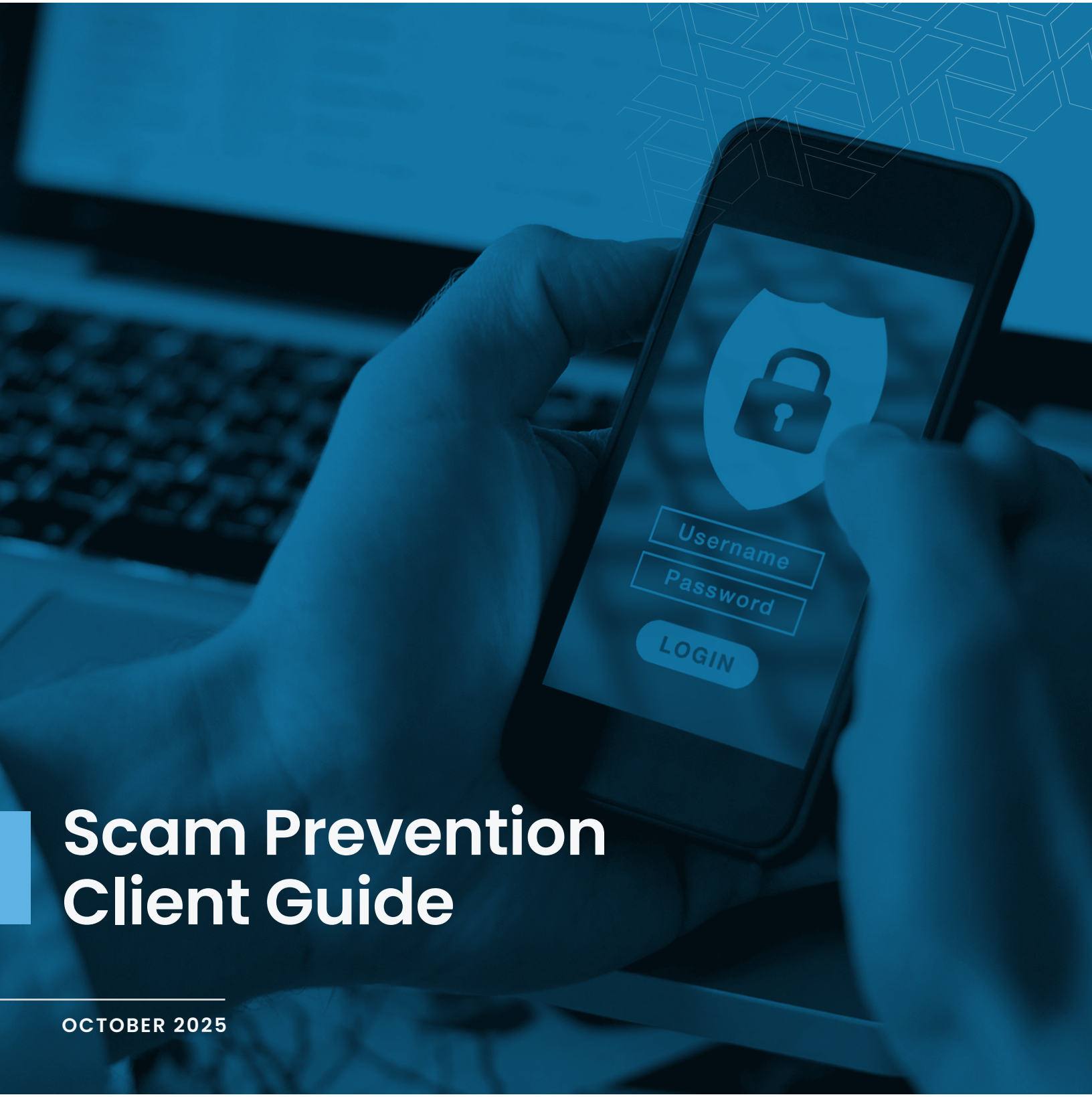
moneywise
FINANCIAL ADVISORS



Scam Prevention Client Guide

OCTOBER 2025

Safeguarding your assets and data is our highest priority. But staying safe online goes beyond our systems—it's also about being aware of potential threats in your everyday digital interactions. Whether you're checking personal email, scrolling through social media, or using dating apps, scammers are constantly devising tactics to steal your information or assets.

