CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a cryptocurrency scam

https://cyberguardlab.com/blog/cryptocurrency-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 cryptocurrency scam is when someone tricks you into buying crypto and sending it to them, or into "investing" on a fake platform. Per FTC consumer advice, only scammers demand payment in cryptocurrency, and only scammers guarantee profits or big returns. This guide is about crypto payment and investment cons, not romance payment asks in general, gift-card PINs, fake job offers, or phishing emails (though those scripts often end in a crypto ask). You do not need to buy antivirus to refuse a crypto payment demand.

1. Know what makes crypto different (before any "deal")

From FTC cryptocurrency guidance:

* It exists mainly electronically - You buy it through an exchange, app, website, or crypto ATM. Bitcoin and Ether are common names; many other coins exist.
* It is not like an FDIC bank deposit - Crypto accounts are not backed by a government the way insured bank deposits are. If an exchange fails or a wallet is drained, there may be no government bailout.
* Values move fast - Prices can swing sharply. A balance that looks large today can shrink quickly.
* Payments are hard to reverse - Credit and debit cards have dispute paths. Crypto usually does not. Once you send it, you typically get it back only if the other person returns it.
* "Anonymous" is oversold - Many transfers land on a public blockchain ledger. That does not make a scam safer for you.

2. Common household crypto-scam stories

Scammers change the script; the ask is still "buy crypto and send it":

* Investment / "guaranteed returns" - Social media, texts, or dating chats promise "lots of money" with "zero risk," then move you to a fake trading site.
* Romance + crypto tutoring - Someone you met online "teaches" you to invest, then asks you to send crypto. FTC line: never mix online dating and investment advice.
* Business, government, or job impersonators - Fake support, fake agency, or fake employer tells you to buy crypto and send it to "protect" or "unlock" funds.
* Blackmail / sextortion - Messages claim they have compromising photos or data and demand crypto. Do not pay; report.
* Any advance crypto demand to buy something or "secure" money - Legitimate businesses do not demand you prepay in crypto that way.

3. What to do in the first 15 minutes

* Stop sending crypto - Do not buy more coins, do not transfer to a wallet address they gave you, and do not "verify" on a site they linked.
* Stop communicating - Block the chat, number, or profile. Do not argue for a refund in the same thread.
* Search the pitch - Search the company or coin name plus "scam," "review," or "complaint."
* If you already paid - Contact the exchange, ATM operator, or app you used right away; report fraud and ask whether a freeze or reverse is possible. Keep screenshots and wallet addresses.
* Report - File at ReportFraud.ftc.gov. For blackmail or major cybercrime, also use IC3.gov.
* If bank logins or IDs leaked - Follow credit card fraud first-hour and, when needed, 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 crypto habits (without buying software)

* Treat any demand to pay in cryptocurrency as a hard stop.
* Ignore "guaranteed" profit pitches on social media, texts, or dating apps.
* Keep early dating chats off investment tutoring; if they ask for crypto, it is a scam.
* Research any seller before you pay; assume transfers are final.
* Turn on MFA on email and exchange accounts (see CISA's MFA guidance in Sources).

FAQ

How do I spot a cryptocurrency scam?

Someone pressures you to buy crypto and send it, or promises easy, risk-free crypto profits - often from social media, a dating match, a fake job, or a fake agency. That pattern is a crypto scam.

Is a crypto investment tip from a dating match different from a romance scam?

It is often both. FTC says never mix online dating and investment advice; treat a crypto ask from someone you have not met in person as a scam.

What if I already sent cryptocurrency?

Contact the company or ATM you used immediately, ask about reversing or freezing the transfer, save evidence, and report at ReportFraud.ftc.gov (and IC3 when appropriate).

Do legitimate companies ask me to pay them in crypto first?

Per FTC consumer advice: only scammers demand payment in cryptocurrency in that advance-demand pattern.

Do I need antivirus to handle a crypto scam?

No. Refuse the payment, 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 crypto payment ask does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is refusing irreversible crypto payments to strangers, researching before you invest, 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 Cryptocurrency and Scams (FTC)
* How To Avoid a Scam (FTC)
* ReportFraud.ftc.gov (FTC)
* Internet Crime Complaint Center - IC3
* Recognize and Report Phishing (CISA)
* Turn On MFA (CISA)
* Windows security overview (Microsoft)

Also read

* How to spot a romance scam
* How to spot a gift card scam
* How to spot a job offer scam
* How to spot a fake IRS or tax refund scam
* How to spot a phishing email