

CyberGuardLab

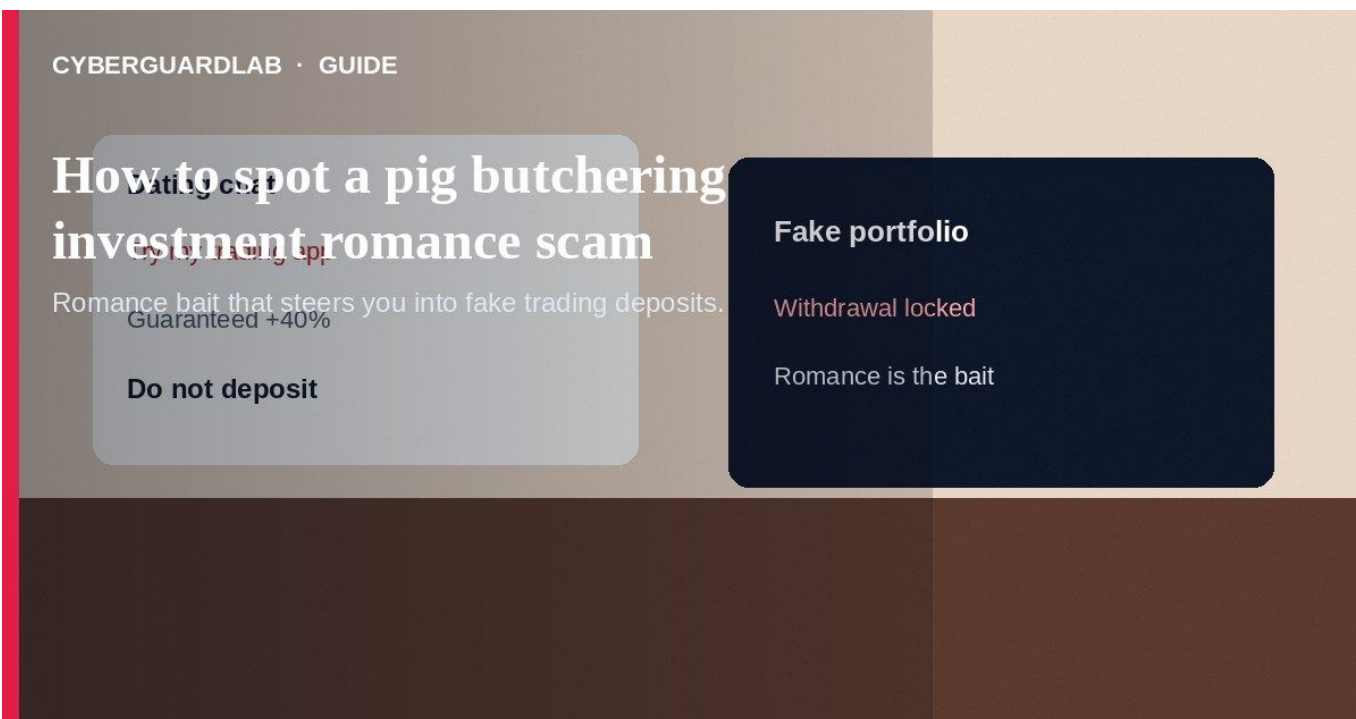
Household antivirus, explained

cyberguardlab.com

How to spot a pig butchering investment romance scam

<https://cyberguardlab.com/blog/pig-butchering-investment-romance-scam>

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 pig butchering investment romance scam starts with a friendly chat-often on a dating app, social media, or a "wrong number" text-then slowly builds trust before steering you into a fake trading platform or crypto "coach." The romance is bait; the goal is repeated deposits into accounts the scammer controls. Do not invest because someone you met online insists on a private app, QR code, or "mentor" dashboard. Do not send crypto, wires, or gift cards to unlock gains. If you already deposited, stop contact, save every chat and wallet address, and report through the FTC and your payment provider. This guide is about romance-plus-fake-investment grooming-not a pure military romance overseas money scam, not a simple catfish dating profile, and not a one-shot wire transfer romance advance-fee story that never mentions trading.

