

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a LinkedIn recruiter phishing scam

<https://cyberguardlab.com/blog/linkedin-recruiter-phishing-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 LinkedIn recruiter phishing scam

Dream remote job

Fake recruiter InMails that phish logins or advance fees.

Onboard on this portal

Look-alike SSO

Open careers yourself

Refuse training fees

No password from DMs

A LinkedIn recruiter phishing scam uses fake recruiter profiles or hijacked accounts to send "job opportunity" messages that lead to credential theft, malware, or advance-fee fraud. Do not enter Microsoft/LinkedIn passwords on pages from cold InMails. Do not pay for training, equipment, or background checks through a stranger's link. If you already submitted credentials or money, lock down accounts and report through LinkedIn and the FTC. This guide is about recruiter phishing and fake hiring funnels-not job reshipping or parcel-mule offers (different crime), and not pig butchering romance-investment grooming that merely started on LinkedIn.

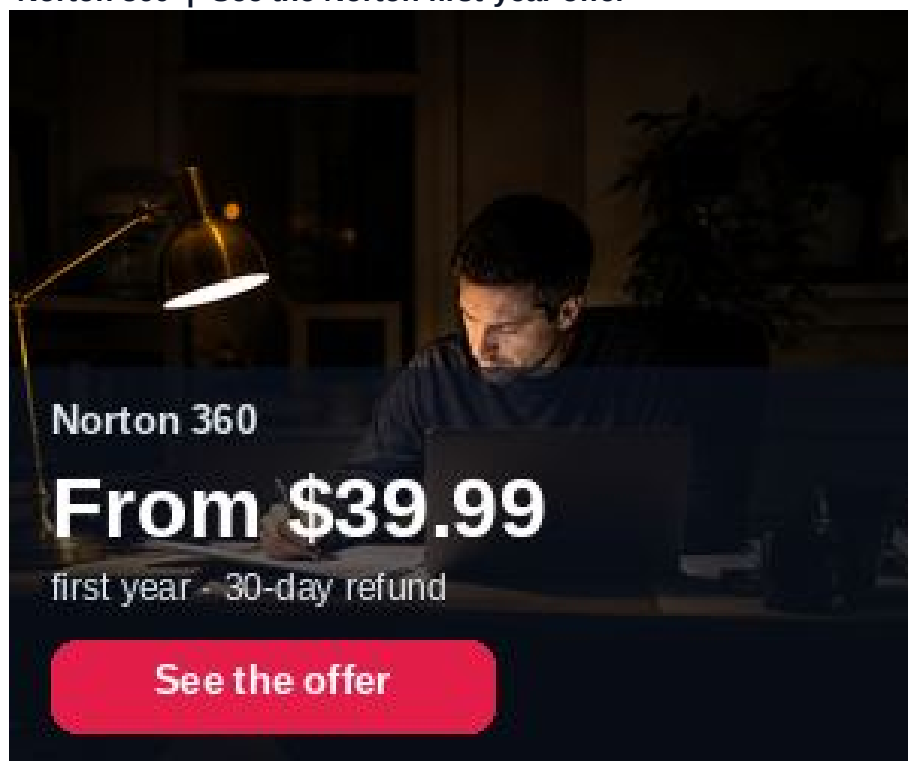
1. How this scam works

You receive InMail: high salary, remote role, minimal interview, attach a document, or "complete onboarding on this portal." The portal mimics Microsoft login, DocuSign, or a careers page. Some ask for your full SSN, banking details, or a check deposit you must refund-classic fake check territory. Others push crypto "equipment stipends." Profiles may show borrowed

logos and few real connections.

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>

Unlike reshipping mule schemes that focus on receiving and forwarding packages, recruiter phishing prioritizes logins, personal data, and fees before any real job exists.

2. Red flags before you pay

3. Safer habits (buy-nothing)

- * Open the company's real careers site yourself; do not rely on InMail links alone.
- * Verify the recruiter's identity through a known corporate directory-not only their LinkedIn page.
- * Refuse any fee to begin work or receive equipment.
- * Do not enter LinkedIn or Microsoft passwords on pages reached from messages.
- * Be wary of unsolicited documents that ask you to enable macros or install software.
- * For phishing page cues, see how to spot a phishing email.

Attackers clone Microsoft 365 and OKTA-style logins. Always check the domain before typing a work password. If you use LinkedIn for job hunting, turn on 2FA and limit what personal phone numbers appear publicly.

4. If you already paid

- * Stop further payments or "onboarding" fees. Save InMails, profile URLs, and receipts.
- * Change LinkedIn, email, and work-related passwords; enable two-factor authentication; review active sessions.
- * Contact your bank if you wired money, deposited a suspicious check, or shared account numbers.
- * Report the profile through LinkedIn's official tools and file at ReportFraud.ftc.gov.
- * Use IdentityTheft.gov if you shared SSN, ID scans, or direct-deposit forms.
- * If you typed credentials or opened attachments on a fake page, 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

Are all LinkedIn recruiters scams?

No. Many legitimate recruiters use LinkedIn. Verify company identity, refuse upfront fees, and avoid password pages from cold messages.

How is this different from a job reshipping scam?

Reshipping schemes recruit you to receive and forward packages (often stolen goods). Recruiter phishing focuses on credential theft, malware, and advance fees for a fake hiring process.

They sent a check for equipment before my first day. Is that normal?

Unexpected checks-especially with instructions to refund part of the amount-are a major red flag. See fake check scams.

The salary is far above market for remote work. Should I be excited?

Be cautious. Unrealistic pay plus rushed onboarding often signals fraud.

If you still want a paid suite

Avoiding a a LinkedIn recruiter phishing 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 ReportFraud](#)
- * [IdentityTheft.gov](#)
- * [FTC: Job scams](#)
- * [FTC: How to recognize phishing](#)
- * [LinkedIn Help](#)

Also read

- * [How to spot a phishing email](#)
- * [How to spot a fake check scam](#)
- * [How to report a scam to the FTC](#)
- * [How to spot a PayPal goods and services scam](#)
- * [How to spot a wire transfer romance or advance-fee scam](#)