WELLS FARGO Wealth & Investment Management

Recognizing a scam can help you avoid becoming a victim

10 things you can do to help protect yourself from scammers

10 ways to help protect yourself

The Federal Trade Commission (FTC) estimates that older adults lose more than $7.1 billion a year to financial scams. By following these 10 practices, you can help protect yourself and your loved ones:

1. Spot imposters

Scammers often create fake profiles, pretending to be someone you can trust. Don't respond, send money in any form, or give out personal information in response to an unsolicited request via text, email, or phone. Be especially wary of gift card, cryptocurrency, or other unusual payment requests, which are usually scams.

2. Be tech security savvy

Use strong passwords, biometric authentication, and 2-Step Verification at Sign-On. Update security patches and antivirus software. Don't share passwords, PINs, or one-time passcodes if you didn't initiate contact. Don't purchase software/services from unsolicited calls or emails, give control of your computer to anyone, or give personal information to someone claiming to be tech support.

3. Don't believe your caller ID

Scammers can fake caller ID names and numbers, so what you see may not be real. Verify the identity with your contact lists or with something only the real person would know. Block unknown callers. If you think the caller is legitimate, call the company on a number you know to be true to verify.

4. Hang up

If you answer the phone and hear a recorded sales pitch, hang up immediately. Scammers can record your voice and use it to impersonate you for future scams and other criminal activity.

5. Don't pay upfront for a promise

Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, or a job. They might even say you've won a prize, but first you must pay taxes or fees. This is most likely a scam.

6. Be cautious how you pay

If you send money to a scammer, it's unlikely you'll get your money back. Treat sending money with Zelle®[1] or other digital payment apps like sending cash. **Tip:** Legitimate organizations don't request reloadable cards, wires, gift cards or cryptocurrency as payment methods.

7. Slow down. Talk to someone you trust.

Before you give up your money or personal information, slow down and talk to someone you trust — con artists want you to make decisions quickly. They might even threaten you. Don't be pressured. Slow down and check out their story thoroughly.

8. Be skeptical about free offers

Some companies use free trials to sign you up for products and bill you every month until you cancel. Always review your monthly statements for charges you don't recognize and cancel any recurring charges immediately.

