# Beginner's Guide To Safe Online Shopping

*Guide · Spot Fake Stores, Avoid Card-Tester Scams, And Use The Tools That Actually Protect You.*

**Who this is for: anyone who shops online — which is everyone now. Online shopping fraud costs Americans $48B+ annually. This guide covers the realistic threats and the simple habits that prevent almost all of them.**

## The Major Threats When Shopping Online

- **Card-tester fraud** — small charges to test if a stolen card works, before larger purchases.
- **Fake stores** — sites built to look like real retailers but run by scammers. They take your money and ship nothing.
- **Compromised retailer** — a real store gets breached, and your card data is stolen during checkout.
- **Triangulation fraud** — scammer takes your order, fulfils it via stolen credentials at a real retailer, then disappears.
- **Shipping label scams** — package never arrives, but tracking shows 'delivered.'
- **Return fraud** — scammer refunds your purchase to a different card, leaving you no recourse.
- **Phishing return / refund** — fake 'your refund is ready, click here' emails after you've shopped.

## Before You Buy

### 1. Verify The Store Is Real

- Search the store name + 'reviews' or + 'scam.' Real stores have years of mixed reviews. Fake stores have none, or all-glowing-from-the-same-week.
- Check the domain age (whois lookup) — fake stores are often days or weeks old.
- Check for HTTPS (the lock icon). All real stores have this. Doesn't guarantee legitimacy, but absence is a hard 'no.'
- Look for a real address and phone number. Search the address — does it lead to a real business?
- Be sceptical of prices 60%+ below market. Especially on premium electronics.

### 2. Check How They Want You To Pay

Payment methods vary in protection level:

| Payment method | Protection level | Notes |
|---|---|---|
| Credit card | ★★★★★ | Best fraud protection. $0 liability for unauthorised charges. |
| Apple Pay / Google Pay | ★★★★★ | Tokenised — actual card number never reaches the merchant. |
| PayPal | ★★★★ | Buyer protection on most purchases. |
| Debit card | ★★ | Money pulled directly from your account; recovery is slower. |
| Wire transfer | ★ | No protection. Never use for online shopping. |

| Payment method | Protection level | Notes |
|---|---|---|
| Gift cards | Zero | Untraceable. If asked, it's a scam. |
| Cryptocurrency | Zero | Irreversible. Only use with vendors you fully trust. |

### 3. Use Virtual / Single-Use Card Numbers

Many banks (Capital One, Citi, Chase) and services (Privacy.com) offer virtual card numbers that auto-generate a unique card per merchant. If a merchant is breached, only that virtual number is exposed — your real card is safe. Bonus: you can lock or delete a virtual card without affecting anything else.

## During Checkout

- Confirm the URL matches the brand. *amazon.com* NOT *amazon.shop-secure.com*.
- Look for the lock icon in the address bar. Click it to see the certificate name — should match the company.
- Don't save card details on sites you'll only use once. Fewer copies = smaller blast radius.
- Skip the 'create an account' option for one-off purchases. Use guest checkout where possible.
- Use Apple Pay / Google Pay if offered — your real card number isn't shared with the merchant.
- Decline 'free trial' / subscription upsells you didn't actively want. They're easy to miss in fine print.

## After You Buy

- Save the order confirmation email. Take a screenshot of the price you paid.
- Watch your card statement for that purchase AND for unfamiliar charges nearby (card-tester signal).
- Track the package via the official carrier site, not links in emails.
- If 'package delivered' but you didn't receive it: file a porch-pirate claim with the retailer first; some offer free re-ship.
- Be sceptical of 'survey' emails post-purchase that ask for personal info.

## Holiday Shopping — Extra Hazards

- **Fake delivery texts** spike around Black Friday through New Year. Never click. Open the carrier app directly.
- **Fake retailer 'order issue' emails** — same playbook. Open the retailer site directly.
- **Charity scams** — fake non-profits posing as real ones. Verify at charitynavigator.org or guidestar.org.
- **Gift-card-for-payment scams** — even from people you know (their account may be compromised).

## If You're Defrauded

1. **Contact your card issuer immediately.** Disputes filed within 60 days of the statement get the strongest protection.
2. **Document the fraud.** Order confirmation, communications, screenshots.
3. **File a complaint at reportfraud.ftc.gov.**
4. **If the merchant is a real business and the issue is a defective product or non-delivery**, file a chargeback through your card.
5. **If the merchant is a scam site**, also report to IC3.gov and your state attorney general.

6 **Watch your credit reports for the next 12 months** — your full info may have been compromised, not just the card.

## Where To Go Next

- **Use the Banking & Card Fraud Quick-Defense Checklist** — daily/weekly/monthly defence routine.
- **Read the Phishing Beginner's Guide** — most post-purchase scams arrive via email.
- **Use the Identity Theft Risk Scorecard** — frequent online shoppers have higher risk.

SCAM ALERT

### Toll-Road SMS Scam Is Spreading Across The U.S.

Texts claiming you owe a small toll fee link to fake DMV-style sites. They steal card numbers and SSNs. Never click a 'toll' link — go to the toll authority directly.

Visit Making Sense Of Security →