BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Fake Stores & Safe Online Shopping

Checking a store before you buy, paying the safe way,
and getting your money back when an order goes wrong

A plain-English guide to shopping online, safely

Two minutes of checking, and the right way to pay

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For shopping on any computer, phone or tablet in the U.S. · facts current November 2026

What's Inside

This is your guide to shopping online safely. Fake online stores look polished and advertise everywhere, but they share telltale signs, and a **two-minute check** catches most of them. Paying the right way catches the rest. Part 2 is the heart of it; Part 5 is there if an order ever goes wrong. Read it in any order; there's no test.

Part 1 — Getting Started

1 A Note from Bill
2 How Fake Stores Work
3 The Words You'll See
4 Your Safe-Shopping Toolkit

Part 2 — Checking a Store Before You Buy

5 Is This Store Real? The Two-Minute Check
6 Making Sure You're on the Real Site
7 Searching a Store's Name
8 Reading Reviews Wisely
9 Chrome Store Reviews & Google's Safety Check
10 How Old Is the Website?
11 Contact Details, Policies & Fine Print
12 The Padlock Doesn't Mean Honest

Part 3 — Ads, Social Media & Too-Good Deals

13 Shopping from Social Media Ads
14 Checking a Facebook or Instagram Shop
15 Deals That Are Too Good
16 Pets, Tickets & Hard-to-Find Items
17 Fake Delivery Texts & Emails
18 Packages You Didn't Order

Part 4 — Paying Safely

19 The Safest Ways to Pay Online
20 Credit Card or Debit Card?
21 Virtual Card Numbers
22 Payments a Store Should Never Demand
23 Checking Out Safely
24 Keeping Records of Every Order

Part 5 — When Something Goes Wrong

25 The Order Never Came, or It's Wrong

26 Disputing a Charge with Your Card
27 I Bought from a Fake Store: What Now?
28 Reporting a Fake Store
29 Helping a Parent Shop Safely

Part 6 — When to Call Bill & Your Cheat-Sheet

30 When to Call Bill
31 Your Safe-Shopping Cheat-Sheet

PART 1

Getting Started

How fake stores work, the words you'll see, and the few simple tools that keep your online shopping safe.

CHAPTER 1

A Note from Bill

Hello, and welcome. Maybe an ad for a half-price quilt or a "closing sale" on boots popped up on Facebook, and you wondered whether it was real. Maybe you ordered something weeks ago and it never came. Or maybe you'd simply like to shop online with the same confidence you have walking into a store you know. Whichever it is, this guide is for **you**.

I'm Bill. Helping folks feel at home with their technology is what I do every day, and I wrote this guide the way I'd explain it sitting beside you at the kitchen table: slowly, in plain English, with nothing taken for granted.

The one thing to remember

A fake store can look every bit as polished as a real one. Pretty pictures and a professional logo prove nothing. What protects you is **a short habit**: check the store before you buy, and **pay with a credit card** so you can get your money back if something goes wrong. Everything else in these pages builds on that.

WHAT THIS DOES FOR YOU

Why this matters

Online shopping saves trips, finds things local stores don't carry, and brings gifts straight to the grandkids' door. A two-minute check and the right way to pay let you enjoy all of that without the worry.

You can't break anything by looking

Every check in this guide is just looking: searching a name, reading a page, peeking at a website's age. None of it costs anything or commits you to anything. The only step that matters is the moment you type your card number, and by then you'll know what you're dealing with.

And I'm a phone call away

If a deal ever leaves you unsure, stop before you pay and call me at **(330) 200-8042**. A few minutes of checking beats weeks of chasing a refund. Now, let's get you shopping with confidence.

— Bill

CHAPTER 2

How Fake Stores Work

A fake online store is a website or social media shop built to take your money and send you nothing, or send you something cheap and different from what you paid for. Knowing how they operate makes them much easier to spot.

The usual pattern

1. The scammer builds a good-looking website, often using **photos and logos copied** from a real brand.
2. They buy **ads on social media** showing popular or expensive items at prices that seem too good to pass up. The ads can even be aimed at things you've recently searched for.
3. You order and pay. You may get a confirmation email that looks normal.
4. Then nothing arrives, or a cheap knockoff arrives, and the store stops answering. Weeks later, the website may disappear entirely.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

The signs the FTC warns about

- **Prices that are unusually low** for the item, especially for big brands.
- **Hard-to-find items** the store claims to have when they're sold out almost everywhere else.
- **Misspellings and sentences that don't make sense** on the website or in emails.
- **Requests to pay by gift card, wire transfer, payment app or cryptocurrency.**

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

GOOD TO KNOW

Not every cheap price is a scam

Real stores have real sales. The point isn't to distrust every bargain; it's to do the quick checks in Part 2 whenever a store is new to you or a deal seems surprising.

SCAM ALERT

Copycats of stores you know

Some fake sites pretend to be a store you already trust, with a web address that's just slightly off. Chapter 6, *Making Sure You're on the Real Site* shows how to make sure you're on the real thing.

