, or suspension of a business or driver's license.

SAFETY TIPS:

- Register your phone number on the Federal Trade Commission's National Do Not Call Registry to reduce telemarketing calls. Visit www.donotcall.gov for more information.
- If you received an unwanted call after your number was on the National Registry Do Not Call Registry for 31 days, report it to the FTC.
- Do not provide personal information (e.g., Social Security number, credit card number, bank routing number) over the phone unless you placed the call and know with whom you are speaking.

Identity Fraud and Identify Theft

Identity fraud and **identity theft**, as defined by the U.S. Department of Justice, are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

The Most Common Ways That Identity Theft or Fraud Can Happen to You

In public

- People may engage in "shoulder surfing" – watching you from a nearby location as you enter your telephone calling card number or credit card number. They may also listen in on your conversation if you give your credit card number over the telephone.

At home

- If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, someone may retrieve them and try to activate the cards for their use without your knowledge.
- If your mail is delivered to a place where others have ready access to it, someone may intercept and redirect your mail to another location.
- If you respond to ***spam*** that promises some benefit but requests your identifying data, without realizing that in many cases, the requester has no intention of keeping his promise.

- Perpetrators of domestic violence often have access to personal information if they are an intimate partner, caregiver, or relative. They may use their knowledge of a victim to steal their identity to further control, stalk, intimidate, and harass.

With enough identifying information about an individual, someone can take over that individual's identity to conduct a wide range of crimes. For example:

- False applications for loans and credit cards
- Fraudulent withdrawals from bank accounts
- Fraudulent use of telephone calling cards or online accounts
- Fraudulent tax refunds
- Obtaining other goods or services which would otherwise be denied if they were to use their real name

SAFETY TIPS:

- Read your credit card and bank statements each month.
- Never give your credit card number over the phone, unless you made the call and trust the business or person.
- Report suspicious transactions to your credit card company or bank.
- Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries.
- Shred any documents with personal or financial information on them.

The above safety tips are offered by the FBI.

To learn more about the warning signs of identity fraud/theft, visit the FTC's Warning Signs of Identity Theft webpage.

Frequently Used Tech Terms

- ***App*** – refers to computer software, or a program, most commonly a small, specific one used for mobile devices. The term app originally referred to any mobile or desktop application, but as more app stores have emerged to sell mobile apps to ***smartphone*** and ***tablet*** users, the term has evolved to refer to small programs that can be downloaded and installed all at once. ***Return***.
  Source: Techopedia

- ***Assistive Technology*** – any device, equipment, item, product, or service used to increase, maintain, or improve accessibility. (E.g., hearing aids, walkers, talking ***GPS***, etc. ***Return***.

- ***Attachment*** – a file (e.g., document, photo, video) that may be sent electronically via email or text message. ***Return***.

- ***Anti-spyware/stalkerware Software*** – computer or phone software that is used to prevent, detect, and remove ***spyware/stalkerware.*** ***Return***.

- ***Anti-virus Software*** – computer software that is used to prevent, detect, and remove ***malware***. ***Return***.

- ***Bluetooth*** – wireless technology that allows two devices, like cell phones or computers, to communicate without cords. ***Return***.

- ***Cache*** – stores recently used information so that it can be quickly accessed at a later time. Computers incorporate several different types of caching in order to run more efficiently, thereby improving performance. Common types of caches include browser cache, disk cache, memory cache, and processor cache. ***Return***.
  Source: Tech Terms

- ***Cookie*** – a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a website server, and containing personal information (such as a user identification code, customized preferences, or a record of pages visited) ***Return***.
  Source: Merriam-Webster

- ***Device*** – a piece of electronic equipment such as a ***smartphone***, ***smartwatch***, laptop, ***tablet***, or e-reader, etc. ***Return***.

