



OATS | OLDER ADULTS
TECHNOLOGY
SERVICES
FROM **AARP**

SENIOR PLANET FROM AARP: ONLINE SAFETY AND OLDER ADULTS

OCTOBER 2, 2024

Ryan Kawamoto

Regional Program Manager, Senior Planet
Older Adults Technology Services (OATS) from AARP



AARP Affiliation



expertise | value | scale



AARP



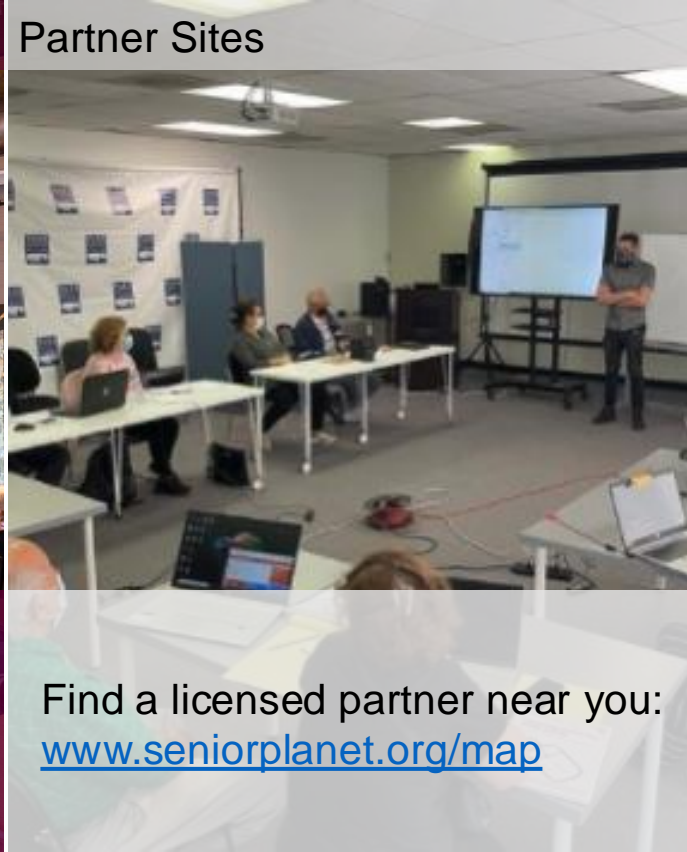
Training Channels

Senior Planet Centers



New York, Colorado, Florida

Partner Sites



Find a licensed partner near you:
