How to Reduce Your Risk of Financial Fraud in the AI Age

8 MIN READ

APR. 30, 2026

BY MELANIE LOCKERT

SUPER
AGE

Deepfakes, voice clones, and AI-generated phishing attacks are getting harder to detect. Here’s how to protect yourself.

You’re smart, savvy, and think financial fraud could never happen to you. That’s what most people believe, until it does. Artificial intelligence (AI) is making scams easier and more sophisticated than ever.

Gone are the telltale warning signs: bad grammar, spelling errors, and fuzzy images. “Criminals can now produce highly convincing messages, clone voices, and even generate realistic videos at a very, very low cost,” making it much harder for consumers to detect them, says Gustavo Paniz, scams and fraud analyst at **Graphika**, an intelligence platform.

The unfortunate reality is that financial fraud is rampant and only increasing. According to the **Federal Trade Commission (FTC)**, the agency received 3 million fraud reports from consumers in 2025, with total losses of $15.9 billion, a significant increase from the year prior.

You’ve spent your life building a **nest egg**, and one misstep could be costly. Here’s how to reduce your risk of financial fraud in the age of AI and **safeguard your finances**.

How AI is Changing Financial Scams

Artificial intelligence is getting bigger, better, and more ubiquitous. We’re no longer

thinking about what it can do, but asking what it *can't* do. Thanks to the power of AI, fraudsters can do more with less.

"AI is accelerating financial fraud by increasing its scale, its speed, and its sophistication as well," says Paniz. "And this, of course, makes it easier to target large numbers of people with these personalized and believable narratives," he tells Super Age.

Scammers are also using AI to create messages that feel tailored to you. "What's happened is AI has made the text messages or the phishing more contextual, more personal, more scalable, and has a higher success rate," says Mary Ann Miller, VP, evangelist & fraud executive advisor at **Prove**, an identity company.

For example, Miller says your bank might email customers about a website update with new features. From there, you might get a text saying that the website update is complete and to click here for a new offer.

"And because it has a little more detail about what the customer might already know and be able to relate to, it's more convincing. So what's happening is AI is gathering information for the bad actors to make these text messages, these phishing attempts, these smishing attempts [phishing attempts delivered via SMS], much more successful," adds Miller.

The 5 Biggest AI Financial Scams Right Now

Being aware of what's going on can help you focus on preserving your health and wealth, mitigating potential stress and loss from fraud. Here are some of the most common AI-powered scams to watch out for right now.

1) Voice Cloning Scams

Imagine you hear your child or grandchild on the phone, panicked and scared, asking for money to get out of a dangerous situation. That's one of the latest ways scammers are using AI to carry out **voice cloning scams**.

Using publicly available audio from social media, videos, and podcasts, scammers can replicate someone's voice with an uncanny resemblance. They can then spoof phone numbers to make it seem like your loved one really is calling you in distress and in urgent need of money.

To help you avoid falling for this scam, call the loved one back directly. You can also consider creating a code word that only family members know, in case of an emergency.

2) Social Media Scams

You might use social media to stay in touch with family and friends, promote your business, or express yourself. But be aware of what you post and how much information you share. Recent **FTC data** shows that 30% of people who lost money to a scam in 2025 said it started on social media, resulting in losses of $2.1 billion. The top culprits include Facebook, WhatsApp, and Instagram.

Scammers can use AI to create websites, ads, or posts for fake companies or opportunities. These may be shopping scams, investment scams, or romance scams.

3) Text and Email Scams

Texts and emails are a part of everyday life. Scams through these methods of communication aren't new, but they're becoming more believable and realistic. In the past, you might get an email riddled with errors that could tip you off that it wasn't legitimate. Using AI, the language is now polished and personalized. Images, such as

company logos, can look nearly identical to the real thing.

Scammers often use everyday situations as their hook: “There are scams associated with common activities, like a notification that a package has been misdelivered and that maybe they have the wrong address. They’re asking you for the address and they’re saying that you owe money on the postage,” says Kimberly Sutherland, global head of fraud and identity at **LexisNexis Risk Solutions**. “It could be a scam of opportunity. I group those as things like an employment opportunity, or you’ve won a prize, or there’s been an overpayment, and you need to be issued a refund.”

If you receive a text or email, especially one asking for information or directing you to take action, proceed with caution. Don’t click links, download attachments, or respond. Instead, it’s best to go directly to the company’s website, app, or account to verify the sender.

4) Imposter Scams

According to the **FTC**, imposter scams have been the most widely reported fraud since 2020. In 2025, the FTC received over a million reports of imposter scams, resulting in more than $3.5 billion in losses.

Scammers impersonate someone with authority to gain your trust and your financial information. The **FBI** recently noted that fraudsters are sometimes specifically impersonating law enforcement. They approach victims via text or email, saying that they’re a victim of fraud or considered a suspect in a fraud investigation. AI makes it easier to clone voices, create personas, and craft realistic, professional emails that support the narrative.

The FBI notes that you should always be suspicious of unsolicited messages and calls. Avoid giving money or personal information to people you’re not familiar with. Additionally, contact law enforcement directly to verify potential claims.

Paniz adds that some of the most concerning cases are sophisticated impersonation scams involving “deepfakes” and financial advisors.

“Deepfake is constructing a persona by artificially imitating his face, his voice, his movements, his facial expressions, his linguistics, his voice tone, everything that you can get,” Paniz explains.

To try and spot AI, Paniz says to look for “a voice that sounds slightly too smooth or emotionally flat, odd phrasings, unusual pauses, or inconsistent pronunciation as well. For text, the signs can include language that is polished but impersonal.”

