



Fake AI Store Websites and Made-Up Reviews

Why that too-good deal and those glowing reviews may be an AI-made trap —
and how to shop safely.

————— **An Extended Guide · No. 1640 · SAFETY** —————

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit — billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

- The 60-Second Version 4
- 1. Why I Wrote This One 4
- 2. How Fake Stores Work 5
- 3. What AI Added to the Con 6
- 4. The One Rule for Shopping Safely 7
- 5. The Too-Good-to-Be-True Price 7
- 6. How to Spot a Fake Store 8
- 7. Seeing Through Fake Reviews 9
- 8. Checking a Store Before You Buy 10
- 9. Why Credit Cards Protect You Best 11
- 10. The Impersonator Store 12
- 11. Where These Ads Find You 12
- 12. The Counterfeit-Goods Problem 13
- 13. The Fake Order and Delivery Texts 14
- 14. Protecting Your Details at Checkout 15
- 15. Why It Works on Savvy People 16
- 16. If You've Been Scammed by a Store 16
- 17. A Word on Marketplace Sellers 17
- 18. Questions People Ask Me 18
- 19. A Five-Minute Safe-Shopping Setup 19
- 20. Reporting It — and Why It Helps 19

21. When to Just Call Me 20

22. Contact Card & a Warm Close 21

Everyday Cheat Sheet 21

A Picture to Follow Along 23

A Second Look 24

A Note From Bill 24

Your Visit — and My Promise 25

SUMMARY

The 60-Second Version

Scammers build professional-looking fake online stores and fill them with AI-generated product photos and glowing fake reviews, then advertise unbeatable prices on social media and in search results. You pay and get nothing, a cheap counterfeit, or your card details are stolen. Shop safely by sticking to retailers you know and trust, being suspicious of prices that are too good to be true, checking a store out independently before buying, and always paying by credit card — which offers the strongest protection if something goes wrong.

- 1 A store or ad offers a popular item at an unbelievably low price.
- 2 The site looks professional, with glowing reviews and great photos.
- 3 Be suspicious: deals too good to be true usually are.
- 4 Check the store independently before buying — not by its own reviews.
- 5 Pay by credit card for the best protection; never by wire, gift card, or crypto.

WATCH OUT

AI can build a convincing store and write hundreds of five-star reviews in minutes. A polished site and great reviews are no longer proof — judge by price, independent checks, and how they want you to pay.

1. Why I Wrote This One

Online shopping got a new kind of trap.

In more than thirty years of helping folks across Portage County with their technology, I have watched online shopping go from a novelty to a part of everyday life — and watched the scams grow right alongside it. The newest twist is that scammers can now build a convincing online store, stock it with realistic AI-made product photos, and fill it with hundreds of glowing fake reviews, all in a matter of minutes. The old signs of a sketchy site — crude design, obvious typos, no reviews — have been erased by artificial intelligence.

These fake stores lure shoppers with deals that seem too good to pass up: a popular item at a fraction of its real price, a hard-to-find product suddenly in stock, a going-out-of-business blowout. You order and pay, and then either nothing arrives, or a cheap counterfeit shows up, or — worst of all — your card details are quietly stolen and used. Meanwhile the glowing reviews that reassured you were written by a computer, and the store may vanish as quickly as it appeared.

The good news is that a handful of simple habits let you keep enjoying the real convenience of online shopping while sidestepping these traps. You do not need to stop shopping online or become an expert; you just need to know how fake stores and fake reviews work, and how to shop in a way that protects your money and your details. We will walk through the warning signs, the safe way to pay, and how to check a store before you trust it. No fear, just confidence.

TIP

The goal isn't to stop shopping online — it's to shop so your money and details stay safe. A few simple habits let you enjoy the convenience while avoiding the traps.

2. How Fake Stores Work

The anatomy of the trap.

A fake online store is a website built to look like a legitimate shop but designed only to take your money or your payment details. Scammers can create these quickly and cheaply, complete with professional design, product listings, a shopping cart, and a checkout page. Some are entirely invented brands; others impersonate real, well-known retailers with a near-identical name and look. Either way, the storefront is a facade with nothing honest behind it.

