CyberGuardLab

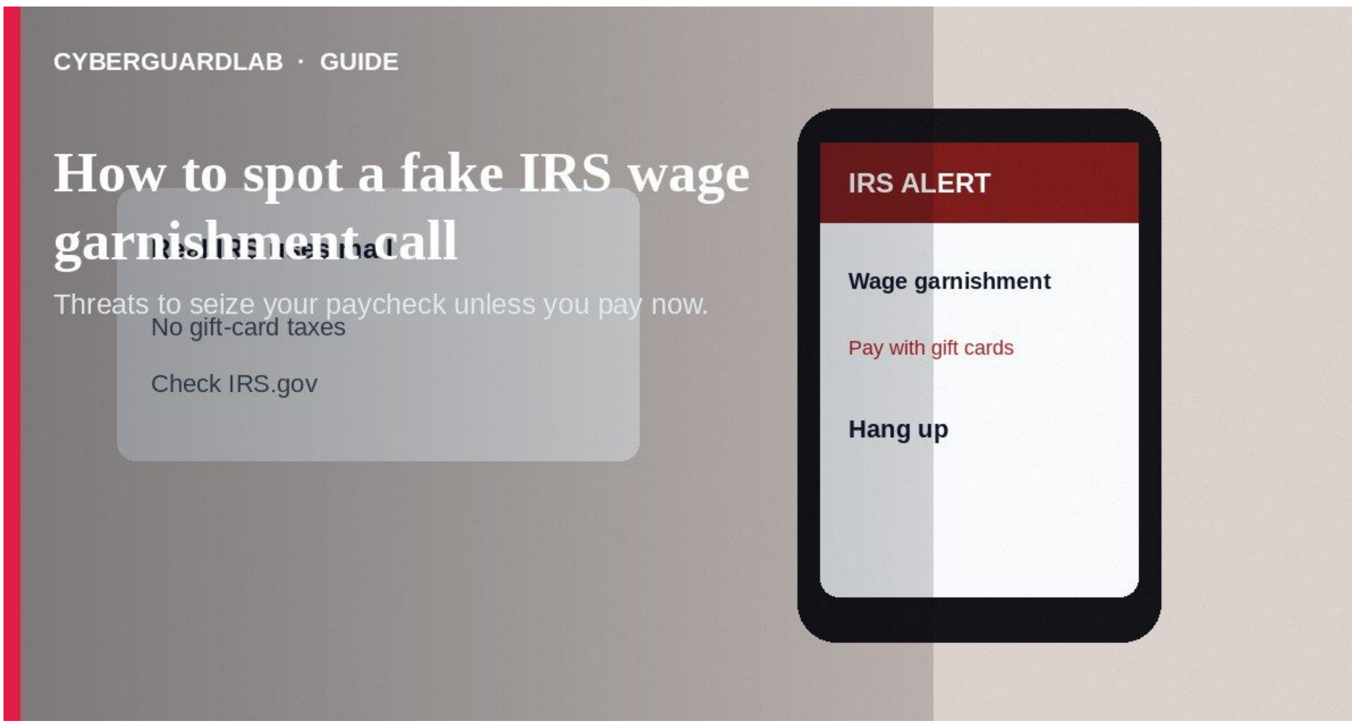
Household antivirus, explained

cyberguardlab.com

How to spot a fake IRS wage garnishment call

https://cyberguardlab.com/blog/irs-wage-garnishment-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 fake IRS wage garnishment call claims the IRS will seize your paycheck today unless you pay immediately-often by gift card, wire, or crypto. Real IRS collection follows notices by mail first in ordinary cases, and agents do not demand gift cards. Do not pay. Hang up.

This article focuses on wage-garnishment threats-not generic refund phishing alone, though both may appear in phishing email patterns and fake IRS tax refund scripts. Payment demands often overlap with gift card scams. No software purchase required.