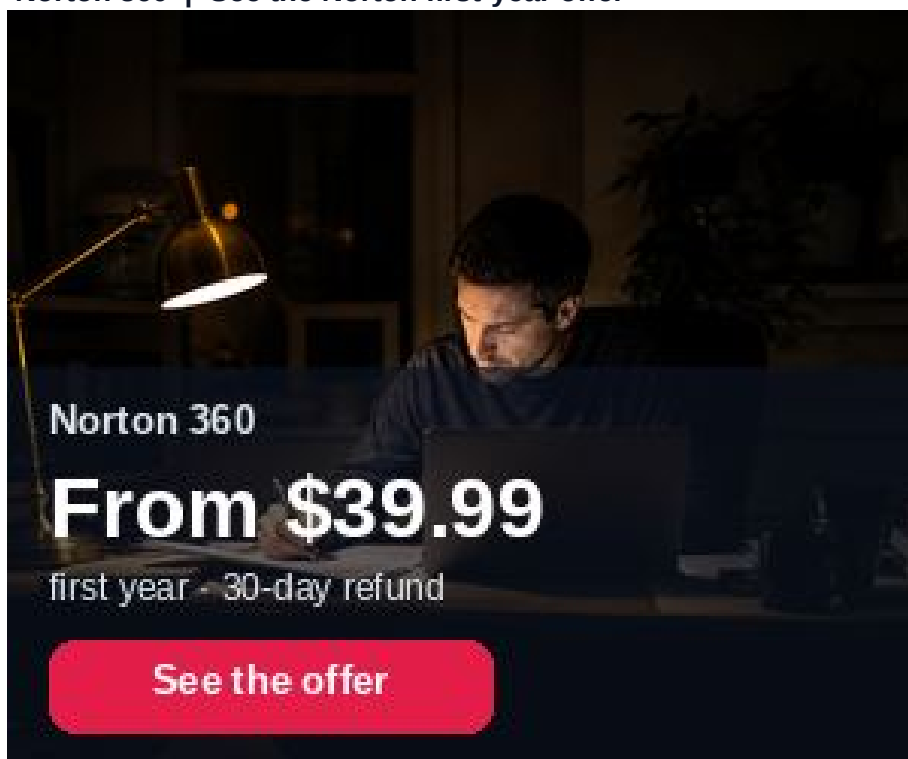
1. How this scam works

Contact feels accidental or flattering: a wrong-number text that turns warm, a dating match who mirrors your interests, or a LinkedIn "investor" who compliments your profile. Over days or weeks they share photos, voice notes, and daily check-ins.

When trust is high they "accidentally" mention big returns from crypto, forex, or a private fund-then send a link to a polished trading site or mobile app.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton>

You may see a dashboard with growing balances you cannot withdraw without "tax," "gas," or "anti-money-laundering" fees. Each fee unlocks a bigger "release." Screenshots of profits are often forged. Unlike a military romance that asks for leave fees or travel cash, pig butchering centers on investment deposits. Unlike catfishing alone, the endgame is financial extraction through fake markets-not only a fake identity.

2. Red flags before you pay

3. Safer habits (buy-nothing)

- * Keep romance and money separate. Anyone who mixes intimacy with investment coaching is a red flag.
- * Do not install trading apps or visit URLs from a dating or chat partner-open known broker sites yourself if you invest at all.
- * Refuse crypto, wire, or gift-card "margin," "tax," or "unlock" payments.
- * Reverse-image-search profile photos and ask for a live video call with specific gestures; hang up on excuses.
- * Talk to a trusted offline friend before sending any funds.
- * For payment-app pressure after a romance pitch, see Zelle and Cash App payment scams.

A polite wrong-number text that never ends, then pivots to markets, is a common grooming script. Mute and block early. Household members who are newly single or recently retired are frequent targets-share this pattern before anyone "tests" a small deposit to see if withdrawals work.

4. If you already paid

- * Stop further deposits or "release" fees immediately. Document chats, wallet addresses, TXIDs, and the fake platform URL.
- * Contact your bank, card issuer, or crypto exchange fraud team the same day; ask about recalls or freezes where possible.

- * Report at ReportFraud.ftc.gov and file with IC3.gov for internet crime involving crypto or wires.
- * If the romance started on a dating or social app, report the profile through that platform's official tools.
- * Change passwords on email and any accounts you reused with the scammer; enable two-factor authentication.
- * If you typed credentials or opened attachments on a fake page, change passwords, enable two-factor authentication, and scan your device with a trusted tool such as Norton or Bitdefender. Keep one primary real-time antivirus-avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

FAQ

Is every online romance that mentions crypto a pig butchering scam?

No-but romance plus a private trading link, guaranteed returns, and blocked withdrawals is a classic pattern. Treat that combination as fraud until proven otherwise through independent channels.

How is this different from a military romance money scam?

Military romance scams usually invent overseas deployment fees, leave paperwork, or travel costs. Pig butchering sells a fake investment relationship and fake portfolio growth.

Can I recover money stuck on the trading dashboard?

Balances on scammer-controlled sites are not real brokerage holdings. Paying extra "taxes" almost never releases funds; it deepens the loss.

What if they video-called me?

Deepfakes and hired actors exist. A video call does not prove honesty when the investment path is still an unverified private platform.

If you still want a paid suite

Avoiding a a pig butchering investment romance scam does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

- * FTC ReportFraud
- * IdentityTheft.gov
- * FTC: Romance scams
- * FTC: Cryptocurrency scams
- * FBI IC3

Also read

- * How to spot a wire transfer romance or advance-fee scam
- * How to spot a military romance overseas money scam
- * How to spot a catfish profile on a dating app
- * How to spot a Zelle or Cash App payment scam
- * How to report a scam to the FTC