P

# Online Pharmacy Scams: Red Flags and Safe Buying Checklist

Fake online pharmacies can sell counterfeit, expired, contaminated, or incorrectly dosed medicines and steal payment data. Learn how to verify licensing and respond after an order.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

## In this guide

01 Warning signs of an unsafe online pharmacy
02 Safe pharmacy vs scam indicators
03 How to verify an online pharmacy
04 Social-media and weight-loss medicine scams
05 What to do if you ordered from a suspicious pharmacy
06 If the site impersonates a real pharmacy
07 Information the scam may misuse
08 Frequently asked questions
09 Authoritative guidance

**An online pharmacy scam uses a fake or unlicensed storefront, social-media account, advertisement, or message to sell unsafe medicine, steal payment and identity data, or take money without delivering a legitimate product.** The site may look professional and use HTTPS, familiar logos, reviews, and official-looking seals. Those features can all be copied.

Unsafe sellers may provide counterfeit, expired, contaminated, incorrectly dosed, or unapproved products. A medicine with too much, too little, no active ingredient, or an undisclosed substance can delay treatment and cause serious harm. Verify the pharmacy through the relevant regulator before ordering.

## 01 Warning signs of an unsafe online pharmacy

- It sells prescription medicine without a valid prescription or meaningful clinical review.
- No licensed pharmacist is available to answer questions.
- The physical address, telephone number, responsible pharmacy, or license cannot be independently verified.
- Prices are dramatically lower than established pharmacies or a scarce medicine is always available.
- The seller operates only through social media, encrypted messaging, direct messages, or marketplace listings.
- Payment is requested by cryptocurrency, gift card, wire transfer, person-to-person app, or another hard-to-reverse method.
- The site claims a product is guaranteed, has no side effects, replaces medical care, or is approved for uses not supported by the regulator.
- Packaging is damaged, foreign or missing required information, has no lot or expiration date, or looks different from the usual medicine.

## 02 Safe pharmacy vs scam indicators

| Check | Safer sign | Warning sign |
|---|---|---|
| Prescription | Requires a valid prescription and appropriate patient information | Offers prescription drugs to anyone after a short form or no review |
| License | License is confirmed in the regulator's own database | Displays only a badge or certificate that cannot be verified |
| Pharmacist | A licensed pharmacist is available | No qualified professional or only a sales chat |
| Contact information | Verifiable legal business and pharmacy address | Hidden ownership, mailbox address, or messaging-only contact |
| Payment | Normal protected payment methods and clear policies | Crypto, gift cards, wire transfer, or pressure to pay immediately |
| Medicine | Approved supply chain, intact labeled packaging, lot and expiry data | Loose pills, altered packaging, unexplained substitutions, or no traceability |

## 03 How to verify an online pharmacy

1. **Start with your jurisdiction.** Rules and databases differ by country and region. Use the government health or pharmacy regulator's official website.
2. **Search the license independently.** Do not trust a badge that links only to a page controlled by the seller. Confirm the business name, address, license number, and current status in the regulator's database.
3. **Confirm the prescription process.** A licensed service should require a valid prescription where legally required and provide access to an appropriate clinician or pharmacist.
4. **Check the exact domain.** Look for misspellings, extra words, subdomains, recently changed addresses, and links sent through unsolicited messages.

5. **Verify the product.** Confirm manufacturer, strength, dosage form, approval status, packaging, storage, and supply chain with a pharmacist.
6. **Review privacy and payment handling.** HTTPS protects data in transit but does not prove the seller is licensed or honest.

In the United States, the FDA recommends checking the pharmacy through the state board of pharmacy and its BeSafeRx resources. Consumers elsewhere should use their national and regional regulators.

## 04 Social-media and weight-loss medicine scams

High demand for weight-loss, pain, erectile-dysfunction, ADHD, and other prescription medicines attracts counterfeiters and impersonators. A social-media account can copy a clinic or pharmacy name, steal clinician photos, and disappear after payment. Do not buy prescription products through comments, direct messages, influencers, or unsolicited texts. Claims about an active ingredient or an FDA-approved brand do not mean the seller's compounded or counterfeit product is approved.

## 05 What to do if you ordered from a suspicious pharmacy

1. **Do not take an uncertain product.** Keep it separated from legitimate medicine and away from children and pets.
2. **Contact a licensed pharmacist or clinician.** Ask how to continue needed treatment and how the product can be assessed or disposed of.
3. **Seek urgent medical help for symptoms.** If a person has taken the product and feels unwell, contact emergency services or the local poison center. Do not wait for the seller's advice.
4. **Contact the payment provider.** Report fraud promptly, dispute eligible charges, and replace exposed card details if advised.

5. **Protect accounts.** Change reused passwords, revoke sessions, and watch for phishing and identity theft using information submitted to the site.
6. **Preserve evidence and report.** Save the URL, screenshots, messages, packaging, lot number, receipts, and transaction records for health and fraud regulators.

Do not mail an unknown medicine to an unverified address or throw it where another person could use it. Follow a pharmacist's or local medicine-disposal program's instructions.

## 06 If the site impersonates a real pharmacy

Contact the genuine pharmacy using the number or domain found independently in a regulator's database, not the suspicious page. Report the impersonating domain to its hosting and payment providers and the appropriate regulator. A copied name, logo, accreditation seal, or address does not establish any relationship with the legitimate business.

## 07 Information the scam may misuse

- Card and bank details for fraudulent charges.
- Identity documents and insurance information for identity theft.
- Medical history for targeted follow-up scams or extortion.
- Email, phone, and address for phishing and fake delivery messages.
- Account passwords reused on other websites.

## 08 Frequently asked questions

### Does HTTPS mean an online pharmacy is legitimate?

No. HTTPS encrypts the connection but does not verify the seller's license, medicine, or business practices.

### Is a pharmacy safe if it has good reviews?

Not necessarily. Reviews and testimonials can be fabricated, purchased, or copied. Verify the license through the regulator's independent database.

### Can I identify counterfeit medicine by appearance?

Not reliably. Some counterfeits closely copy genuine packaging. An unexpected appearance is a warning, but professional verification and a trusted supply chain are necessary.

### Is an online consultation enough for a prescription?

Telehealth can be legitimate, but the prescriber and pharmacy must follow applicable licensing and prescribing rules. A token questionnaire designed only to approve every buyer is a warning sign.

## 09 Authoritative guidance

- FDA: How to buy medicines safely from an online pharmacy
- FDA BeSafeRx: online pharmacy information
- FTC: Buying health products and services online

**NEED MORE HELP?**

### We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

**Open this guide online at support.gridinsoft.com**