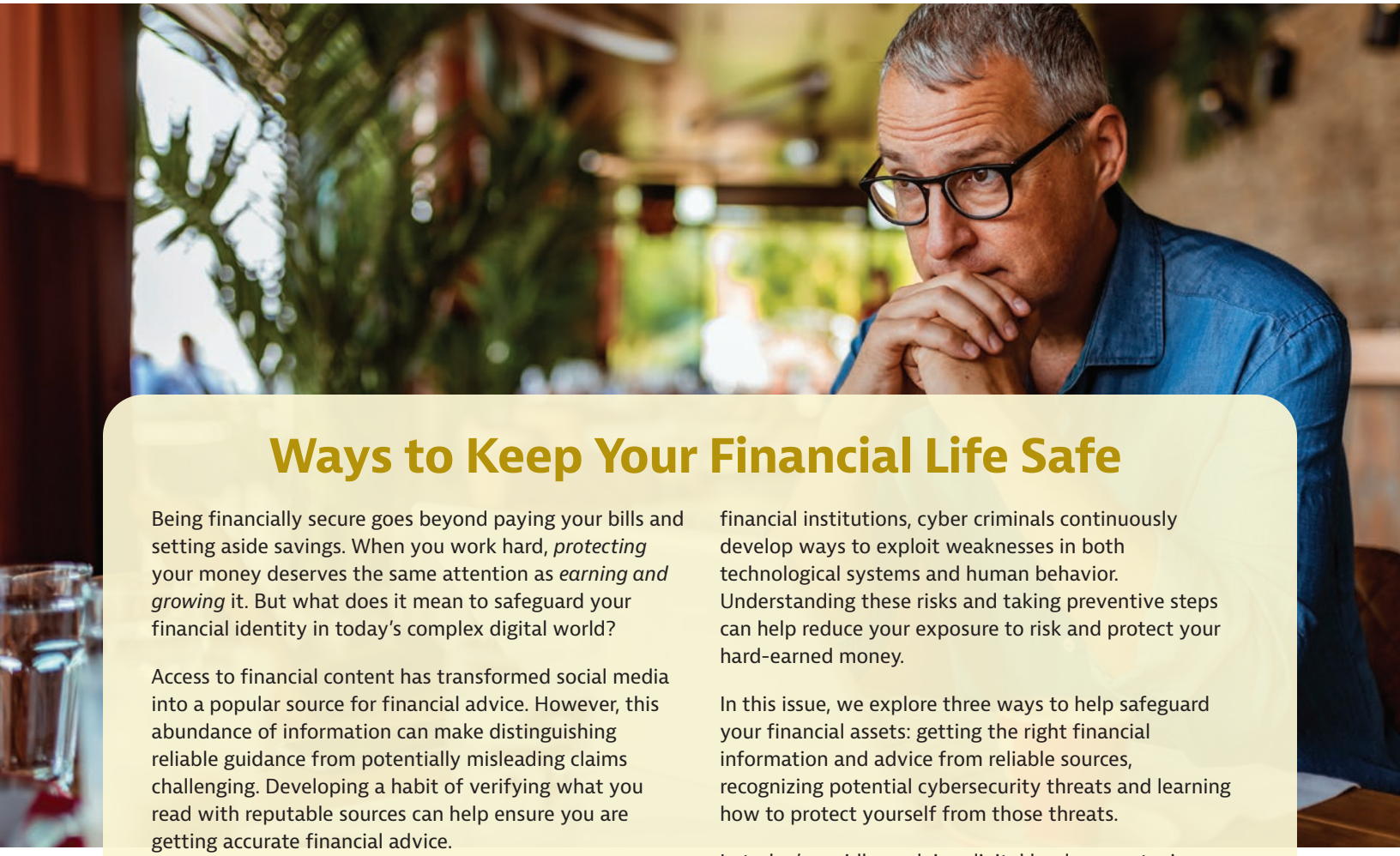
ULTI0193

Horizons

A QUARTERLY NEWSLETTER FOR HOMESTEAD FUNDS' CLIENTS



Ways to Keep Your Financial Life Safe

Being financially secure goes beyond paying your bills and setting aside savings. When you work hard, *protecting* your money deserves the same attention as *earning and growing* it. But what does it mean to safeguard your financial identity in today's complex digital world?

