

CONNECT TO THE INTERNET

# How To Keep Seniors Safe in the Digital Age: A Social Media Guide

We've put together an in-depth guide for both seniors and caretakers that looks at common forms of social media fraud, how to prevent them, and resources for when you get scammed.

**Mary James**, Author **Catherine McNally**, Editor

Last updated Mar 2, 2023

We may receive compensation from the products and services mentioned in this story, but the opinions are the author's own. Compensation may impact where offers appear. We have not included all available products or offers. Learn more about [how we make money](#) and [our editorial policies](#).

Whether you grew up with a digital or analog childhood, you're probably now an avid user of technology and social media platforms. Learning new technologies as an adult can be tricky though, especially when tech companies have user manuals that seem like they require an advanced law degree to decipher.

- **Americans over 65 are the fastest-growing segment of social media users. In 2021, 45% of seniors over 65 use social media.**
- **Seniors are the most targeted group for fraud in the U.S. In 2021, the FBI reported more than 92,000 fraud victims over 60, with losses in excess of \$1.6 Billion.**
- **According to the FTC, 1 in 4 Americans who lost money in in 2021 said they were first contacted via social media.**
- **Annually, Americans lose more than \$770 million from social media scams.**

## 2021 Fraud Cases in the United States, by Age

Victim Age Range	Total Cases	Total Money Lost	Average Amount Lost Per Case
Under 20	14,919	\$101,435,178	\$6,799
20-29	69,390	\$431,191,702	\$6,214
30-39	88,448	\$937,386,500	\$10,598
40-49	89,184	\$1,192,890,255	\$13,376
50-59	74,460	\$1,261,591,978	\$16,943
Over 60	92,371	\$1,685,017,829	\$18,242



Understanding privacy and security settings as well as how to spot a fraudster is becoming increasingly difficult even for the savviest social media users. As an older adult or a caregiver to an older adult, you may feel overwhelmed — but social media safety is achievable.

Social media platforms don't have to be a privacy nightmare. Strong passwords, quality antivirus software, knowing how to spot a [phishing scam](#), and other online safety tips all translate to being a more savvy internet user. From the much-debated TikTok to Meta's flagship platform, Facebook, let's look at ways to keep your sensitive information private on social media.

---

### In this article

---


## 1. Don't overshare personal info

This is probably the most difficult tip to remember because social engineering attacks started on social media can seem like harmless fun.

Links where you allow a site access to your profile and it generates a fun qualifier like “Which Avengers characters are your circle of friends” or “What kind of bread are you” are more than likely there to steal all the information you’ve listed about yourself in your profile — and you just granted them access.

Quizzes, games, and even the popular “What’s your Elf name” or “What’s the first sentence of your autobiography” memes can be a trap to gather your information.

When you’re sharing information like your first pet’s name or the make and model of your first car, you’re potentially sharing the answers to your password recovery questions on other sites. While these feel like fun ways to connect, they could end in your identity being stolen. A good [identity theft guide](#) can help you navigate what to do if you find yourself in this predicament.



Sharing travel photos is an amazing way to connect with peers, but wait until after you’ve returned home to avoid criminals knowing your house is empty and unguarded.



## 2. Double up on account security

Two-factor authentication or multi-factor authentication is the darling of the Cybersecurity and Infrastructure Security Agency (CISA), the agency that sets security guidelines for the federal government. Two-factor authentication works by requiring sign-in or authentication from a secondary device.

For instance, if you’re logging into your Facebook with two-factor authentication turned on, you may need to enter a code that was emailed to you or log into Facebook from another device to let them know it’s really you.

This oftentimes shows up in the notifications on your Facebook page. It’s usually when you log on from a device you haven’t logged on from before or from one you haven’t used in awhile. This second step to security ensures you are who you say you are.



## 3. Change your passwords

Regularly changing your passwords is a proven way to reduce the chances of being hacked. We’ve all had strange private messages from people we’ve connected with on a social platform.

Suddenly, it seems like they don't know you at all. Likely, their social media account was hacked and the person sending you the message is a hacker. Social media hacking is an easy and common way to spread malware-infected files to large groups of people.