They reach you mostly through advertising and search. You might see an ad on social media for an amazing deal, find the store high in search results, or get a link in an email or message. The ad shows a popular product — electronics, clothing, tools, a trendy gadget — at a price far below normal, which is the hook. When you click through, the store looks real and reassuring, so you place an order and enter your card details, believing you have found a great bargain.

What happens next varies, but none of it is good. Often nothing arrives at all, and the store stops responding or disappears. Sometimes a cheap counterfeit or a completely different, worthless item shows up instead of what you ordered. And in some cases the real goal was never to sell you anything but to harvest your card details at checkout, which are then used for fraud or sold. Understanding that the whole store may be a facade is the first step to shopping safely.

WATCH OUT

A fake store's goal may be to take your payment for nothing, send a counterfeit, or simply steal your card details at checkout. The professional storefront can be pure facade.

3. What AI Added to the Con

Why these are harder to spot now.

Artificial intelligence has made fake stores far more convincing and far faster to produce. Where a scammer once had to design a site and might give themselves away with crude work, AI can now generate polished store designs, realistic product photographs of items that may not exist, fluent product descriptions, and — critically — large volumes of believable customer reviews, all in minutes. The whole apparatus that once signaled a store's legitimacy can now be fabricated wholesale.

The fake reviews deserve special attention, because reviews are how many of us decide to trust a store or a product. AI can write hundreds of varied, natural-sounding five-star reviews, complete with plausible details and even fake reviewer names and photos, making a brand-new scam store appear to have a long history of happy customers. The reassurance you feel seeing glowing reviews may be entirely manufactured, which is exactly what the scammer intends.

The takeaway mirrors the other AI scams: you can no longer judge a store's legitimacy by how professional it looks or how good its reviews are, because those are precisely what AI makes easy to fake. So your defense shifts to things the scammer cannot easily fabricate — the store's real reputation checked through independent sources, the suspiciousness of the price, how they ask you to pay, and whether you are dealing with a retailer you already know and trust. The polish is no longer any guide; your habits are.

GOOD TO KNOW

AI writes hundreds of believable five-star reviews in minutes, giving a brand-new scam store a fake 'history' of happy customers. Great reviews are no longer proof of anything.

4. The One Rule for Shopping Safely

Stick to trusted stores, pay by credit card.

Here is the heart of shopping safely, in one sentence: buy from retailers you already know and trust, reached through their official site or app, and pay by credit card — and treat any store or deal that found you, especially one too good to be true, with real caution. That combination — trusted store, reached yourself, paid by credit card — handles the great majority of online-shopping risk, and it lets you shop freely at the places you rely on.

Sticking to known, reputable retailers is the single biggest protection, because an established store you reach through its genuine site or app is overwhelmingly likely to be legitimate. The danger lives mostly at the edges — unfamiliar stores, too-good deals, links from ads and messages, sites you have never heard of. You can shop with confidence at the major, well-known retailers and the local and specialty shops you already know, while bringing extra caution to anything new, unknown, or suspiciously cheap.

Paying by credit card is the other pillar, because credit cards offer the strongest protection if something goes wrong. If you never receive an item, get a counterfeit, or your details are misused, a credit card lets you dispute the charge and typically recover your money, with the card company's fraud protection on your side. That safety net is why a credit card is far safer than a debit card, a bank transfer, or any of the untraceable methods scammers prefer — and it is a big reason to make it your default for online shopping.

GOOD TO KNOW

Two habits cover most of the risk: shop at retailers you already know (reached through their own site or app), and pay by credit card for the strongest protection if anything goes wrong.

5. The Too-Good-to-Be-True Price

The hook that should raise your guard.