- ***Digital Footprint*** – a trail of data you create while using the Internet, including website visits, emails, attachments, photos, social media posts, etc. ***Return***.
  Source: Tech Terms

- ***Doxing*** – to publicly identify or publish private information about (someone) especially as a form of punishment or revenge.
  Source: Merriam-Webster

- ***E911*** or ***Enhanced 911*** – a system that allows for the location of a person calling 911 on their cell phone to be accessible by the 911 call center. ***Return***.

- ***Email*** – electronic messages distributed by electronic means from one user's ***device*** to one or more recipients. ***Return***.

- ***Firewall*** – computer hardware or software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users (as of the Internet) ***Return***.
  Source: Merriam-Webster

- ***Geotagging*** – the process of adding geographical information to various media in the form of metadata. The data usually consists of coordinates like latitude and longitude, but may even include bearing, altitude, distance and place names. Geotagging is most commonly used for photographs and can help people get a lot of specific information about where the picture was taken or the exact location of a friend who logged on to a service. ***Return***.
  Source: Techopedia

- ***GPS*** – stands for Global Positioning System and is a space-based satellite navigation system developed by the U.S. military. GPS is capable of providing precise information about the location, speed, and direction of an object. GPS receivers are commonly found in automobiles, smartphones, and smartwatches. ***Return***.
  Source: Tech Terms

- ***Hardware*** – also known as computer hardware, refers to the external physical elements of a computer (e.g., keyboard, monitor, mouse, etc.).

- ***HTTP*** – HyperText Transfer Protocol. Websites that use the standard HTTP protocol transmit and receive data in an unsecured manner. ***Return***.

- ***HTTPS*** – HyperText Transfer Protocol over SSL (Secure Socket Layer). Websites use the HTTPS protocol for security purposes. With HTTPS, data is encrypted so that it cannot be read by anyone except the recipient. Some websites that commonly use HTTPS include those that require logins, e-commerce websites and banks, or other financial institutions. ***Return***.
  Source: Tech Terms

- ***Instant Messaging*** – real-time online chat over the Internet. ***Return***.

- ***Internet*** – an electronic communications system that connects computers and computer networks around the world. ***Return***.
  Source: Merriam-Webster

- ***Internet of Things (IoT)*** – refers to devices connected to each other and to a device or app that can control them. These devices may be connected through the Internet, Bluetooth, or other means. Some examples include thermostats, electronic appliances, alarm clocks, and speaker systems.

- ***Intranet*** – a private network for sharing information, collaboration tools, operational systems, and other computing services within an organization.

- ***Location Services*** – use GPS and Bluetooth (where they're available), along with crowd-sourced Wi-Fi hotspots and cellular towers to determine the approximate location of a device. *Note:* Location services depend on the type of device.

- ***Malware*** – also known as malicious software, refers to any software developed to harm, disrupt, or disable cell phones, computers, devices, etc. ***Return***.

- ***Non-Consensual Intimate Image*** – also known as revenge porn, refers to the sharing or distribution of intimate images or videos without consent to harass, intimidate, isolate, and to cause harm. ***Return***.

- ***Offline*** – not connected to a computer, computer network, or the Internet. ***Return***.

- ***Online*** – connected to a computer, computer network, or the Internet. ***Return***.

- ***OnStar*** – in-automotice technology that provides subscription-based communications, in-vehicle security, emergency services, hands-free calling, turn-by-turn navigation, and remote diagnostics systems. ***Return***.
  Source: Wikipedia

- ***PC*** – stands for personal computer. A typical PC consists of a system unit, monitor, keyboard, and mouse.
  Source: Tech Terms

- ***Phishing*** – scammers use fake email, text messages, or copycat websites to steal your identity or personal information. Their goal is to get credit card and bank account numbers, debit card PINs, and account passwords. The scammer may say your account has been compromised or charged incorrectly.
  Source: USA.GOV Online Safety

- ***Privacy Mode*** – also known as private browsing or incognito mode, is a privacy feature in some web browsers, which when enabled, prevents a browser from storing information from a selected browsing session. ***Return***.

