

CyberGuardLab

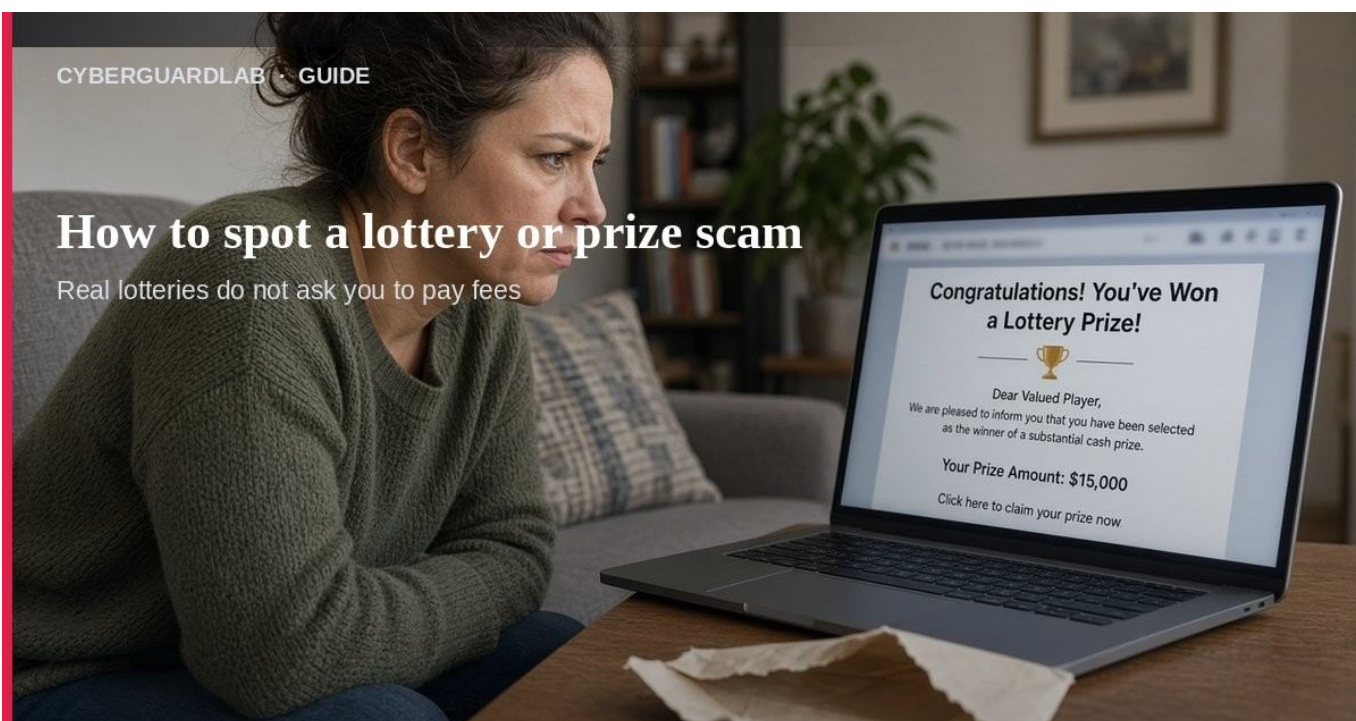
Household antivirus, explained

cyberguardlab.com

How to spot a lottery or prize scam

<https://cyberguardlab.com/blog/lottery-prize-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 lottery or prize scam is when someone says you won money, a car, a gadget, or a sweepstakes - then asks you to pay or hand over account details to "claim" it. Per FTC consumer advice, real prizes are free, and anyone asking for taxes, shipping, processing fees, or customs duties to release a prize is a scammer. This guide is about prize / lottery / sweepstakes claims, not gift-card payment asks, fake checks, or crypto payment demands (those payment rails often show up inside a prize script). You do not need to buy antivirus to hang up on a prize call.

1. Three FTC signs it is a prize scam

- * You must pay to get the prize - Taxes, shipping, processing, customs: all scam tells. Real prizes are free.
- * You must pay to improve your odds - Real sweepstakes are free and by chance. Asking you to pay to raise odds is illegal; only scammers do that.
- * You must give bank, card, or SSN details to claim - There is no reason to give financial or Social Security numbers to

claim a prize. Delete the message; do not click.

2. Common household scripts

- * "You've won!" call or text - Big cash, car, watch. You do not remember entering. Reply and they demand fees.
- * Fake well-known brand - Names that sound like Publishers Clearing House or other real contests. Real companies do not demand money to release a prize.
- * Fake government lottery bureau - Made-up "National Sweepstakes Bureau" or pretending to be the FTC. The government will not call demanding money to collect a prize.
- * Foreign lottery tickets - FTC: messages about a foreign lottery are almost certainly a scam; it is illegal for U.S. citizens to play a foreign lottery that way.
- * Fake check "winnings" - They send a check and ask you to wire some back. Banks can take weeks to bounce a fake check - see fake check scam.
- * Hard-to-reverse payment rails - Wire, gift cards, crypto, cash apps, cash in the mail.