To help you stay one step ahead, we've created this guide. Inside, you'll find:

- A clear explanation of common scams
- Key warning signs to watch for
- Practical steps to take if you ever become a target

By staying informed, practicing smart online habits, and remaining vigilant, you play a vital role in protecting yourself—and we're here to support you every step of the way.

Types of Scams

Romance Scams | 02

Sweepstakes Scams | 04

Government Impersonator Scams | 06

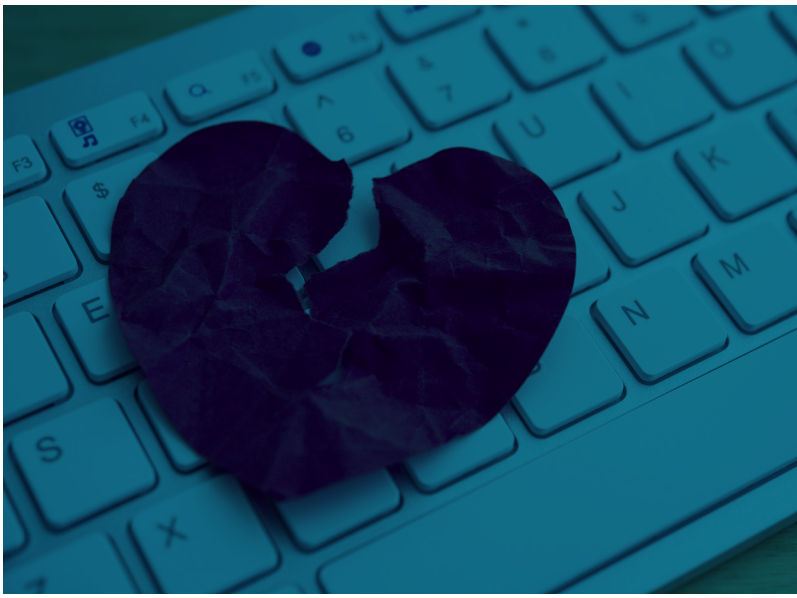
Tech or Fraud Support Scams | 08

Real Estate Scams | 10

Business Email Compromise | 12

Investment Scams | 14

Romance Scams



Seeking romance online can have a major downside: the internet is rife with scammers ready and willing to take advantage of people looking for love. According to a recent study, as many as 10% of online dating profiles are fraudulent.[1]

In addition to using online dating profiles, scammers have been known to initiate contact through more general platforms that have messaging or chat features, including social media and gaming sites. These types of schemes avoid in-person interactions, preferring instead to focus exclusively on messaging apps and other online channels.

The scam works something like this: Your romantic interest may claim to live in another part of the country or to be abroad for business or military deployment. They seem to be really interested and eager to get to know you. They work to cultivate an emotional attachment by:

- **Asking a lot of personal questions to help prepare responses that appeal to you;** for example, "Are you interested in a lifetime relationship?"
- **Quickly urging you to communicate through personal email or text** rather than a monitored channel like messaging through a dating app.
- **Lavishing you with attention and often professing love very early in the relationship** or claiming to have no immediate family, sometimes mentioning the loss of a loved one.

Once an emotional attachment is established, the scammer is eager to meet you in person. When the opportunity arrives, however, something invariably comes up—an accident, a health crisis, or other such unexpected occurrence; that is usually followed by an urgent request for financial assistance. For example, the scammer may claim to be stranded or detained, needing to pay a medical bill, or unable to meet an expense related to a quick business payout. If you can help out, they will pay you back as soon as they're out of the current circumstances.

