

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a home warranty cold call scam

[Read online: https://cyberguardlab.com/blog/home-warranty-cold-call-scam](https://cyberguardlab.com/blog/home-warranty-cold-call-scam)

Published September 25, 2026 | Updated September 25, 2026

Short answer

Hang up on unexpected home-warranty sales or "coverage expiring" calls; verify any real plan only with your own contract or a phone number you already trust; never pay by gift card, wire, or remote access from a cold call.

Advertising disclosure: CyberGuardLab is an independent comparison site. We are not TotalAV, Norton, Bitdefender, McAfee, or Avast. If you buy through our links, we may earn a commission, which can affect ranking and placement.

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 home warranty cold call scam

Pushy renewal calls, fake deadlines, and requests for payment



A home warranty cold call (or robocall, or "final notice" mailer that pushes you to call) is usually a high-pressure pitch for a service contract you did not ask for - not proof that your coverage is about to vanish. The FTC notes that so-called home warranties are typically service contracts that cost extra, may duplicate coverage you already have, and that unwanted calls about service contracts can be telemarketers seeking money or personal information. Hang up. Do not give a card number,

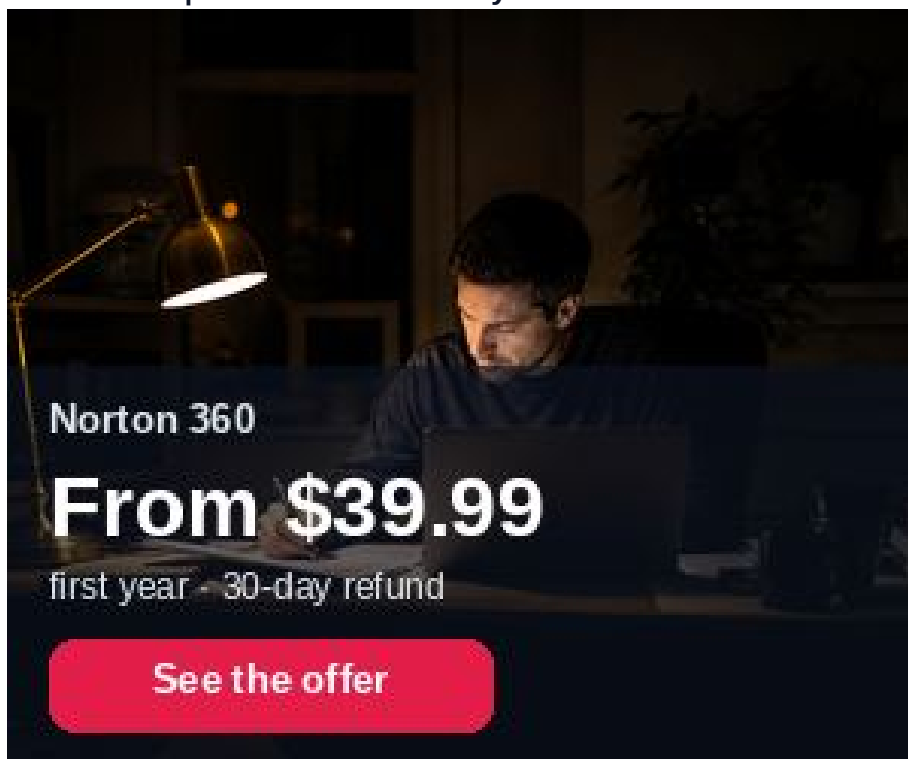
Social Security number, or remote-access tool. Do not pay with gift cards, wire, crypto, or a payment app because a stranger on the phone told you to. If you already bought a real home warranty or builders' coverage, verify it yourself with the contract, insurer, or lender contact you already have - never with the number printed on the cold call or mailer. This pattern is distinct from a utility shutoff scam (same urgency, different fake threat). CyberGuardLab is independent. Referral fees may affect product placement on other pages. Buying nothing and sticking to free verification habits is a valid outcome.

The short answer

Hang up on unexpected home-warranty sales or "coverage expiring" calls; verify any real plan only with your own contract or a phone number you already trust; never pay by gift card, wire, or remote access from a cold call.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://trysecurities.com/offer/norton?dtm=gg&cid=)

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

What a home warranty cold call usually looks like

Scammers and aggressive telemarketers reuse the same fear: "your home warranty / appliance coverage expires today." The job is not to protect your HVAC - it is to get payment details or enough personal data to keep selling.

