LET'S GET THERE FIRST

Protecting Yourself From Scams, Fraud, and Cybercrime

A GUIDE FOR OLDER ADULTS
BROUGHT TO YOU BY LET'S GET THERE FIRST!

www.letsgettherefirst.com

Did you know that older Americans are now a top target for scammers around the world? According to the Federal Trade Commission, this one group of consumers could be losing as much as $80 billion every year to all kinds of scams. That's more than a billion dollars every week.

And thanks to AI those scams are becoming much more common, much more sophisticated, and much tougher to spot. But it doesn't mean you're helpless.

The key to spotting these scams is to understand the warning signs -the red flags to always be on the watch out for - and to find ways to remind yourself of just a handful of good and simple habits.

In this guide, security and fraud expert Neal O'Farrell has condensed his more than 40 years fighting cybercrime and fraud around the world into a handful of tips that will keep you one step ahead.

So print it out and keep it in places you're most likely to read it most often – on your fridge, near a phone, or by a computer.

And remember that all our tips are also available as one-pagers that you can print out and keep handy.

How Can You Tell If It's A Scam?

If you get a message by phone or on your computer, whether it's a text, phone call, or email, the scammy ones usually have great big telltale giveaway signs, like:

They say they're a government official and are contacting you about a legal issue, a fine, or a payment. Government officials will almost always contact you by mail.

They say they're from your bank, that there's a fraud issue they want to discuss, and they need you to do something like share a code or an account number.

It's a call, text message, or e-mail from a complete stranger who sounds like they contacted you by accident, tell you that you sound nice, and want to keep you chatting.

They claim to be looking for a friendship or a relationship, even though they've never met you.

They have an investment opportunity for you, perhaps in crypto.

They tell you they discovered a security or technical issue with your computer and want to help you solve it.

They need you to pay something, perhaps a fine, but you can only do it with gift cards or by going to your bank or an ATM.

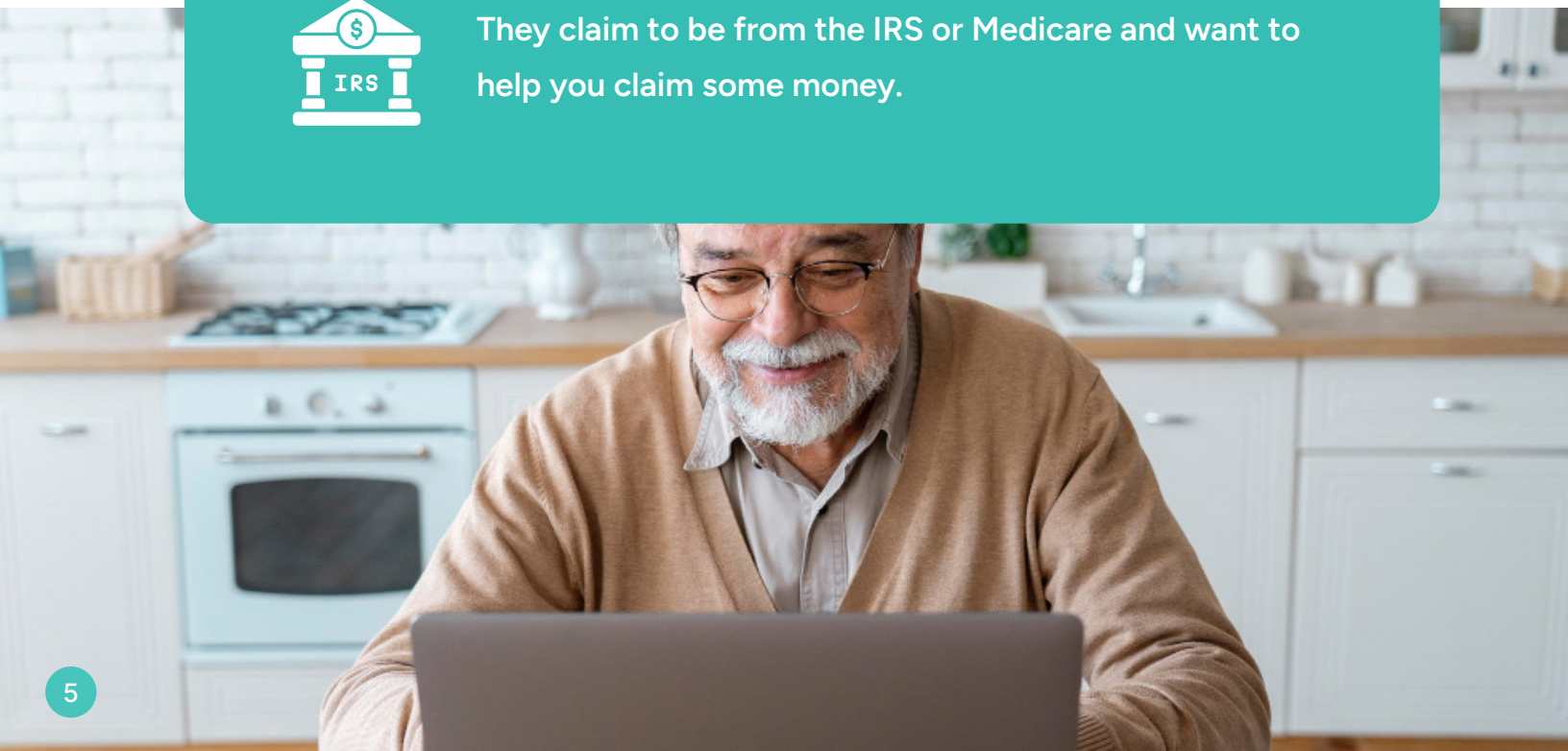
They threaten that if you don't do what they say, you'll get into legal trouble, perhaps be arrested.