9. Don't deposit a check and send money back

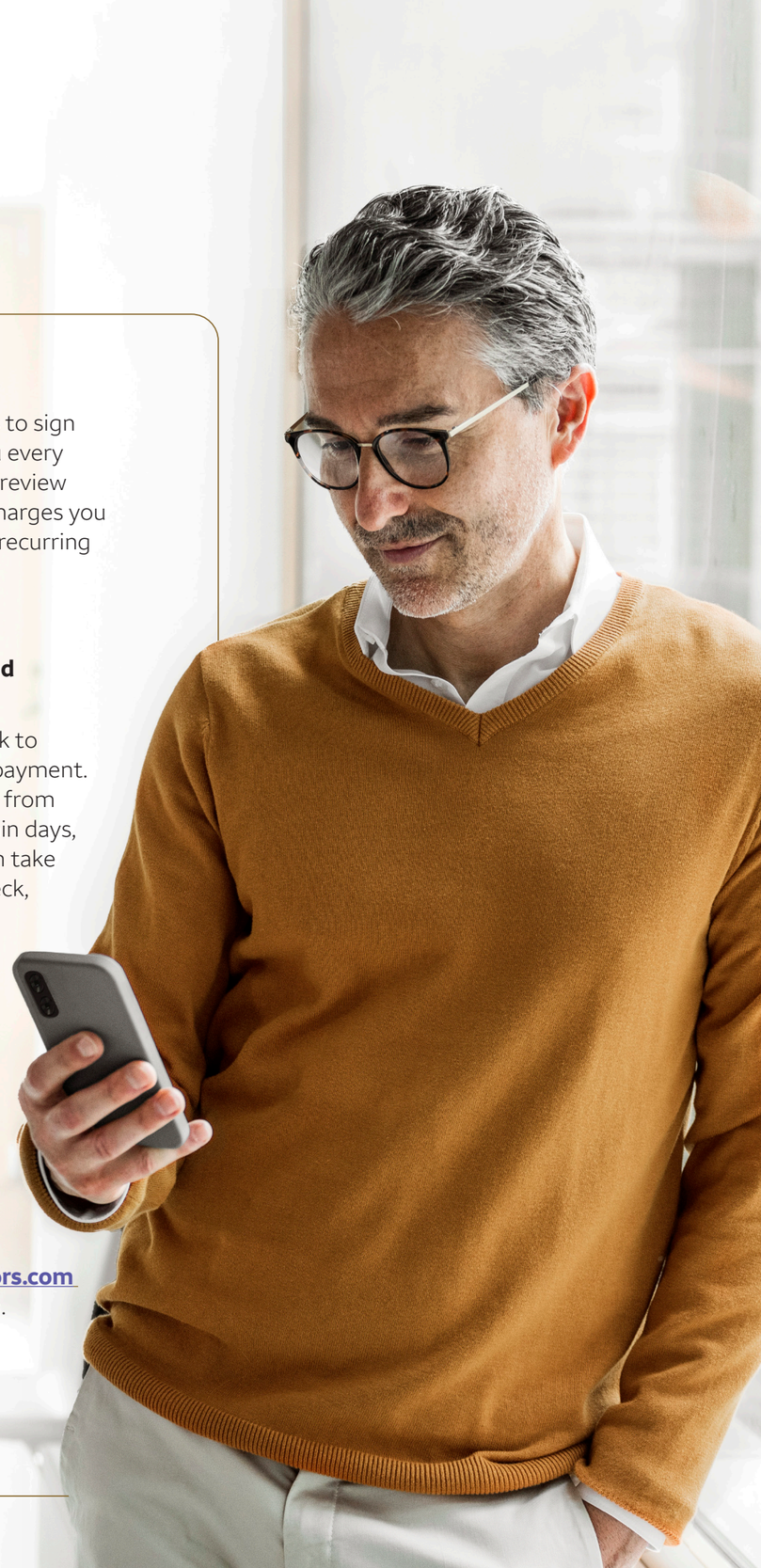
Scammers may give you a check to deposit then ask you to wire a payment. By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If you deposit a fake check, you're responsible.

10. Be informed

Subscribe to free Consumer Alerts at **ftc.gov/scams**.

Remember, you are in charge when it comes to your money.

For more information, visit **https://www.wellsfargoadvisors.com** and search for scam prevention.