The most reliable warning sign of a fake store is a price that is too good to be true, because an unbeatable deal is the bait these scams depend on. When you see a popular, in-demand item — a well-known brand of electronics, a trendy product, a tool or appliance — offered at a tiny fraction of its normal price, your excitement at the bargain is exactly the reaction the scammer is counting on to override your caution. A deal that seems impossibly good usually is.

This does not mean every low price is a scam; there are legitimate sales and genuine discounts. But there is a difference between a sensible markdown and a price so low it makes no business sense — a current, popular item at ninety percent off, a product that is sold out everywhere suddenly cheap and in stock, a luxury brand at bargain-bin prices. When a deal is dramatically better than anywhere reputable, that is precisely when to slow down and apply extra scrutiny, rather than rushing to grab it before it is gone.

Scammers reinforce the too-good price with urgency: a countdown timer, 'only 3 left,' a 'flash sale ending soon,' a 'closing down' blowout. This manufactured pressure is designed to stop you from pausing to check, pushing you to buy immediately on impulse. So let the combination of an unbelievable price and pressure to hurry be a bright warning sign. A genuine good deal from a trustworthy source does not evaporate if you take a few minutes to make sure the store is real.

WATCH OUT

A current, popular item at a tiny fraction of its real price — especially with a countdown or 'only a few left' — is the classic fake-store hook. If a deal seems impossibly good, slow down and check.

6. How to Spot a Fake Store

The warning signs beyond the price.

Beyond the suspicious price, several signs can reveal a fake store, and noticing even one or two should prompt caution. None of these is proof on its own, and a sophisticated fake may avoid some, but together they help you judge an unfamiliar store before you trust it with your money and card.

- A web address that is slightly off — a misspelling, odd extra words, or a strange ending — especially if it mimics a known brand.
- The store is brand-new or you've never heard of it, yet advertises amazing deals on popular items.
- Little or no legitimate contact information — no real address, no working phone, only a web form or a generic email.
- Poor or oddly-worded policies on returns, shipping, and privacy, or none at all.
- Prices far below everywhere else, with pressure to buy immediately.
- Only payment methods that are hard to reverse — wire, gift cards, cryptocurrency, or direct bank transfer.

The payment methods are an especially strong tell, so they are worth their own emphasis. A legitimate online store lets you pay by credit card and other standard, protected methods. A store that only accepts, or pushes you toward, wire transfers, gift cards, cryptocurrency, or direct bank transfers is a major red flag, because those methods leave you no recourse if you are cheated. When a 'store' will not take a normal credit-card payment, that alone is reason to walk away.

WATCH OUT

A store that only takes wire transfers, gift cards, crypto, or direct bank transfers — not normal credit cards — is a glaring red flag. Those methods leave you no way to get your money back.

7. Seeing Through Fake Reviews

When the glowing praise is manufactured.

Since reviews are now so easily faked, it helps to know how to read them more skeptically. Fake reviews, whether AI-written or bought, tend to share certain qualities, and learning to notice them keeps you from being reassured by manufactured praise. Reviews can still be useful, but only when you read them with a critical eye rather than taking a sea of five stars at face value.

- A flood of glowing, generic five-star reviews that praise without specific, believable detail.
- Reviews that all appear around the same time, or on a store that is brand-new.
- Oddly similar wording or phrasing across many reviews, as if produced in bulk.
- A suspicious absence of any critical or mixed reviews, which real products almost always have.
- Reviews only on the store's own site, with nothing independent found elsewhere.

The most important shift is to weigh independent reviews over a store's own. A scammer controls what appears on their own site, so their reviews prove little; what matters is the store's reputation on sources the scammer does not control — independent review sites, the Better Business Bureau, broader web searches, and the experiences of real people you can find outside the store itself. If a store looks wonderful on its own pages but you can find nothing legitimate about it elsewhere, that gap is a serious warning.

GOOD TO KNOW

A store controls its own reviews, so they prove little. Weigh independent reviews and reputation — from outside the store — far more heavily than the glowing praise on its own pages.

8. Checking a Store Before You Buy

A few minutes that protect you.

