

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

What to do if you get a package you didn't order

[Read online: https://cyberguardlab.com/blog/package-you-didnt-order-brushing-scam](https://cyberguardlab.com/blog/package-you-didnt-order-brushing-scam)

Published October 9, 2026 | Updated October 9, 2026

Short answer

Don't scan a QR code in the package and don't contact the sender. Check your order history and card statements to rule out an order on your own account. Then report it to the marketplace and to the FTC, change your shopping passwords, and look at your credit reports. You don't have to pay for it or send it back.

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

What to do if you get a package you didn't order

Don't scan or contact the sender. You can keep it, then report it.



A package you didn't order is usually a brushing scam: a seller ships a cheap item to your name and address so it can post fake "verified buyer" reviews as if you bought it. The FTC, the U.S. Postal Inspection Service (USPIS), and Amazon all describe this pattern. The bigger risks are a QR code tucked inside that leads to a phishing page, which the FBI has warned

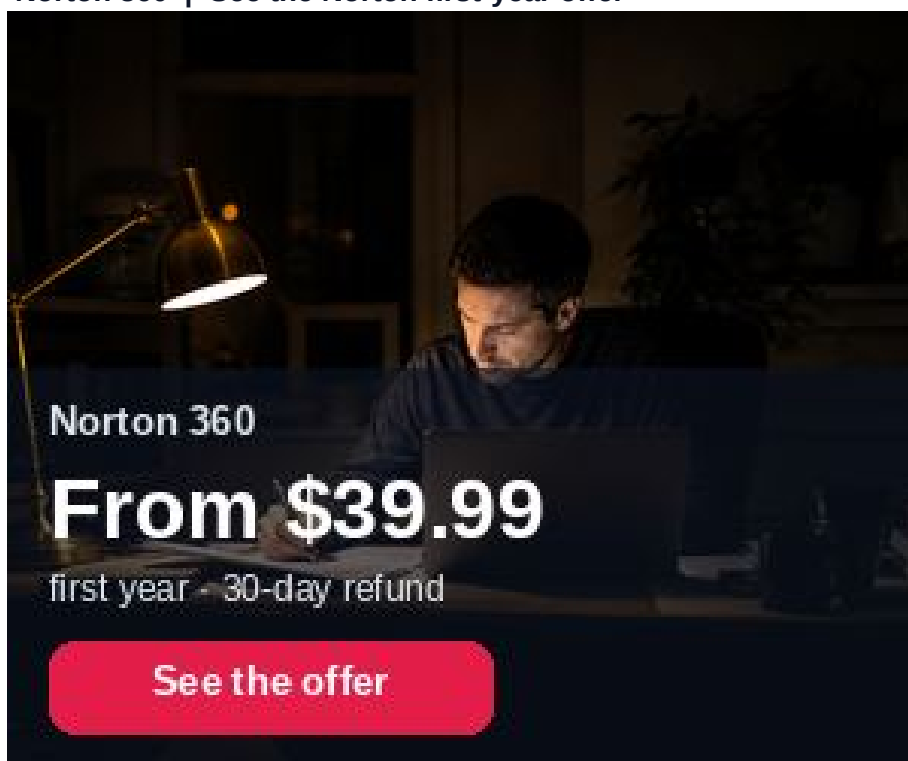
about, and what the package says about your personal information. The short version: don't scan anything in the box or contact the sender, check that no one used your own account, then report it. By U.S. law you can keep it. This page is about physical packages that show up unasked. Texts that say a package is waiting for a fee are a different trick, covered in How to spot a package holding fee delivery scam. We're an independent site; a few other pages earn referral fees, which can affect which products appear there. Nothing on this page requires a purchase.

The short answer

Don't scan a QR code in the package and don't contact the sender. Check your order history and card statements to rule out an order on your own account. Then report it to the marketplace and to the FTC, change your shopping passwords, and look at your credit reports. You don't have to pay for it or send it back.

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=>

Why someone mails you things you never bought

Brushing turns your address into proof of a sale. Here is how the official sources describe it:

- * The goal is fake reviews. USPIS says the sender is usually a third-party seller who found your address online and wants it to look like you are a verified buyer, so it can write a positive review in your name. The FTC calls it "brushing up" sales.
- * The items are cheap and random. The FTC says recent reports describe things like baby wipes, toothpaste, or seeds. An earlier FTC alert mentions fake "luxury" items such as rings, beauty products, and Bluetooth speakers.
- * The sender is hard to identify. USPIS says there may be no return address, or the return address may be a retailer. The FTC says the box may look like it came from a known company such as Amazon, or from someone you've never heard of.
- * Some boxes carry a QR code. The FBI warns that criminals send unsolicited packages with a QR code, often with no sender information, so you'll scan it to find out who sent it. The code can lead to a page that asks for personal and financial details or to software that steals data from your phone.
- * Your details are already out there. Amazon says brushing targets publicly available names and addresses. The FTC adds

that an unexpected package can be a sign someone has, or is trying to get, your personal information.