The scammer then instructs you to send money, promising a quick payback. But there is no return of funds, and, in some instances, they ask for yet more money.

[1] besedo.com/blog/welcome-to-the-age-of-fake-dating-profiles/

HOW TO PROTECT YOURSELF

- Be wary of any profiles set up recently.
- Right-click and use your browser's search feature to see if the person's profile picture was copied from somewhere else on the internet, if the person is known by more than one name, or if the photo has been associated with other fraud or scam claims.
- Take things slowly, asking plenty of questions and noting any inconsistencies or red flags. If they are unwilling to meet in person or speak on the phone, that can be cause of concern.
- Use caution when sharing personal information with someone you only know online.
- Ask a friend, family member, or another trusted individual if red flags arise. Be willing to listen if they express concern.
- Do not send money or gift cards or accept money or gift cards on behalf of an individual you have never met in person.

QUESTIONS TO ASK YOURSELF

- Is this too good to be true?
    - It's possible that if the person asks many questions about your likes and interests and agrees or shares each one with you, it may be a scam.
- Do you know the recipient of funds and have I met them in person?
    - In many romance scams, the victim has never met the scammer face-to-face and the scammer refuses to meet in person.
- Have they requested funds in the past?
- When they are requesting funds, is it an "emergency" need or situation that caused the financial need?
    - A scammer may send a video or picture of an accident or other event to lend credibility.

If you answered yes to any of the above questions, cease communication with the individual and discuss the potential fraud with your advisor.



Sweepstakes Scams

Too Good to be True? It probably is.

Who wouldn't be thrilled by the idea of winning a million dollars, a luxury car, or a dream vacation? Scammers know this—and they exploit those hopes by mimicking legitimate sweepstakes and contests.

These fraudsters may reach out via mail, email, social media, text, or even a phone call, congratulating you on your "big win." But there's a catch: to claim your prize, you're asked to pay a small fee—supposedly for taxes, shipping, or customs.

They might also request personal details to "verify your identity" or banking information to "deposit your winnings." In reality, this is how they gain access to your accounts and steal your money.

Stay alert: if it sounds too good to be true, it probably is.

If you suspect a sweepstakes scam report it to the Federal Trade Commission at ReportFraud.ftc.gov



HOW TO PROTECT YOURSELF

- Ask yourself if you entered a particular contest. If you didn't, the prize notice is likely false.
- Don't wire money, mail cash, checks, or money orders, or share gift card numbers with someone claiming to represent a sweepstakes or lottery. A legitimate contest would not ask you to pay to collect your prize.
- Don't deposit a check from a sweepstakes or lottery without doing due diligence, such as researching the sender's name on the Better Business Bureau website to validate the source of the request. Also note that many scams will ask you to send part of the payment back. Legitimate sweepstakes send only certified checks to prize winners.
- Don't provide personal or financial information to anyone who contacts you about a lottery prize.

QUESTIONS TO ASK YOURSELF

- Is there a sense of urgency or a strict deadline to redeem the prize?
- Did I enter a sweepstakes or lottery?
- Was I told that I must pay (a small fee) in advance to get the prize?
- Did I receive any advance payment in paper form, such as a check or money order?

Government Impersonator Scams

This type of scam is when a criminal pretends to be from a government agency like the Social Security Administration (SSA), the Internal Revenue Service (IRS), or law enforcement. The criminal attempts to intimidate you into paying a fine or penalty that you supposedly owe to the government.

Initial contact may be through email, text message, or social media, but usually these scams start with a simple phone call. The scammer advises you to act immediately or you will suffer the loss of a benefit or even face a large fine or criminal charge. The scammer then may become aggressive and may threaten to confiscate property, freeze bank accounts, or send authorities to arrest you.

SSA and Medicare scams

Scammers in this type of fraud claim that unless you pay immediately, your Social Security or Medicare benefits will be suspended. They often request personal information such as your Social Security or Medicare number to steal your identity while they are scamming money out of your pocket.