CHAPTER 3

The Words You'll See

A short glossary. Come back to it whenever a word puzzles you.

Word	What it means
Web address (URL)	The name of a website as it appears in the bar at the top of your browser, such as **target.com**.
Domain	The main part of the web address, the part right before .com, .net, .shop and so on.
Lookalike address	A web address made to resemble a real store's, with an extra word, a missing letter or a different ending.
Checkout	The page where you enter your shipping address and payment.
Chargeback / dispute	Asking your card company to reverse a charge because of a problem with the purchase.
Virtual card number	A stand-in card number some banks create for online shopping, so your real number stays private.
Return policy	The store's rules for sending something back and getting a refund.
Restocking fee	A charge some stores take out of your refund when you return an item.
Dropshipping	A store that doesn't stock items itself; it orders from a supplier who ships to you, often from overseas. Legal, but often slow.
Smishing	A scam text message, such as a fake "your package couldn't be delivered" text.
Brushing	When a seller mails you something you never ordered, usually to post fake reviews.

CHAPTER 4

Your Safe-Shopping Toolkit

You don't need special software to shop safely. You need a few ordinary things set up the right way.

What	Why it helps
One credit card you use for online shopping	Credit cards give you the strongest right to dispute a charge if an order never arrives or isn't what you paid for.
An up-to-date browser (Chrome, Safari, Edge)	Modern browsers warn you about many known dangerous sites.
A strong, different password for each store	If one store is breached, your other accounts stay safe.
An email address you check	Order confirmations and shipping notices go there; they're your paper trail.
Card alerts from your bank's app	You see every charge the moment it happens.
A place to keep order records	A folder in your email, or a notebook, so you can find details if you need to dispute something.

Checked against the FTC's online shopping advice and Google's Safe Browsing Transparency Report on November 13, 2026.

Turn on charge alerts

1. Open your credit card company's or bank's official app (or sign in on its website).
2. Look for **Alerts**, **Notifications** or **Account alerts**, often under your profile or settings.
3. Turn on alerts for **card purchases**, or for **online and card-not-present purchases** if that choice appears.
4. Choose a text or app notification so you see charges right away.

TIP

Use one card for online shopping

Keeping all your online purchases on one credit card makes it easy to spot a charge you don't recognize, and keeps your debit card, which is tied straight to your checking account, out of online checkouts.

FROM BILL

Want help setting this up?

Setting up alerts and a password manager is a good half-hour together. $49 remote · $99 in your home. Call **(330) 200-8042**.

PART 2

Checking a Store Before You Buy

A short routine that takes a couple of minutes and tells you most of what you need to know about any store that's new to you.

CHAPTER 5

Is This Store Real? The Two-Minute Check

Whenever a store is new to you, or a deal seems surprisingly good, run through this short routine before you type your card number. Each step is explained in the chapters that follow.

1. **Look at the web address.** Is it the store's real name, spelled correctly? (Chapter 6, *Making Sure You're on the Real Site*)
2. **Search the store's name** with the words **scam**, **complaint** and **review**. (Chapter 7, *Searching a Store's Name*)
3. **Check the reviews somewhere other than the store's own site.** (Chapter 8, *Reading Reviews Wisely*)
4. **Peek at the store's rating** in Chrome or run the address through Google's safety check. (Chapter 9, *Chrome Store Reviews & Google's Safety Check*)
5. **Check how old the website is.** A store selling designer goods from a site made last month is a warning. (Chapter 10, *How Old Is the Website?*)
6. **Find a real address, phone number and return policy.** (Chapter 11, *Contact Details, Policies & Fine Print*)
7. **Plan to pay with a credit card.** If the store won't take one, walk away. (Chapter 19, *The Safest Ways to Pay Online*)

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

TIP

When you can skip the check

If you typed the address of a big store you already know, such as your usual pharmacy or department store, and you're on its real site, you don't need the full routine every time. The check is for stores that are new to you, stores you found through an ad, and deals that seem too good.

HEADS UP

The pressure clock

Countdown timers, "only 2 left!" banners and "sale ends tonight" messages are designed to rush you past these checks. A real bargain will still be there in five minutes.

CHAPTER 6

Making Sure You're on the Real Site

Some fake stores don't invent a new name; they copy a real one. The giveaway is almost always the web address, so it's worth learning to read it.

How to read a web address

Look at the part just before the first single slash. The words right before **.com** (or .net, .shop, .store and so on) are the website's real name. Anything to the left of that is just a label the owner chose.

Address	Whose site is it?
www.target.com/gift-ideas	Target's
target.com-holiday-sale.shop	Not Target's. The real name is **com-holiday-sale.shop**.
targett-outlet.com	Not Target's. Extra letter and an extra word.
target.deals-today.net	Not Target's. The real name is **deals-today.net**.

GOOD TO KNOW

This is just an example

The lookalike addresses above are made up to show the pattern. They aren't real sites to visit.