- ***Search Engine*** – computer software used to search data (such as text or a database) for specified information. Some commonly used search engines include: Google, Bing, and Yahoo. ***Return***.
  Source: Merriam-Webster

- ***Search Engine Index*** – data that is collected and stored to improve the speed and performance of web searches. Without an index, a web search could take hours instead of seconds.
- ***Sexting*** – the sharing of intimate messages, photos, or videos via cell phone, computer, or any digital device. ***Return***.
- ***Smartphone*** – a cellular phone that commonly features computer functions such as email and Web browsing, as well as text messaging, a camera, and MP3 player. ***Return***.
- ***Smartwatch*** – a digital watch that, via ***Bluetooth***, extends the capabilities of a user's ***smartphone***. ***Return***.
- ***Smishing*** (SMS text phishing) – scammers text, pretending to be with a company you know to steal your personal information. They may direct you to call a phone number to verify an account or to reactivate a debit or credit card.
  Source: USA.GOV Online Safety
- ***Social Media*** – a term used to describe how the Internet, technology, and social interaction come together to create online communities for people to share information. ***Return***.
- ***Social Media Tool*** – Internet technology and/or website that allows people to interact with one another online, such as:
  - ***Blog*** – where an individual or group of users record opinions, news, resources, information, etc. on a regular basis and share those posts with others who read or subscribe to their blog. ***Return***.
  - ***Chat Room*** – an online, real-time, and interactive ***forum*** that allows people to send messages or chat instantly over the Internet.
  - ***Dating Apps*** – programs that allow people to meet potential romantic partners. Some popular dating apps include: Bumble, eHarmony, and Tinder.

- ***Forum*** – an online discussion site that allows people to read and post messages by and for others. Also known as an Internet Forum or Message Board. ***Return***.
- ***IM*** or ***Instant Messaging*** – a system for sending messages instantly over the Internet from one device to another. ***Return***.
- ***Microblog*** – a form of blogging that allows users to post or blog short messages which can be viewed and reposted by other users. The most popular microblog is Twitter.
- ***Photosharing***/***Videosharing Website*** – allows users to upload, publish, and share digital photographs or video files. Popular sites are: Flickr, Instagram, Periscope, Pinterest, ***Snapchat***, TikTok, Vimeo, and YouTube. ***Return***.
- ***Podcast*** – an audio program, usually consisting of music or talk, that is available in a digital format for automatic download or streaming over the Internet.

- ***Social Networking Site*** – an interactive website with message boards, group spaces, events, and chat spaces, which allow users to connect and share information with "friends" or "connections" and to leave/view comments on a user's page. Some popular social networking sites include: Ello, Facebook, Google+, LinkedIn, and Older is Wiser. ***Return***.
- ***Software*** – also known as computer software, refers to the installed programs that direct the operations of a computer. ***Return***.
- ***Spam*** – unsolicited or unwanted junk email. ***Return***.
- ***Spyware/Stalkerware*** – a computer software program or hardware device that enables an unauthorized person to secretly monitor and gather information about a person and their computer use. Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person's computer over the Internet. ***Return***. Source: Tech Terms

- ***Tablet*** – a portable computer that is primarily operated by touchscreen. ***Return***.

- ***Text Messaging*** – electronic communications that are sent and received via cell phone. ***Return***.

- ***TTY/TDD*** – Text Telephone/Telecommunication Device for the Deaf is a special device that lets people who are Deaf, hard of hearing, or speech-impaired use the telephone to communicate, by allowing them to type messages back and forth to one another instead of talking and listening. A TTY is required at both ends of the conversation in order to communicate. ***Return***.
  Source: AboutTTY.com

- ***URL*** – the web address of a resource, such as a document or website, on the Internet. ***Return***.

- ***Virus*** – a computer program developed to harm computers by deleting data or removing files, then spreading secretly from one computer to another. See also ***malware***.