To be clear, the SSA and Medicare will not threaten to end your benefits, nor will they suspend your personal ID number.

IRS impersonators

Scammers in this type of fraud will claim you owe taxes and use threats of arrest or deportation if you do not pay immediately. They may also claim that your driver's or professional license will be revoked if you fail to cooperate. Often times they attempt to appear more legitimate by pretending to have information about you, including your Social Security number of tax ID number.

The IRS communicates primarily through mail, including cases with delinquent taxes. The IRS never demands immediate payment, nor do they make threats to call the local police.

Law enforcement impersonators

Scammers in this type of fraud will claim to be with your local court, sheriff's office, or police department and claim you missed a court date, failed to appear for jury duty, or have delinquent taxes or unpaid tickets. They may threaten you with fake infractions, such as a warrant for your arrest if they do not receive immediate payment.

Law enforcement agencies do not call individuals and demand money, nor do they accept gift cards as payment. To report a Medicare or Social Security scam contact the Officer of the Inspector General.

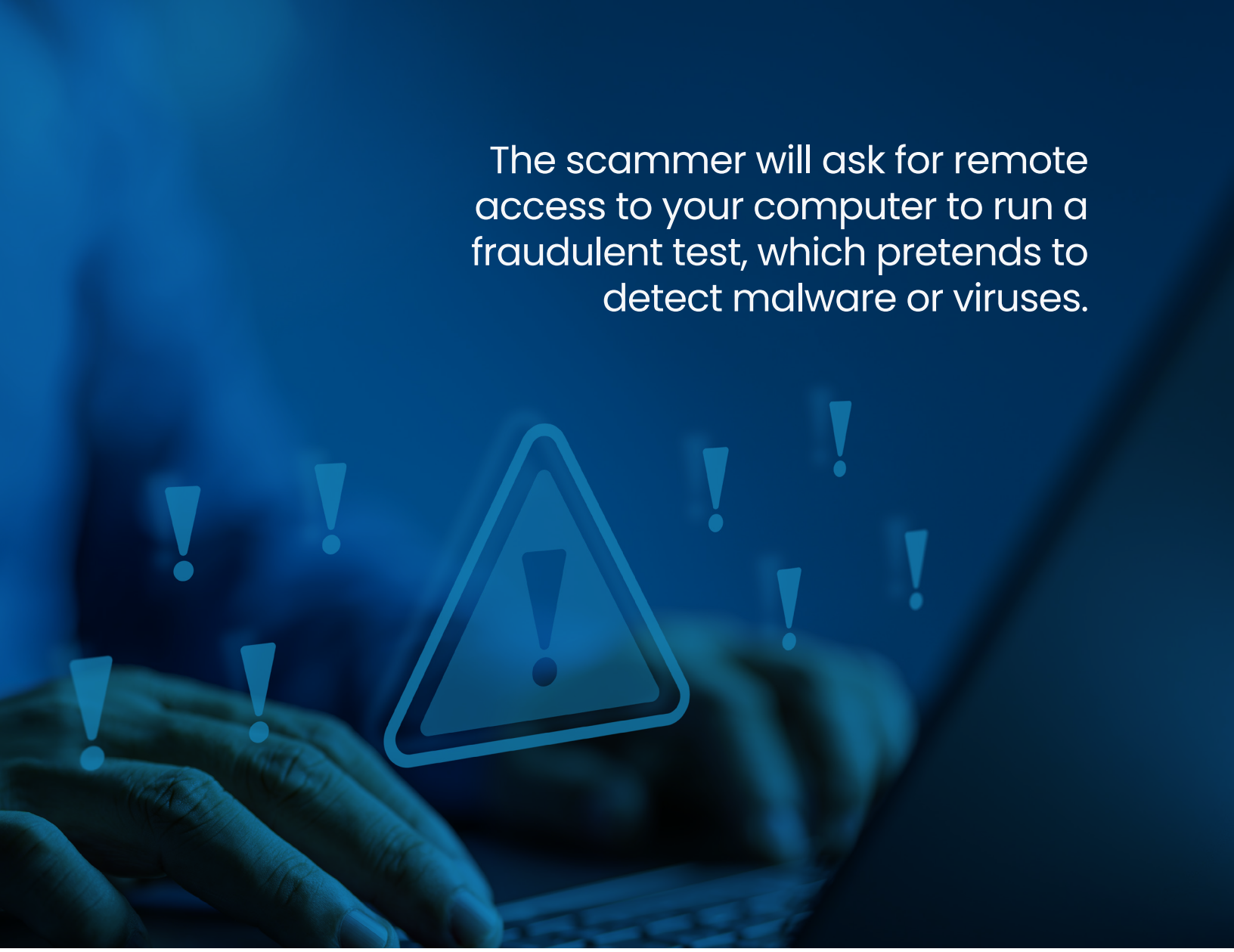
HOW TO PROTECT YOURSELF

- Never wire money, mail cash, or use gift cards or cryptocurrency to pay someone who claims to be from a government agency. These methods are often used by scammers because they are hard to track and almost impossible to get your money back.
- Do not give your personal or financial information to anyone claiming to be from a government agency. Call the agency directly to confirm if it's a scam.
- Do not trust your caller ID, as these can often be spoofed with the names and numbers of government agencies.
- Do not click on any links in unexpected emails or texts from someone claiming to be from a government agency. Report to the real government agency and delete the message.

QUESTIONS TO ASK YOURSELF

- Did you call the person from the number they provided? Can you find the same phone number on the government agency's website?
- Was there a sense of urgency for the payment or a threat if the payment wasn't made?
- How did they contact me?
- Did I click on any hyperlinks in an email or text message?





Tech or Fraud Support Scams