Access to financial content has transformed social media into a popular source for financial advice. However, this abundance of information can make distinguishing reliable guidance from potentially misleading claims challenging. Developing a habit of verifying what you read with reputable sources can help ensure you are getting accurate financial advice.

Cybersecurity threats can pose another risk to your financial life. Even with robust protections put in place by financial institutions, cyber criminals continuously develop ways to exploit weaknesses in both technological systems and human behavior. Understanding these risks and taking preventive steps can help reduce your exposure to risk and protect your hard-earned money.

In this issue, we explore three ways to help safeguard your financial assets: getting the right financial information and advice from reliable sources, recognizing potential cybersecurity threats and learning how to protect yourself from those threats.

In today's rapidly evolving digital landscape, staying informed and vigilant may be your most powerful tool in preserving your financial health and peace of mind.■

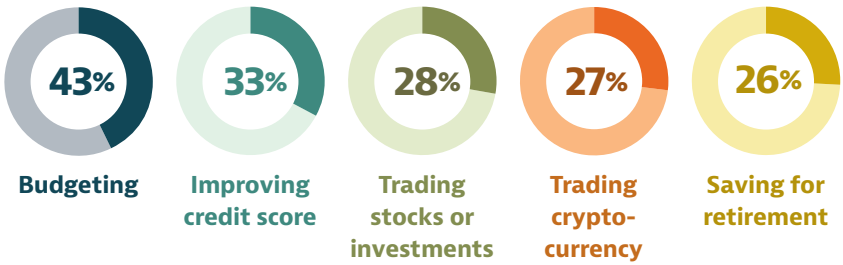
BAD INFORMATION: *When Financial Influencers Lead You Astray*

Social media is a growing source of financial information and advice. It's also a leading source of misinformation.

Continued on page 2

ACTIONS TAKEN BASED ON ADVICE FROM SOCIAL MEDIA

The most common actions included:



Source: Federal Reserve Bank of Philadelphia, "How Americans Use Social Media for Financial Advice"

BAD INFORMATION: When Financial Influencers Lead You Astray *continued from page 1*

The rise of financial content on social media platforms has exploded in recent years. Social media has emerged as a primary source of financial education for younger generations. According to a recent survey, nearly half (49%) of Gen Z consumers who sought financial guidance turned to social media influencers — making these platforms second only to friends and family as trusted information sources. The financial conversation is happening primarily across Facebook (21%), Instagram (19%) and TikTok (17%), transforming these entertainment platforms into unexpected hubs of financial education.[1]

This shift isn't necessarily negative. Social media has democratized financial information and brought educational content to audiences who might otherwise never engage with investing concepts. Many reputable financial professionals maintain valuable social media presences.

The problem with influencer finance

The challenge lies in distinguishing credible guidance from content designed primarily to generate views, clicks and affiliate commissions. Social media platforms reward engagement above accuracy, creating an environment where sensational financial claims often outperform sound advice.

Many self-proclaimed financial experts may have limited qualifications beyond their ability to attract followers. Research indicates that a concerning 71% of financial advice consumed by Gen Z and millennials contains misleading information, while just 13% of influencers possess legitimate qualifications to provide financial guidance.[2]

Red flags in financial content

Be wary of influencers who:

- Promise "guaranteed" returns or "risk-free" investments
- Promote get-rich-quick schemes or unusual investment vehicles
- Emphasize urgency ("act now before it's too late")
- Lack transparency about their qualifications or compensation models
- Delete or ignore critical comments and questions

Finding reliable financial information

Rather than abandoning social media entirely, develop a thoughtful approach:

- **Verify credentials:** Look for recognized financial certifications (e.g., CFP, CFA)
- **Check multiple sources:** Compare information across different platforms
- **Consider the business model:** Understand how the influencer makes money
- **Look for nuance:** Be skeptical of overly simplistic financial advice
- **Seek established sources:** Balance social media with traditional financial resources

Remember that genuine financial advice should acknowledge complexity, discuss both risks and benefits, and recognize that financial decisions are highly personal. No one-size-fits-all approach works for everyone, regardless of how many likes or shares it receives.

