TECH

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 general rule is that it is becoming increasingly improbable to remain completely anonymous online. Personal information from photos, emails and social media posts and behavorial 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 Web.

This document 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.

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, information that a site saves to your computer using a web browser, 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. 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. 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. 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.

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.

- 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. 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 and Yahoo!, allow you to limit who can see your profile information.

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

- 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. 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.

- Information about you can end up online when friends, community members, or relatives post information or photos that include you.
  TIP: 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 inadvertently share your location with your exact GPS coordinates.
  TIP: Be aware of what your photos share. Turn off the geotagging settings on your smartphone camera and photosharing apps (e.g., Flickr, Instagram).

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. For more information, please visit the National Network to End Domestic Violence Technology Safety resource, People Searches & Data Brokers.

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