Scammers often will pretend to be from reputable companies like Apple, Microsoft, or Amazon, claiming to help you with some tech support or an issue with your account. They may often pretend to be from security software companies such as Norton or McAfee reaching out to help you with a “virus” on your computer. The storyline varies but the tactics are similar.

Tech Support scam

Scammers in this type of fraud will start with an unsolicited phone call or pop-up warning on your device. The scammer will ask for remote access to your computer to run a fraudulent test, which pretends to detect malware or viruses. After the pressure and scare tactics, the scammer will make you pay for the fraudulent repairs, new software, and other unnecessary products.

The scam can involve a claim that you are due a refund for a canceled subscription service,

one you likely do not recall signing up for. The scammer may request (and steal) your credit card number, then use remote access to install actual malware that will continue stealing your information and funds.

Fraud Support scam

Scammers pretending to be fraud support may start with an unsolicited phone call or email claiming a charge on your account. Once you deny the charge, the scammer may claim that they can assist you in getting a refund. They request access to your computer and have you sign into your bank account to "deposit" the refund. However, once you log in, the scammer may steal your money or credentials and could even claim you requested too much and you have to pay them back—usually via wire, cryptocurrency, or a gift card.

Remember: these are often preferred forms of payment by a scammer because they are hard to trace and almost impossible for you to get your money back.

HOW TO PROTECT YOURSELF

- Do not give remote access to your computer or payment information to an unsolicited caller.
- Do not rely on caller ID as the scammer can look like they are calling from a legitimate number or company.
- Do not call a number on a pop-up virus alert.
- Do not click any links on a pop-up, even a prompt to "close the window".
- Only purchase security software from a reputable, well-known company.
- Do not provide your financial information to someone who calls a few days, weeks, or months after you've made a purchase. If they ask for your financial information, it is probably a refund scam.

QUESTIONS TO ASK YOURSELF

- Did I click any links or navigate to any websites per their instructions?
- Did the caller mention any consequences if the problem was not resolved?
- Did I provide my login ID or password to allow others to view my information?

