

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a work-from-home package reshipping scam

<https://cyberguardlab.com/blog/work-from-home-reshipping-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.

CYBERGUARDLAB · GUIDE

How to spot a work-from-home package reshipping scam

Strip labels

Fake WFH jobs that forward stolen packages.
Reship overseas

Not a real job

- Keep the receipts
- Do not forward boxes
- Report mule pitches

A work-from-home package reshipping scam hires you to receive boxes at home, strip the original packaging, and forward the goods-often overseas-while the "employer" pays with stolen cards. Reshipping goods is never a real job. Do not accept packages for strangers, throw away receipts, or send items to addresses your "boss" texts you. If you already forwarded packages or shared ID and bank details for "payroll," stop, keep the boxes and labels, and report to the FTC and the U.S. Postal Inspection Service. This guide is about fake home-based package-handler jobs-not a mystery shopper check scam, not an unpaid internship fee scam, and not a LinkedIn recruiter phishing login steal.

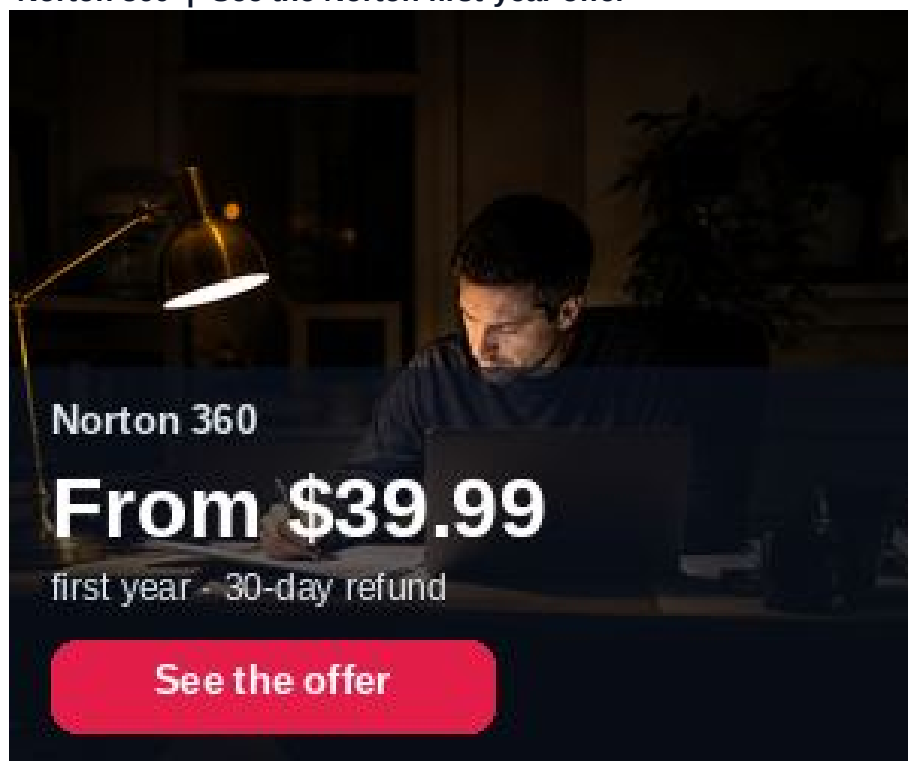
1. How work-from-home reshipping scams work

Ads promise easy pay as a "delivery operations specialist," "quality control manager," or virtual assistant. After a quick "hire," the company ships high-dollar electronics or other goods to your door. Instructions say: open the box, discard receipts and labels, repackage, and ship to a new address-often abroad-using postage they "provide" or reimburse later.

Paychecks are delayed a month, then never arrive; the site and phone go dark.

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>

The packages were bought with stolen payment data. By reshipping, you may help move stolen merchandise and risk civil or criminal exposure. Some scripts also collect your Social Security number, photo ID, and bank account "for direct deposit," which feeds identity theft.

Scammers sometimes mail counterfeit postage labels or ask you to front shipping costs for a later refund. Do not use mystery postage or spend your own money to move someone else's boxes. Tell household members who apply to work-from-home ads that stripping labels is a hard stop.

2. Red flags before you accept packages

Cue | Likely legitimate | Likely scam

Job task | Clear employer you can verify; no hiding labels or receipts | Receive, strip packaging, and forward goods you did not order

Company check | Real HQ, reviews, and careers page you opened yourself | New domain, free email, or "affiliate of Amazon/FedEx" you cannot verify

Pay | W-2/1099 setup through known payroll; pay on schedule | Pay after a "trial month"; counterfeit checks or money orders

Packages | You ordered them, or your known employer ships work tools | Unexpected high-value boxes with instructions to destroy paperwork

Destination | Normal business shipping you initiate with a known company | Rush overseas addresses and secrecy about the end recipient

Personal data | Minimal data after a real offer letter | Immediate SSN, ID scan, and bank details before any real work proof

3. Safer habits (buy-nothing)

- * Treat "receive and reship packages from home" as a scam-walk away.
- * Search the company name plus "scam," "complaint," and "reshipping" before answering further.
- * Do not accept packages addressed to you from unknown "employers."
- * Never discard original packaging, invoices, or shipping labels on someone else's instructions.
- * Do not send SSN, driver's license photos, or bank account numbers for a cold work-from-home hire.
- * For recruiter login and document phishing that is not about packages, see LinkedIn recruiter phishing.

4. If you already shipped or shared data

- * Stop forwarding packages. Keep remaining boxes, labels, postage, and all chat or email instructions.
- * Contact your local post office or shipper about any items still in your possession; ask how to return to sender or hold for inspection.
- * Report at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and to the U.S. Postal Inspection Service at [uspis.gov/report](https://www.uspis.gov/report).
- * If you deposited a "paycheck" or money order, tell your bank immediately-counterfeit instruments often bounce and you may owe the funds.
- * If you shared SSN or ID images, start a plan at [IdentityTheft.gov](https://www.identitytheft.gov) and consider a credit freeze (see how to place a credit freeze).
- * If you opened attachments or typed credentials on a fake careers portal, change passwords, enable two-factor authentication, and scan your device with a trusted tool such as Norton or Bitdefender. Keep one primary real-time antivirus-avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

FAQ

Is any home package-forwarding job legitimate?

FTC guidance is clear: reshipping goods is never a real job. Legitimate work-from-home roles do not ask you to erase receipts and move high-value goods for strangers.

How is this different from a mystery shopper scam?

Mystery shopper scams usually send a fake check and ask you to buy gift cards or wire "test" money. Reshipping centers on physical packages bought with stolen cards.

Could I get in legal trouble for forwarding packages?

You may face risk because the goods are often stolen. Stop immediately, preserve evidence, and report-do not keep shipping "one more batch."

The company said they are partners with a big retailer. Does that make it safe?

No. Scammers name-drop familiar brands. Verify employers yourself through official careers pages-not through links in the offer email.

If you still want a paid suite

Avoiding how to spot a work-from-home package reshipping scam does not require paid antivirus. Careful habits and official support 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

- * FTC: Job scams (includes reshipping)
- * FTC alert: Signs of a reshipping scam
- * FTC ReportFraud
- * IdentityTheft.gov
- * U.S. Postal Inspection Service

Also read

- * How to spot a LinkedIn recruiter phishing scam
- * How to spot a mystery shopper check scam
- * How to spot a fake unpaid internship fee scam
- * How to place a credit freeze at all three bureaus
- * How to spot a fake check scam