They claim to be a relative, maybe a grandchild, and are in some kind of trouble - arrested or even kidnapped - and need financial assistance.

They claim to be from the Social Security Administration, telling you that they suspect your social security number has been used in a fraud and ask you to confirm the number for them.

They claim to be a charity soliciting donations for some recent event.

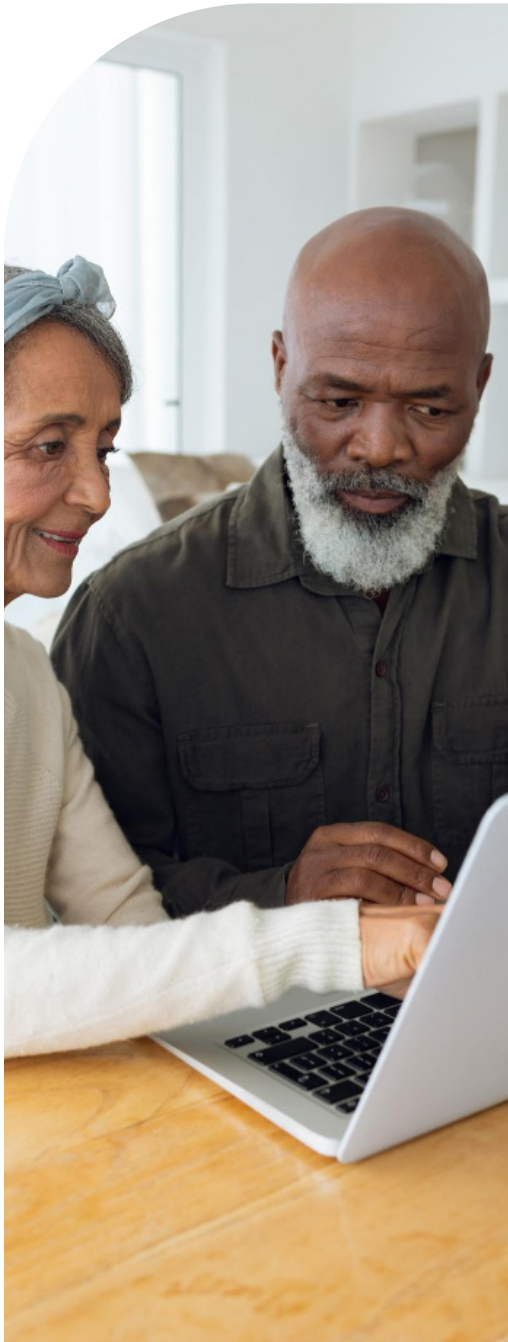
They claim to be from the IRS or Medicare and want to help you claim some money.