Common shapes US households report:

- * Robocall or live cold call claiming your warranty file is "closing," your coverage lapsed, or your mortgage company required a renewal.
- * "Final notice" mailer that names your lender or street address (often pulled from public records) and pushes a callback number.
- * Callback after you pressed a digit - a closer who asks for a card "to activate" or a deposit "today."
- * Payment asks that legitimate renewals do not use from a cold call - gift cards, wire, crypto, cash apps, or remote desktop so they can "process the claim."
- * Follow-up that morphs into tech support - "we need to check your PC for the warranty portal" is the tech support scam phone call playbook with a new opening line.

FTC robocall guidance is blunt: sales robocalls you did not authorize in writing are almost always illegal; hang up; do not press numbers to "speak to someone" or "remove yourself"; caller ID is easy to fake. Report unwanted robocalls at DoNotCall.gov and scams at ReportFraud.ftc.gov.

A real home warranty or builders' service contract you already bought is a different product. Keep the paperwork. Renew only through the company named on your contract, after you typed the URL or dialed the number yourself.

Cold warranty pitch vs utility shutoff vs real coverage

Signal | Home warranty cold call / mailer | Utility shutoff scam | Coverage you already bought

Opening hook | "Your home warranty expires today - renew or pay huge repair bills." | "Power / gas / water will be cut in an hour unless you pay now." | You have a signed contract, policy ID, and a company you chose.

Ask | Card on the spot, gift cards, wire, remote access, SSN "for the file." | Immediate payment by card, gift card, or payment app. | Renewal or claim through the vendor named on your paperwork.

Pressure | "Final notice," fake mortgage branding, countdown on the call. | Same-day shutoff threat. | Normal billing calendar - not a stranger's urgency.

Safe next step | Hang up. Check your own contract / insurer / lender contacts. | Hang up. Call the utility number on a bill you already have. | Use only contacts printed on your contract or statement.

Related guide | This page | Utility shutoff scam | Your contract + FTC service-contract shopping tips

If the caller demands gift cards, treat it like a gift card scam immediately - stop and hang up.

How to handle a home warranty cold call (US household steps)

Do this when any unexpected warranty pitch appears. You do not need a paid product to finish these steps.

* Hang up. Do not press digits. Close the robocall or live pitch. Do not call back a number from the message or mailer. FTC robocall advice: hang up; pressing buttons often leads to more calls.

* Ignore payment and remote-access asks. Card numbers, SSN, "activation fees," gift cards, wires, crypto, cash apps, or AnyDesk/TeamViewer-style tools from a cold call are stop signs - not renewal steps.

* Check whether you already have coverage - yourself. Look at closing paperwork, homeowner insurance endorsements, builder warranty documents, or any service-contract email you saved. Use only phone numbers and URLs printed on those documents or on your insurer's/lender's known site.

* If you want a new service contract later, shop on your schedule. The FTC's home-warranty / service-contract guidance: compare cost vs likely repairs, read deductibles and exclusions, research the company with "review" / "complaint," and get terms in writing. Do that on a calm day - not during a cold call.

* If you already paid or shared data, treat it as incident response. Contact your bank or card issuer to dispute charges; change passwords for any account you mentioned; if personal data was stolen, start at IdentityTheft.gov. Report the scam at ReportFraud.ftc.gov and report robocalls at DoNotCall.gov. Our checklist: How to report a scam to the FTC.

* Tell the household. Agree that nobody renews "home warranty" from a cold call, and that gift-card payment for a warranty is never valid.

Signs the pitch is fake or unsafe (scan table)

Use this as a quick pass before you spend money or time.