The safest habit: go there yourself

1. Instead of tapping a link in an ad, email or text, open your browser yourself.
2. Type the store's address you already know, or use a bookmark you saved earlier.
3. Or open the store's official app that you downloaded from the App Store or Google Play.
4. Search for the item on the real site. If the deal is real, it'll be there.

SCAM ALERT

Search ads can be fakes too

Scammers sometimes buy ads that appear at the top of search results. If you search for a store's name, look past anything labeled **Sponsored** and check the address before you tap.

CHAPTER 7

Searching a Store's Name

This is the single most useful check, and it takes under a minute. Other shoppers often post warnings long before a fake store disappears.

1. Open a search engine such as Google or Bing yourself, not through the ad.
2. Type the store's name, or its web address, followed by the word **scam**.
3. Read the first page of results. Then search again with **complaint**, and again with **review**.
4. Look for patterns: "never received," "knockoff," "won't answer emails," "refund refused."

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

What the results mean

What you find	What to do
Lots of complaints about missing orders	Don't buy. Close the page.
Nothing at all	Not proof it's fine. A brand-new fake store has no history yet. Do the other checks.
A mix of normal reviews and a few complaints	Typical of a real business. Read what the complaints say and how the store responded.
A scam-warning website or news story	Take it seriously.

TIP

Search on the web, not on the social media site

If you found the store through a Facebook or Instagram ad, do your search in a regular search engine. Comments under an ad can be deleted or faked by whoever runs the ad.

CHAPTER 8

Reading Reviews Wisely

Reviews help, but only if they're real. Fake stores often show a wall of glowing five-star reviews on their own pages, and those reviews can be written by anyone.

Where to look for honest reviews

- **Not on the store's own site.** The store controls what appears there.
- **On independent sites**, such as the Better Business Bureau (**bbb.org**), Google's store ratings, or well-known review sites.
- **In news stories and scam-warning pages** that turn up in your search.

Signs a review may be fake

- Many reviews posted in the same few days, all glowing.
- Vague praise that could fit any product: "Great product! Fast shipping! Love it!"
- Reviews that talk about a different product than the one listed.
- Only five-star and one-star reviews, with nothing in between.

The law is on your side

Since **October 21, 2024**, a Federal Trade Commission rule bans fake reviews and testimonials, including reviews from people who don't exist (such as AI-written fakes), buying positive or negative reviews, and buying fake followers or views. Businesses that break it can face civil penalties. Fake reviews still appear, but they are now clearly illegal.

Checked against the FTC's Trade Regulation Rule on the Use of Consumer Reviews and Testimonials (Federal Register, August 22, 2024) on November 13, 2026.

GOOD TO KNOW

Star ratings are a starting point

A store with a 4.5-star average on an independent site is usually a good sign. But read a few of the low ratings. They tell you what goes wrong when it does, and how the store handles it.

CHAPTER 9

Chrome Store Reviews & Google's Safety Check

Two free tools from Google can tell you a lot about a store without leaving your browser.

Store reviews in Chrome

In the United States, the Chrome browser can show a short summary of what shoppers say about an online store, covering things like product quality, pricing, service and returns. Google draws it from Google Shopping and other review sites.

1. On a computer, open the store's website in **Google Chrome**.
2. Click the small icon just to the left of the web address (it opens **View site information**).
3. Look for **Store reviews**. Click it to read the summary and see the reviews it's based on.
4. If there's no Store reviews entry, Chrome doesn't have enough information about that store. That's not proof of a scam, but it means you rely on your other checks.

Checked against Google Chrome Help, "Get started with Store reviews in Chrome," on November 13, 2026.

Google's Safe Browsing site check

Google keeps a list of websites known to be dangerous, such as sites that spread harmful software or trick people into giving up passwords. You can look up any address.

1. Go to **transparencyreport.google.com/safe-browsing/search**.
2. Type or paste the store's web address into the box and press Enter.
3. Read the result. "No unsafe content found" means Google hasn't flagged it; a warning means stay away.

Checked against Google's Safe Browsing Transparency Report on November 13, 2026.

HEADS UP

"No unsafe content" isn't a seal of approval

Safe Browsing looks for harmful software and phishing. A store that simply takes your money and ships nothing may not be on its list yet. Use it alongside your search and review checks, not instead of them.

CHAPTER 10

How Old Is the Website?

Fake stores come and go quickly. A shop that claims to have been "serving customers since 1998" but whose web address was registered three weeks ago is not telling the truth. You can check the date for free.

1. Go to **lookup.icann.org**. ICANN is the nonprofit that coordinates web addresses worldwide.
2. Type just the store's domain name, such as **example-store.com** (no www, no slashes), and click **Lookup**.
3. Find the **Created** or **Creation date** line. That's when the address was first registered.
4. Compare it with what the store says about itself.

Checked against ICANN Lookup (lookup.icann.org) on November 13, 2026.

