

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot an Instagram giveaway or influencer scam

<https://cyberguardlab.com/blog/instagram-giveaway-influencer-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

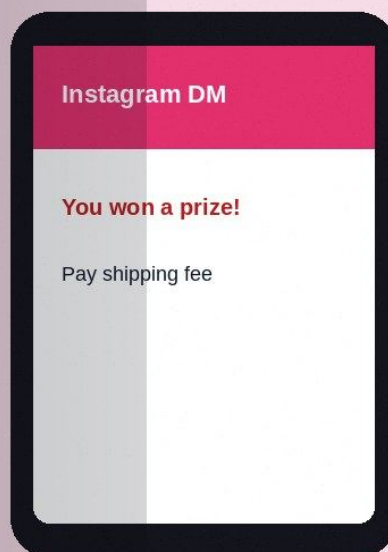
How to spot an Instagram giveaway or influencer scam

Clone an influencer

Fake contests and influencer clones that charge claim fees.

No fee for free prizes

Open brand site yourself



An Instagram giveaway or influencer scam uses fake contests, cloned creator accounts, or look-alike brand pages to harvest logins, ship "fees," or crypto deposits for a prize you will never receive. Do not tap "claim prize" links from DMs. Do not pay shipping, tax, or "verification" fees to receive a giveaway. If you already entered credentials or paid, lock down accounts and report through Instagram and the FTC. This guide is about Instagram prize and influencer impersonation scams-not TikTok shop or livestream purchase fraud, and not Discord Nitro giveaways.

1. How this scam works

A post or Story says you won a phone, gift card, or meet-and-greet. A DM from a "brand manager" or "verified" look-alike asks you to click a link, join a Telegram group, or pay a small fee. Some clone influencer handles with extra characters. Others run comment pods: "Like, share, tag 3 friends, then DM us." Payment asks escalate after each step.

Paid link

Norton 360 | See the Norton first-year offer



Norton 360

From \$39.99

first year - 30-day refund

See the offer

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

Offer page: <https://cyberguardlab.com/norton>

Unlike TikTok shop scams that fake product sales in live shopping, Instagram giveaway scams center on prize claims and fake creator endorsements.

2. Red flags before you pay

3. Safer habits (buy-nothing)

- * Open Instagram or the brand's official website yourself-do not use DM links.
- * Check the handle character-by-character against the real account.
- * Refuse any fee to receive a "free" prize.
- * Never enter Instagram passwords on pages reached from DMs.
- * Report impersonation and scam DMs through Instagram's official tools.
- * For phishing-style pages, see how to spot a phishing email.

Swipe-up and bio links can be swapped on compromised accounts. Prefer typing a brand domain you already know. Teach teens that "you won" DMs are usually traps.

4. If you already paid

- * Stop further fees. Screenshot DMs, handles, and payment records.
- * Contact your bank, card issuer, or gift-card fraud line immediately.
- * Change your Instagram and email passwords; enable two-factor authentication.
- * Report the account in the Instagram app and file at ReportFraud.ftc.gov.
- * Warn followers if a clone used your image or a friend's giveaway branding.
- * 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

Can a real influencer ask me to DM a manager to claim a prize?

Treat unsolicited prize DMs as suspicious. Real brands publish rules and do not demand gift cards or crypto to deliver prizes.

How is this different from a TikTok shop scam?

TikTok shop/livestream scams push fake merchandise purchases during lives. Instagram giveaway scams push prize claims and influencer look-alikes-often before any "product" ships.

The page has a blue check. Is it safe?

Verification helps but fakes and compromised accounts still appear. Fees to claim prizes remain a red flag.

I only shared my address. Am I at risk?

You may get junk mail or further phishing. Monitor accounts; do not pay follow-up "customs" asks.

If you still want a paid suite

Avoiding a an Instagram giveaway or influencer 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: Online shopping tips](#)
- * [FTC: How to recognize phishing](#)
- * [Instagram Help Center](#)

Also read

- * [How to spot a TikTok shop or live-stream scam](#)
- * [How to spot a Discord nitro or crypto giveaway scam](#)
- * [How to spot a phishing email](#)
- * [How to spot a fake friend emergency Facebook message](#)
- * [How to report a scam to the FTC](#)