- ***Vishing*** (voice phishing) – scammers call, pretending to be with a company you know to steal your personal information. They may direct you to call a phone number to verify an account or to reactivate a debit or credit card.
  Source: USA.GOV Online Safety

- ***Web Archiving*** – a process of collecting web pages, web data, images and videos to ensure the information is preserved in an archive for future access.

- ***Web Browser*** – an application used to access and view websites. Common web browsers include Microsoft Edge, Google Chrome, Mozilla Firefox, and Apple Safari. ***Return***.
  Source: Tech Terms

- ***Web Page*** – a single, usually hypertext document on the World Wide Web that can incorporate text, graphics, sounds, etc.
  Source: Dictionary.com

- ***Website*** – a connected group of pages on the World Wide Web regarded as a single entity, usually maintained by one person or organization and devoted to a single topic or several closely related topics. ***Return***.
  Source: Dictionary.com
- ***World Wide Web*** – abbreviated as www or W3 and also known as the Web refers to a collection of text documents and other resources, linked by hyperlinks and URLs, usually accessed by web browsers.

Resources

- **AARP** offers guidance on strategies for safeguarding your computer, online privacy, using social media and much more. http://www.aarp.org/home-family/personal-technology/
- **Consumer Financial Protection Bureau** offers resources to help you or your loved one prevent, recognize, and report scams and fraud. https://www.consumerfinance.gov/consumer-tools/fraud/
- **National Clearinghouse on Abuse in Later Life (NCALL)** promotes victim-defined advocacy and services for older survivors by providing information and resources on equitable and accessible programs, safety planning, outreach, and mandatory reporting. NCALL also advocates for elder justice by providing information on legal remedies and resources to enhance victim safety and to hold offenders accountable. https://www.ncall.us
- **National Cyber Security Alliance (NCSA) Stay Safe Online** works to educate and empower a digital society to use the Internet safely and securely at home, work, and school. http://www.staysafeonline.org/
- **National Network to End Domestic Violence (NNEDV) Safety Net: National Safe & Strategic Technology Project** focuses on the intersection of technology and intimate partner abuse and works to address how it impacts the safety, privacy, accessibility, and civil rights of victims. https://nnedv.org/content/technology-safety/
- **The Stalking Prevention, Awareness, and Resource Center (SPARC)** ensures first responders and other allied professionals have the specialized knowledge to identify and respond to the crime of stalking. https://www.stalkingawareness.org/

- **U.S. Department of Justice, Elder Justice Initiative** is committed to combatting all forms of elder abuse and financial exploitation through enforcement actions, training and resources, research, victim services, and public awareness.
  https://www.justice.gov/elderjustice
- **U.S. Postal Inspection Services** offers tips to protect yourself and your loved ones from mail fraud and other scams.
  https://www.uspis.gov/tips-prevention/older-americans/
- **Working to Halt Online Abuse (WHOA)** works to fight online harassment through education of the general public, education of law enforcement personnel, and empowerment of victims. http://www.haltabuse.org/

Acknowledgments

Sincerest thanks to Rachel Gibson and the National Network to End Domestic Violence Safety Net Project for providing external review and insightful feedback on the original resource and this updated version. My gratitude to NCALL's Katie Block, Ann Laatsch, and Alicia Lord for their internal review and substantive contributions to this guide. Finally, appreciation to NCALL's Bonnie Brandl and OVW's Janice Green for their continued support of this project.

Sara Mayer, *author*

About the Author

Sara Mayer is the Communications Coordinator for the National Clearinghouse on Abuse in Later Life (NCALL), an End Domestic Abuse Wisconsin initiative. She has authored resources on abuse in later life, elder abuse, and technology and designed numerous training materials and curricula, presentations, and publications aimed at increasing public knowledge of abuse in later life and elder abuse. She has more than 20 years of professional writing and graphic design experience. Mayer received a Bachelor of Arts from the University of Wisconsin-Madison and a Master of Arts from the University of Virginia.

www.ncall.us