* Sometimes it isn't brushing at all. USPS notes that some criminals use a person's address and account information to have goods delivered, then grab the box before the resident does. That is why checking your own accounts comes before anything else.

Brushing package vs fee text vs an order on your own account

Signal | Brushing package | Package fee text or email | Order placed on your own account

What you see first | A real box at your door with your name on it | A message saying a parcel is held until you pay | An order in your history or a card charge you don't recognize

What the scammer wants | Fake reviews in your name; sometimes a QR scan | Your card number on a fake payment page | Goods paid with your account or card

Money taken so far | Usually none | Only if you pay | Yes, from your account or card

First move | Don't scan or reply; report to the marketplace | Delete it; check tracking in the carrier's own app | Secure the account and dispute the charge

Where to read more | This page | Package holding fee scam | Amazon account hacked - first hour

What to do if you get a package you didn't order (US household steps)

Work through these in order. All of them are free.

* Make sure it really isn't yours. Read the name and address on the label, then ask the people you live with and close friends or family whether they sent a gift. Amazon's own advice is to confirm it wasn't a gift before you report it.

* Check your own accounts and cards for the order. Look at the order history in your Amazon, Walmart, or other shopping accounts, and scan your recent card and bank statements. If the order is in your account or charged to your card and you didn't place it, treat it as account takeover, not brushing: follow What to do in the first hour if your Amazon account is hacked and dispute the charge with your card issuer.

* Don't scan any QR code and don't contact the sender. The FBI says not to scan QR codes from unknown origins. The FTC warns that if you look up the sender and reach out, whoever answers will likely try to get more personal information from you. A USPS notice adds that engaging can confirm your address and bring more packages. If you already scanned one, see How to spot a QR code scam for what to do next.

* Decide what happens to the item. You can keep it: the FTC says the law lets you keep unordered merchandise as a free gift without paying. USPS says an unopened package with a return address can be marked "Return to Sender" and USPS returns it at no charge, or you can throw it away if that is safe. The FTC advises caution about using products when you don't know who sent them. Seeds: the USDA says don't plant them; seal them in a bag, put them in the freezer, keep the packaging, and contact your State Plant Health Director. An unknown liquid or substance: follow USPS guidance on suspicious mail.

* Report it. If it came through Amazon, use Amazon's Report Unwanted Package form or customer service, with at least one tracking number from the label. USPS says to file a fraud report with the retailer, such as Amazon or eBay, and ask it to remove any fake reviews under your name. Then report the scam at ReportFraud.ftc.gov, and file at IC3.gov if a QR code led to a loss. Walkthrough: How to report a scam to the FTC.

* Lock down your accounts and check your credit. The FTC says to change passwords on your online shopping accounts and to check your credit for free at AnnualCreditReport.com; the FBI also suggests a free credit report from Equifax, Experian, or TransUnion. Turn on two-step verification where you can (Turn on 2FA for Gmail, Apple, and your bank), and see How to get a free annual credit report and read it for what to look for.

Quick check: harmless oddity or a reason to act fast?

Most brushing packages need only a report. These signs call for more.

What you notice | Why it matters | What to do now

A card says "scan to see who sent this" or "scan to return" | The FBI and FTC say these codes can lead to phishing pages or data-stealing apps | Don't scan; report it with the package details

The order shows up in your own account or on your card | USPS describes criminals using your account details and then stealing the delivery | Change the password, remove unknown cards, dispute the charge

Packages keep coming | Your name and address are being reused by sellers | Report each one to the marketplace with a tracking number

The box holds seeds or plant material | The USDA says non-compliant seeds can carry pests or plant diseases | Don't plant; bag, freeze, and report to your State Plant Health Director

Unknown powder or liquid | USPS has separate suspicious mail steps | Don't open further; follow USPS suspicious mail guidance

New accounts or inquiries on your credit report | Someone may be using your identity beyond fake reviews | Freeze your credit and report at IdentityTheft.gov

Cheap habits that make your address less useful to scammers

None of these needs a subscription.