Sign | Why it matters | What to do

You never bought a home warranty / service contract | "Renewal" for coverage you do not have is a classic lure | Hang up; shred or ignore the mailer

Caller or mailer claims to be your "mortgage home warranty division" | Public records make lender names easy to paste onto a sales pitch | Call your real lender only with a number you already trust

Asks for gift cards, wire, crypto, or cash-app payment | Legitimate renewals do not collect that way from a cold call | Stop; see gift-card scam guide; report to FTC

Wants remote access "to process the warranty" | Tech-support takeover | Hang up; see tech-support guide

Threatens immediate loss of coverage, lawsuits, or huge repair bills unless you pay now | Fear used to skip verification | End the contact; verify on your own paperwork

Caller ID looks local or "official" | Caller ID is easy to spoof | Do not trust the display; hang up

Free habits that reduce the blast radius

You do not need a new subscription to lower damage if a warranty pitch gets through.

- * Household rule: no warranty purchases from cold calls or unexpected mailers.
- * Keep real contracts (builder warranty, service contract, homeowners policy) in one folder so "expiring coverage" claims are easy to check.
- * Register numbers on the National Do Not Call Registry and use carrier call-blocking / labeling - they reduce volume; they do not stop every scammer.
- * Unique passwords and 2FA on email and bank accounts limit what a stolen card or SSN fragment can unlock.
- * Optional antivirus / web filtering is a separate layer for malware after a bad click; it does not replace hanging up.

What this page is not

This page is not a ranking of home warranty brands, not a coupon page, and not legal advice about your specific contract.

It does not claim CyberGuardLab lab scores or "#1 anti-scam" ranks. It does not tell you to ignore a real renewal notice from a company named on a contract you already have - it tells you to verify there, not with the cold caller. Official reporting stays on ReportFraud.ftc.gov, DoNotCall.gov, and IdentityTheft.gov if personal data was stolen.

If you decide a paid extra is a real job

Most households can handle warranty cold calls with the free steps above. Open a paid page only if you already named a job - for example broader web filtering, cross-device AV, or identity alerts after you gave a scammer personal data - and you will actually use it.

- * PC / Mac suite with phishing and web protections many households already compare: Norton plans (paid link; confirm renewal price).
- * Independent-test-oriented suite option: Bitdefender plans (paid link).
- * Household suite shopping starting point: TotalAV plans (paid link; confirm renewal).
- * Multi-device bill under one vendor: McAfee plans (paid link; confirm device limit).
- * Another suite path some homes already use: Avast plans (paid link).

Buying nothing beyond free hang-up and contract-check habits is still valid. Paid links above are on-site only.

FAQ

Is a home warranty cold call always a scam?

Often it is an illegal or unwanted sales robocall / high-pressure pitch. Even if someone is selling a real-looking service contract, you should never buy under cold-call pressure. Hang up and research on your own time using FTC service-contract shopping tips.

The mailer has my lender's name and address. Doesn't that mean it's official?

No. Mortgage and property details are often public. The FTC and consumer reporting have flagged official-looking warranty mailers that push you to call a sales line. Contact your lender only with a number from your statement or the lender's known website.

They want gift cards or a wire to "keep coverage active." What now?

Stop. That is a payment method scammers love. Read Gift card scam, hang up, and report at ReportFraud.ftc.gov.

How is this different from a utility shutoff call?

Utility scams threaten same-day cut-off of power, gas, or water. Warranty cold calls threaten expensive repairs or "lapsed coverage." Both want urgent payment; both require you to hang up and use contacts you already trust. See Utility shutoff

scam.

I already gave a card number on a warranty call. What should I do first?

Call the number on the back of your card to report possible fraud and dispute the charge. Change passwords for accounts you discussed. Report at ReportFraud.ftc.gov. If SSN or ID data was shared, use IdentityTheft.gov.

Do I need paid antivirus to stop these calls?

No. Spotting is a hang-up and verify-yourself habit. Antivirus can be an optional layer for malware after a bad click; it does not replace ending the call.

Sources

- * So what's the deal with "home warranties"? (FTC)
- * Extended Warranties and Service Contracts (FTC)
- * Robocalls (FTC)
- * Hang up on auto warranty robocalls (FTC) - same hang-up playbook
- * DoNotCall.gov
- * ReportFraud.ftc.gov
- * IdentityTheft.gov
- * Avoiding Social Engineering and Phishing Attacks (CISA)

Also read

- * Utility shutoff scam
- * Gift card scam
- * Tech support scam phone call
- * How to report a scam to the FTC