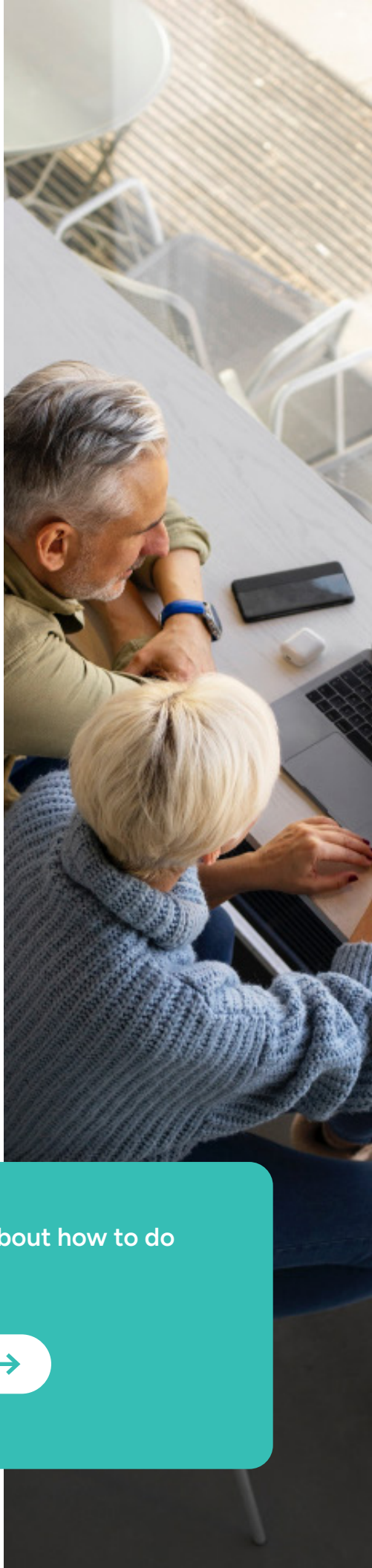
So What Should You Do?
How Should You React?

These are just some of the things you can do to protect yourself from phone scams:

- Just ignore them. Don't respond, don't engage, and don't click on anything.
- Don't answer the phone, have the caller leave a message instead.
- If you do answer and you feel under pressure, tell them your daughter is at the door and you'll call them back.
- Contact your Police Department for advice and support.
- Contact your bank or credit union, they'll usually have plenty of advice and resources.
- Contact a family member, friend, or trusted neighbor.



- Don’t share your phone number or email address unless you really have to.
- Use call screening or verification. They’re not perfect, but they can help.
- If you get repeat messages from the same number, learn how to block it.
- Don’t be panicked and especially if it appears to be your bank or credit union. Call the number on their website to double check.
- Don’t trust your caller ID – it can be spoofed to look legitimate.
- Create a family code word or phrase in case someone contacts you pretending to be a family member.



Our website has lots more information about how to do many of the things suggested above.

Visit us at LetsGetThereFirst.com →

General Security Tips

01

Focus on protecting your money and your bank account - start by talking to family members or trusted friends about how you can do that.

02

Talk to your bank and credit union about what security mechanisms you can put in place to prevent people from taking out money.

03

Only carry your ATM card with you when you think you'll need it. Otherwise leave it at home.

04

Pay using your credit card and not a debit card or check. A credit card has much better protection.

05

Freeze your credit reports. It's easy and it's free and it doesn't hurt your credit. And you can unfreeze at any time, also free.

06

Close any credit cards you don't need or are not using.

07

Consider banking online or getting e-statements instead of paper statements. Banking online gives you greater control over your accounts, and e-statements can't be intercepted in the mail like paper ones.

08

Consider using a password manager to make it easier to create complex passwords and protect them.

09

Keep the master password to your password manager written down and hidden somewhere in the home.