Changing your password periodically is good for a few reasons. There's a chance your old account credentials were stolen without your knowledge, and changing your password makes it that much harder to access your bank account, credit card numbers, and even your Social Security number.

It also gives you the opportunity to log out of your account on all devices and sign back in. If one of your devices is hacked or stolen, this could be a great way to block the hacker from getting into your online accounts.

## 4. Be wary of "friend requests"

Is your new co-worker, Linda, sending you a follow request on Instagram? It's likely her, and she might just want to share her potato salad recipe with you. But that girl with very little online personality who is "new to the platform" is more than likely a scammer.

This is true of anyone you don't know personally. If the potential new friend's profile looks new or strangely curated (for example: a U.S. veteran with only pictures of them beside military equipment and other soldiers), there's a good probability it's a fake account looking to gather your personal information.

A good rule to follow is, if you've met the person in real life or you can verify their identity, you can go ahead and add them as a friend. If someone tries to connect out of the blue and you've never heard of them before, it's best to delete that request.

Unless you're an influencer trying to build a following, make sure your social media profile settings are toggled to private.

## 5. Beware of social media scams

No social media platform is safe. From Snapchat creepers to [TikTok scams](#), every part of social media is prone to crime.

Like we mentioned before, a friend sending you a spammy-looking link could have been hacked and the hacker is trying to trap you next. A duplicate friend request from someone you're already connected with is definitely a spoofed account looking to scam you. Offers of romance and friendship in the comments sections of posts unrelated to romance and friendship could be honeytraps (a common [social engineering scam](#)).

We have levels of familiarity with people we know and those levels of familiarity don't change just because the interaction is online. If someone is acting "off" it may be because they're a bot or a person unfamiliar with your native language. These can be telltale signs of a scammer.

If something looks or feels strange, it might be a fraudulent interaction. Double-check with people off the platform to make sure what they're sending is genuine.

## **6 common social media scams**

There are common scams that, once you're aware of them, become easier to spot. You'll probably see commonalities between these scams and newer or more advanced scams that emerge. Becoming familiar with the specifics of a scam can help [keep you safe online](#).

# Common Social Media Scams

Scam Type	Scam Description	How to Prevent
<b>Account Takeover Fraud</b>	Scammers take over your social media accounts. They can pretend they're you to defraud others.	Keep your passwords private and don't click links from people you don't recognize.
<b>Account Authentication Scams</b>	Scammers send a message that your password is compromised and ask for you to authenticate it. They are using this information to get into your account.	Never change your password if prompted from outside the social media site.
<b>Fake Online Stores and Products</b>	Scammers create fake web stores or products.	Use credit cards with buyer protections for online purchases and read reviews before pressing "buy."
<b>Giveaways Scams</b>	Scammers pretend you've won a contest and ask for your personal information to receive a prize.	Double-check with the actual business that you've won before submitting any personal information.
<b>Investment Scams</b>	Scammers propose investment opportunities with huge returns, only to disappear when you follow up for your earnings.	Be wary of any unsolicited investment opportunities. Any good investment advice should come with risk warnings.
<b>Link Scams</b>	Scammers entice you with clickable links that actually contain malware or other identity-compromising links.	Be mindful not to click anything that seems like it's trying too hard to draw you in.



## 1. Account takeover fraud

This happens when the cybercriminal gains access to your social media accounts. They begin by changing details like your contact email or password on the site.

They can then pose as you to defraud friends and followers or try to hack your more sensitive accounts like your bank, credit card, or even utilities.

## 2. Account authentication scams

This scam starts when you receive a text or an email saying your account has been compromised and you need to share the authorization code being sent to verify your account.

What's happening is a hacker has your user name and password, but can't access your account because of multi-factor authentication. They're trying to gain access by having you share the code specifically meant to stop this type of scam. Never offer this information to a third party.

### **3. Fake online stores and products**

It's easy to set up a fake store and begin "selling" products in less than 30 minutes. While social media allows small businesses to advertise their wares on your page, the sites aren't able to verify every single one of those retailers.