What you see	What it suggests
Created years ago	A good sign, though not a guarantee.
Created in the last few months	Be very careful, especially with big discounts or famous brands.
Created recently, but the site says "established decades ago"	Don't buy.

GOOD TO KNOW

Owner names are usually hidden now

The lookup rarely shows who owns a site; most owners' personal details are kept private. The date is the useful part.

CHAPTER 11

Contact Details, Policies & Fine Print

Real businesses make it easy to reach them and explain their rules plainly. Before you buy from a store that's new to you, scroll to the bottom of its page and look.

What a real store usually shows

- A **physical address** you can look up on a map, not just a contact form.
- A **phone number** or a customer-service email that isn't a free Gmail or Yahoo account.
- A clear **return and refund policy**.
- **Shipping times**, and where items ship from.

Read the terms before you pay

1. Check the **total price**, including shipping, taxes and any other charges.
2. Read the **refund policy**. Can you return the item? Within how many days?
3. Find out **who pays return shipping**. If it ships from overseas, that can cost more than the item.
4. Look for a **restocking fee** that would come out of your refund.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

HEADS UP

Warning signs in the fine print

No returns at all; returns only for "store credit"; refunds only if you mail the item to an overseas address at your own cost; or a policy page full of another store's name that someone forgot to change. Any of these is a reason to shop elsewhere.

CHAPTER 12

The Padlock Doesn't Mean Honest

For years people were told to "look for the padlock" before shopping. The padlock still matters, but it's widely misunderstood.

What the padlock really means

The padlock (or an address beginning with **https**) means the connection between your device and the website is **private**: other people can't read what you type as it travels. It says nothing about whether the business on the other end is honest. Scam sites get padlocks too.

What you see	What it means
Padlock present	Your card number travels privately. You still need to check the store.
"Not secure" warning	Don't type a card number or password on that page at all.

GOOD TO KNOW

Many browsers no longer show a padlock

Recent versions of Chrome replaced the padlock with a neutral "tune" icon (two small sliders), and show a warning only when a page isn't secure. So look for the warning, not the lock.

Checked against coverage of Google's Chrome 117 lock-icon change (Chromium Blog, as reported by TechSpot and iTnews) on November 13, 2026.

TIP

Private connection, checked store

Think of it this way: the padlock is a sealed envelope. It keeps your letter private on the way, but it doesn't tell you whether you've addressed it to an honest person. The checks in this part do that.

PART 3

Ads, Social Media & Too-Good Deals

Where most fake stores find their customers, and the traps to watch for in your feed, your texts and your mailbox.

CHAPTER 13

Shopping from Social Media Ads

Facebook, Instagram, TikTok and other apps are full of shopping ads. Many are from real businesses. But they're also where fake stores do most of their advertising, because an ad can reach thousands of people in an afternoon and the scammer can disappear just as fast.

What the FTC says to watch for

- Ads that **impersonate well-known brands**, using their logos and photos.
- Expensive items at **unusually low prices**.
- Ads for things you've **just been searching for**; scammers can target ads that way too.
- Products that are **sold out everywhere else** but somehow available here.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

A safer way to act on an ad you like

1. Don't tap **Shop Now** right away. Note the brand and the product.
2. Open your browser and go to the brand's real website yourself, by typing its address or searching its name.
3. See whether the same product and price appear there.
4. If the deal only exists in the ad, run the Two-Minute Store Check (Chapter 5, *Is This Store Real? The Two-Minute Check*) before you go any further.

SCAM ALERT

"Closing down" and "warehouse clearance" ads

Sad stories about a family shop closing, or a warehouse dumping stock at 80% off, are a favorite way to make an implausible price sound believable. Treat them as a reason to check, not a reason to hurry.

CHAPTER 14

Checking a Facebook or Instagram Shop

When a shop's ad runs on Facebook, the Page behind it has a public history you can look at. This shows you how long the Page has existed and whether it's changed names.

Look at Page Transparency

1. Tap the shop's name at the top of the ad to open its Facebook Page.
2. Look for **Page transparency**. On many Pages it's in the **About** section; on others, tap the three dots and look for it there.
3. Read **when the Page was created**, whether it has had **previous names**, and, for larger Pages, the **countries** where the people managing it are located.
4. On the same screen you can usually see **ads the Page is running now**.

Checked against Meta's announcements on Page and account transparency (about.fb.com) on November 13, 2026.

What should make you pause

- A Page created very recently, for a business claiming to be decades old.
- A Page that used to be named something completely different, such as a meme or a giveaway page.
- A "local" boutique whose managers are all located in another country.
- Dozens of nearly identical ads for many unrelated products.

GOOD TO KNOW

Menus move around

Facebook and Instagram change where things live fairly often. If you can't find Page transparency, search the shop's name on the web instead (Chapter 7, *Searching a Store's Name*). That check works no matter how the app is arranged.

TIP

Facebook Marketplace is different

Buying from a person on Marketplace has its own rules and risks. Bill's separate Facebook Marketplace manual covers that in detail.

