

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fake Geek Squad renewal email

Read online: <https://cyberguardlab.com/blog/fake-geek-squad-renewal-email>

Published October 4, 2026 | Updated October 4, 2026

Short answer

Do not call the number in an unexpected Geek Squad renewal email or text. Check your plans only in the Best Buy account you open yourself, call your card issuer about any real charge, and never let a "refund agent" remote into your computer or watch you log in to your bank.

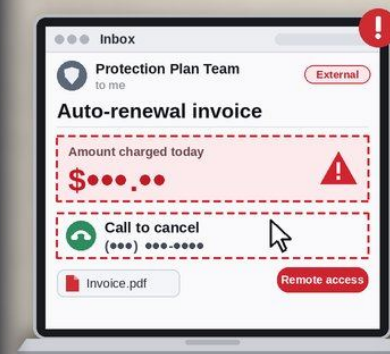
Advertising disclosure: CyberGuardLab is an independent comparison site. We are not TotalAV, Norton, Bitdefender, McAfee, or Avast. If you buy through our links, we may earn a commission, which can affect ranking and placement.

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 fake Geek Squad renewal email

Don't call the number in the email. Check plans in an account you open yourself



A fake Geek Squad renewal email (or text) is an unexpected message that claims you were - or are about to be - charged hundreds of dollars to renew a Geek Squad membership or "protection plan," and tells you to call a phone number inside the message within a short deadline to cancel or dispute it. The FTC describes exactly this pattern: an alarming renewal charge

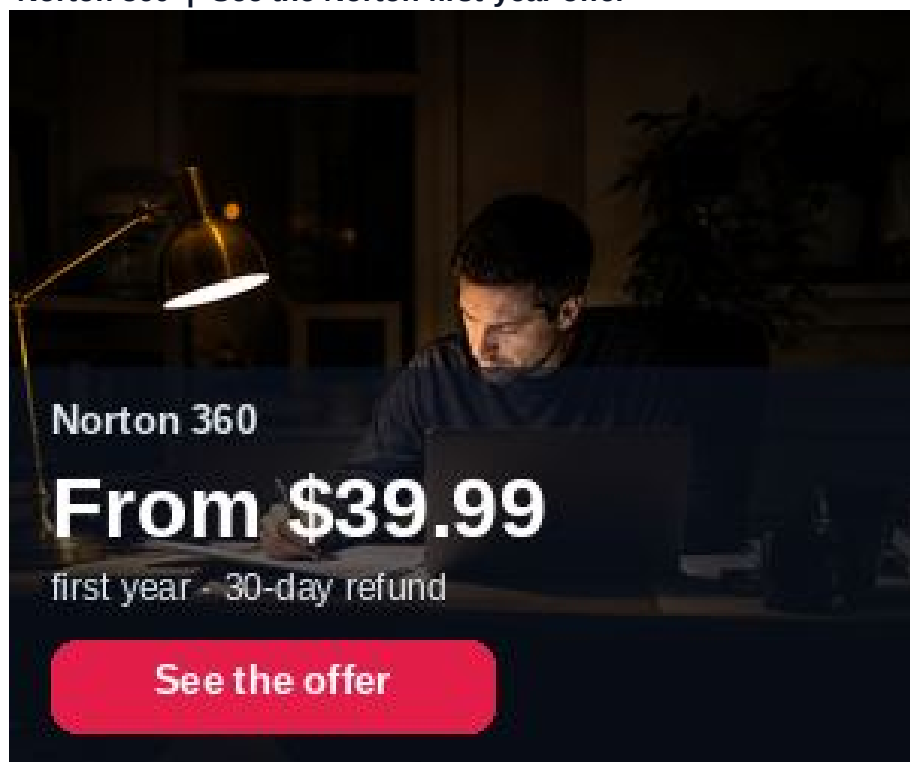
plus a "call within 24 hours" number. The number reaches the scammer, not Best Buy. The safe habit is to ignore the number, attachment, and link in the message, check any real plan only inside the Best Buy account you open yourself (bestbuy.com or the Best Buy app), and never give a caller remote access, bank login, or a "refund" transfer. This page is about Geek Squad / Best Buy-branded renewal and invoice emails or texts only. The generic fake-invoice costume is Fake invoice bill pay scam; the cold "Microsoft / tech support" call is Tech support scam phone call. 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

Do not call the number in an unexpected Geek Squad renewal email or text. Check your plans only in the Best Buy account you open yourself, call your card issuer about any real charge, and never let a "refund agent" remote into your computer or watch you log in to your bank.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

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

What a fake Geek Squad renewal email usually looks like

The message is built to make you panic about a large charge so you call before you think. The job is remote access, bank or card details, or a fake "refund" that turns into you sending money.