Report fraud to Wells Fargo

Zelle®/Wires/Online Fraud
866-867-5568

Credit Card
800-642-4720

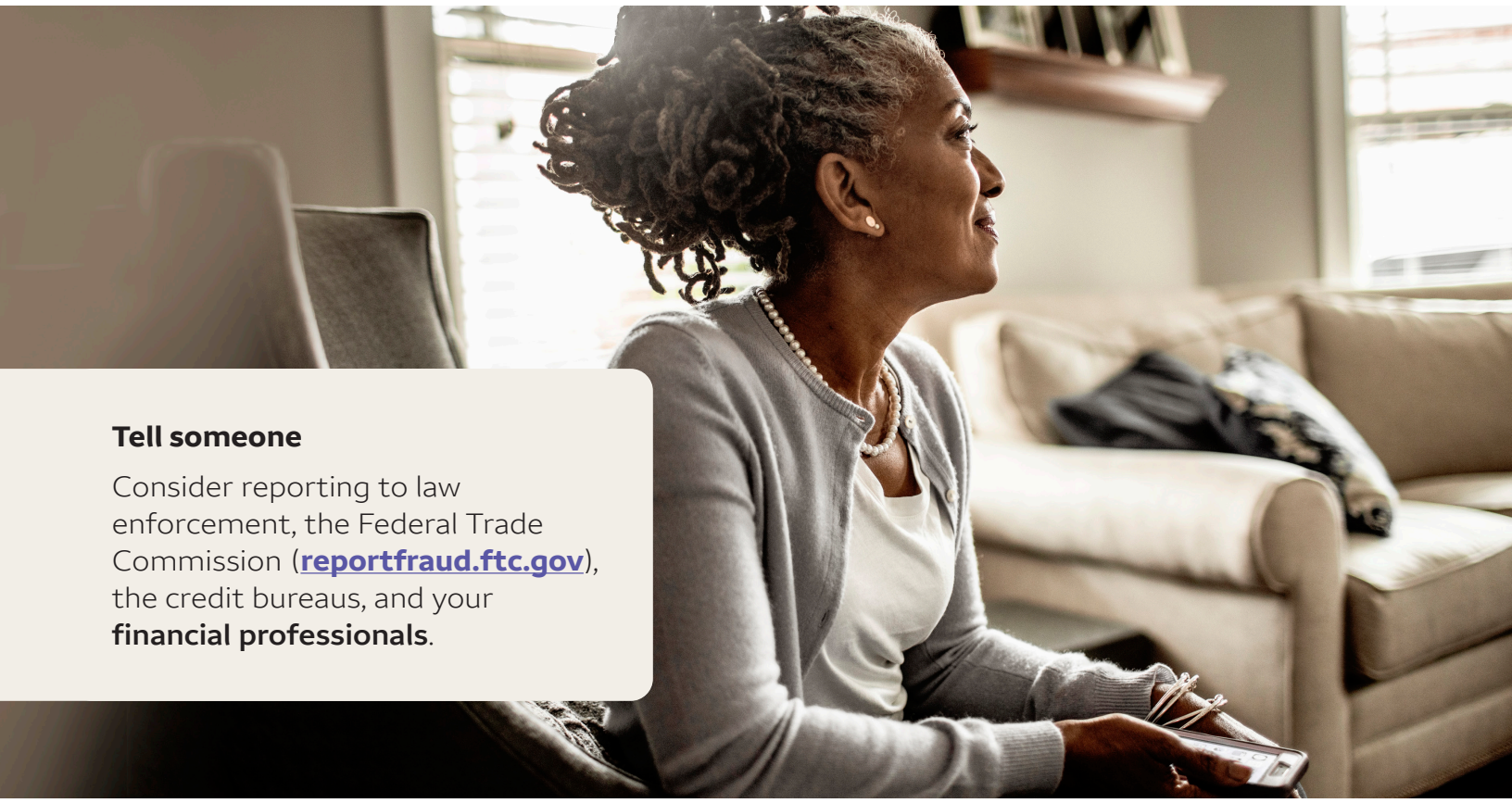
Checking
800-869-3557

Small Business accounts
800-225-5935

Phishing email/text messages
reportphish@wellsfargo.com

Phishing/bank imposter phone calls
reportimposter@wellsfargo.com

Identity Theft
800-869-3557



Tell someone

Consider reporting to law enforcement, the Federal Trade Commission (**reportfraud.ftc.gov**), the credit bureaus, and your **financial professionals**.

1. Enrollment with Zelle® through Wells Fargo Online® or Wells Fargo Business Online® is required. Terms and conditions apply. U.S. checking or savings account required to use Zelle®. Transactions between enrolled users typically occur in minutes. For your protection, Zelle® should only be used for sending money to friends, family, or others you trust. Neither Wells Fargo nor Zelle® offers purchase protection for payments made with Zelle® - for example, if you do not receive the item you paid for or the item is not as described or as you expected. Payment requests to persons not already enrolled with Zelle® must be sent to an email address. To send or receive money with a small business, both parties must be enrolled with Zelle® directly through their financial institution's online or mobile banking experience. For more information, view the Zelle® Transfer Service Addendum to the Wells Fargo Online Access Agreement. Your mobile carrier's message and data rates may apply. Account fees (e.g., monthly service, overdraft) may apply to Wells Fargo account(s) with which you use Zelle®.