CHAPTER 15

Deals That Are Too Good

"If it's too good to be true" is old advice, but it's still the best. Here's how to make it practical.

A quick price reality check

1. Search for the exact product name at two or three stores you already know.
2. Note the usual price. Big, reliable stores rarely differ by more than a modest amount on the same item.
3. If the new store's price is **half or less** of everyone else's, assume something is wrong until proven otherwise.

Common bait

What's advertised	Why it's a favorite of fake stores
Famous brand shoes, purses, jewelry	People know the real price, so a big discount feels exciting.
Popular toys and gadgets at the holidays	Hard to find, high demand, shoppers in a hurry.
Outdoor gear, tools, furniture	Big-ticket items where a discount sounds like real savings.
"Free" items: just pay shipping	Often a way to collect card numbers or start a subscription.

HEADS UP

"Free, just pay shipping"

Before you enter a card for a "free" item, read the fine print for words like **membership**, **trial** or **auto-renew**. Some offers quietly sign you up for monthly charges.

WHAT THIS DOES FOR YOU

What this does for you

A minute of price checking protects you from the most common online shopping loss, and it often finds you a real deal at a store you trust.

CHAPTER 16

Pets, Tickets & Hard-to-Find Items

Some purchases are especially popular with scammers because buyers are excited and can't easily check the item first.

Item	What to watch for
Puppies and kittens	Photos are copied from real breeders. After you pay, "shipping," "insurance" or "vet" fees keep appearing. Meet the animal in person, or buy from a shelter or breeder you can visit.
Concert and game tickets	Sold-out events are prime bait. Buy from the venue's official seller or a well-known resale site with a guarantee, and pay by credit card.
Sold-out gadgets and consoles	"In stock here!" when it's sold out everywhere is a warning sign the FTC highlights.
Rental homes and vacation cabins	Never wire a deposit for a place you haven't seen or verified.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

SCAM ALERT

Extra fees after you pay

A legitimate seller doesn't come back after checkout asking for more money for shipping, customs, insurance or "release" fees. The Better Business Bureau says if that happens, stop communicating, call your credit card company, and report it to BBB Scam Tracker.

Checked against Better Business Bureau scam alerts on online purchase scams on November 13, 2026.

CHAPTER 17

Fake Delivery Texts & Emails

Once you start shopping online, you'll get real shipping notices, and scammers know it. A very common trick is a text saying a package couldn't be delivered and you must pay a small fee or update your address.

What the Postal Inspection Service says

- **USPS doesn't send unexpected texts.** You only get USPS tracking texts if you signed up for them yourself.
- If you didn't ask for tracking, **don't tap the link**.
- To check a package, go to **usps.com** yourself and type in the tracking number from your order email.

Checked against the U.S. Postal Inspection Service's smishing guidance (uspis.gov) on November 13, 2026.

Report it, then delete it

1. Forward the text to **7726** (it spells SPAM). This helps your phone company block the sender.
2. For fake USPS texts, you can also email a screenshot to **spam@uspis.gov**, including the sender's number and the date.
3. Then delete the text.

Checked against the U.S. Postal Inspection Service's smishing guidance (uspis.gov) on November 13, 2026.

TIP

Track from the store's order page

The safest way to check any delivery, from any carrier, is to open the store's website or app yourself, go to **Your orders** or **Order history**, and follow the tracking link there.

GOOD TO KNOW

More on packages

Bill's Package Tracking & Informed Delivery manual covers tracking and delivery alerts in depth.

CHAPTER 18

Packages You Didn't Order

Sometimes a box shows up with your name on it that you never ordered: a phone case, seeds, a cheap gadget. It can be unsettling, but it's usually a scheme called **brushing**.

What's going on

A seller ships a cheap item to a real address so they can pose as a "verified buyer" and post fake glowing reviews of their own product. Your name and address were probably taken from a list somewhere.

What to do

1. **You can keep it.** In the U.S. you have the right to keep merchandise you didn't order, and you don't have to pay for it or send it back.
2. **Don't pay** anyone who later contacts you asking for money for it.
3. **Don't scan any QR code or follow links** that came in the box.
4. If it came from a store where you have an account, such as Amazon, **sign in yourself and check your recent orders** and change your password if anything looks wrong.
5. Report it to the store, and you can report it at **ReportFraud.ftc.gov**.

Checked against FTC guidance on unordered merchandise and brushing, as quoted in consumer press coverage, on November 13, 2026.

HEADS UP

Why it's worth a look at your accounts

The FTC has noted that an unordered package can sometimes mean someone opened an account in your name or got into yours. A quick check of your order history and a password change put your mind at rest.

PART 4

Paying Safely

How you pay matters as much as where you shop. The right card turns a bad purchase into a fixable one.

CHAPTER 19

The Safest Ways to Pay Online

When you buy online, you're trusting a store you can't see. How you pay decides whether you can get your money back if that trust turns out to be misplaced.

