

Online Safety for Older Adults: Protecting Your Personal Information Online


The internet has become an important tool for daily life—playing a critical role in connecting with others, exploring new information and places, and conducting business. This makes knowing how to use the internet safely essential. This fact sheet includes tips to help protect your personal information when using the internet, whether you are searching for information, connecting on social media, attending online events or shopping.

Protect Your Personal Information

As a rule of thumb, never share information online that you would not share publicly. Sensitive information like your Social Security Number, banking information or credit card number should never be shared by email. Entering personal information into a secure platform—such as an online bank account or a medical portal—when using a password-protected (not public) internet connection is okay.

Use Strong Passwords

Think of passwords for your digital life the way you think about keys for your real life. You need a separate key for your house, your car, and your shed or garage, and none of those keys is the same. Treat passwords the same way. The more sensitive the information, the stronger the password should be. Whenever possible, add two-factor authentication. This means that when you log in, you will be sent a code by email or text message as a second layer of protection.

 **ACTION STEP:** At a minimum, passwords should be eight characters long, include upper and lowercase letters, as well as numbers and a special character such as an asterisk or exclamation point. Passwords should be easy to remember and hard to guess. A line from a favorite poem or song in which you have swapped some letters for symbols and numbers often makes for a good, strong password.

Password managers are safe, popular tools that can help manage the many passwords that we all have!

Passwords should contain combinations of the four character types:

Uppercase letters: **A-Z**

Lowercase letters: **a-z**

Numbers: **0-9**

Symbols: **~ ` ! @ # \$ % ^ & * ()
_ - + = { [] | \ ; : ' " < , > . ? /**

Password managers generate and remember your passwords for all your online accounts, so you only need to remember one master password. Your master password should be very strong and be used along with two-factor authentication or biometric authentication, such as a fingerprint or facial recognition. Some popular password managers have free options, while others provide enhanced features for a monthly fee.

Be Alert for Scams

Online scams are all over the internet and can creep into our inboxes and text messages every day. “Phishing” is a trick scammers use—they send false messages, often via text or email, to elicit your personal information. Fortunately, most scams share several basic characteristics. Look for these telltale signs to avoid scams and phishing attempts like a pro!

❶ **Generic salutation.** Banks and companies that you do business with will address you by your name, not a generic salutation. Familiarize yourself with the style used by the legitimate businesses you interact with most in your inbox.

❷ **Awkward language or typos.** Legitimate emails are always written in a clear and professional manner. Typos and grammatical errors are obvious signs that an email is not legitimate. However, even if there are no mistakes, it does not mean that it is not phishing!

❸ **Creates a false sense of urgency.**

Fearmongering is a common tool used by scammers. Any language that tries to pressure you into taking immediate action is a sign that it is a scam.

❹ **Questionable links.** Always be cautious of links in emails or text messages that seem even slightly suspicious. These links may go to a database where the information you enter is captured by the scammer. When on a computer, you can hover over a link with your mouse and look to the pop-up at the bottom of your screen to see what the actual internet address (URL) is without clicking on the link.

❺ **Generic signature.** Legitimate emails from institutions you do business with will have a professional sign-off. Be aware of false logos and corporate addresses as well! If something looks off, it probably is. A quick Google search can confirm the actual logo or corporate headquarters of most businesses.



Remember to use your best judgement. If something seems too good to be true, it probably is. And pressure to act quickly without thinking—whether it comes by email, phone, text or even traditional mail—is a sign of a scam.

Resources

For more information, visit the Senior Planet website (www.seniorplanet.org) or call the Senior Planet Hotline at (888) 713-3495.

Access additional information and tips on how to protect your personal information online by visiting the Federal Trade Commission's Online Privacy and Security webpage (www.consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security).

For additional resources and support, contact the Eldercare Locator at (800) 677-1116 or eldercare.acl.gov.

Remember...

As with most of the things we do every day, there are risks associated with using the internet, but the benefits of enjoying online activities and connecting virtually outweigh the risks. Keeping in mind the tips and best practices presented in this fact sheet will help you explore and connect with others online safely and with confidence!

This fact sheet is part of a series of fact sheets on online safety for older adults. Visit www.engagingolderadults.org to learn about the other fact sheets in this series.

This fact sheet was produced by engAGED: The National Resource Center for Engaging Older Adults in partnership with Older Adults Technology Services (OATS) from AARP. OATS serves on the engAGED Project Advisory Committee. engAGED is administered by USAging and funded by the U.S. Administration for Community Living. For more information, visit www.engagingolderadults.org.

This project #90EECC0002 is supported by the U.S. Administration for Community Living (ACL), U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling \$450,000 (or 74 percent) funded by ACL/HHS and \$161,554 (or 26 percent) funded by non-government sources. The contents are those of the authors and do not necessarily represent the official views of, nor an endorsement, by ACL/HHS, or the U.S. Government.

August 2023