

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a romance scam

<https://cyberguardlab.com/blog/romance-scam-online>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

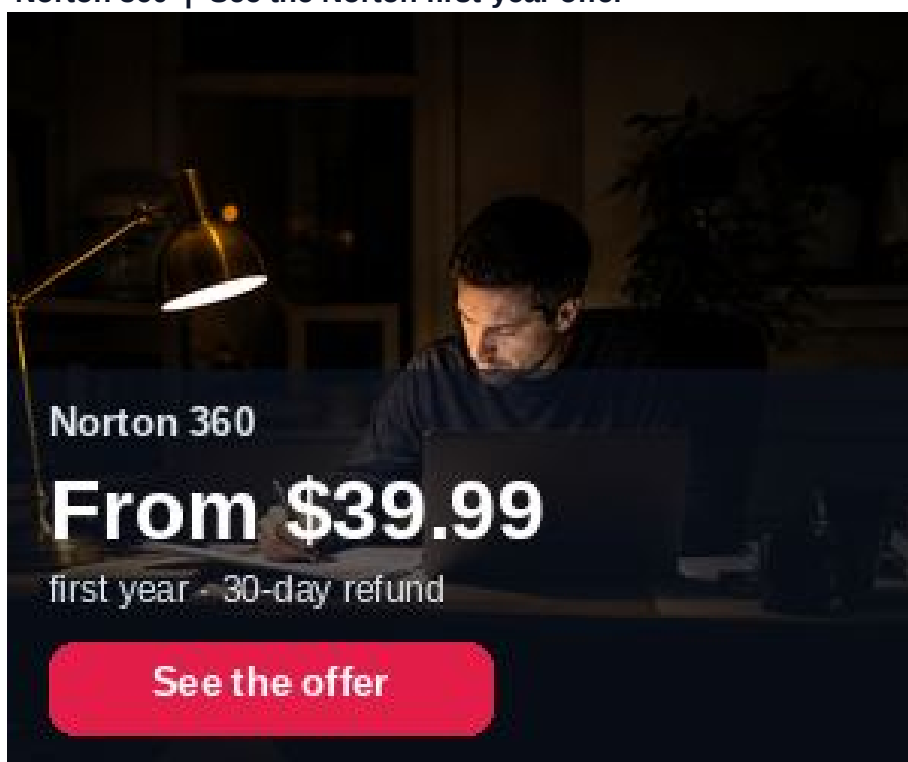
A romance scam is when someone builds a fake relationship on a dating app or social media, then invents an urgent story so you send money, gift cards, wires, or crypto. The FTC bottom line is simple: never send money or gifts to a sweetheart you have not met in person. This guide is about online romance / dating payment scams, not gift-card payment demands in general, phishing emails, fake IRS messages, or tech-support calls (though those stories sometimes mix with romance scripts). You do not need to buy antivirus to stop chatting and report.

1. Know the romance-scam pattern

From FTC romance-scam guidance, watch for this arc:

Paid link

Norton 360 | See the Norton first-year offer

A man is sitting at a desk in a dimly lit room, working on a laptop. A desk lamp is on to his left, casting a warm glow. The background is dark, with some plants visible. The text 'Norton 360' is in the top left, 'From \$39.99' is in large bold letters in the center, and 'first year - 30-day refund' is below it. A red button with white text 'See the offer' is at the bottom.

Norton 360

From \$39.99

first year - 30-day refund

See the offer

[See the Norton first-year offer](#)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

- * They move you off the dating platform fast - They push email, text, or calls so the app cannot flag them.
- * They cannot meet in person - Common excuses: overseas work, oil rig, military deployment, or an international organization.
- * They ask for money after trust builds - Plane tickets, medical bills, visas, getting out of trouble, or crypto investing help.
- * They pick a hard-to-reverse payment - Wire (Western Union / MoneyGram), gift-card PINs, payment apps, or cryptocurrency.
- * They pressure you to act now - Same four scam signs the FTC lists elsewhere: pretend to be someone you trust, invent a problem or prize, pressure you, and control how you pay.

2. Common household romance-scam stories

Scammers change the love story; the ask stays money:

- * Emergency travel - Need a ticket to visit you this week.
- * Medical crisis - Surgery for them or a relative; you must send money today.
- * Military / oil-rig / overseas work - They cannot leave, cannot video call, or need cash to clear a transfer.
- * Crypto or investment help - They offer to teach you and then move you into a fake trading site.
- * Gift cards or wires just this once - Same trap as gift-card scams; codes and wires are hard to reverse.
- * Isolation - They ask you not to tell family or friends. That secrecy is part of the scam.

3. What to do in the first 15 minutes

- * Stop sending money - Do not buy gift cards, wire funds, use a payment app, or transfer crypto for them.
- * Stop communicating - Block and leave the chat. Do not argue one last time.
- * Talk to someone you trust - FTC says telling a friend or family member often exposes the scam.
- * Search and reverse-check - Search their claimed job plus the word scammer. Do a reverse image search on the profile photo. Mismatched names or reused photos are red flags.
- * If you already paid - Contact the gift-card company, wire service, bank, card issuer, or crypto platform right away and ask about a freeze or refund. Keep receipts and screenshots.
- * Report - File at ReportFraud.ftc.gov. Also report the profile to the dating app or social network where you met them.
- * If bank or identity details leaked - Follow credit card fraud first-hour and, when needed, report identity theft on IdentityTheft.gov.
- * Optional device check - Only if you clicked a link, opened an attachment, or installed remote-access software: run Windows Security / Microsoft Defender. Buying a suite is not required first - see [Is Microsoft Defender enough?](#)

4. Safer dating habits (without buying software)

- * Keep early chats on the platform messaging tools when you can.
- * Video-call before you get emotionally invested; excuses to avoid video are a warning.
- * Never share Social Security numbers, bank logins, one-time codes, or photos of IDs for verification.
- * Treat any money ask from someone you have not met in person as a hard stop.

FAQ

How do I spot a romance scam?

Someone you met online builds a fast emotional bond, cannot meet in person, then asks for money with urgency and a specific payment method (wires, gift cards, apps, crypto). That pattern is a romance scam.

What is the number one way to avoid losing money?

Per the FTC: never send money or gifts to a sweetheart you have not met in person.

What if I already sent gift cards or a wire?

Contact the card issuer, wire company, bank, or app immediately; ask to reverse or freeze what you can; then report at

[ReportFraud.ftc.gov](https://reportfraud.ftc.gov).

Is a crypto investment tip from a dating match different?

Still a romance / investment hybrid scam. Do not send crypto because a chat partner told you to.

Do I need antivirus to handle a romance scam?

No. Stop payments, block the person, and report. Defender or good habits are enough unless you also clicked malware or installed remote tools.

If you still want a paid suite

Stopping a romance payment ask does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is refusing money to people you have not met, talking to someone you trust, and reporting. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV ([paid link](#)), Norton ([paid link](#)), Bitdefender ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * [What To Know About Romance Scams \(FTC\)](#)
- * [How To Avoid a Scam \(FTC\)](#)
- * [Avoiding and Reporting Gift Card Scams \(FTC\)](#)
- * [ReportFraud.ftc.gov \(FTC\)](https://reportfraud.ftc.gov)
- * [Recognize and Report Phishing \(CISA\)](#)
- * [Windows security overview \(Microsoft\)](#)

Also read

- * [How to spot a gift card scam](#)
- * [How to spot a phishing email](#)
- * [How to spot a fake IRS or tax refund scam](#)
- * [Tech support scam phone calls: what to do](#)
- * [What to do in the first hour after credit card fraud](#)