It's always best, if you're going to purchase from any of these stores at all, to use a credit card or a service like PayPal which will make sure your money is returned if the product or store turns out to be a scam. And be wary of [Facebook marketplace scams](#) that may look like a harmless buy/sell/trade situation but end up being fraud.

### **4. Giveaway scams**

Who doesn't love to win a giveaway? Giveaways are great tools used by businesses to engage new customers and drive awareness about their products and services. They're also a great way for scammers to get your information.

The scammer creates a fake account that looks very similar to a real business, then contacts you to let you know you've won something. They then ask for some kind of personal information that helps them steal your identity, financial information, or other credentials.

The best way to avoid these is to double-check with the actual business.

### **5. Investment scams**

Investment scams have evolved from pyramid schemes and multi-level marketing companies. Social media investment scams may actually look legitimate — so much so that the [U.S. Securities and Exchange Commission \(SEC\) made an entire guide](#) on avoiding them.

As with any information you get online, make sure you can verify the source. Scammers may pose as legitimate investors or pay people to make it look like they've made money from these schemes.

Legitimate investment opportunities should come with cost and risk analysis and shouldn't pressure you into giving money without being completely transparent about the opportunity.

## 6. Link scams

Links can be some of the most malicious ways to deposit malware or other credential stealing methods onto your device. Clickbait articles, flashy advertisements, and overly opinionated "news" sources are all hotbeds for link scams.

You may be thinking you're doing your due diligence by researching something on your own when all you're really doing is feeding your data (or worse) to a hacker. Examples are links with titles like "This 1 weird tip shrinks belly fat overnight" or an advertisement for a sweatshirt with a sassy saying like "It's wine o'clock somewhere."

To stay safe, start by [disabling Facebook ads](#) and be mindful not to click anything that looks too much like it's trying to draw you in.



## 6. Be careful where you click

How many times have you been online looking at something when you move your mouse or scroll on the screen and you're suddenly transported to another site? This isn't a direct scam, but it is a way to make you accidentally click on links that may give access to malicious software downloads.

Many times, these links or ads take up a large portion of the screen in an effort to get you to accidentally click on them.

Being careful of where your mouse is located, what part of the page you scroll on, or where your fingers are is a start to avoiding accidental clicks. Be intentional with your clicking so you don't stumble into something unpleasant.



## 7. Update your security settings

While it may look like only younger generations know what they're doing when it comes to social media safety, it's possible for anyone to be security savvy. You'll want to start by taking a look at your [security settings](#) to make sure you aren't sharing with more people than you'd like.



Setting your account to private and having to approve follow or friend requests is the next step. Also, [stopping Facebook tracking](#) can be an extra barrier against targeted ads that may be out to steal your information.

Depending on your goals, you can set your profile to show certain information to certain people. If you're doing outreach for an organization, but still want to share pics of grandkids or nieces and nephews, you can create groups of trusted friends who see your personal shares. There are plenty of ways to customize your social media experience.

## 8. Check sources before you share

This tip is all about protecting your good name. You want to make sure you don't lose credibility with friends and family by being the person who always shares spam or worse.

As we mentioned in the beginning, social media is like the Wild West. Anyone who can access the internet can create a profile or a website and pretend to be an expert.

Whether it's news, contests, videos, memes, health information, or any other topic, make sure you're sharing your information from a credible, verified source.