Trusted financial professionals, whether online or offline, will encourage questions, provide transparent information about their qualifications and help you understand not just what to do but also why it makes sense for your specific situation. ■

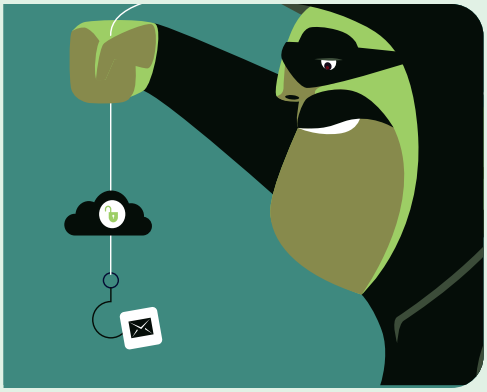
Source notes on page 4

Monthly Habits for Financial Safety

- **Monitor accounts weekly:** Review bank and investment accounts for unauthorized transactions
- **Update passwords quarterly:** Use unique, complex passwords for financial accounts and change them regularly
- **Enable alerts:** Set up text or email notifications for all financial transactions above a certain dollar amount
- **Check credit reports:** At a minimum, review your credit report annually to identify potential problems; however, quarterly reviews may offer faster issue detection
- **Update security software:** Ensure your devices have the latest security updates and antivirus protection
- **Verify requests:** Call your financial institutions directly before responding to emails requesting information
- **Back up data:** Regularly back up important financial documents to a secure, encrypted location
- **Shred financial documents:** Physically destroy documents containing sensitive information before disposal

BAD ACTORS:

Six Common Cyber Scams and Ways to Protect Yourself



Another major threat is a bad actor who tries to obtain your personal information, money or both. As cybercriminals become increasingly sophisticated, protecting yourself requires awareness of their tactics. Here are six common scams targeting investors and practical steps to help defend yourself against them.

1 Phishing Attacks

THE SCAM: Criminals send emails, texts or messages that appear to come from legitimate financial institutions, requesting that you verify account information, reset passwords or address "urgent" security issues.

PROTECTION STRATEGY: Financial institutions rarely request sensitive information via email or text. When in doubt, contact your financial provider directly using the phone number on your statement or card—not links provided in the message. Enable multi-factor authentication wherever possible.

BONUS TIP: Look for subtle signs of fraud: misspellings, slightly altered email addresses (e.g., ***service@homesteadfunds-secure.com*** instead of ***invest@homesteadfunds.com***) and generic greetings rather than your name.

2 Investment Pump-and-Dump Schemes

THE SCAM: Fraudsters artificially inflate the price of investments (often cryptocurrencies or penny stocks) through false statements, then sell their holdings when prices rise, leaving other investors with worthless assets.

PROTECTION STRATEGY: Be extremely wary of investments promoted primarily through social media, especially those promising extraordinary returns or claiming "insider information." Research investments thoroughly using established financial sources.

3 Romance Scams with Financial Hooks

THE SCAM: Criminals build online relationships and gradually introduce investment "opportunities," often involving cryptocurrency or foreign exchange trading platforms.

PROTECTION STRATEGY: Keep financial and romantic relationships separate. Be suspicious if an online romantic interest begins discussing investment opportunities, especially if they're reluctant to meet in person or via video call.

4 Impostor Scams

THE SCAM: Scammers pose as government officials (IRS, Social Security), tech support or financial institution representatives, claiming there's a problem that requires immediate payment or personal information.

PROTECTION STRATEGY: Government agencies don't call demanding immediate payment via gift cards, wire transfers or cryptocurrency. Financial institutions won't ask for complete account numbers they already have. Hang up and reach out to these organizations directly through the contact information provided on their official websites.

5 Free Seminar and Webinar Scams

THE SCAM: Fraudsters offer "exclusive" investment seminars or webinars promising to reveal secret strategies for building wealth. These events often use high-pressure sales tactics to push questionable investments or expensive financial products with hidden fees.

PROTECTION STRATEGY: Research the presenter's credentials through independent sources before attending. Be skeptical of any investment pitched as "exclusive" or "limited-time." Never make on-the-spot investment decisions and always get a second opinion from a trusted financial advisor.

