How to Protect Yourself from an Online Dating Scam

Here are tips for defensive dating, including warning signs that you could be the target of an online romance scam

By
Katherine Bindley
THE WALL STREET JOURNAL
March 15, 2018

More and more people are looking for love online. A large chunk are those age 50 to 64, and dating services aimed at baby boomers are expected to grow the most over the next five years. You know who else is prowling around websites and apps, looking to score? Scammers.

Last year, more than 15,000 victims lost some $210 million in "confidence frauds" and romance scams, according to the Federal Bureau of Investigation. The lesson: Meeting people online comes with risks. And the way to protect yourself or someone you love isn't as simple as "Don't be foolish." Smart people fall prey to scams.

Scammers are really good at what they do. They've got crafty ways to make you believe their stories and a range of places to find targets these days. So you must know the warning signs, recognize the script, learn to sleuth and adopt some defensive rules. Here's how:

Know Where Scammers Lurk

Scammers don't limit their hunting grounds to old-school dating sites like Match.com. They're trolling for victims on any number of apps, even ones that aren't associated with dating, such as the Scrabble-like online social game Words With Friends, according to the Better Business Bureau's Scam Tracker.

Amy Nofziger, a director with the AARP Fraud Watch Network, says it has received complaints about seniors defrauded by people they met on the dating app Tinder, but also through Facebook.

Ms. Nofziger says seniors might join Facebook at the urging of a family member without a full understanding of who can see their profiles or send friend requests. "When you sign up, it's not like someone comes up and pops out of a box and says, 'Hey, there might be scammers on here,'" she says.

Last fall, Facebook published a blog post outlining what users should be looking out for when it comes to scams, which often begin with messages from an unfamiliar person claiming to be divorced or widowed and seeking to start a conversation.

A Match.com spokeswoman said the company patrols for fraud and reviews member profiles, looking for "red-flag language" and activity from "high-alert countries." It also asks members to

pledge not to send money or financial information to others on Match. Tinder has a similar warning for users.

Keep Your Own Profile Safe

It's understandable to want to be open and honest in your dating profile, but remember that scammers look for ways to exploit whatever information is available. If you lost your husband to cancer, they might say their wife died of cancer. If you are religious, they might quote scripture or suggest praying together.

Think about whether pieces of your profile could be used against you. The AARP's Ms. Nofziger says to leave out anything that someone might "glom onto in the initial stages," including details like being financially independent.

Most important: Check your Facebook privacy settings. Make sure only friends can see your posts. You may feel comfortable sharing certain things, but just know that even "friends of friends" is a massive population of people which could easily include scammers. Also, don't accept friend requests from people you don't know, even if they try to explain why you should recall them. You could put your whole friend network at risk.

Verify, Verify, Then Verify Again

Once you've matched with a person, start googling—hard. "Do some cyberstalking," Ms. Nofziger says.

Use reverse Google image search to see if your match's photos have been recycled from other websites. Look up employer names and any other details you can search for. Be aware that anyone can create a LinkedIn, Facebook or Twitter profile, even if names and titles look legitimate.

"It doesn't 100% validate authenticity of the person," she says. "That's just another piece of the puzzle for you."

Chat Smarter

Scammers try to move their targets off the platform where they met as soon as possible, says Patti Poss, a senior attorney with the Federal Trade Commission. Someone may say their subscription is ending, or that they don't use the site much. That may be an excuse to start using standard text messages, email—or the phone.

Remember that a phone call doesn't mean someone is legit. Scammers can and do call their targets; sometimes they even send gifts.

Another red flag? Professing love superfast. "Slow down," Ms. Poss says. "Don't let them rush you."

Look out for grammar and spelling errors. (English often isn't a scammer's first language.) Paste portions of messages into Google, and see if you get any hits: Scammers sometimes repeat the same lines. A previous target may have posted the information online.

Recognize the Script

Scammers often say they live in the U.S. but their work takes them overseas. Or they do mission work abroad. Or they're in the military—the U.S. Army has a guide on what to look for if you suspect a scammer is impersonating a serviceman.

When they keep saying they want to meet but can't, that's another flag. These circumstances make for an easy cover.

What often happens before a planned meeting is suddenly they have to travel internationally. Then it's emergency time: Their child is sick. They were injured in an accident. A business deal went south. Something bad happened, and they can't access their money. Or maybe they just need money for a plane ticket to come see you. Lies. Lies. Lies.

Avoid Giving Money or Other Assistance

When asking for money, scammers might want iTunes gift cards—either the physical cards or a picture of the code on the back. Don't fall for that or any other shady-sounding forms of payment.

Assistance can take a variety of forms. A scammer might ask you to accept a shipment and send it elsewhere or to accept money into your own account and then wire it somewhere else.

"Sometimes they don't actually ask you for money," says Katherine Hutt, communications director at the Better Business Bureau. "They get the romance scam victim to be their money mule."

Protect Your Loved Ones

Go through their social media pages. See how much of their information is public. Try to get details about their previous matches and do some verifying of your own.

The AARP has a fraud watch section on their website and a number you can call for help. If you are trying to warn a family member, be prepared to be disbelieved.

People can be hesitant to believe something negative about someone they're falling for—especially if they're hearing things like "You're beautiful" or "I'm in love with you" for the first time in years.

Think You've Been Scammed?

Don't continue communicating with your suspected scammers under any circumstances, even if you're hoping to bust them. If they know you're onto them, they might threaten to release information or pictures that could be embarrassing if you don't give them more money. Victims can also be the targets of secondary scams, where people pretend to help get their money back.

Just cut them off cold turkey and start filing complaints.

"File complaints with anyone you think might be working on this," says the FTC's Ms. Poss. "Get it in front of your state attorney general, the federal folks, the criminal folks, the payment processor and the FTC." She also recommends the BBB's Scam Tracker.