How to spot a fake check scam

https://cyberguardlab.com/blog/fake-check-scam

A fake check scam is when someone you do not know asks you to deposit a check (often for more than they owe you), then tells you to send some of that money back by wire, gift cards, money order, or crypto. Per FTC guidance, do not rely on money from a check unless you know and trust the person, and never use money from a check to send gift cards, money orders, cryptocurrency, or wires. This guide is about overpayment and fake-check scripts, not gift-card payment demands alone, crypto investment pitches, or job-offer scams without a check (though those often combine). You do not need to buy antivirus to refuse an overpayment check.

1. Know the fake-check pattern

From FTC fake-check guidance:

* A stranger sends a check - It may look like a business check, personal check, cashier's check, money order, or an electronic check.
* The amount is too high - They "overpay" and ask you to refund the difference or pay fees, taxes, supplies, or installers.
* They invent a story - Mystery shopping, personal assistant, car-wrap ad, prize, online sale overpayment, and similar scripts.
* They rush you to send money out - Gift-card PINs, Western Union / MoneyGram wires, money orders, or crypto.
* Funds in your account are not proof - Banks must make deposits available quickly. Fake checks can take weeks to bounce. You can still owe the bank.

2. Common household fake-check stories

* Mystery shopping - Deposit a check, then wire money while "testing" gift cards or a transfer service.
* Personal assistant - Deposit a check, buy gift cards, and send the PIN numbers to a "boss."
* Car wrap advertising - Deposit a check, then send money to fake "decal installers."
* Prize / sweepstakes - You "won," but must send taxes or shipping fees from the check.
* Online sale overpayment - Buyer "accidentally" sends too much and asks you to refund the balance.

3. What to do in the first 15 minutes

* Do not send any money from the check - No gift cards, wires, money orders, or crypto.
* Do not spend the deposit - Even if the balance looks available.
* Talk to your bank - Tell them you suspect a fake check; ask what to do with the deposit.
* If you already paid out - Contact the gift-card issuer, wire company, money-order issuer, or crypto app immediately and report fraud. Ask about a reverse or freeze. Keep receipts.
* Report - File at ReportFraud.ftc.gov.
* If identity details leaked - Use credit card fraud first-hour and IdentityTheft.gov when needed.
* Optional device check - Only if you also clicked a malware link or installed remote tools: run Microsoft Defender. A suite is not required first.

4. Safer habits (without buying software)

* Only trust checks from people or businesses you already know.
* Toss "free prize" offers that require you to pay fees.
* Never accept a check for more than the selling price on an online sale.
* Treat gift-card payment demands as a scam - gift cards are for gifts, not payments.
* If a job or romance chat starts with a check plus a wire/gift-card ask, walk away.

FAQ

How do I spot a fake check scam?

A stranger asks you to deposit a check, then send some of that money elsewhere. The story can be a job, prize, sale, or assistant role - the overpayment plus outbound payment is the tell.

The bank already showed the money. Is it safe?

No. FTC notes banks make funds available quickly; a fake check can still fail weeks later, and you may owe the bank.

What if I already bought gift cards or wired money?

Contact the card issuer or wire company immediately, ask to reverse or freeze what you can, then report at ReportFraud.ftc.gov.

Is an overpayment on a Facebook Marketplace sale different?

Same pattern. Do not refund an "accidental" overpayment from a stranger's check.

Do I need antivirus to handle a fake check scam?

No. Stop outbound payments, contact your bank, and report. Defender is enough unless you also opened malware.

If you still want a paid suite

Stopping a fake check overpayment does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is refusing to send money from a stranger's check, talking to your bank, 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

* How To Spot, Avoid, and Report Fake Check Scams (FTC)
* How To Avoid a Scam (FTC)
* What To Know About Cryptocurrency and Scams (FTC)
* ReportFraud.ftc.gov (FTC)
* Recognize and Report Phishing (CISA)
* Windows security overview (Microsoft)

Also read

* How to spot a gift card scam
* How to spot a job offer scam
* How to spot a cryptocurrency scam
* How to spot a romance scam
* What to do in the first hour after credit card fraud