

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a catfish profile on a dating app

<https://cyberguardlab.com/blog/catfish-dating-app-profile>

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.

CYBERGUARDLAB · GUIDE

How to spot a catfish profile on a dating app

Reverse image search

Stolen or AI dating photos that hide a false identity.

Require live video

No money, no codes

Dating app

Stock / AI photos

Avoids live video

A catfish profile on a dating app uses stolen, AI-generated, or heavily misleading photos and life details to build a false identity. The goal may be attention, social engineering, later financial fraud, or access to your personal data. Do not send money, intimate images, or account codes to someone whose identity you cannot verify. Do not move to private apps solely because a match insists. If you already shared sensitive material, lock down accounts and report through the app and the FTC when money or blackmail is involved. This guide is about fake dating identities-not the full pig butchering investment funnel, not military overseas money scripts, and not sextortion blackmail that starts from explicit images.

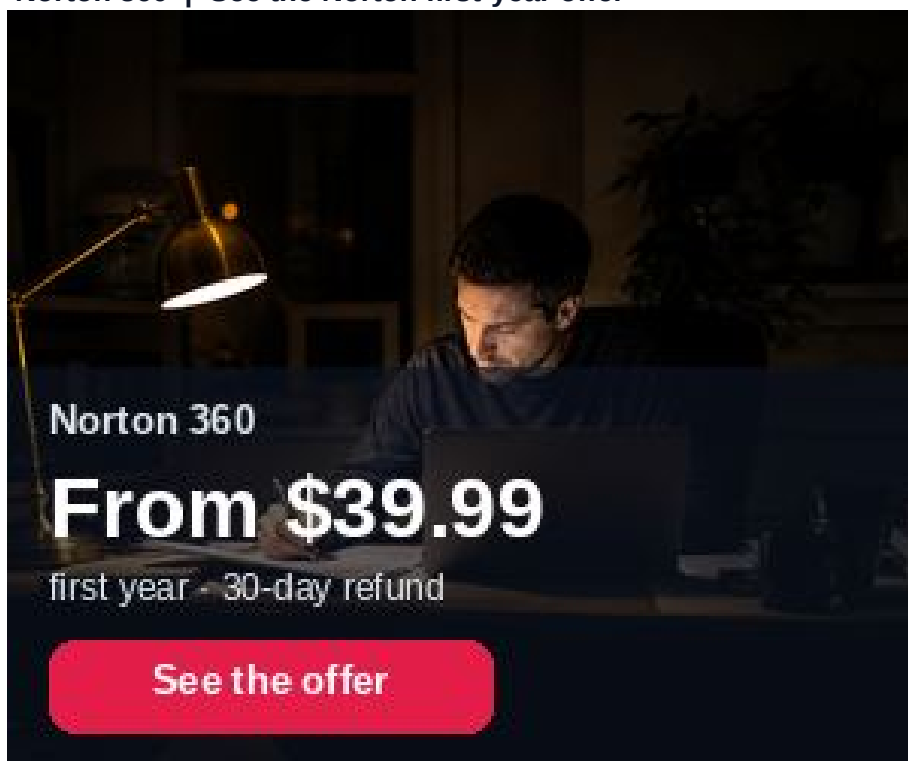
1. How this scam works

Profiles look polished: model-like photos, few or no casual shots, inconsistent ages or locations, and bios that are vague or copied. Matches avoid live video, invent travel excuses, or send only pre-recorded clips. Some ask for your full name, workplace, or family details early. Others push quickly to WhatsApp, Telegram, or text-then disappear or pivot into money or

investment talk.

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>

Catfishing alone is identity deception. It becomes other scam types when money, fake trading, military emergencies, or blackmail appear. Spotting the fake profile early reduces those follow-on risks.

2. Red flags before you pay

3. Safer habits (buy-nothing)

- * Reverse-image-search profile photos before sharing personal details.
- * Require a live video call with a random gesture before meeting or sending money.
- * Keep early chats inside the dating app's messaging tools.
- * Never send one-time codes, passwords, or ID scans to a match.
- * Decline any request for money, crypto, or "help with fees."
- * If the chat pivots to investments, see pig butchering investment romance scams.

AI-generated portraits and voice clones are getting better. A single video still is not proof-prefer interactive live calls and offline meetings in public places when you choose to meet.

4. If you already paid

- * Stop contact and payments. Save profile URLs, usernames, and chat exports.
- * Report the profile through the dating app's official safety tools.
- * Contact your bank or payment provider if money left your account.
- * File at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov) if you lost money or shared financial data.
- * If intimate images were shared and threats began, treat it as sextortion-do not pay, and use [IdentityTheft.gov](https://www.identitytheft.gov) / [ReportFraud](https://www.reportfraud.ftc.gov) as needed.

* 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 attractive profile a catfish?

No. Focus on verification: live video, consistent details, and no money asks-not attractiveness alone.

How is catfishing different from pig butchering?

Catfishing is fake identity. Pig butchering usually starts with social trust (sometimes via catfish photos) but centers on fake investment deposits.

They want my Social Security number to "book a flight to visit." Should I?

No. That is identity-theft bait, not romance.

What if we already met once in person?

Meeting reduces photo fraud risk but does not make money requests safe. Still refuse wires, gift cards, and investment links from new partners.

If you still want a paid suite

Avoiding a a catfish profile on a dating app 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: Online dating](#)
- * [FBI IC3](#)

Also read

- * [How to spot a pig butchering investment romance scam](#)
- * [How to spot a military romance overseas money scam](#)
- * [How to spot a sextortion blackmail scam](#)
- * [How to spot a phishing email](#)
- * [How to report a scam to the FTC](#)