Real Estate Scams

In this type of scam, during the closing process of a new home purchase scammers may send a spoofed email to the homebuyers, posing as the real estate agent, settlement agent, legal representative, or another trusted individual with false instructions for wiring closing funds. Often, these scams are not caught in time because of the sense of urgency and pressure applied during the closing process.

Scammers often employ different strategies during the closing process to carry out a real estate scam, including but not limited to:

- Monitoring the victim's email inbox to watch for upcoming real estate transactions and intercept communication with title/escrow agents.
- Compromising the email address of the title/escrow company that sends the wire instructions.
- Providing phony contact information on correspondence.
- Fraudulently establishing accounts in the name of the title/ escrow agent or law firm.
- Using phishing to install malware onto the victim's devices.

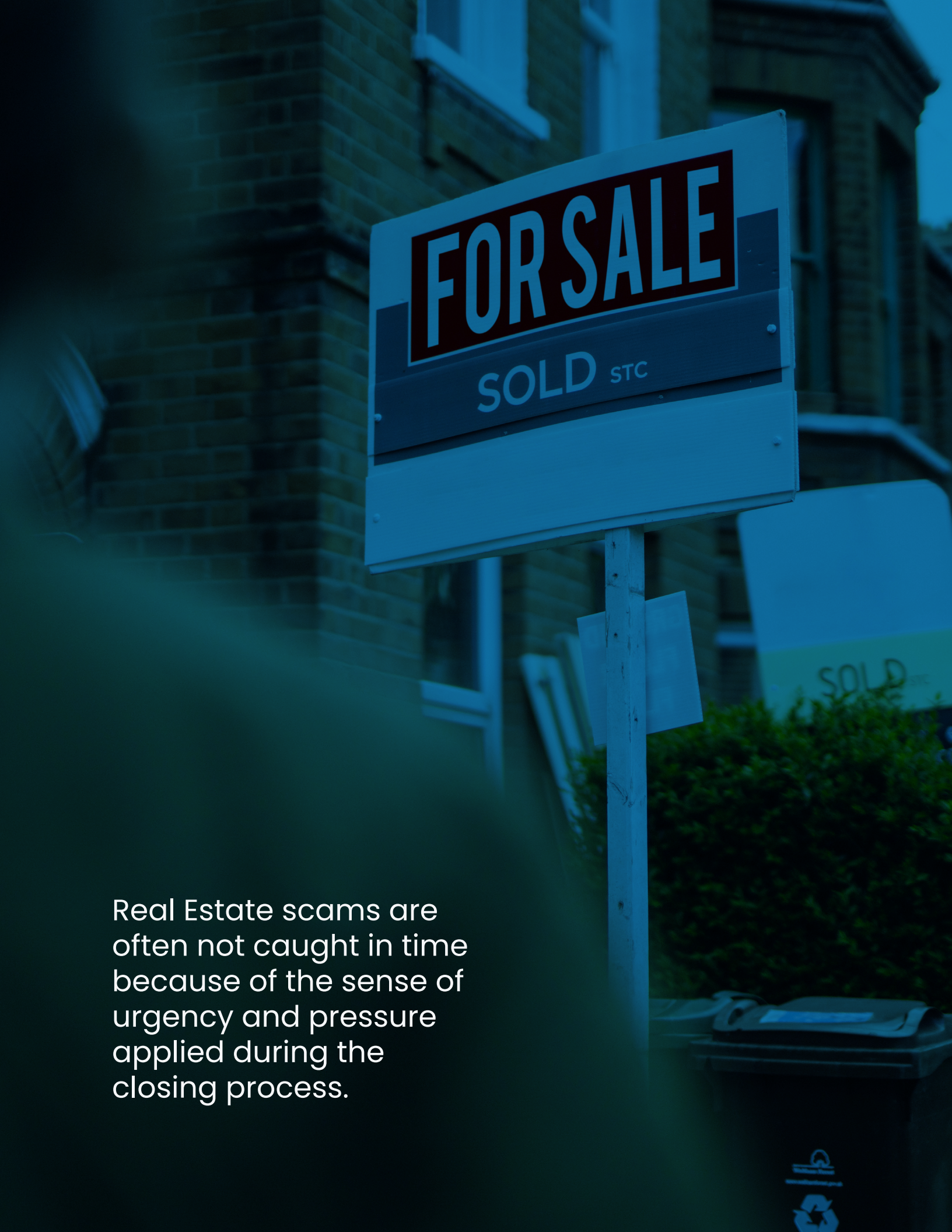
Always verify wire instructions verbally with an outbound call to the title company after searching for a phone number online. Try not to call the number provided in an email as it may be spoofed and direct you to a scammer.

