Wealth & Investment Management

Protecting your financial life online

August 10, 2026

James Botte, Private Wealth Financial Consultant

01 Protecting your financial life online

Why protect your financial life online?

In 2025, nationwide fraud losses amounted to over $15 billion according to the Federal Trade Commission[1]

What to know:

- Sophisticated Scams
  - Scams are becoming more sophisticated and harder to detect
- Young Adults at Risk
  - Young adults are particularly at risk due to frequent online activities
- Investment Scams
  - Investment scams, particularly in cryptocurrency, are on the rise
- AI-Powered Scams – Voice, Video, Email, Etc.
  - Can now impersonate loved ones, banks, employers, and government officials
  - Why: Fraud is no longer “obviously fake”; realism is now the threat
- Irrecoverable Money
  - Once money is stolen, you may not be able to recover it
- Stressful Identity Recovery
  - Recovering your identity can be stressful and time-consuming

Potential outcomes: Financial loss and setbacks in achieving your financial goals

[1]. Source: Federal Trade Commission.gov, data as of December 31, 2025

Staying Ahead of Scammers: The Good News

1 Educate yourself on common scams

2 Know:
- What to look for
- What to avoid
- When to ask Questions

3 Seek out useful tips to help you verify whether someone is acting in good faith or not

4 And if you fall victim…know who to ask for help

02 Protecting your financial life online

01
How your online life can derail your financial life

02
Common social media scams

03
Common college and job scams

04
Payment and other scams

05
Tips and tricks to help protect yourself online

Common social media scams

1. **Social media phishing**
   - Deep discounts on expensive products
   - Requests to report vaccine side effects
   - Requests for charitable donations
   - Quizzes that launch an app and malware

2. **Hacked profiles with requests for money**

   Beware friends or family asking for money on social channels!

3. **Online dating**

   Is this person really who they say they are?

4. **Job scams**

   Legitimate employers won't ask for a "fee" or your bank details online

5. **Sextortion scams**

   Never share private photos or videos of yourself with strangers online

Social media tips:

1. Set your social media accounts to private
2. Don't fill out all personal information fields
3. Don't accept friend requests from strangers
4. If an online offer seems too good to be true, it usually is

03 Protecting your financial life online

01
How your online life can derail your financial life

02
Common social media scams

03
Common college and job scams

04
Payment and other scams

05
Tips and tricks to help protect yourself online

Starting your next chapter

Whether you are starting college, graduating college, moving apartments and starting a new job, being careful to avoid the following may help you safeguard your finances:

- **Rental scams:** You are pressured to act quickly and pay a deposit before seeing the rental
- **Scholarship scams:** Scholarship providers contact you and ask for an upfront fee
- **Identity theft:** Sharing Social Security and account details through non-secure channels can lead to issues
- **Job scams:** A recruiter reaches out and after the interview asks for financial information and even upfront payment before you are offered the job





Steps to protect yourself

Here are some simple steps that you can take to help protect yourself and your financial life:

- Avoid any posting or solicitation that requires you to act immediately
- Don't send money requested via wire transfer—wire transfers cannot be reversed
- Avoid correspondence or ads with misspellings, oddly written language, or unusual formatting: the "kindly" rule
- If you didn't apply for a "guaranteed" scholarship don't accept it
- Avoid services that claim you will be eligible only if you provide an upfront payment
- Store your personal information securely and shred everything else
- Have sensitive information mailed to a permanent address (i.e. your parents' address)
- Double check company websites and recruiter email addresses before responding to a solicitation

04 Protecting your financial life online

01
How your online life can derail your financial life

02
Common social media scams

03
Common college and job scams

04
Payment and other scams

05
Tips and tricks to help protect yourself online

Digital Payment Scams

Scammers often target payment methods in ways in which it is difficult for you to recover your money.

Common scam methods include:

1. Get-rich-quick schemes. If an offer seems too good to be true, it probably is.
2. Unexpected calls, texts, social media posts, or emails where someone asks you to:
   - Send money
   - Provide your account information
   - Give them access to your device
3. Scammers impersonating:
   - Tech support companies
   - Government agencies (often the IRS)
   - Your bank (even Wells Fargo)

Don't be afraid to end communication with the person who contacted you so you can have time to do more research.

Doing Your Due Diligence

The Cardinal Rule of Online Financial Security

Don’t ever send money or give your bank account or Social Security number to someone who contacts you via text or phone without checking they are legitimate first—even your bank.

- Don’t be pressured into giving away your personal information
- Never use the following payment methods without researching the recipient first:
  - Money wire transfers
  - Digital payment apps
  - Gift and prepaid cards
  - Cryptocurrency

Steps to help protect yourself

- Do double check your payment details to make sure that you're sending money to the right person
  - Check to ensure website URLs are correct
  - Hang up and call your bank or the company directly through a verifiable phone number

- Do **add extra layers of security** to your banking and payment apps such as two factor authentication

- Don't send money or give your account information to:
  - Anyone you don't know
  - A company you can't verify as legitimate

- Don't send money back to someone who has provided a check or overpayment for goods or services

- Don't cash checks for others

- Don't provide your account or sign-on information

- Don't allow anyone else to use your desktop or mobile device

05 Protecting your financial life online

Do’s and don’ts to help protect yourself online

Steps to take:

- Do set your profiles to private
- Do restrict social media contacts to people you know
- Do be on the lookout for suspicious posts, including:
  - Limited-time offers
  - Discounts that seem too good to be true
  - Requests for personal or account information
- Do be cautious of people you meet through social media or gaming apps
- Do create a unique username and password for each app and website you use

Things to avoid:

- Don't accept friend requests from strangers.
- Don't respond to online solicitations for "easy money"
- Don't click on suspicious links even from friends
- Don't fill out every field on your social media profile such as your phone number and home
- Don't send money to someone you have only met online
- Don’t send money to friends or family without checking with them to see if the request is genuine
- Don’t send money or share information without doing your due diligence
- Don’t trust caller ID, voice, or video alone – verify everything independently

What can you do if you’ve been scammed?

Know that you are not alone and the actions you take can help mitigate any future financial harm.

- If your financial information has been compromised contact your bank fraud center immediately: Wells Fargo Security Center: https://www.wellsfargo.com/privacy-security/fraud/protecting-you/
- If you believe you been a victim of a job scam, report to the Federal Trade Commission https://reportfraud.ftc.gov/*
- Report scams to your local police, and report crypto, investment, and impersonation scams to the FBI at IC3.gov
- Consider credit monitoring services to help keep an eye on any unusual or unauthorized activity on your credit report

*Wells Fargo has provided this link for your convenience but does not control or endorse the website and is not responsible for the products, services, content, links, privacy policy, or security policy of the website.

Wealth & Investment Management

Thank you