



HOW TO AVOID ONLINE ROMANCE SCAMS

It's well known that people online aren't always as they appear. However, tens of thousands of internet users fall victim to online romance scams each year. These scams can be incredibly convincing and are increasingly found across dating sites and social media platforms. By appealing to victims' emotions and feigning personal connections, scammers will try to steal large sums of money and personal information. Luckily, there are ways to identify a scam and protect yourself online.



KNOW YOUR THREAT MODEL

Threat modeling is a process used by IT professionals for anticipating cybersecurity threats, but it can also be a helpful exercise for individuals looking to stay safe online. Ask yourself the following questions:

1. How could a scammer target me?
2. Why would a scammer choose to target me?
3. What information could a scammer use to target me?

TIPS FOR STAYING SAFE ONLINE



SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others. Consider creating an alternate persona that you use for online profiles to limit how much of your own personal information you share.



CHECK ACCOUNT SETTINGS

Consider setting your social media profiles to "private". This will make it harder for scammers to target and communicate with you. A public profile will make it easy for scammers to find your profile and learn about you through old posts and photos.



THINK BEFORE YOU ACT

Be wary of communications that push you for immediate action or ask for personal information. Never share personal information through email, especially if you do not know the sender.



WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, texts, posts, social media messages and online advertising are an easy way for cyber criminals to get to you. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting.



USE REVERSE IMAGE SEARCH

If you are unsure if you are being scammed, do a reverse image search of the potential scammer's profile picture. You may see that image belongs to a completely different person, or has been affiliated with different online identities.

HOW TO AVOID ONLINE ROMANCE SCAMS

IF YOU THINK YOU ARE BEING SCAMMED

LOOK OUT FOR RED FLAGS

Scammers can be very convincing, however there are ways to identify a scammer, including but not limited to the following red flags:

1. There's a request for money for urgent matters, such as medical expenses or a plane ticket. Never send money to someone you haven't met in person.
2. The person claims to live overseas or be in the military.
3. The person professes love quickly.
4. There's pressure to move the conversation off the platform to a different site.

KNOW WHAT ACTION TO TAKE

If you believe you are the victim of a scam, it is important to take the following steps:

1. Cease communications with the scammer immediately.
2. Take note of any identifiable information you may have on the scammer, such as their email address, IP address, or other information in their [full header](#).
3. Contact your bank or credit card company if you think you've given money to a scammer.
4. Report the scammer to the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).
5. Notify the website or app where you met the scammer.



DID YOU KNOW?

People who said they were ages 40 to 69 reported losing money to romance scams at the highest rates – more than twice the rate of people in their 20s. At the same time, people 70 and over reported the highest individual median losses at \$10,000. [\(ETC\)](#)

ADDITIONAL RESOURCES

- ✓ [FTC: Report a Scam to the Federal Trade Commission](#)
- ✓ [NCSA: Own Your Role in Cybersecurity: Start With the Basics](#)
- ✓ [ESET: Keep scammers from stealing your heart](#)



CyberSecurity4biz.com

can your business survive without its data?