Published on *University of Colorado* (https://www.cu.edu)

How to Spot Fake Online Stores [1]

Holiday deals bring holiday scams. During peak shopping seasons, scammers set up fake online stores that look real, lure you in with “too-good-to-be-true” deals, and disappear with your money or personal data. Here’s how these scams work, the risks, the red flags to watch for, and what to do if you’ve already entered personal or payment information.

A quick scenario: “70% off—today only!”

Jordan sees a social media ad for a popular brand of headphones, 70% off, free rush shipping. The site looks slick, with a countdown timer and “limited stock” alerts. At checkout, the site only accepts debit card or peer-to-peer payment. Jordan pays.

Days later, no tracking number. The “order support” email bounces. Jordan’s bank shows unexpected charges from unfamiliar merchants. The store domain disappears a week later.

What happened? Jordan bought from a fraudulent storefront designed to collect payment details and personal data during the holiday rush.

The risks

- Financial loss: charges for goods that never arrive or additional unauthorized charges later.
- Identity theft: stolen names, addresses, phone numbers, and passwords can fuel account takeovers and new-account fraud.
- Account compromise: if you reused a password at checkout, scammers may try it on your email, bank, shopping, or campus accounts.
- Malware: some fake stores push invoice attachments or links that install malware, including ransomware.

Red flags: how fake stores might hook you

- Prices far below market, like “50–80% off a hot item.”
- Pressure tactics, like countdown timers or ‘limited stock’ warnings.
- Odd payment options (wire transfer, crypto, gift cards, peer-to-peer payment) or no credit card option.
- A URL that doesn’t match the brand (misspellings, extra words).
- No physical address or phone number or contact info that doesn’t work.
- No presence beyond the site: few or no independent reviews, or many near-identical 5-star reviews posted within days.

Quick validation steps

- Search online the store name plus “reviews” + “scam” (e.g., Too Good To Be True Tronics reviews).
- Search for the store on trusted review sites (e.g., BBB, Trustpilot).
- Check the URL carefully on desktop and mobile.
- Look up the domain’s About/Contact; search the listed address or phone number.
- Prefer well-known marketplaces—but still buy from top-rated, long-standing sellers within those marketplaces.

What to do if you already entered personal data

Follow these steps in order, as soon as you realize the site was fraudulent:

Protect your money

- Paid by credit card: contact your card issuer and dispute the charge; ask for a new card number.
- Paid by debit card or through a peer-to-peer app: call your bank immediately; request a transaction reversal if possible and a new card.
- Paid by gift card or crypto: contact the issuer/exchange right away—recovery is harder but speed helps.

Secure your accounts

- If you created an account on the fake site or reused a password, change that password

everywhere it’s used.
- If you haven’t already, turn on multi-factor authentication (MFA) for email, banking, retail, and campus accounts.

Monitor your accounts and set up alerts

- Set up transaction alerts on your bank and card apps.
- Set up credit monitoring or fraud alert with a credit bureau.
- Review statements closely for the next 2–3 months.

Watch for follow-on scams

- Scammers may contact you posing as “support” to “refund” your order. Do not share codes, passwords, or remote-access permission.

Bottom line

For a secure shopping experience, stick to reputable, well-known websites. **Trust your instincts**—if something seems suspicious, it probably is.

Bookmark your campus information security website for guidance and contacts

- CU Anschutz [2]
- CU Boulder [3]
- CU Denver [2]
- UCCS [4]
- System Administration [5]

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/how-spot-fake-online-stores
[2] https://www.cuanschutz.edu/offices/information-security-and-it-compliance
[3] https://oit.colorado.edu/services/it-security [4] https://oit.uccs.edu/security [5] https://www.cu.edu/uis