www.seniorplanet.org/map

Online



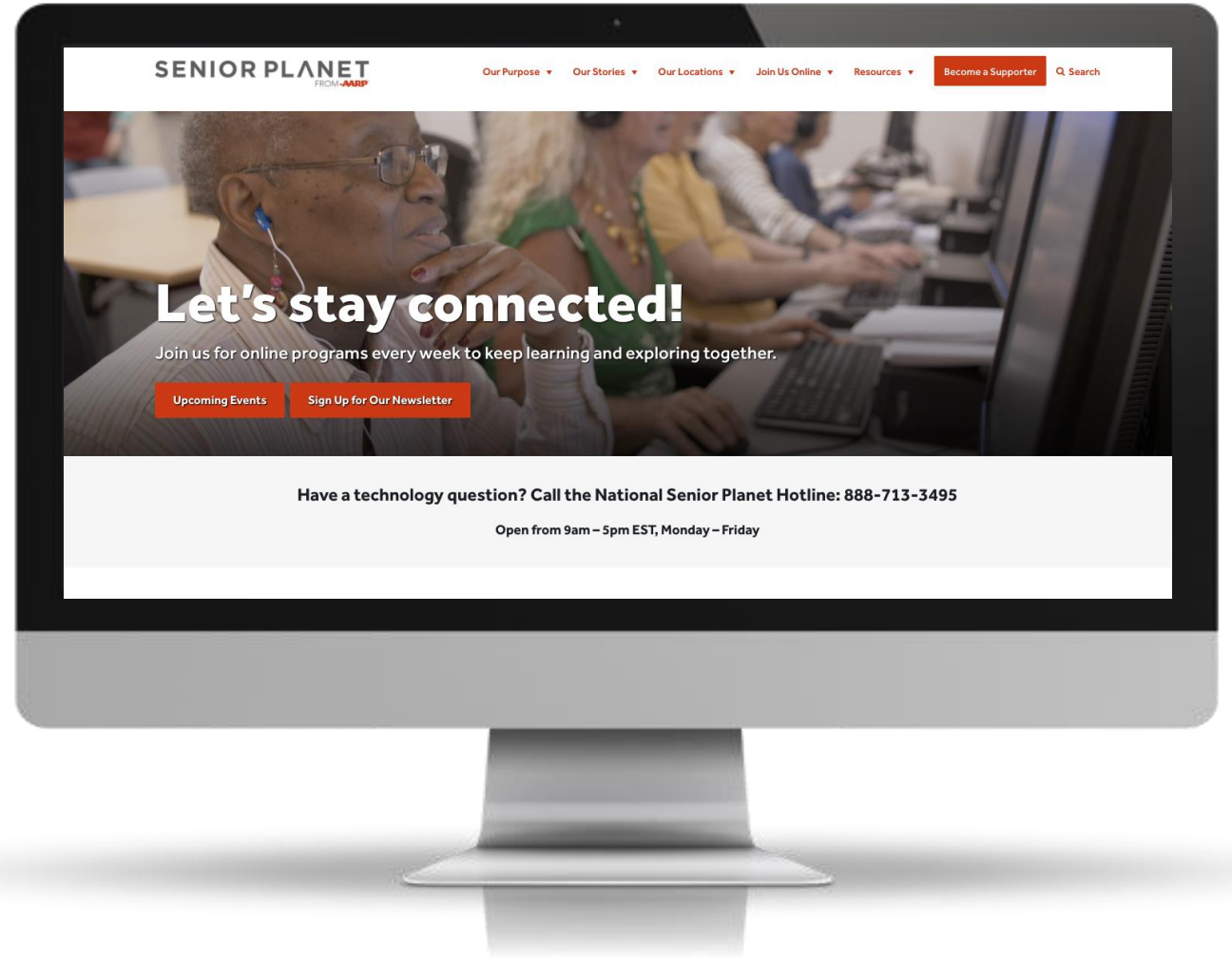
www.seniorplanet.org



Online Offerings and Support

- Free virtual classes, Monday – Friday. Variety of topics including tech basics, stretch and strength, finance, and more!
- Virtual discussion groups
- Multilingual programming in Spanish, Mandarin, and Vietnamese
- Articles for 60+ readers
- Tech Tip videos
- 1:1 tech support and coaching
- Toll-free national hotline: **(888) 713-3495**