How you pay	If the order never comes	Use it?
Credit card	Strong federal right to dispute the charge.	Yes, the best choice
Apple Pay, Google Pay with a credit card	Uses your credit card behind the scenes, so the card's dispute rights apply.	Yes
PayPal (buying goods)	PayPal has its own buyer protection for eligible purchases.	Usually
Debit card	You can dispute, but it's your own checking money that's tied up meanwhile.	Less ideal
Zelle, Venmo, Cash App to a stranger	Like handing over cash. Usually gone.	No
Gift cards, wire transfer, cryptocurrency	Almost impossible to recover.	Never for a store

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

TIP

The rule in one line

Pay online with a credit card, or a wallet like Apple Pay or Google Pay backed by a credit card. If a store won't accept those, don't buy there.

GOOD TO KNOW

More detail elsewhere

Bill's PayPal, Zelle and Apple Pay & Apple Wallet manuals explain those services step by step.

CHAPTER 20

Credit Card or Debit Card?

They look alike and both have a Visa or Mastercard logo, but when something goes wrong online, they behave very differently.

	Credit card vs. debit card
Whose money is at risk	**Credit:** the bank's, while the dispute is sorted out. **Debit:** yours, straight from checking.
Purchase problems (never arrived, wrong item)	**Credit:** the Fair Credit Billing Act lets you dispute it in writing within 60 days of the statement. **Debit:** depends more on your bank's policy and the card network's rules.
Someone steals your card number	**Credit:** your legal limit is $50, and most issuers charge you nothing for online fraud. **Debit:** $50 if you report within two business days, up to $500 if later, and possibly more if you wait past 60 days after your statement.

Checked against FTC and FDIC guidance on lost or stolen credit and debit cards on November 13, 2026.

WHAT THIS DOES FOR YOU

What this does for you

Using a credit card online means a bad store is a nuisance rather than a loss: you dispute the charge and wait for it to be sorted out, while your checking account and bills stay untouched.

HEADS UP

Pay the card in full

A credit card is only a bargain if you pay the statement in full each month. If carrying a balance worries you, use one card just for online shopping and pay it off every month.

CHAPTER 21

Virtual Card Numbers

Some card companies can create a **virtual card number**, a stand-in number you use for online shopping instead of the one printed on your card. Purchases still land on your regular statement, but your real number never reaches the store.

Why it's handy

- If a store's website is hacked, thieves get a number you can simply delete.
- Some virtual numbers only work at the one store you made them for, so they're useless elsewhere.
- You can lock or delete a number whenever you like, such as after a free trial.

An example: Capital One

Capital One's assistant, **Eno**, creates virtual card numbers for most Capital One credit cards. Each number is tied to one merchant, appears on your statement like any other purchase, and can be locked or deleted at any time. You can create them through the Eno browser extension or by signing in to your Capital One account.

Checked against Capital One's virtual card numbers page (capitalone.com) on November 13, 2026.

TIP

Ask your own card company

Other banks offer similar features under different names. Call the number on the back of your card or search its official website for "virtual card number." If your bank doesn't offer one, a regular credit card is still a safe choice.

CHAPTER 22

Payments a Store Should Never Demand

A real store takes ordinary payments at an ordinary checkout. If an online seller steers you toward any of these, stop. The FTC calls it a red flag.

- **Gift cards**, including Amazon, Apple, Google Play, Target or prepaid Visa cards.
- **Wire transfers** (Western Union, MoneyGram, a bank wire).
- **Payment apps** such as Zelle, Venmo or Cash App, especially "friends and family" payments.
- **Cryptocurrency**, such as Bitcoin, or a Bitcoin ATM.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

SCAM ALERT

"Our card machine is down, pay by Zelle instead"

A seller who suddenly can't take cards, or offers a discount for paying by app, wire or gift card, is usually trying to get money you can't reverse. Walk away.

GOOD TO KNOW

Gift cards are for gifts

Bill's Gift Cards manual explains why scammers love gift cards and what to do if you've been asked to buy them.

CHAPTER 23

Checking Out Safely

A few small choices at checkout keep your information safer, whatever store you're using.

1. **Check the address bar once more** before typing your card number. Are you still on the store's real site?
2. **Consider guest checkout** for a store you'll use only once, so it doesn't keep an account with your details.
3. If you do make an account, **use a strong password you don't use anywhere else**. A password manager makes this easy.
4. **Don't save your card** on small or unfamiliar sites. Saving it at a big store you use often is a convenience trade-off you can choose.
5. **Avoid shopping on public Wi-Fi** in coffee shops and libraries; use your home Wi-Fi or your phone's data.
6. **Read the order summary** carefully before you click Place Order: item, size, color, quantity, total.

TIP

Watch for pre-checked boxes

Some checkouts add protection plans, memberships or newsletter sign-ups with boxes already checked. Uncheck anything you didn't ask for.

FROM BILL

A password manager is worth it

If keeping track of passwords is the hard part, I can help you set up a password manager so every store gets its own strong password. $49 remote · $99 in your home.