3. What to do in the first 15 minutes

- * Do not pay and do not share account numbers - Hang up, delete, block.
- * If you already paid - Contact your bank, card issuer, or payment app immediately and ask about a reverse or fraud report. Act fast.
- * If you gave personal info - Start at IdentityTheft.gov recovery steps.
- * Search the pitch - Company name + "scam" / "complaint" / "review."
- * Report - File at ReportFraud.ftc.gov. For larger cybercrime or when money moved online, also use IC3.gov.
- * Warn family - Especially anyone who gets "you've won" calls.
- * Optional device check - Only if you clicked a link or opened an attachment: run Defender. Suite purchase is not required first.

4. Safer habits around real contests

- * Real sweepstakes are free and by chance.
- * Look up the real company yourself - never use the caller's contact info.
- * Expect more junk mail and ads if you enter legitimate drawings.
- * Skills contests that keep charging for harder rounds are a common money pit; treat them with extreme caution.
- * Never send gift cards, crypto, or wires to "unlock" a prize.

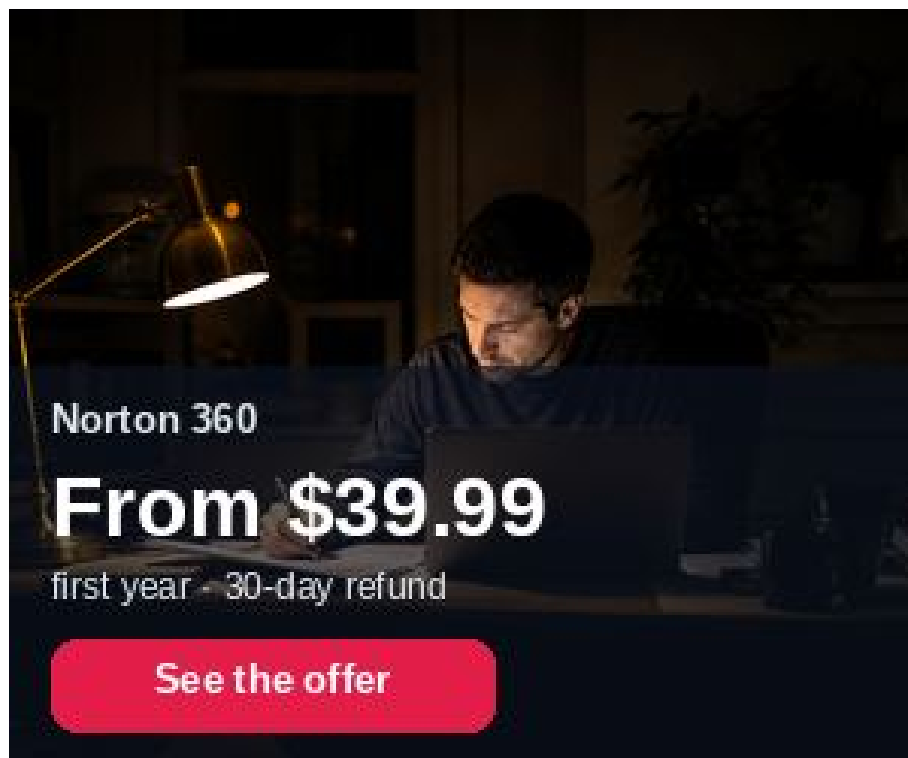
FAQ

How do I spot a lottery or prize scam?

Anyone who says you won and then asks for money, gift cards, crypto, wires, or bank/SSN details is running a prize scam. Real prizes are free.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](#)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

I didn't enter any contest - can I still have won?

If you did not enter, you did not win. Unexpected "winner" messages are a classic scam opener.

What if they already sent a check?

Do not spend it or send money back. Treat it as a fake check pattern and talk to your bank.

Will antivirus stop a prize scam call?

No. The fix is refusing payment and reporting. Antivirus only matters if you also clicked malware.

Is Publishers Clearing House always a scam?

Real companies run real contests, but scammers impersonate those names. A demand for money to claim a prize is never from a legitimate sweepstakes company.

If you still want a paid suite

Stopping a prize scam does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is refusing fees, hanging up, 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

- * Fake Prize, Sweepstakes, and Lottery Scams (FTC)
- * Don't pay for a prize (scam) (FTC alert)
- * How To Avoid a Scam (FTC)
- * ReportFraud.ftc.gov (FTC)
- * Internet Crime Complaint Center - IC3
- * Turn On MFA (CISA)
- * Windows security overview (Microsoft)

Also read

- * [How to spot a gift card scam](#)
- * [How to spot a fake check scam](#)
- * [How to spot a cryptocurrency scam](#)
- * [How to spot a phishing email](#)
- * [Report identity theft at IdentityTheft.gov](#)