

2. Payment Scams

Before Paying a contractor for work at your home, investing in a company or purchasing a new property, a fraudster intercepts the email communication and replaces legitimate payment instructions with fraudulent ones. Red flags include last-minute changes to instructions, a change in the tone or word choice from prior emails, a new sender address and multiple payment requests. With this scam, the email account belonging to you, the service provider or both has been compromised.

3. Computer Scam

Someone calls pretending to be from a major tech company and says that your computer has a virus. They offer to get rid of it by asking you to log into a website that lets the caller control your computer. The caller can then steal your ID information and can gain access to your accounts.

4. Grandchild/child scam

Your grandchild or child calls and frantically requests money to pay a kidnapper, a legal bill or an emergency medical expense - and begs you not to tell anyone. But it's not real: Fraudsters commonly pose as loved ones and , preyin gon you compassion, claim to need money urgently. Recent technology can even allow them to successfully imitate your loved one's voice.

5. Charity scam

You donate to one charity and end up on every charity list. That's because they sell your name, phone number and email to other nonprofit and commercial organizations. These could include companies with similar names to charities you support - but they exist solely to scam donations.

6. Lottery scam

You get an unsolicited phone call or email saying you've won a large prize. All you need to do is send money to pay for shipping, taxes or some other fee before the prize can be released to you. You send the money, but the fictional prize never arrives.

7. Timeshare scam

If you own a timeshare, you may get a call from someone claiming they're authorized to sell it for you, for a fee. After paying, however, you never hear from them again.

8. Discount products/services scam

You get an unsolicited call or knock at the door offering a product or service for a discounted price (e.g., heart monitor, wheelchair, bathtub bench, home maintenance, tree trimming). You're asked for a deposit or prepayment and the product never arrives or the work is never completed.

9. Missed payment scam

You're approached by a "professional" who claims your home is under threat of foreclosure and offers to pay off your mortgage or taxes if you sign over the deed to the property. Or, you receive a call from you electric company threatening to turn off services unless payment is made immediately.

10. Caregiver and sweetheart scam

These predators claim to care deeply for you or your well-being. After spending weeks and months winning your trust, they may gain access to your accounts to steal money or your identity information. They may also ask you to accept money on their behalf fooled by a request to send those funds to another location.

These scams are common and widespread. Keep these additional tips in mind to protect your identity and your accounts:

- Don't allow remote access to your computer.
- Don't give a caller verification codes that you receive via text or email.
- Don't click links in the body of suspicious emails or text messages, especially if they claim to come from your bank, credit card company, real estate agent or title company. Instead, log in to the company's official website or call them directly to verify.
- Don't pay for things you don't remember ordering.
- Don't give your personal information to unknown third parties.
- Work with financial institutions that use fraud protection to safeguard your credit card and banking information.
- Don't click links in the body of suspicious emails, especially if they claim to come from your bank, credit card company, real estate agent or title company. Instead, log in to the company's official website or call them directly to verify.
- Don't let strangers into your house. Instead, ask for a business card and say your spouse, kids or lawyer will be in touch.
- Be wary of caregivers and suitors, especially if conversations center around finances or financial transactions.
- Limit the purchases and donations you make by check, which may list your home address or other key data.

"In investing, what is comfortable is rarely profitable."

-Robert Arnott

"Compound interest is the eighth wonder of the world; he who understands it, earns it, he who doesn't pays it."