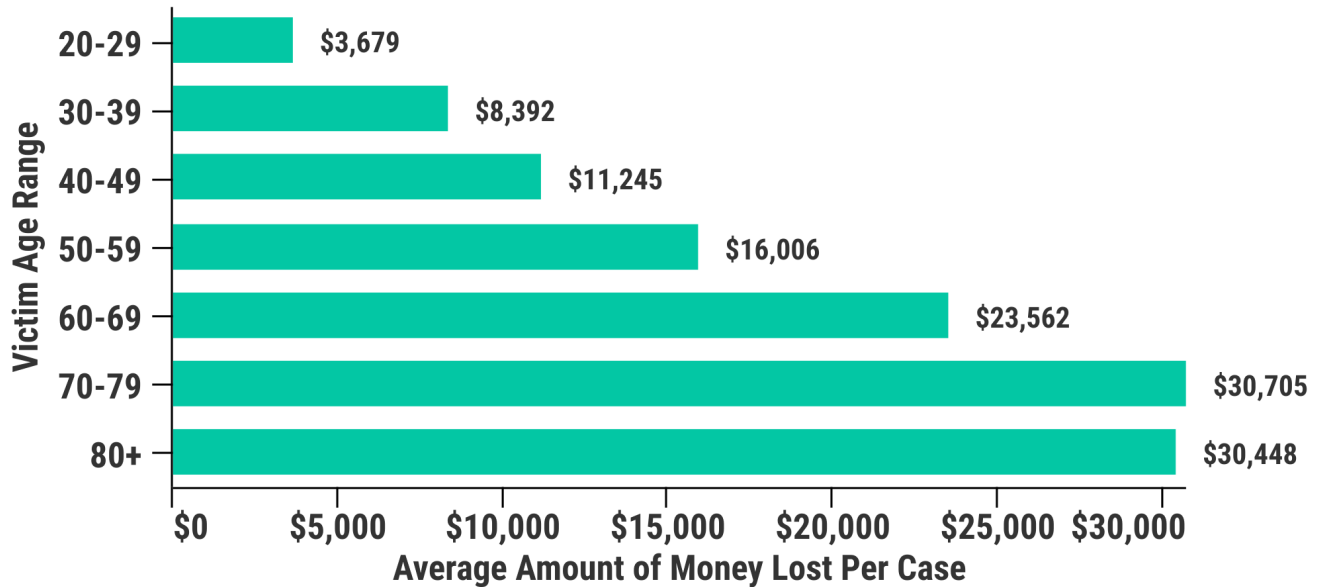
The University of Washington University Libraries website has a [helpful tool](#) for checking sources. The tool is meant for writing students, but the knowledge there can apply to anyone.

## 9. Don't get caught in a catfishing scam

Online dating can open up a world of possibilities, especially if it's been a while since you've been in the dating pool. It's a low-stress, low-commitment way to meet other singles. But social media is full of honeypot and romance scammers you need to watch out for.

These individuals pretend to be looking for a relationship in an effort to get you to send them personal details, gifts, and even money. If you'd like to use the internet to search for someone to hang out with, use a verified match site like [Bumble](#) or [Meetup](#). There's also the option to use social media to find groups of people who share your hobbies and interests and meet up with them. Plenty of romantic relationships start from discovering a shared interest.

# Impact of Catfishing on Different Age Groups 2019-2022



Remember, you don't want to ever send money to someone on the internet who you don't know personally. Even if you do know them personally, be wary of sending money unless it's through a site like [Gofundme that works to protect you from fraud](#).

## Additional tips for family members and caretakers

If you're reading this looking for a way to protect older adults from fraudulent practices on social media, please look at the additional tips below. It may be difficult to have these conversations with someone you care about, but remember that being concerned and being respectful can go hand in hand.

The person you're looking to protect should know this comes from a place of caring rather than admonishment. If you're still concerned about being disrespectful or insensitive, suggest the two of you approach these tips as a way to learn together.

## 1. Practice tough love

Remember that social media can be a way to combat loneliness, especially for people in the middle of a big life transition such as losing a partner, becoming an empty nester, or retiring from a job. Making sure your loved one is safe can be achieved through honesty, education, and mutual respect for each other's knowledge and interests.

## 2. Talk to them about online scams

Even the most tech-savvy person can fall victim to scams. Researching different scams, reading guides like this one, and looking at official government notices regarding fraud on social media together can keep you both informed.

## 3. Set up passwords on their devices

Help your loved one create complex passwords and enable them with a system like a [password manager](#) to make sure they stay secure.

## 4. Help them secure their internet and Wi-Fi

Learn together about all the ways to secure your modem and router, including how to keep the network private and [how to change your Wi-Fi password](#).

You may even decide together to install a virtual private network (VPN). A VPN encrypts your data and hides your location so scammers can't tell who and where you are based solely on internet activity. This not only keeps your online data safe but prevents criminals from knowing where you live.

## 5. Help them secure their smartphone and apps

Smartphones do so much more than we realize and most of us never learn all the functions available to us. Directly searching for smartphone safety tips can help you both learn what features are available for phone security.