HOW TO PROTECT YOURSELF

- Whenever possible, verify closing instructions in person, and if not, call the title/ escrow company outbound from a number not provided via email.
- Verbally verify payment instructions and any changes to an account number with the person making the request.

QUESTIONS TO ASK YOURSELF

- Have I wired to the specific account before? Did the title/escrow company acknowledge receipt of the funds?
- How did I receive the wire instructions?
- Did I verify the wire with the phone number found on the title/escrow company's website?
- Did I see the property in person with a registered real estate agency/broker?



Real Estate scams are often not caught in time because of the sense of urgency and pressure applied during the closing process.

Business Email Compromise

A business email compromise is possibly one of the most financially damaging online crimes because it exploits the fact that many of us rely on email to conduct business, both personal and professional.

In a business email compromise scam, scammers will send an email message which appears to come from a known source making a legitimate request. For example:

- A regular vendor sending an invoice with an "updated" mailing address.
- A request from an "executive" asking to purchase dozens of gift cards to send out as employee rewards. The "executive" then asks for the serial numbers so they can email them out right away.
- A client who is in the process of purchasing a home receives a message from the "title company" with a change in wire instructions for the down payment.
- A direct deposit request from a "payroll representative".

How scammers carry out a business email compromise

- **Spoof an email or website.** Scammers often use small variations of a legitimate website, often unnoticed, to fool you into thinking that fake accounts are authentic (i.e. service@paypals.org vs. service@paypal.org).
- **Send spear-phishing emails.** Messages appear to be from a trusted sender to trick you into revealing confidential information, enabling criminals to access company accounts, calendars, and data that give them the details they need to carry out the business email compromise schemes.
- **Use malware.** Malicious software, installed through a fraudulent link, can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information can then be used to send messages or time payment requests so that accountants or financial officers don't question their legitimacy. Malware also allows criminals to gain undetected access to your data, including passwords and financial account information.

HOW TO PROTECT YOURSELF

- Verify payment and purchase requests in person, if possible, or call the person at a number known to you.
- Verbally verify any change to an account number or payment instructions with the person making the request.
- Be careful what you share on social media. By sharing pet names, schools attended, links to family members, or birthdays, you give scammers all the information they need to guess your passwords or answer security questions.
- Scrutinize email addresses and URLs in correspondence.
- Set up two-factor authentication where possible.

QUESTIONS TO ASK YOURSELF

- Do I personally know the sender?
- Did I check for minor spelling errors in the email?
- Is the information requested something the sender should already know?
- Was there a change in the original instructions?
- Did I call the sender to confirm the request or information after receiving the email?
- Did I click the link or go directly to the official website?
- Was I expecting an attachment?





Investment Scams

This type of scam involves the promise of a "once in a lifetime opportunity" that can double or triple your money in a short time, followed by promises of high returns with little risk. Sounds perfect, right? This is often how an investment scam is started, by touting incredible gains, breakout stocks, huge upside, and minimal risk. Financial manipulation schemes often lure individuals into investing their own money in seemingly legitimate and profitable ventures. Scammers gain trust, manipulate emotions, and exploit financial vulnerabilities to steal money.