-Albert Einstein

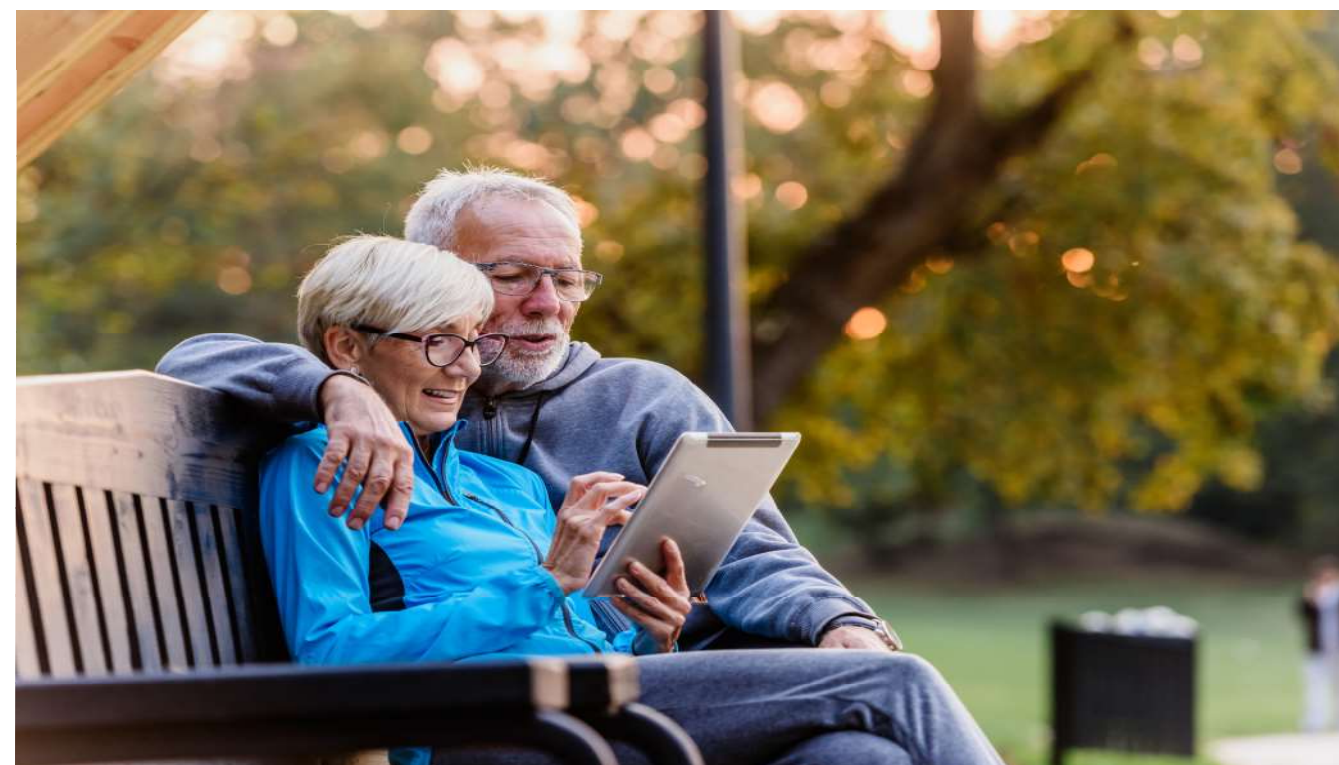
"How many millionaires do you know have become wealthy by investing in a savings accounts? I rest my case."

