Using AI for Financial Advice? 4 Ways To Protect Your Money (and Privacy)

Nicholas Morine

Nicholas Morine

Thu, May 8, 2025 at 11:04 AM EDT 4 min read

The proliferation and gradual sophistication of generative AI tools such as Gemini, Claude, and of course ChatGPT has turned most casual users into experimenters themselves, whether it be asking these models to provide a complete shopping list or to help with this year's tax filing.

However, as CardRates reported, a majority of Americans (67%) now also feel comfortable letting AI tools assist them with their banking routines. While only about one-fifth (18%) of those surveyed reported using AI tools to help with banking on a monthly basis, an even greater proportion (nearly a quarter, at 28%) expressed concerns over privacy in this regard.

What can be done to help mitigate the privacy risks associated with allowing AI tools to have a hand in your personal banking regimen?

Ignorance may be bliss, but it can be extremely costly when it comes to your financial knowledge, particularly as AI integrates itself into the banking realm at a breakneck pace.

As J.P. Morgan suggested, it's vital for consumers of banking products to educate themselves as to the current and prospective future capabilities of generative AI assistants and AI banking tools, lest they be taken advantage of.

"Publicly available tools capture, share and build on information, making it potentially accessible by those with malintent," the firm stated. "Many of these generative AI tools, apps and chatbots are currently not subject to any government regulations, ethics rules and governance structures, no matter how sophisticated these tools might seem."

Know that any public-facing information about you on the internet is likely scraped by these models, and that any information in your overall user profile is generally captured, as well.

While most online banking portals already require this step, be sure that you are taking advantage of every opportunity to avail of multi-factor or two-factor authentication protocols. These typically come in the form of requiring a text message or email sent to a verified address with a PIN code, or for biometric information (such as a facial scan, or a fingerprint) to be inputted through your smartphone.

Malicious hackers (or even malicious AI models themselves) may be stymied by your deployment of this sort of authentication on all banking and investment accounts. It never hurts to have a second barrier to entry for dishonest parties to clear before gaining access to your finances.

Simply put, making sure that you do not offer up any personal details you do not have to provide when dealing with AI assistants or chatbots is good cybersecurity practice — as is enabling a reliable and trustworthy VPN whenever engaging with AI tools. A VPN can help to obscure your IP address

in addition to other geographical or personal details about you, and refusing to offer any more information than is directly necessary when speaking to artificial intelligence tools can help to restrict data or privacy leaks, should they occur.

Central Michigan University professor Qi Liao was firm in his assessment on today's tech-heavy banking and financial sphere: We are now living in a brand-new era when it comes to the elevated sophistication of phishing schemes mining your personal financial information.

"Beyond exploiting system weaknesses, AI is revolutionizing social engineering attacks. Attackers can now automate and personalize phishing schemes by analyzing social media data. AI-generated deepfakes, including realistic audio, video and images, have been weaponized for scams such as blackmail, impersonation and financial fraud," Liao said.

Advertisement: High Yield Savings Offers

"These tools enable attackers to execute crimes like online banking fraud, fake ransom demands and large-scale financial scams," he added.

So, be sure to second-guess your interactions online or on the phone, even if the messages or calls appear to be from a trusted friend, family member or financial advisor. If something seems "off" or is setting of alarm bells in your head, trust your instinct and follow-up with some due diligence before proceeding any further. You could end up saving yourself a great deal of trouble, and your wallet, in so doing.

More From GOBankingRates

- **6 Used Luxury SUVs That Are a Good Investment for Retirees**
- The New Retirement Problem Boomers Are Facing
- **7 Overpriced Grocery Items Frugal People Should Quit Buying in 2025**
- How Far $750K Plus Social Security Goes in Retirement in Every US Region

Sources:

- CardRates.com, "America's Banking Habits: Survey Finds 84% Concerned About Banking Cybersecurity"
- Central Michigan University, "How can you protect your privacy, money from AI?"
- J.P. Morgan Private Bank, "AI tools and your privacy: What you need to know"

This article originally appeared on GOBankingRates.com: Using AI for Financial Advice? 4 Ways To Protect Your Money (and Privacy)

- Brian Baker, CFA

  Wed, May 14, 2025 at 10:56 AM EDT 9 min read

Most people are aware of financial advisors and may even hire one at some point in their lives,