CHAPTER 24

Keeping Records of Every Order

If something goes wrong, the person with the records wins. Keeping them takes seconds.

What to keep

- The **order confirmation email**, with the order number, items, total and date.
- A **screenshot of the product page** showing the description and price, for anything expensive or from a new store.
- **Shipping and tracking** emails.
- Any **messages** with the seller.

An easy system

1. In your email, create a folder or label called **Orders**.
2. Move each order confirmation there as soon as it arrives.
3. Keep them until the item has arrived, works and the return window has passed. For big purchases, keep them until the warranty ends.

> GOOD TO KNOW
>
> **Screenshots on a phone**
>
> On most iPhones, press the side button and volume-up together. On most Android phones, press power and volume-down together. The picture goes into your Photos app.

PART 5

When Something Goes Wrong

The order didn't come, or it isn't what you paid for. Here's the order of steps that gets most people their money back.

CHAPTER 25

The Order Never Came, or It's Wrong

Not every late package is a scam. Real stores have delays too. Here's how to work through it calmly.

Step one: contact the seller

1. Check the tracking from the store's own website or app.
2. Reread the shipping time the store promised.
3. Contact the store through its website, with your order number. Ask plainly for the item or a refund.
4. Save a copy of what you send and any reply.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

Your rights on shipping times

Under the FTC's Mail, Internet or Telephone Order Merchandise Rule, a seller must ship within the time it promised, or within **30 days** if it didn't say. If it can't, it must tell you and offer you the choice to agree to the delay or **cancel for a prompt refund**. A store credit or gift card doesn't count as a refund under this rule.

Checked against the FTC's Business Guide to the Mail, Internet, or Telephone Order Merchandise Rule (ftc.gov) on November 13, 2026.

HEADS UP

Don't let the clock run out

While you wait on a store, keep an eye on your card's dispute deadline, usually 60 days from the statement that first showed the charge. If the store is stalling, move on to Chapter 26, *Disputing a Charge with Your Card*.

CHAPTER 26

Disputing a Charge with Your Card

If a store won't fix the problem, or you can't reach it at all, your credit card company can step in. This is the protection you earned by paying with a credit card.

1. Find the charge on your statement or in your card's app.
2. Use the app's **Dispute** or **Report a problem** option on that charge, or call the number on the back of your card.
3. Explain simply: what you ordered, what happened, and when you contacted the seller.
4. Attach or keep ready your order confirmation, screenshots and messages.
5. For the strongest legal protection, also **send a written dispute** to the card company's billing-error address so it arrives within 60 days after the first statement showing the charge was sent to you.

Checked against the FTC's guidance on disputing credit card charges under the Fair Credit Billing Act on November 13, 2026.

What happens next

- The card company must acknowledge your written dispute within **30 days**, unless it's already fixed.
- It must resolve it within **two billing cycles**, and no more than 90 days.
- You don't have to pay the disputed amount, or interest on it, while it's being investigated, though you still pay the rest of your bill.

Checked against the FTC's guidance on disputing credit card charges under the Fair Credit Billing Act on November 13, 2026.

GOOD TO KNOW

Debit cards and other payments

If you paid with a debit card, call your bank right away and ask about a dispute; act quickly. If you paid with PayPal, open a dispute in PayPal. Bill's Returns, Refunds & Disputing a Charge manual walks through each kind in more detail.

CHAPTER 27

I Bought from a Fake Store: What Now?

First: you're in good company. Fake stores fool careful, intelligent people every day; they're built by professionals to do exactly that. What matters now is acting quickly.

1. **Call your card company** using the number on the back of your card. Say the store is a scam, dispute the charge, and ask whether you should get a new card number.
2. **If you used a debit card,** call your bank today. The sooner you report, the better your protection.
3. **If you made an account on the site,** and you used that same password anywhere else, change it on those other accounts now.
4. **Don't reply** to the store's emails or texts, and don't pay any "fees" to get a refund.
5. **Report it** (Chapter 28, *Reporting a Fake Store*).
6. **Watch your statements** for a few months for any other charges you don't recognize.

Checked against the FTC's consumer advice on online shopping (consumer.ftc.gov) on November 13, 2026.

SCAM ALERT

Beware the "refund" call

After you've been cheated, you may get calls or messages offering to recover your money for a fee. These are almost always a second scam. Your card company handles disputes for free.

GOOD TO KNOW

If a lot of money is involved

Bill's "I Think I've Been Scammed" manual has a fuller checklist, including freezing your credit if your personal details were taken.

CHAPTER 28

Reporting a Fake Store

Reporting won't always get your money back, but it helps investigators connect cases, and helps warn the next shopper.