www.seniorplanet.org



Impact Areas

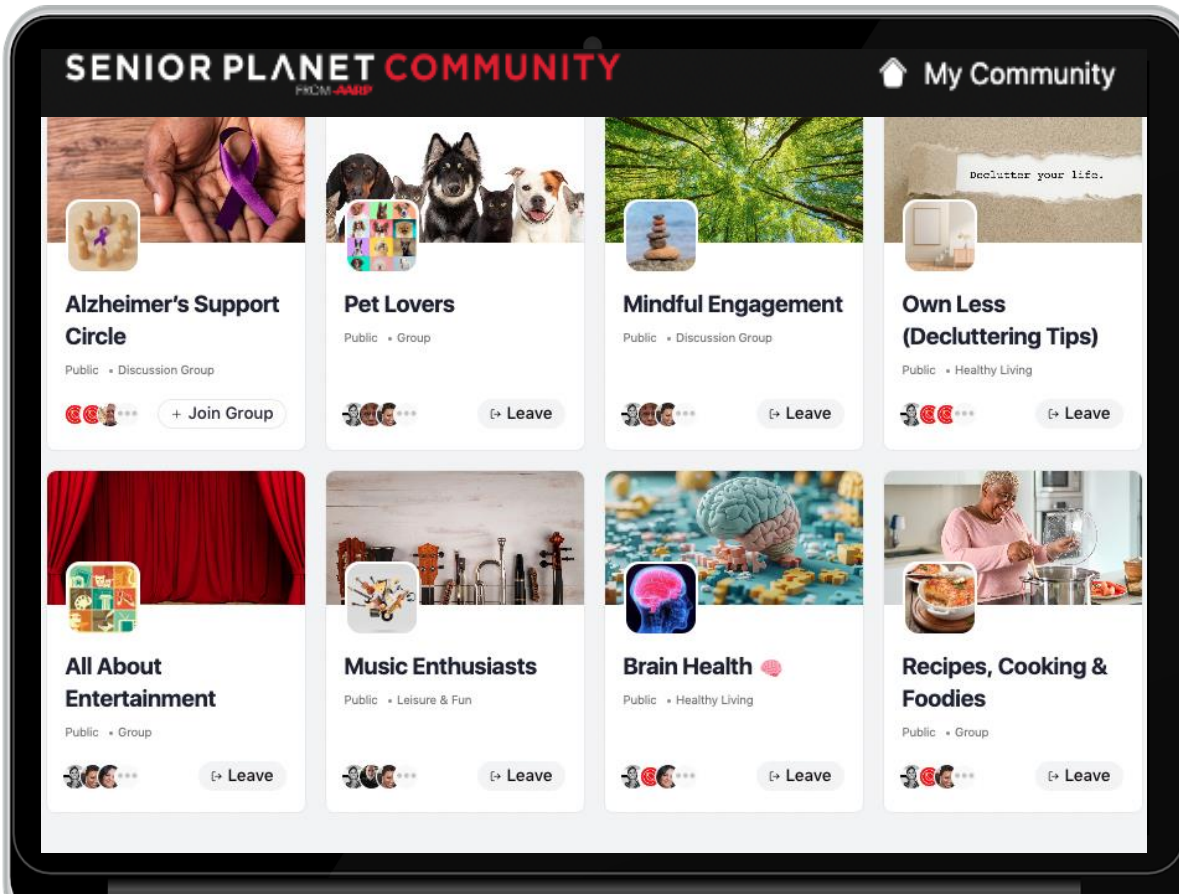


Senior Planet Community

A social media platform with over 12K users made with older adults, for older adults.

- Group-based interest areas
- Safe, trusted, and Ad-free space
- User-generated content with engaging discussions, shared experiences, "Ask a Tech Expert" groups and more

Community.seniorplanet.org





Addressing Online Safety

Online safety best practices are built into all of our programs. We teach:

- Privacy and security for apps, websites, etc.
- Best practices for using social media safely.
- How to spot, avoid, and respond to scams via email, text messages, phone calls, and other methods. Remember that emails, texts, etc.



Online Safety & Older Adults

Protecting your Personal Information

- Create unique and strong passwords
- Password managers are safe and secure
- Be wary of communications that create a sense of urgency and/or play on emotions
- Never open links or call phone numbers in emails or texts from unknown sources
- Learning about AI is key to online safety



Confident Web Browsing

- Only access sensitive accounts, such as banking and health portals, on secure, password-protected Wi-Fi connections
- Use the "Safe Browsing" or "Enhanced Security" web browser options
- Only shop on secure websites

Best Practices for Social Media

- Never give out sensitive information over social media
- Check & adjust your privacy settings
- Avoid linking different social media accounts
- Always log out when using a public computer or public WiFi



Resources

- All Senior Planet virtual classes: seniorplanet.org/classes
- Senior Planet financial security classes: seniorplanet.org/financial
- Senior Planet AI classes and virtual resources: seniorplanet.org/ai
- Download online safety fact sheets created by OATS & USAging at engagingolderadults.org/consumer-materials

SENIOR PLANET
FROM AARP

© Copyright 2024 Core Health Technology, Inc.
A subsidiary of AARP. All rights reserved.
© 2024 AARP. All rights reserved.