10

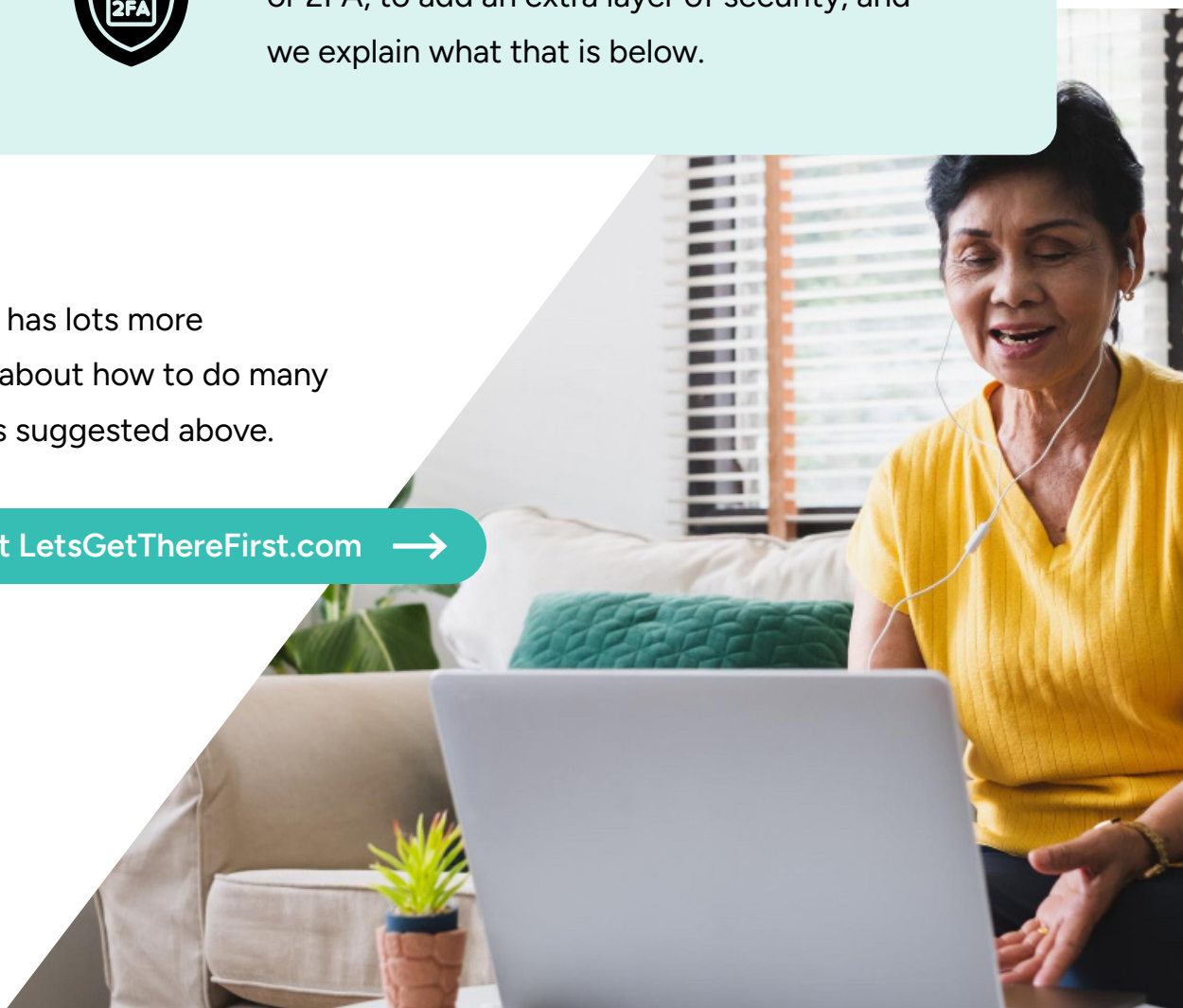
If you're not comfortable using a password manager, write your passwords down and hide them amongst old documents, like old high school photos. See our tips on passwords below.

11

Avoid anything to do with an investment or the word "crypto."

12

Use something called 2 Factor Authentication, or 2FA, to add an extra layer of security, and we explain what that is below.



Our website has lots more information about how to do many of the things suggested above.

Visit us at LetsGetThereFirst.com →

Banking Security Tips

01 Get to know your bank or credit union personally if you can. The better they know you personally, the greater the chance they'll spot something suspicious on your behalf.

02 Ask them to explain, and apply, any security measures they have in place. This can include:

- Preventing larger amounts of money from being transferred, and especially to a stranger or another country.
- Requiring that you show up in person to make any larger transfers.
- Alerting you to any attempts to change a password or email address or add another name to your account.
- Sending you an alert whenever there's a transaction above a certain amount, like more than $50.

