Pharma scams - What they are, red flags, and how to stay safe

Gridinsoft Help Center

What it is

In cybersecurity, pharma refers to spam and scam websites that push fake, illegal, or improperly sourced medications. They often copy the look of real pharmacies to trick buyers into sharing credit cards, prescriptions, or personal data.

Why it matters

Pharma scams can steal money and identities, deliver dangerous or counterfeit drugs, and spread malware through booby-trapped carts or downloads. They also pollute search results and hijack hacked sites to funnel traffic.

How it works - quick tour

- SEO poisoning: hacked blogs and forums secretly link to pharmacy pages to rank higher.
- Brand impersonation: cloned logos, fake seals, and sham "doctor" reviews.
- Illegal sales: no valid prescription checks, cross-border shipping, mystery pills.
- Data theft: fake checkout forms harvest payment and medical details.

Red flags

- Prices far below market, bulk discounts on prescription meds.
- No prescription required for controlled drugs.
- Vague contact info, offshore addresses, or throwaway domains.
- Payment limited to crypto, wire, or gift cards.
- Seal badges that don’t link to a real accreditation page.

Prevent it

- Buy only from licensed pharmacies listed by your national regulator.
- Bookmark trusted sites and avoid email or SMS links to "special offers."
- Use credit cards with fraud protection, never gift cards or crypto.
- Keep browser and security tools updated; enable DNS/web filtering.
- If you run a website: patch fast, watch for pharma spam injections, and lock down admin access.