- * Use a different password for every shopping account and keep them in a password manager. Setup help: Password manager setup for a US household.
- * Check whether your email address turned up in a known breach, and change any password you reused: How to check if your email was in a data breach.
- * Turn on purchase alerts from your card issuer so an order you didn't place shows up within minutes, not at the end of the month.
- * If your credit report shows accounts you didn't open, a freeze stops most new credit in your name: How to place a credit freeze at all three bureaus.
- * Treat any delivery-related text, email, or card with a link or QR code the same way: go to the store or carrier yourself instead. More on the texts: How to spot a fake delivery text scam.

What this page is not

This is a guide to one situation: a real box arrives, addressed to you, and nobody you know ordered it.

It is not about texts or emails that claim a package is held for a fee (package holding fee scam) or that ask you to reschedule a delivery (fake delivery text scam). It is not the general QR code guide for parking meters, menus, or posters (QR code scam). And it is not the recovery guide for when someone actually placed orders from your account (Amazon account hacked - first hour). It doesn't claim to know who sent your package, doesn't accuse Amazon, USPS, or any named seller of running the scheme, and doesn't give legal advice beyond what the FTC and USPS publish. If your personal data was misused, the official route is IdentityTheft.gov, alongside ReportFraud.ftc.gov and IC3.gov.

When paid security software might fit

A brushing package on its own is handled with the free steps above. Software can't stop strangers from mailing you things. Look at a paid product only if you already have a specific need, such as identity monitoring because your credit report showed accounts you didn't open, or a malware scan for a phone or computer after someone scanned a code and installed something.

- * Norton plans: suites that bundle device protection with identity features (paid link; check the renewal price).
- * Bitdefender plans: an option to compare if lab test results matter to you (paid link).
- * TotalAV plans: a household suite to price out (paid link; check what renews).
- * McAfee plans: one bill covering several devices (paid link; check the device limit).
- * Avast plans: another suite some homes already use (paid link).

Skipping all of these is a perfectly good choice. These paid links point only to pages on this site.

FAQ

Is it legal to keep a package I didn't order?

Yes. The FTC says companies can't send you unordered merchandise and then demand payment, and you're legally entitled to keep it as a free gift. USPS says the same: you may keep unsolicited merchandise and you are under no obligation to pay for it.

Do I have to send it back?

No. You don't need to return it. If it is unopened and has a return address, USPS says you can mark it "Return to Sender" and USPS will return it at no charge. If it came through Amazon and you want return options, Amazon says to contact its customer service.

Does a brushing package mean I've been hacked?

Not necessarily. Amazon says brushing uses publicly available names and addresses, so the sender may only have your name and address. The FTC says it can also be a sign that someone has, or is looking to steal, your personal information, so check your order history and card statements and change your shopping passwords to be safe.

There's a QR code in the box. What if I already scanned it?

Don't enter anything on the page it opened, and close it. If you typed a password, change it from a trusted device and turn on two-step verification; if you gave card details, call your card issuer. If an app was installed, remove it. The FBI says these codes can lead to requests for personal and financial information or to malicious software, and asks that you report it at IC3.gov. More first-hour steps: Clicked a phishing link - first hour.

I keep getting packages. How do I make it stop?

Report each package to the marketplace it came through, with a tracking number from the label, and file a report with USPS. Amazon says it investigates brushing reports and may suspend sellers and withhold payments. Don't contact the sender; a USPS notice says engaging can confirm your address and lead to more packages.

Should I freeze my credit after a brushing package?

Not automatically. Start by checking your reports for free at AnnualCreditReport.com, as the FTC suggests. If you see accounts or hard inquiries you don't recognize, freeze your credit at Equifax, Experian, and TransUnion and report identity theft at IdentityTheft.gov.

Sources

- * That unexpected package you got could be a brushing scam (FTC Consumer Advice, Aug 2026)
- * Got a package you didn't order? It's probably a scam (FTC Consumer Advice, Jan 2025)
- * What To Do if You're Billed for Things You Never Got, or You Get Unordered Products (FTC)
- * Brushing Scam (U.S. Postal Inspection Service)
- * Suspicious Mail (U.S. Postal Inspection Service)
- * Report (U.S. Postal Inspection Service)
- * Did you get a package you didn't order? (USPS News)
- * Unsolicited Packages Containing QR Codes Used to Initiate Fraud Schemes (FBI IC3 PSA I-073125-PSA)
- * Report Unsolicited Packages or Brushing Scams (Amazon Customer Service)
- * Non-Compliant Seeds: What You Need to Know (USDA APHIS)
- * AnnualCreditReport.com
- * ReportFraud.ftc.gov
- * Internet Crime Complaint Center (FBI IC3)
- * IdentityTheft.gov

Also read

- * Fake delivery text scam
- * QR code scams
- * Freeze your credit at all three bureaus
- * Check if your email was in a data breach