Common shapes US households report:

- * Email "invoice" or "order confirmation" for a Geek Squad renewal - often a few hundred dollars - with a phone number to call "if you did not authorize this."
- * Text message saying your Geek Squad membership will auto-renew today unless you call within 24 hours (the pattern the FTC warns about).
- * PDF attachment styled as a receipt with Best Buy or Geek Squad logos, sent from a free webmail address or a look-alike domain rather than a Best Buy account you recognize.

* Phone "refund department" after you call - the agent asks you to install a screen-sharing app, log in to your bank "to receive the refund," or read back a code.

* "We refunded too much" twist - the screen shows a bigger deposit than promised and you are asked to send back the difference by gift card, wire, crypto, or cash. That is the pattern in Fake refund overpayment scam.

FTC guidance: if you think the message might be real, contact the company using a phone number you know is real - not the number in the message - and report scams at ReportFraud.ftc.gov.

We do not claim Best Buy or Geek Squad "never emails about plans." Real customers do get real order and plan messages. The safe habit is always the same: leave the unexpected message and check your plans inside the Best Buy account you open yourself.

Fake Geek Squad renewal email vs real Best Buy notice vs related lure

Signal | Fake Geek Squad renewal email / text | Real Best Buy / Geek Squad notice (typical) | Related lure (cold tech support call)

Opening hook | "Your Geek Squad plan renewed for \$xxx - call within 24 hours to cancel." | Order or plan details you can also see after you sign in to your Best Buy account yourself. | "Your computer has a virus - this is tech support" on a call or pop-up (see Tech support scam phone call).

Ask | Call the number in the message; install remote access; log in to your bank for a "refund." | Usually none inside the message - manage plans inside your account. | Remote access, "security fee," or gift card payment over the phone.

Pressure | Short deadline, large charge, "final notice." | You check on your schedule; the plan is visible in your account. | Same-call fear and urgency.

Safe next step | Ignore the number. Open bestbuy.com or the Best Buy app yourself; call your card issuer if a charge appears. | Confirm the plan only inside the account you opened. | Hang up; see Tech support scam phone call.

Related guide | This page | bestbuy.com / Best Buy app opened by you | Tech support scam phone call | Fake invoice bill pay scam

If the "agent" asks you to open your bank website while they watch your screen, stop and hang up - that is the setup for a fake refund, not a cancellation.

How to verify a Geek Squad renewal message (US household steps)

Do this when any unexpected Geek Squad or Best Buy renewal, invoice, or "auto-renew today" message appears. You do not need a paid product to finish these steps.

* Do not call the phone number, reply, open the attachment, or tap a link in the message. Close it. A number printed inside an unexpected invoice is the scammer's line.

* Open Best Buy the way you already trust. Type bestbuy.com yourself or open the Best Buy app you installed earlier, sign in, and look at your orders and plans. If you need to talk to Best Buy, use contact details you find on bestbuy.com yourself or on a real receipt - not the number in the email.

* Match the charge against your own records. If no plan appears in your account, and no matching charge appears on your card or bank statement, treat the message as spam. If a real unexpected charge does appear, call the number on the back of your card (Credit card fraud - first hour).

* Never install remote-access software, log in to your bank, or read back a code for a "refund agent." A cancellation does not require someone to control your computer or watch your bank session. If anyone says they "refunded too much," hang up - do not send anything back.

* If you already called, gave access, or shared details, treat the first hour as incident response. Disconnect the computer from the internet, remove any remote-access app the caller had you install, call your bank and card issuer from the numbers on your card or statement, and change passwords from a different device you trust. Follow Clicked a phishing link - first hour. If identity data was stolen, use IdentityTheft.gov.

* Report the message and tell the household. Mark the email as phishing / junk; forward scam texts to 7726 (SPAM); file at ReportFraud.ftc.gov. Agree that nobody calls numbers from unexpected renewal emails. Checklist: How to report a scam to

the FTC.

Signs the message is fake or unsafe (scan table)

Use this as a quick pass before you pick up the phone.