03 Make sure you have a very strong password for any financial accounts, and that you don't use it anywhere else.

04 Ask that they enable something called 2 Factor Authentication on your account, and we have a separate tip sheet that explains how this works.

05 Add a trusted contact to your account.

Security Tips About Caregivers

Seniors and the elderly lose billions of dollars every year, often their life savings, to scams and frauds. And sadly, many of these crimes are committed by trusted insiders like relatives, neighbors, and even caregivers.

Tips to protect yourself from caregivers include:

- Only hire or use a caregiver who comes highly recommended.
- If possible, vet the caregiver by enquiring with previous employers.
- Consider running a criminal background check.
- Be alert for any unusual behavior or questions by your caregiver, and especially about your finances.

- Protect your personal information and especially bank and credit card statements, your Social Security Number, tax returns and information, and correspondence with your bank.
- Don’t leave passwords where they can easily be discovered.
- Don’t keep large amounts of cash around the house.
- If you’re worried, share your concerns with a trusted family member or neighbor.
- Call the AARP Fraud Watch Network Helpline at 877-908-3360. It’s a free service and you don’t have to be an AARP member.

Tips About **Passwords**

Because of advances in crime tools and especially the use of AI, passwords are becoming more vulnerable to being guessed or cracked.

A simple solution is something called a password manager, but not everyone is comfortable using tools like these. There is a good and often safer alternative.

It's called a passphrase, a phrase that you can make up based on something about you and something you know, and that no one outside your inner circle would know.

You can even write your passphrases down in a way that looks like nothing more than some fun memory exercises.

And by using passphrases you can make them as long and complex as you want and without having to remember them. Just don't forget where you put them!

Here's a passphrase example:

> "Christine graduated from Clermont High in the Summer of 1982, and then took a year off."

By taking the first letter in every word, and including the numbers, you now havea password with19 upper and lower case letters, as well as some numbers..

That means you get "CgfCHitSo1982attayo" and if you include the comma, that can make the password even harder to guess. That password would take hackers many centuries to crack – and hopefully you'll have changed it by then!

Or

> "Tom got his first job working at Wells Fargo in Chicago in the Fall 1971 and his first paycheck was $127.80."

That's a massive 30 characters and includes numbers and symbols.

Or

> "Don't forget to tell them the story of when Dad fell in the lake, I think in 92 - We all laughed so hard!!!."

Upper and lower case letters, numbers, and even symbols or special characters. You get the idea.

About Two Factor Authentication

Two factor authentication, or 2FA, sounds like a complicated mouthful but it's very easy once you think about it a little. In most cases it means that you opt in to having your account, like your bank or credit union, send a short code – 4 or 6 numbers - to your phone or your e-mail any time you want to log in to your account.

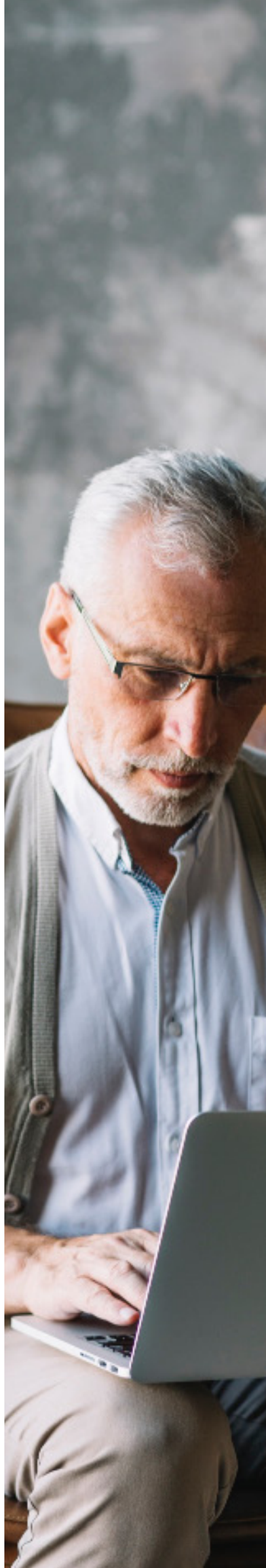
You simply respond with the code they send you and that's it, you're in. The challenge for hackers is if they don't have your phone in their hands, they can't receive that code and the bank will not allow them in.