6 Data Breach Response Scams

THE SCAM: After publicized data breaches, scammers pose as the affected company offering "help" with security measures, when they're actually gathering additional personal information.

PROTECTION STRATEGY: Companies experiencing breaches typically communicate through official channels and don't ask for passwords or full Social Security numbers. When in doubt, contact the company directly using information from their verified website—not from the communication you received. ■

Wisdom from Willie Wiredhand

Welcome to Wisdom from Willie Wiredhand, a new series featuring NRECA's beloved electricity mascot who has electrifying financial guidance.

Dear Willie,

How can I teach my kids about managing money in today's digital world without them falling prey to online spending traps and scams? —DIGITAL AGE PARENT

Dear Digital Age Parent,

That's an excellent question that combines two important goals: teaching financial literacy and keeping kids safe online.

I have three practical suggestions for you. First, start with the basics of money management using both digital and physical tools. While apps can track spending and saving, there's something powerful about a child physically putting money in a jar and watching it grow. This tangible experience helps build the foundation for understanding digital transactions later.

Second, create safe learning environments for digital money skills. Many banks offer youth debit cards with parental controls where you can set spending limits, receive transaction alerts and block certain merchant categories. These "training wheels" for digital money let kids practice real financial decisions while providing a safety net against major mistakes or impulse purchases.

Third, teach critical thinking about online offers and marketing. Help your children recognize common tactics used to separate them from their money — including "free" games requiring in-app purchases and social media influencers promoting products. Have regular conversations about how to evaluate whether something is worth their hard-earned money and how to spot when something seems too good to be true.

The goal isn't to make children fearful of digital transactions but to help them become savvy digital consumers who understand both the convenience and the potential pitfalls of managing money online. When they inevitably make small mistakes, try using these as learning opportunities rather than reasons to restrict access completely.

Remember that financial literacy combined with critical thinking skills can help provide protection against digital money traps both now and in their future.

—Willie

Do you have a question for Willie?
*Email it to **invest@homesteadfunds.com**, and maybe we will feature it in next quarter's newsletter!*

Past performance does not guarantee future results. Investing in any mutual fund, including Homestead Funds, involves risk, including the possible loss of principal. *An investment in a mutual fund is not insured or guaranteed by the Federal Deposit Insurance Corporation or any other government agency.*

Before investing in any Homestead Fund, you should carefully consider the fund's investment objectives, risks, charges and expenses before investing. The prospectus contains this and other information about each of the Homestead Funds and should be read carefully before investing. To obtain a prospectus, call 800.258.3030 or visit homesteadadvisers.com.

The views expressed are those of the individuals as of April 22, 2025, and may have changed since that date. The opinions stated may contain forward-looking statements and may discuss the impact of domestic and foreign markets, industry and economic trends, and governmental regulations of the funds and their holdings. Such statements are subject to uncertainty, and the impact on the funds might be materially different from what is described here.

Homestead Funds' investment adviser and/or administrator, Homestead Advisers Corp., is an SEC-registered investment adviser. Homestead Funds are distributed by Homestead Financial Services Corp. Homestead Advisers Corp. receives compensation from the Homestead Funds for serving in these roles. Homestead Advisers Corp. and Homestead Financial Services Corp. are indirect, wholly owned subsidiaries of the National Rural Electric Cooperative Association (NRECA). Homestead Financial Services Corp., Distributor 5/25

HRZNNEWS

PHOTO CREDITS: PAGE 1: PHOTO © ISTOCK/LJUBAPHOTO. SOCIAL MEDIA INFLUENCER © ISTOCK/RUNEER. **PAGE 2 ICONS:** PROBLEM WITH INFLUENCER FINANCE © ISTOCK/BLANKSTOCK. RED FLAGS AND RELIABLE FINANCIAL INFORMATION © ISTOCK/SPEECH BUBBLE. **PAGE 3:** ONLINE PHISHING © ISTOCK/ID-WORK. **PAGE 4:** WILLIE WIREDHAND © NRECA.

***Source notes** from page 2*

[1] Bankrate, "Tired of their parents' outdated advice, young adults are learning about money on TikTok. But is it more reliable?"

[2] Social Capital Markets, "71% of Social Media Financial Advice Misleads Gen Z and Millennials"