-Robert G. Allen

THE JKA REPORT

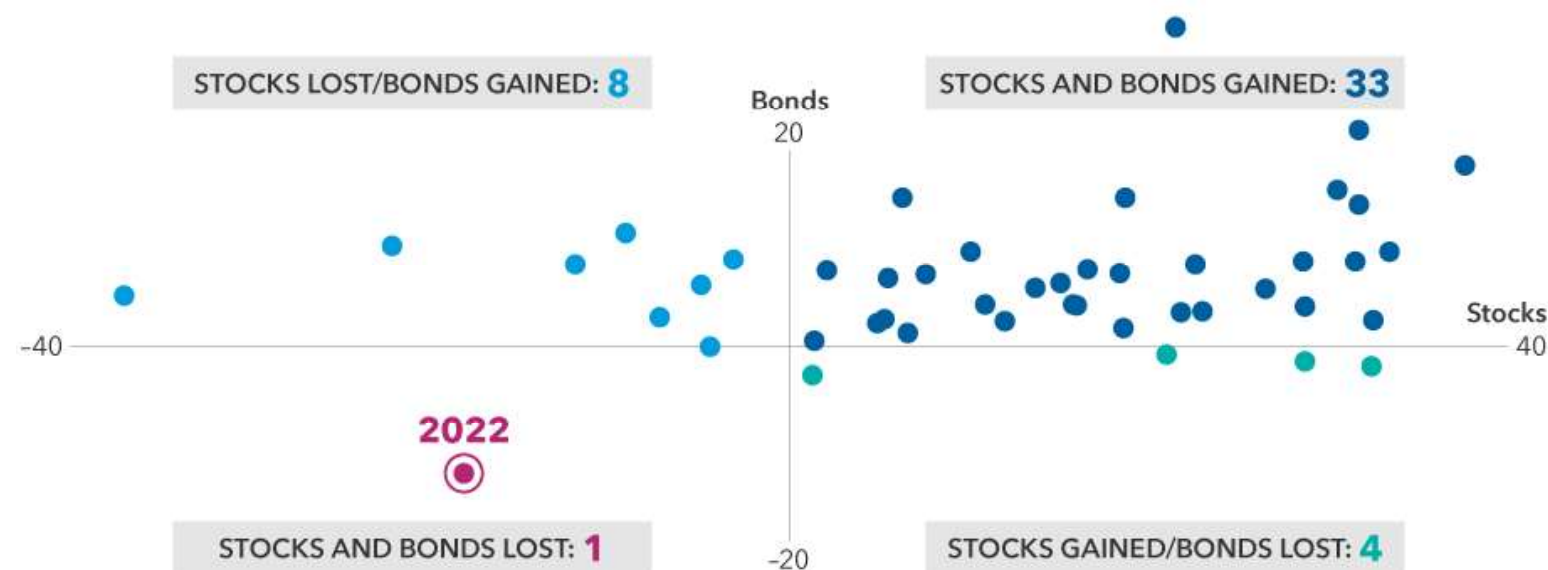
AN INVESTMENT NEWSLETTER FOR CLIENTS & PROSPECTS

Provided by Jerry K. Ask Investment Services



Most investors had never faced a year as challenging as 2022

Distribution of stock and bond returns (%), 1977-2022



If you suspect you've fallen victim to a scam or that your identity has been compromised, it's time to act. Report the incident to your advisor right away to help protect your accounts, and consult [identitytheft.gov](https://www.identitytheft.gov/#/) (<https://www.identitytheft.gov/#/>) to see the Federal Trade Commission's recommendations for critical next steps. Additionally, reporting cybercrime incidents to the FBI (<https://www.ic3.gov/>) can help federal agencies respond quicker and more effectively to threats. Sources: Capital Group, Bloomberg Index Services Ltd., Standard & Poor's. Each dot represents an annual stock and bond market return from 1977 through 2022. Stock returns represented by the S&P 500 Index. Bond returns represented by the Bloomberg U.S. Aggregate Index. Past results are not predictive of results in future periods. The foregoing information has been obtained from sources considered to be reliable, but we do not guarantee that it is accurate or complete, it is not a statement of all available data necessary for making an investment decision, and it does not constitute a recommendation. Any opinions are those of Jerry K. Ask and not necessarily those of Raymond James

10 COMMON SCAMS AND HOW TO AVOID THEM

TECHNOLOGY & INNOVATION

Familiarize yourself with these common swindles.

1. Compromised bank account scam

You receive a call or email from someone claiming to be from a financial institution or federal/state agency (e.g., IRS, Federal Reserve, FBI) saying that your financial accounts are at risk of fraud. They instruct you to move your funds to a new account they provide to you, coach you on how to answer questions from your financial institution and instruct you not to tell anyone.

INSIDE THE ISSUE

10 common scams and how to avoid them.....1-3

Quotes.....3

Chart.....4

(Continued on page 2)