

threat level: **human**

The attack vector you can't patch.

Romance and Pig-Butchering Scams

How an online relationship turns into a fake investment, and the move that ends it.

\$1.14B

reported losses to romance scams in 2023

FTC, 2024

\$8.6B

investment-fraud losses in 2025, the top crime type

FBI IC3, 2025

\$2,000

median loss per romance-scam victim

FTC, 2024

HOW THE APPROACH STARTS

01 A fast, intense connection

Love-bombing within days, then a quick push to a private chat app.

02 Always a reason not to meet

The camera is broken, they are overseas, on a rig, or deployed in the military.

03 The relationship races ahead of reality

Talk of marriage or soulmates before you have ever met in person.

WHEN MONEY ENTERS (PIG BUTCHERING)

04 A 'can't-miss' investment they teach you

A trading or crypto platform a new partner kindly helps you set up.

05 Small wins you can withdraw, at first

Early payouts build trust before a big deposit you can never pull back out.

06 Fees to unlock your own money

Taxes, release fees, or a minimum balance demanded before any withdrawal.

TACTICS THAT KEEP YOU HOOKED

07 Isolation from friends and family

They discourage you from sharing the relationship or the 'investment' with anyone.

08 Recycled photos and scripts

Stolen pictures and lines that surface in a reverse-image search or scam databases.

09 Constant contact, then sudden crises

Endless messaging builds the bond, then an emergency suddenly needs money fast.

DO / DON'T

DO

- Reverse-image-search their profile photos before you trust anyone.
- Insist on a live video call early, and watch closely for excuses.
- Tell a friend or family member about anyone you meet online.
- Keep your money and savings completely separate from an online relationship.
- Research any platform with your national regulator before depositing a cent.

DON'T

- Do not send money, gift cards, or crypto to someone you have not met in person.
- Do not move funds to a trading or crypto app a new partner introduced.
- Do not pay 'fees' or 'taxes' to unlock a withdrawal. That money is gone too.
- Do not keep the relationship secret from people who could spot the scam.

THE ONE MOVE

Reverse-image-search their photos, insist on a live video call, and never move money or savings to a platform someone you met online introduced. Real love does not require a wire transfer, and a platform that blocks a small withdrawal has already taken the rest.

IF IT HAPPENS

- Stop all payments immediately. Do not send a 'final' fee.
- Screenshot the profiles, chats, and transactions before they vanish.
- Contact your bank or the crypto platform to try to halt or recall transfers.
- Report to the FBI at ic3.gov and the FTC at reportfraud.ftc.gov.
- Block and do not re-engage. Victims are deliberately targeted a second time.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: U.S. FTC (2024); FBI Internet Crime Complaint Center (IC3) Annual Report (2025). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.