Where	How	Why
Federal Trade Commission	**ReportFraud.ftc.gov**	The main national place to report fraud; shared with law enforcement.
Better Business Bureau	**bbb.org/scamtracker**	Public warnings other shoppers can search.
Ohio Attorney General	**ohioattorneygeneral.gov** or **(800) 282-0515**	Consumer complaints about purchases for personal or home use.
FBI Internet Crime Complaint Center	**ic3.gov**	For internet fraud, especially larger losses.
The social media site	Use **Report ad** on the ad	Helps get the ad taken down.

Checked against the FTC, the Ohio Attorney General's consumer complaint page and BBB Scam Tracker on November 13, 2026.

TIP

Have your details ready

The store's web address, the date, the amount, how you paid, and copies of your order email and any messages. That's why Chapter 24, *Keeping Records of Every Order* matters.

CHAPTER 29

Helping a Parent Shop Safely

If you look after an older parent, online shopping can be a real gift: no driving, no lines, deliveries to the door. A little setup makes it much safer.

- **Set up one credit card** just for online shopping, with a modest limit and purchase alerts.
- **Bookmark the stores they use** on their home screen or browser, so they don't have to search or follow ads.
- **Agree on a simple rule:** anything new, unusual or found through an ad gets a call to you first.
- **Share this guide's cheat-sheet** (Chapter 31, *Your Safe-Shopping Cheat-Sheet*) and keep a copy by the computer.
- **Offer to be the second opinion** without judgment. People hide mistakes when they're afraid of being scolded.

WHAT THIS DOES FOR YOU

What this does for you

A few minutes of setup gives your parent independence and gives you peace of mind, without taking over their accounts.

GOOD TO KNOW

Related help

Bill's Helping a Parent from Afar manual covers remote help and shared settings in more depth.

PART 6

When to Call Bill & Your Cheat-Sheet

When a second opinion saves worry, and the whole safe-shopping routine on one page.

CHAPTER 30

When to Call Bill

This guide covers what you need to shop online safely on your own. But part of being helpful is being honest about when a hand saves you time and worry. Here's when I'd pick up the phone.

Good reasons to call

- You've found a store or deal and you'd like a **second opinion before you pay**.
- You'd like help setting up **card alerts**, a **password manager** or **bookmarks** for the stores you use.
- You think you **bought from a fake store** and want help securing your accounts and devices.
- You clicked a link in a delivery text or email and **typed in a password or card number**.
- You'd like to set up a **parent's** computer or phone for safer shopping.
- You'd like a full **Digital Safety Check-Up** of your accounts, passwords and devices.

Things you can handle yourself

Checking a store's name and age, reading reviews in the right places, typing addresses yourself, paying by credit card, keeping your order emails, and disputing a charge with your card company. These are yours now.

SCAM ALERT

I'll never ask for your card number

When I help, you stay in control of your accounts. I'll never ask for your card number, your bank password or the codes your bank texts you.

FROM BILL

How to reach me

I'm Bill, and I bring 30+ years of professional experience to helping folks feel at home with their technology, right here in Portage County, Ohio. I don't rush, and there's no such thing as a silly question. $49 remote · $99 in your home. Call or text **(330) 200-8042** or book at **billshometech.com/book**. If you reach my assistant, Sophie, on the main line, she can answer simple questions and get you on my schedule.

Thank you for taking the time to learn this. A careful shopper with a credit card and a two-minute habit is a very hard target.

— Bill

CHAPTER 31

Your Safe-Shopping Cheat-Sheet

Keep this handy. The whole routine, in one place.

The Two-Minute Store Check

Check	How
Real address?	Type the store's address yourself; read the name just before .com.
Any complaints?	Search the store name + **scam**, **complaint**, **review**.
Honest reviews?	Look on bbb.org or Chrome's **Store reviews**, not the store's own page.
Flagged as unsafe?	transparencyreport.google.com/safe-browsing/search
How old is the site?	lookup.icann.org > Created date.
Real contact info?	Physical address, phone, clear return policy.
Credit card accepted?	If not, don't buy.

The safety rules

1. If the price is half of everyone else's, assume something's wrong.
2. Go to stores yourself; don't shop from ads, texts or emails.
3. Pay with a credit card (or Apple Pay or Google Pay backed by one).
4. Never pay a store by gift card, wire, payment app or crypto.
5. Keep every order confirmation in an **Orders** folder.
6. Problem? Contact the seller, then dispute with your card within 60 days.
7. Scammed? Call your card company now, then report at **ReportFraud.ftc.gov**.

Keep these handy

My shopping details	
My online-shopping credit card (last 4 digits)	_____
Card company's phone (back of card)	_____
Stores I've bookmarked	_____
FTC fraud reporting	ReportFraud.ftc.gov
Ohio Attorney General consumer line	(800) 282-0515
Bill's Home Tech	(330) 200-8042 · billshometech.com/book

WHAT THIS DOES FOR YOU

Shopping with confidence

You can now tell a real store from a fake one in a couple of minutes, pay in a way that protects you, and know exactly what to do if an order goes wrong. Happy shopping.

Bill's Home Tech · Complete Manuals Series · (330) 200-8042 · billshometech.com · Portage County, Ohio