5) Relationship/Investment Scams

Consumers lost the most money to investment scams in 2025, resulting in $7.9 billion of losses, according to the FTC.

When scammers contact you through text or online, it may start as a friendly conversation. As they build trust or start to foster a romantic connection, they may tell you about a great investment opportunity.

NBC News recently published a story on how a 76-year-old lost **$1.6 million to an AI investment scam**. AI can create personas and lifelike videos, making you believe you’re talking to a real person. Plus, AI can create images showing a fake investment balance and fabricated growth.

5 Ways to Protect Yourself from Financial Fraud

A major part of **longevity** is being proactive. You eat right and exercise now to reap

the rewards later. Similarly, you can take proactive steps to preserve your assets and protect yourself from financial fraud.

1. Review Your Credit Report

Using **AnnualCreditReport.com**, you can access all three of your credit reports from the major credit bureaus.

Check your accounts to make sure they're accurate and there aren't any major red flags. If there are errors or inconsistencies, reach out to the credit bureaus to fix any mistakes, which could hurt your credit score.

The **Consumer Financial Protection Bureau (CFPB)** provides resources on how to dispute errors on your credit report, including a sample letter to use.

2. Freeze Your Credit

One way to stop potential fraudsters from opening an account in your name is to **freeze your credit**. When you freeze your credit, creditors won't be able to access the information in your credit report, preventing them from approving new lines of credit. In the event a scammer is using your identity to take out a loan or a credit card, this step can stop them.

This is not something to do if you're about to apply for a mortgage or open a new credit card. You can also unfreeze your credit report at a later date if you know you'll be applying for a loan.

To start, contact the three major credit bureaus to place a credit freeze online:

- **Experian**

- **Equifax**
- **TransUnion**

3. Opt-In to Account Alerts and Credit Monitoring

Financial fraud can happen in seconds. Being able to stop it before it starts or remedy the issue right away can help. That's why it's essential to sign up for account alerts, notifications, and credit monitoring.

"Always sign up for what they call opt-in alerts, so they notify you of transactions. They might give you updates on your balance daily. Sign up for those alerts so that you can look at them," says Miller.

This can include your bank accounts, credit cards, and social media accounts. Just last week, I received a notification that there was a request to change my password on Instagram. It wasn't me. I notified Instagram of the attempt and went on with my day.

4. Set Up Two-Factor Authentication

To better safeguard your accounts, set up **two-factor authentication** when possible. When you rely only on a password to access your account, it may leave you more vulnerable if there's a data breach or a scammer has your login credentials.

Two-factor authentication adds an extra step that can act as an additional barrier. So, for example, after entering your password, you might receive a code from a text message, email, or authentication app that you must enter to log in. Having this set up can help thwart scammers trying to access your account.

5. Don't Click or Respond

Scammers prey on our fears and create a sense of urgency to get what they want. Whether you receive an email or text, take a moment before reacting. This is where mindfulness, instead of being on autopilot, can help.

For starters, don’t click on links or respond to text messages, especially from unknown numbers. If personal or financial information is being requested, that should raise your level of suspicion.

“Pause before responding to any unexpected requests. Avoid sharing any sensitive information. Always verify identities through the official channels,” says Paniz.

If it appears to be your bank or credit card company, call the number on the back of your card or contact a customer service representative through your online account.

Questions to Ask Yourself First

Any time you’re contacted out of the blue, it’s always a good idea to pause for a moment and ask yourself a few questions first. Sutherland says these questions can help determine whether something is a scam or not.

- Is the message, call, email, or text unexpected?
- Are they asking for more personal information than feels comfortable?
- Why are they asking for your date of birth, your Social Security Number, or information that’s not consistent with the type of transaction that you’re actually making?

“At least that way, you immediately increase your senses around the situation,” adds Sutherland.

What to Do Next If You’re a Victim of

Financial Fraud

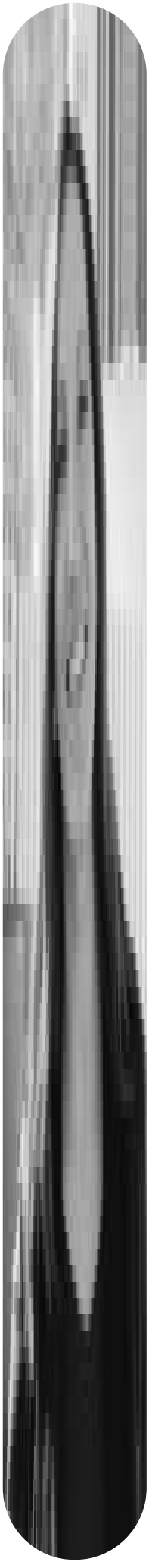
If you believe you're a victim of financial fraud, it can be disorienting and devastating. You shouldn't suffer in silence. Here's what to do next.

1. Block the number or email of the scammer and stop contact
2. Follow FTC guidance on **who to follow up with if you paid a scammer**
3. Report fraud through the **FTC**
4. If applicable, report on **IdentityTheft.gov**
5. Change passwords
6. Call local law enforcement

Artificial intelligence is changing fast. By staying up to date on the latest advancements and taking added precautions, you can protect your financial health and well-being.

*The information provided in this article is for educational and informational purposes only and is not intended as health, medical, or financial advice. Do not use this information to diagnose or treat any health condition. Always consult a qualified healthcare provider regarding any questions you may have about a medical condition or health objectives.**Read our disclaimers**.*

WRITTEN BY:



Melanie Lockert