Sign | Why it matters | What to do

The only way to "cancel" is a phone number inside the message | Routes you to the scammer | Ignore; open your Best Buy account yourself

Sender is a free webmail address or a look-alike domain | Not an account you recognize from past Best Buy orders | Mark as phishing; do not reply

"Call within 24 hours" or "charge posts today" | Fear used to skip checking | Slow down; check your card statement and account

Caller wants remote access or a screen-sharing app | Full control of your computer and sessions | Hang up; never install it

Caller asks you to log in to your bank to "receive the refund" | Setup for a fake overpayment and send-back | Hang up; call your bank from the card number

Asked to return an "over-refund" by gift card, wire, crypto, or cash | Direct cash-out; hard to recover | Stop; report at ReportFraud.ftc.gov

Free habits that reduce the blast radius

You do not need a new subscription to lower damage if a fake Geek Squad renewal email gets through.

- * Bookmark bestbuy.com and check plans only there or in the Best Buy app.
- * Household rule: no one calls a number printed in an unexpected invoice or renewal message.
- * Keep card alerts on so a real charge shows up in your banking app, not only in an email.
- * Never let anyone you did not call yourself remote into a household computer. Related costume: Tech support scam phone call.
- * Optional antivirus or web filtering is a separate layer after a bad tap or a remote-access install; it does not replace the check-your-own-account habit. Built-in Microsoft Defender plus those habits is enough for many households.

What this page is not

This page is not a guide to buying, cancelling, or comparing real Geek Squad or Best Buy protection plans, and not legal advice about a specific charge.

It does not claim CyberGuardLab lab scores or "#1 anti-phishing" ranks. It does not tell you to ignore a real plan you can also see inside your Best Buy account - it tells you to check there, not in the cold message. It is not the generic fake-invoice guide (see Fake invoice bill pay scam) and not the cold tech-support call guide. It is also not the software-subscription renewal guide: Fake Microsoft 365 renewal scam covers fake software subscription renewals, while this page covers fake Geek Squad or Best Buy protection-plan renewals that push a callback and a remote "refund." Official recovery and reporting stay with Best Buy (through contact details you find yourself), your card issuer, ReportFraud.ftc.gov, and IdentityTheft.gov if personal data was stolen.

If you decide a paid extra is a real job

Most households can handle fake Geek Squad renewal emails with the free steps above. Open a paid page only if you already named a job - for example broader web filtering, cross-device AV after a remote-access install, 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 check-your-own-account habits is still valid. Paid links above are on-site only.

FAQ

Is the Geek Squad renewal email real if I actually have a Geek Squad plan?

Having a real plan is exactly why the scam works. Do not use the number in the message. Sign in to your Best Buy account yourself and look at the plan there; if something looks wrong, contact Best Buy using details you find on bestbuy.com or a real receipt.

I opened the PDF attachment. Is my computer infected?

Opening a PDF is lower risk than installing an app a caller sends you, but it is not zero. Update your PDF reader and operating system, run a full scan with Microsoft Defender or the antivirus you already use, and do not call the number in the PDF. If you also typed passwords anywhere, change them from a device you trust.

I called and let them remote into my computer. What should I do first?

Disconnect from the internet, remove the remote-access app, and call your bank and card issuer using the number on your card. Change passwords from a different, trusted device and follow Clicked a phishing link - first hour. Report at ReportFraud.ftc.gov.

They said they refunded too much and I need to send the difference back. Should I?

No. That is the overpayment trick: the "deposit" is usually money moved between your own accounts or a fake screen. Hang up, call your bank from the number on your card, and see Fake refund overpayment scam.

How do I report a fake Geek Squad renewal email?

Mark the email as phishing / junk, forward scam texts to 7726 (SPAM), and file at ReportFraud.ftc.gov. Steps for the FTC side are in How to report a scam to the FTC.

Do I need paid antivirus to spot these emails?

No. Spotting is a habit: ignore the number, check your own Best Buy account and card statement, and never give remote access. Microsoft Defender plus those habits is enough for many households. Antivirus can be an optional layer after a bad install; it does not replace that habit.

Sources

- * How to recognize a fake Geek Squad renewal scam (FTC)
- * How To Spot, Avoid, and Report Tech Support Scams (FTC)
- * How To Recognize and Avoid Phishing Scams (FTC)
- * How to Recognize and Report Spam Text Messages (FTC)
- * ReportFraud.ftc.gov
- * IdentityTheft.gov
- * Avoiding Social Engineering and Phishing Attacks (CISA)

Also read

- * Fake invoice bill pay scam
- * Tech support scam phone call
- * Fake refund overpayment scam
- * Fake Microsoft 365 renewal scam
- * How to report a scam to the FTC