How bad actors carry out investment scams

- **Scammers make contact through a call, a text, an email, or a social media message.** They may send you a friend request or claim to know you through a "mutual" party.
- **Scammers spend weeks or months building a relationship with you,** often feigning romantic interest. They engage in frequent, friendly communication, showing interest in your life, and sharing personal stories to create a false sense of intimacy. They do not initially bring up anything about money or investments. They may use "mirroring" techniques to match your language, interests, and beliefs to create a sense of connection and familiarity. Scammers may sometimes even send small gifts or tokens of affection to gain your trust and emotional investment.
- **The scammer then encourages you to pay through wire transfer or cryptocurrency.** They may use websites that make it appear that your money has actually been invested and is earning the promised returns.
- **For claims of an offshore investment, the scammer wants you to transfer the funds overseas,** knowing that once the money is out of the country, it is more difficult for U.S. law enforcement to assist you in getting it back.
- **Investment scams often use fake images and impressive yet fraudulent investment portfolios** to convince you of the legitimacy of their schemes. Once you are hooked and have invested a significant amount of money, the scammer suddenly disappears, leaving you no way to contact them to recover your funds.



HOW TO PROTECT YOURSELF

- Be cautious of unsolicited messages and group chats.
- Don't give in to pressure to invest immediately, and don't be influenced by promises that seem too good to be true.
- Be skeptical of investments with promises of high returns and low risks. Don't invest just because the person offering the investment seems nice, trustworthy, or has professional titles.

QUESTIONS TO ASK YOURSELF

- Do I know the person who contacted me? Did I recognize the phone number?
- What research have I performed on the broker and/or firm that contacted me?
- Was I promised a certain return or high profits? Was it mentioned that this offer is available only for a limited time? Was there an aspect of "everyone is doing it"?
- Was I given investment details, such as a prospectus and performance history, in writing?
- Were there any misspellings or unusual things about any documents or correspondence?

As a reminder, if you are ever suspicious of any situation like the ones discussed here, please call us. We are eager to help you, especially when it comes to your security.

For additional information about protecting your money and investments, please reach out to your advisor.

DISCLOSURES:

For educational purposes only. The information provided is general in nature and is not intended to be, nor should it be construed as, specific scam prevention, personal information protection, cybersecurity advice, or legal advice. The content does not purport to present a complete picture of scam prevention, but we believe the information is representative of issues and needs facing some clients. Because of the many variables involved, an individual should not rely on the information herein alone.

Nothing contained in this presentation may be relied upon as a guarantee, promise, assurance, or representation as to the future and the ability to protect and prevent against potential scams, cybersecurity incidents, vendor system breaches, compromise of firm security, and/or improper access to confidential information. Individuals should seek advice from industry professionals and other advisors before undertaking actions in response to the matters discussed. Representatives and organizations may provide tools, resources, and processes that vary from the information described herein. The appropriateness of any particular prevention method will depend on each individual's personal circumstances. The information is not designed to guarantee or protect against potential scams, cybersecurity incidents, vendor system breaches, compromise of firm security, and/or improper access to confidential information.

Certain statements contained in this document may be forward-looking statements. Forward-looking statements necessarily involve risks and uncertainties, and undue reliance should not be placed on them. There can be no assurance that forward-looking statements will prove to be accurate, and actual results and future events could differ materially from those anticipated in such statements. This is prepared using third party sources considered to be reliable; however, accuracy or completeness cannot be guaranteed. The information provided will not be updated any time after the date of publication.

©2025 Focus Partners Advisor Solutions, LLC. All rights reserved. RO-25-4848233

SOURCES:

Charles Schwab & Co.

https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business

https://www.ipsos.com/en-us/nearly-1-3-americans-report-being-victim-online-financial-fraud-or-cybercrime#:~:text=Nearly%201%20in%203%20Americans%20(31%25)%20report%20being%20a,18%2D34%20(22%25)