Programs on Online Safety

Our dedicated one-off sessions include:

- Protecting your Personal Info Online
- Intro to Managing your Online Privacy
- Intro to AI
- AI & Disinformation
- Staying Safe Online is an in-person, hands-on workshop.



Online Safety for Older Adults: Socializing Safely Online

www.engagingolderadults.org/consumer-materials

Online Safety for Older Adults: Socializing Safely 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 best practices for safely socializing online, whether you are connecting on social media or attending online events.



Social Media

Social media allows you to connect with others and create a network of people with whom you can interact using the internet. Over time, a lot of personal information can potentially be gathered from your social media posts. Do you post about family? Kids? Grandkids? Do you include their names? Although there is nothing wrong with sharing these details about your life online, you should keep in mind that this information could potentially be used by scammers. Being aware of how much information that someone with malicious intentions can learn about you online can help you protect yourself against scams.

Below are some steps you can take to ensure your safety on social media, while still enjoying all the benefits of online connections.

ACTION STEPS:


- Only post what you would be comfortable sharing on a public forum. Assume that anything you post on social media can be seen by the general public, regardless of your privacy settings.
- Periodically review your privacy settings to control who sees your posts and who can contact you on social media platforms. You do this in the Privacy section of the platform's settings.
- Make sure that only the people you know in real life can send you direct messages, also known as DMs. Depending on your privacy settings, you may receive message or friend requests from people you do not know. There is no reason to accept friend requests from

people you do not actually know. If you receive completely unsolicited message requests, you should not accept those. If you accidentally accept a message or friend request from someone and you realize the mistake, it is easy to block that person from contacting you again. You can visit the social media platform's help page to learn how to block someone.

- As a rule of thumb, the following should never be shared on social media:
 - Your address or phone number,
 - Your credit card number or other financial information and
 - Your Social Security Number.

Navigating New Relationships

It is smart to use caution and look for signs of a scam when meeting new people online. Scammers play on your emotions by using tactics like fearmongering, flattery or sympathy.

 **ACTION STEPS:** When meeting new people online, consider the following:

- Check out their profiles. How long have they been on the platform? Do they post photos or information about their daily lives? If their account is new or if they give little to no information on their profile, use caution.
- Search before you friend or like someone. Conduct an online search to confirm their identity. (No online presence is a red flag.)
- Ask to video chat! Repeat excuses or claiming to have a broken camera could be red flags.
- Never agree to send money to or buy gift cards for anyone.
- Block and report anyone who you suspect of being a scammer. Social media and online dating platforms have conduct guidelines and ways to report users who break those guidelines.



Hosting Virtual Events

Video chat platforms like Zoom are a great way to stay connected with friends and family who are geographically far from you. If you are hosting a virtual event for your book club, condo association, family reunion or just a get-together, here are some best practices to keep in mind to avoid any uninvited guests crashing your virtual event.

- Require a passcode for participants.
- Enable the waiting room.
- Set audio options to “mute upon entry” and video settings to “on.” Muting large groups reduces confusion at the beginning, and encouraging the use of video makes for a more fun experience. Additionally, you can quickly see if someone you do not recognize joins the event.

Resources

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

When socializing online, it is important to be aware of potential scams and fraud. AARP provides a national helpline where you can report a possible scam or fraud and a map that tracks scams near you. The AARP website also offers education on common scams to be on the lookout for and tips on how to avoid fraud.

- AARP Fraud Watch Network Helpline: (877) 908-3360 or www.aarp.org/money/scams-fraud/helpline.html.
- AARP Scam-Tracking Map: www.aarp.org/money/scams-fraud/tracking-map.
- AARP Scams & Fraud: www.aarp.org/money/scams-fraud.
- AARP's Top 14 Scams to Watch Out for in 2023: www.aarp.org/money/scams-fraud/info-2023/top-scammer-tactics-2023.html?intcmp=AE-FRDSC-MOR-R2-POS3.

