

# 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 [Internet 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 cell phones, [assistive technology](#), home security systems and medical alerts.

Unfortunately, technology is also misused by some people to harm others. This document provides a general overview of computer, cell phone and [Internet](#) safety. For information about online privacy considerations, please see the info sheet [Tech Tips for Older Adults: Online Privacy & Safety Tips](#). You can also visit the [National Network to End Domestic Violence Technology Safety page](#) for specific technology safety planning strategies.

## [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](#).

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 monitoring software, known as [spyware](#), to your computer or device.

Once spyware 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 monitoring to turn on the computer's camera or microphone to eavesdrop or actually control the device itself.

For a cell phone or [tablet](#), physical access to the [device](#) is typically needed to install spyware, although for a computer, physical access it is not required. [Spyware](#) can be sent via email as an image, attachment or link. When opened, the spyware can install without your knowledge.

## 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.

- **Computer/Device**

- Install and enable a **firewall** to prevent unauthorized access of your computer or device.
- Install **anti-virus** and **anti-spyware** software and set your computer or device to update automatically.
- If you suspect there is spyware on your computer or device, try using a safer computer, such as one at a public library or community center, for personal or private online activities to prevent the person from monitoring what you are doing.

- **Cell Phone**

- Lock your phone with a unique passcode.
- Install and run anti-virus and anti-spyware 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** to be sure you know what information is being shared about you.
- Turn off the **Bluetooth** when it is not in use.
- 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.
- To temporarily suspend signals from being sent or received, turn off the phone and remove the battery. Keep in mind that once you turn the phone on all data waiting to be sent and received will be transmitted. If someone is monitoring your whereabouts they will know once your phone is back on.

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

**Developed by the U.S. military, GPS is a space-based satellite navigation system. GPS is capable of providing precise information about the location, speed and direction of a receiver.**

- 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 **private browsing** option, 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.

## http:// versus https:// What's the difference?

**TIP: Download the HTTPS Everywhere extension: <https://www.eff.org/HTTPS-EVERYWHERE> to make your browsing more secure.**

- Email

- Keep your primary email address private and use it only with people you know and trust.
- Create a free email account (e.g., Google, Yahoo!) to use for all your other online activities.
- Avoid using email for sensitive or personal information. Email is not a private form of communication and can be monitored and intercepted in a variety of ways, even without your knowledge.
- Be cautious of **attachments** regardless of who sent them. These files may contain malware or spyware. Never open or download **attachments** from unknown senders.
- Beware of **phishing** messages that ask you to confirm or provide personal information such as financial records, bank account numbers, Social Security numbers, etc. Legitimate companies don't ask for sensitive information through email.
- If you think your email is being monitored, consider creating a new email account on a safer computer and never access the new account on a computer you suspect is being monitored.

- [Email addresses and Usernames](#)
  - Don't use identifying information in your email addresses and usernames. Including your full name, birthdate or location will make it that much easier for someone to obtain details about you and your whereabouts.
- [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, and do not contain your user name, real name, family member's name, pet's name or complete words. You can test the strength of your password by visiting [www.howsecureismypassword.net](http://www.howsecureismypassword.net).
  - 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.
  - 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.

Source: Safety Net: The National Safe & Strategic Technology Project, National Network to End Domestic Violence ([www.nnedv.org](http://www.nnedv.org)); OnGuardOnline.gov



ncall

© 2015 National Clearinghouse on Abuse in Later Life,  
a project of End Domestic Abuse Wisconsin  
[www.ncall.us](http://www.ncall.us)