



## LESSON 4

# Safe Online Shopping and Banking

Quick reference — print this page and keep it nearby.

## HABITS THAT REMOVE ALMOST ALL THE RISK

- 1 Look at the URL**  
Before typing a card number, check the address starts with https and shows a padlock — and that the domain really is the company you think it is.
- 2 Trust your gut on price and feel**  
Prices that are too good, stolen-looking photos, and no real phone number all point to a scam store. If it feels off, leave.
- 3 Pay with a credit card, not debit**  
By law, credit card fraud liability is capped at \$50 — usually waived. With a debit card, the missing money is your money while it's sorted out.
- 4 Turn on three bank settings**  
Two-factor authentication, login and transaction alerts, and card lock. All three are free and already in your bank's app.
- 5 If a card number leaks**  
In order: lock the card, report the fraud, turn on alerts, change passwords, report to the FTC. Card fraud happens to careful people — don't blame yourself.

### IF YOU TAKE ONE THING FROM THIS LESSON

Open your bank's app today and turn on transaction alerts. The first time a scammer tries something, you'll know within seconds.

**TRY THIS TODAY** Look at your last five online purchases. Did you type the store's name yourself, or click a link? If you clicked, that's the habit to change first.