The following resources provide more information on possible scams, including grandparent and sweetheart scams, and actions you can take if you suspect a scam.

- Eldercare Locator | Protect Your Pocketbook: <https://eldercare.acl.gov/Public/Resources/BROCHURES/docs/FinancialExploitationBrochure-508.pdf>.
- National Council on Aging | The Top 5 Financial Scams Targeting Older Adults: www.ncoa.org/article/top-5-financial-scams-targeting-older-adults.
- National Council on Aging | Sweetheart Scams: How to Avoid Being a Victim: www.ncoa.org/article/sweetheart-scams-how-to-avoid-being-a-victim.
- AARP | Grandparent Scams: www.aarp.org/money/scams-fraud/info-2019/grandparent.html.

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.



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!

1 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.

2 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!

3 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.

4 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.

5 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.

Online Safety for Older Adults: Browsing the Internet Confidently

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 best practices to help you do so.

Pop-Ups

Many websites have pop-ups, those small browser windows that suddenly appear in the middle of the screen. Pop-ups are a way for websites to draw your attention and are often used as an advertisement. They often aim to re-direct you to another site. Most pop-ups are just a nuisance and are not harmful.

ACTION STEP: If you encounter pop-ups, look for the “X” to close it. The “X” is often intentionally hard to find. It will generally appear in one of the corners of the pop-up window. If you happen to click on the pop-up itself, do not panic. You can select the back button in your browser or close the tab or window. Avoid clicking on the page that opens as a result of the pop-up.




Ads and Sponsored Content

When you use a search engine like Google, the first several search results will be advertisements. You will know they are ads because they will be labeled “Ad,” and they are often the top three search results. Scrolling past the ads and carefully reading the website address or URL of the search results can make for a better browsing experience.


Sponsored or paid content is another type of advertisement you will encounter on the internet. These ads are designed to be subtle and blend in with the rest of the content on a webpage, making it difficult to tell the difference between sponsored content and the actual content of a

webpage. You will also find sponsored content on social media platforms like Facebook, Twitter and Instagram. These posts blend into your feed, and you may not realize at first glance that they are ads.

 **ACTION STEP:** Ads and sponsored content are often, but not always, labeled as “Sponsored” or “Promoted.” Always check the byline and description of a video for signs that it might be an ad before you click to watch.


Website Spoofing

A spoofed website is one that is designed to look like a legitimate site but is actually a website that will capture any information you enter. Once the websites obtain your personal information, the people behind them then use or sell the information. These spoofed websites often have similar URLs as legitimate websites. For example, the URL for a website spoofing Bank of America’s site may be missing a letter, such as www.bankoamerica.com.

 **ACTION STEP:** If you use Google Chrome as your web browser, make sure that “Safe Browsing” is turned on so that the browser can catch any mistakes. You can do this by going to **Settings → Privacy & Security → Security** and selecting the level of Safe Browsing you want. We recommend choosing **Enhanced Protection**.

Secure Websites

Websites with https in their URL have added an extra level of security that safeguards any information you enter on the site—the “s” stands for “secure.” Websites that do not include the “s” (http) are not necessarily unsafe; they simply did not take the extra step to ensure a secure connection.

 **ACTION STEP:** If you enter sensitive information (e.g., your address, phone number, banking information, credit card number, Social Security Number, etc.) while browsing online, you should only do so if you see https in the website address and trust the organization or company.



Tips for Evaluating Information Online

Remember that anyone can post false or misleading information on the internet. When evaluating whether information is accurate and trustworthy, ask yourself whether you are using the correct website domain extension—.com, .org, .gov, etc.—for the type of information you are seeking.

Here are additional questions that can help you determine whether the information you are reading online is accurate.

- Who owns and runs the website?
- Who wrote the information?
- Is this organization or person knowledgeable?
- Is this organization or person reputable?
- Are they trying to sell you a product?