Also, make sure to read the terms and conditions on any apps downloaded. If reading them makes your brain feel fuzzy, check out the app or service on the [Terms of Service; Didn't Read](#) site for a breakdown of what you're really agreeing to when you sign.

## 6. Set up antivirus and run a scan on their device

Download a [good antivirus program](#) and run regular scans on their devices. Show your friend or family member how this works and how they can run scans themselves in your absence.



# What to do if you're a victim of a social media scam or abuse

Anyone is susceptible to falling victim to a social media scam. It doesn't matter your age, technical prowess, education level, or security awareness, there's always the chance you'll be caught by a scammer. If that happens, most social media sites have methods for reporting the scam.

- **Facebook** has a [reporting center](#) with instructions on how to report everything from scams to harassment. (You can even request safety checks.)
- **Instagram**, another Meta-owned app, also has a clear-cut way to [report scams and abuse](#).
- **Twitter's** reporting page walks you through all the ways to [report violations of conduct](#).
- Rounding out the Big Four is **TikTok**, which not only [helps you report scams](#) but provides information and resources for a variety of issues.

To find reporting for other platforms or apps, perform an internet search with words like “report [name of app or site] scams” or “how to report scams on [name of app or site],” putting the name of the app or the site in where appropriate.

---

## Social media safety FAQs

---

### How can we keep older adults safe on the internet?

The best way to keep older adults safe on the internet is to learn about safety with them. Include them in the conversation and process of securing their social profiles to make sure you're giving them the tools to empower themselves.

---

### How do I protect my older family members on Facebook?

You can protect your older family members on Facebook by helping them understand the policies they agree to on the app as well as helping them learn about common scams and fraud, such as these [common Facebook Marketplace scams](#).

---

## Which social media platform is best for older adults?

Facebook seems to be the preferred app for older adults. Although there are a growing number of older people joining TikTok to share their expertise and knowledge.

### Bottom line

Social media is a way to have fun with friends, stay active, and combat loneliness. It can be a useful and worthwhile tool for anyone looking to connect or learn new skills.

While there is a myriad of schemes to defraud people on social media, there's equally as much information on how to stay safe. Sometimes it may be necessary to help a loved one with internet safety, but that doesn't mean it can't be a positive experience for both of you.

By learning together and staying vigilant about online safety, you can use these platforms to enhance your life or the lives of those you care about. Simple tips like [using complex passwords](#) and being careful about what you click can go a long way toward social media safety.

Since social media and the internet as a whole are ever-changing entities, it's good to continue to learn about how they work and what they're doing to keep you protected.

### Author Details



**Mary James**

About the Author

Mary lives in Los Angeles and has been writing about tech for over 5 years. When she's not writing for work or fun, you'll find her in a theatre, at the movies, volunteering, or hiking the gorgeous SoCal landscape.

## Related Articles

---



### **How to Stop Getting Facebook Ads in 2023**

Are you annoyed with all the Facebook ads you see when scrolling through your news feed? There are ways to block those ads, learn how here.

---



### **NordVPN Review 2023: Is It Worth the Cost?**

Despite its higher-than-average cost, NordVPN offers excellent standards of security and privacy without compromising on internet speed.

---



### **How to Speed Up Your Internet Connection**

Slow internet can be disruptive, but you can fix it. Here's how.

---



## How to Watch Netflix with a VPN (and Change Your Netflix Region)

Learn how to watch Netflix with a VPN if you want to access geo-restricted streaming content from another country.



Copyright © 2023 **All About Cookies**

111 E. Atlantic Ave., Suite 200

Delray Beach, FL 33444

All About Cookies is an informational website that provides tips, advice, and recommendations to help you with Online Privacy, Identity Theft Prevention, Antivirus Protection, and Digital Security. We strive to provide up-to-date information, but make no warranties regarding the accuracy of our information. Ultimately, you are responsible for your digital security. All About Cookies is not a digital security product and does not provide any digital security products.

[About Us](#)

[Privacy Policy](#)

[Do Not Sell or Share My Personal Information](#)

[Terms of Use](#)

[DMCA](#)