SCAMS AND FRAUD

Got a New Online Friend? Be Wary

Scammers may be harder to spot when they pose as pals rather than romantic partners

By Matt Alderton, AARP

Published September 10, 2025

CHRIS GASH

Call AARP Fraud Watch Network™ Helpline for assistance with and advice on scams: 877-908-3360. Toll-free service is available Monday through Friday, 8 a.m. to 8 p.m. ET.

If you are a scam victim or have questions about scams, call the AARP Fraud Watch Network Helpline toll-free at 877-908-3360 for free advice from trained fraud specialists.

Romance scams have been a reliable source of income for digital criminals for years. But a new, more subtle variation of that fraud is seeing an uptick. Instead of seducing vulnerable people online with promises of romance, some scammers are creating a (false) bond with victims by convincing them they share a common interest, according to Amy Nofziger, AARP director of fraud victim support

Fraud experts often refer to this as affinity fraud, where the criminal will take advantage of a shared affiliation with the victim — they might both belong to the same religious group, for example — and the trust that comes with it.

A recent caller to the AARP Fraud Watch Network Helpline (who asked not to be named) met someone on a friendship app who seemed to share many interests with her. When the new "friend" claimed to be locked out of his bank account, he asked for a loan via the Cash App. He promised to repay the money but never did and ended up stealing $10,000 from her.

Another caller met someone while playing online video games. When they asked for money, she agreed to help, ultimately losing over $100,000 sent via Bitcoin and gift cards.

"These are online romance scams with a twist," Nofziger says. "Instead of pretending to fall in love, the criminals act like they share your hobbies or struggles. Whether it's a sober support group or a Facebook group for classic car lovers, scammers are slipping into these spaces just to gain your trust and take advantage of it."

Join Our Fight Against Fraud

Here's what you can do to help protect people 50 and older from scams and fraud:

- Sign up to become a digital fraud fighter to help raise awareness about the latest scams.
- Read more about how we're fighting for you every day in Congress and across the country.
- AARP is your fierce defender on the issues that matter to people 50-plus. Become a member or renew your membership today.

How friendship scams work

The scams follow a predictable script, says Jason Zirkle, a certified fraud examiner and training director at the Association of Certified Fraud Examiners: Criminals lurking on sites like Facebook, Instagram or Reddit initiate contact by sending direct messages or commenting on posts.

Or they might try to initiate a relationship using a wrong number text (*"Hi, is this Jane?"*). If you reply, they'll quickly try to engage you in conversation and forge a connection.

Then they often use empathy and "mirroring" — appearing to be in the same circumstances as you — to establish deep emotional connections quickly.

Eventually, conversations move to platforms that are harder to trace, such as encrypted text messaging apps like WhatsApp and Telegram. Finally, scammers invent a personal crisis to ask for financial help, often requesting money via nontraditional channels like gift cards, cryptocurrency or peer-to-peer payment apps. Or they'll say they have an investment opportunity. They have a relative who's done well in cryptocurrency, and they want you to benefit from their knowledge. (The process of creating trust before proposing this sort of bogus investment is known as financial grooming.)

Since people might not question platonic relationships as much as romantic ones, scammers can be harder to spot. "The relationship building is a little bit more subtle," Zirkle says. "For that reason, I think friendship scams are more insidious than romance scams."

AI's role

Friendship scams (like many forms of fraud) are becoming even more insidious with the help of artificial intelligence, according to Roy Zur, cofounder and CEO of Charm Security, whose fraud protection platform uses AI to prevent scams. For example, a male criminal living overseas can use AI to pose as an older American woman who lives in the South and is a master gardener. If he meets you in a Facebook gardening group, he can use ChatGPT to translate his native tongue into perfect English, infuse his writing with Southern dialect, generate insights and observations about growing flowers and vegetables suited to Southern climates, and even fabricate real-looking images of his female alter ego working on rosebushes.

"It makes it feel much, much more real," Zur says. "And it makes it much easier to do this type of crime in the first place."

How to avoid friendship scams

Keep these tips in mind to build online connections safely, says Iskander Sanchez-Rola, director of AI and innovation at Gen, which owns cybersecurity brands Norton, Avast and LifeLock.

- **Be skeptical of sudden closeness.** Scammers want to build rapport fast. So proceed cautiously when a new connection gets intimate soon after you meet them.
- **Beware of secrecy and evasion.** If online friends want you to keep your relationship secret, or if they avoid speaking on the phone, having a video chat or meeting you in person, they may be hiding something.
- **Avoid messaging platforms.** If your new friend wants to move your conversation to a messaging service like WhatsApp, Telegram, or Signal, that's a red flag.
- **Don't send money.** Eventually, inevitably, scammers always ask for money. If someone you've never met in person solicits you for cash, that's a red flag — and a red light. Requests that are urgent or involve nontraditional payment methods like gift cards or crypto are especially suspicious.
- **Seek a second opinion.** If something about a new friendship feels off, consider confiding in a trusted friend or family member to get a fresh perspective. There are also tools you can use to sniff out scammers. Norton Genie,* AI Scam Detective and ScamSniper all use AI to detect likely scams by analyzing text messages, social media posts, emails and websites.
- **Cut off contact.** Immediately stop communicating if you suspect the individual may be a scammer, and do not re-engage with them.

**Norton pays AARP a royalty for use of its intellectual property and provides a benefit to AARP members.*

Matt Alderton is a contributing writer who specializes in health and wellness, travel and technology. His work has also appeared in USA Today, Forbes *and* The Washington Post.