Resources

For more information on how to browse safely online, visit the Senior Planet website (www.seniorplanet.org) or call the Senior Planet Hotline at (888) 713-3495. For additional resources and support, contact the Eldercare Locator at (800) 677-1116 or eldercare.acl.gov.



Artificial Intelligence (AI)

AI is making scams more sophisticated. Understanding the capabilities of AI is important for everyone. OATS has built up its AI content and program teach:

- Tips for detecting if something was created by AI and available tools.
- AI is new for everyone and when you experiment with it, you become more familiar with what AI-generated content is like.
- To be careful with what information you share when using AI.



Find Us

SeniorPlanet.org

- Online classes
- Articles for 60+
- Videos and quizzes

OATS.org

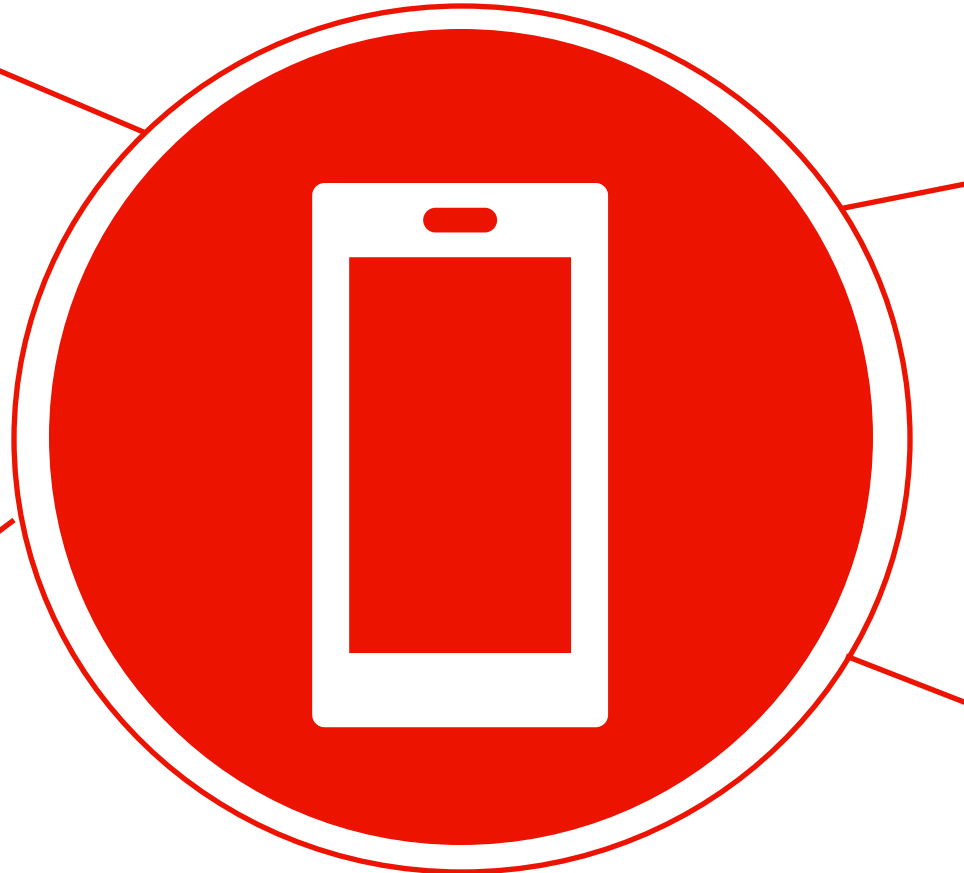
- Client Projects
- Licensing Info and Application

Senior Planet Hotline:

(888) 713-3495

Senior Planet Community:

Community.seniorplanet.org





Thank you

www.oats.org

@OlderAdultsTech



Ryan Kawamoto

rkawamoto@oats.org

www.seniorplanet.org

@SeniorPlanet



OATS | OLDER ADULTS
TECHNOLOGY
SERVICES
FROM **AARP**