It's not foolproof but it's widely regarded as one of the best ways to add a vital extra layer of security to your password. So we recommend using 2 Factor Authentication every time it's offered.

Two factor authentication is not only available through your bank or credit union, but probably from every other site or service that you use including your e-mail, your investment accounts, government accounts like the IRS or Social Security Administration, and even your favorite online streaming accounts like Netflix or Amazon.

Just be very wary of scams calls that claim to be from something like your bank or credit union, telling you there's a security problem, and asking you to confirm a code they send.

If you get such a call or text, politely hang up and contact your bank or credit union directly.



About this Guide

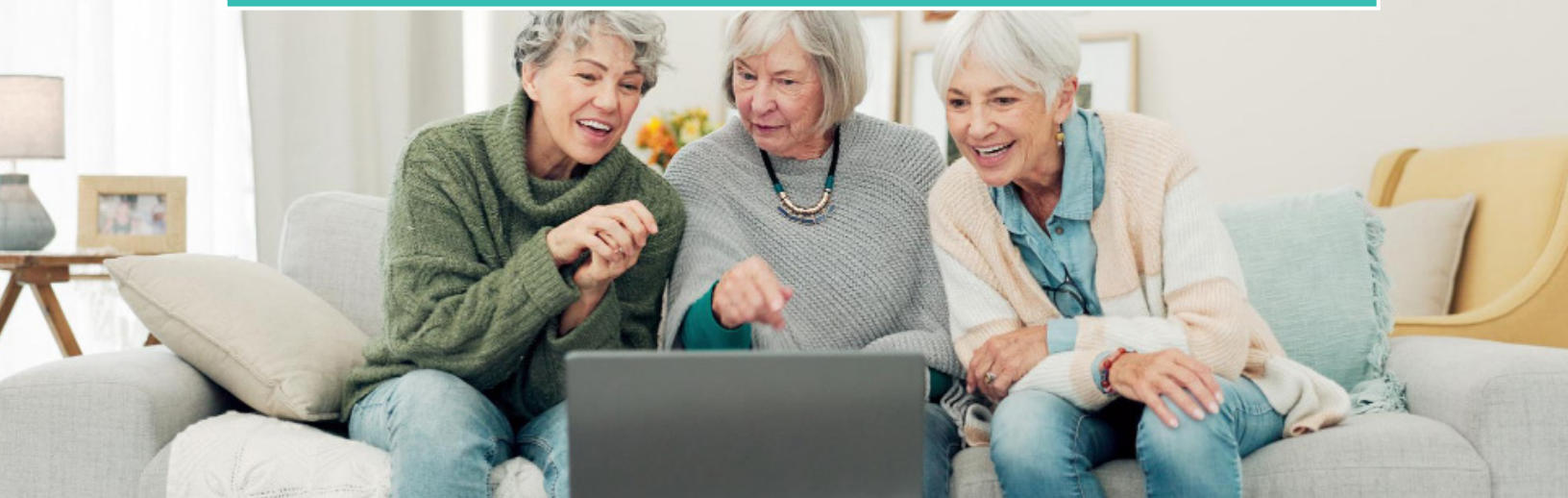
This guide was created by Let's Get There First, a security awareness initiative driven by America's real estate community.

LOOKING FOR MORE HELP WITH FRAUD AND SCAMS?

Check out the AARP FraudWatch website at www.aarp.org, where you can speak with a fraud expert, gets tips and advice, and sign up for security alerts. And it's all free.

Worried about identity theft? Visit the Identity Theft Resource Center (www.identitytheftcenter.org) where you can speak to a fraud counsellor, learn how to prevent identity theft, and get help if you're a victim.

- AARP Fraud Hotline 877-908-3360
- Identity Theft Resource Center victim assistance hotline 888.400.5530



BROUGHT TO YOU BY

The Tammy Ernhardt Real Dream Team

"I'm so delighted to be your local supporter of Let's Get There First!, and also an active and licensed real estate professional in this great community for more than a decade.

Always reach out to me for any questions about your real estate needs."

Tammy Ernhardt

Tammy Ernhardt | Licensed Realtor since 2015

(123) 456 7890

me@myemail.com

VISIT US AT

www.MyGreatWebsite.com