1. How fake IRS wage-garnishment scripts work

* Spoofed caller ID - The phone shows a local or official-looking number. The caller says you owe back taxes, a lawsuit is filed, or wages will be garnished within hours (IRS tax scam alerts).
* Borrowed facts - They may name your employer, recite a partial SSN from a breach, or put a fake "agent" and "police officer" on a conference call.
* Gift-card or crypto demand - Payment instructions push retail cards, wires, or crypto ATMs (How to know it is really the IRS).
* Fake levy paperwork - Follow-up emails or texts include case numbers and PDF "levy" notices.
* Secrecy pressure - Protect your job, protect your family, pay now, stay quiet-panic is the product.

2. Red flags before you pay

Cue	Likely legitimate	Likely scam
First notice	IRS typically starts many collection actions with mail to your address on file	Sudden threat-only phone call with no prior mail you can verify
Payment methods	IRS payment options through official IRS.gov processes	Gift cards, crypto, wire to an individual, cash drop
Arrest threats	You can hang up and verify	Immediate arrest stories meant to keep you on the line
Caller ID	Can be spoofed either way-do not trust it alone	Pressure based solely on an "IRS" caller ID label
Secrecy	You can consult a tax professional	"Do not tell your employer or family"
Data asks	You initiate contact via IRS.gov tools when needed	Demands full SSN, PINs, or remote access on the spot

3. Safer habits (buy-nothing)

* Hang up. Do not engage with payment instructions.
* Call the IRS only using numbers published on IRS.gov if you truly need to check your account-not numbers from the

suspicious call.
* Check your postal mail for real IRS notices. Review any online IRS account access you already set up through official channels.
* Never pay tax debts with gift cards or crypto because a caller said so.
* If your employer mentions a real levy, verify through official IRS and employer HR or payroll processes-not a random call.
* Ignore threats that you must stay on the line while driving to a store.

4. If you already paid or shared data

* Contact your bank, card issuer, or gift-card companies immediately with receipts.
* Preserve call logs, numbers, card PINs if any remain, and scripts used.
* Report to TIGTA and to ReportFraud.ftc.gov.
* If SSN or other identity data was shared, start IdentityTheft.gov steps and monitor tax transcripts carefully.
* Tell a trusted tax professional if you have real filing questions. A real balance does not mean the threatening caller is real.
* Remove remote-access apps if installed and change passwords (FTC guidance if you were scammed).

FAQ

Does the IRS ever call taxpayers?

The IRS may call in some situations, but unexpected threats demanding gift cards or instant wires are classic impersonation. Verify through official IRS.gov information and mail.

They knew part of my SSN. Does that mean it is real?

No. Partial SSNs appear in breaches and prior scams. Knowledge of data is not proof of authority.

How is a wage garnishment scam different from an IRS refund scam?

Garnishment scams threaten to take your paycheck unless you pay now. Refund scams lure you with money owed to you to steal credentials or deposits. See fake IRS tax refund scams.

Will the IRS demand Apple or Amazon gift cards?

No. Gift-card tax payments demanded by phone are a scam hallmark.

What if I ignored prior real IRS mail?

Address real notices through official channels or a trusted tax pro. Do not catch up by paying a threatening cold caller.

Do I need paid antivirus to avoid an IRS garnishment scam?

No. Hanging up and verifying through IRS.gov are enough. Buy-nothing is valid.

If you still want a paid suite

Avoiding a fake IRS wage garnishment call does not require paid antivirus. Hang-up habits and official IRS.gov 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

* Tax Scams / Consumer Alerts (IRS)
* How to know it's really the IRS contacting you (IRS)
* Treasury Inspector General for Tax Administration (TIGTA)
* ReportFraud.ftc.gov
* IdentityTheft.gov

Also read

* How to spot a fake IRS tax refund scam
* How to spot a gift card scam
* How to spot a Social Security scam
* How to spot a phishing email

* How to report a scam to the FTC