When you are tempted by an unfamiliar store, a few minutes of independent checking can save you from a scam. The key word is independent: you investigate the store through sources it does not control, rather than trusting what it says about itself. This is quick and easy, and it is exactly how you tell a genuine small retailer from a convincing fake.

- Search the store's name plus words like 'scam,' 'complaint,' 'reviews,' or 'legit' to surface others' experiences and warnings.
- Look the business up on the Better Business Bureau and independent review sites.
- Check the web address carefully for misspellings or oddities, and look for how long the site has existed if you can.
- Look for real, verifiable contact details — a genuine address and working phone — not just a web form.
- Read the return, shipping, and privacy policies to see if they're real and reasonable.

If your checking turns up warnings, complaints of orders never arriving, or simply a blank — no independent trace of the store existing before its sudden amazing deals — treat that as your answer and do not buy. A legitimate store, even a small one, generally leaves some verifiable footprint: real reviews across the web, a findable business, honest policies. A store that exists only as a glossy site advertising unbeatable prices, with nothing real behind it when you look, is one to avoid.

WATCH OUT

Before buying from an unfamiliar store, search its name plus 'scam' or 'reviews,' and check the BBB. A few minutes of independent checking is how you tell a real small shop from a fake.

9. Why Credit Cards Protect You Best

The safety net that matters most.

I keep urging you to pay by credit card, so let me explain why it matters so much, because it is one of your strongest protections in all of online shopping. Credit cards come with robust fraud protections and dispute rights: if you are charged for something you never received, sent a counterfeit, or billed fraudulently, you can dispute the charge with your card company and typically get your money back. The card company stands between you and the merchant, and the loss is not simply yours to absorb.

Contrast that with the alternatives. A debit card pulls money directly from your bank account, and while it has some protections, recovering funds can be slower and harder, and the money is gone from your account in the meantime. A bank transfer, wire, gift card, or cryptocurrency payment typically has no such protection at all — once sent, it is usually gone for good, which is exactly why scammers push those methods. The payment method you choose largely determines whether a bad outcome is a recoverable inconvenience or a total loss.

So make a credit card your default for online shopping, especially with any store you are not fully sure of, precisely because it gives you that safety net. If a store will not accept a normal credit-card payment, treat that as a serious warning and shop elsewhere. The modest discipline of paying by credit card online turns many potential disasters into simple disputes, and it is one of the easiest, most powerful habits you can adopt to shop with confidence.

WATCH OUT

A credit card lets you dispute and recover money for goods never sent, counterfeits, or fraud. Debit, wire, gift cards, and crypto offer far less or no protection — make the credit card your default.

10. The Impersonator Store

When the fake pretends to be a real brand.

A particular kind of fake store impersonates a real, well-known retailer or brand, which can catch even careful shoppers. The scammer creates a site that closely mimics the genuine company's name, logo, design, and products, often with a web address that is a near-copy of the real one — a slight misspelling, an extra word, a different ending. You believe you are on the real brand's site, so you shop and pay with confidence, when in fact you are on a convincing counterfeit.

These impersonator sites reach you the same way other fakes do — through ads, search results, and links in messages — which is how you can end up on the fake rather than the real site even for a brand you know. An ad for a familiar brand's 'sale,' a link that looks right, a search result that is actually a scammer's lookalike: any of these can land you on the counterfeit. The familiar branding then does the scammer's work, because you trust the look and do not scrutinize the address.

The defense is to reach brands and retailers the safe way: by typing their known web address yourself, using their official app, or going through a bookmark you saved, rather than through an ad, a link, or a search result when you are shopping. That way you land on the genuine site, not a lookalike. And watch the web address carefully for the tiny discrepancies that reveal an impersonator. When you reach a brand through a channel you control, the counterfeit sites simply cannot intercept you.

WATCH OUT

Reach brands by typing their address or using their official app — not through an ad, link, or search result. Scammers run near-identical lookalike sites that intercept shoppers who click.

11. Where These Ads Find You

Social media, search, and messages.

It is worth knowing where fake-store ads reach you, because recognizing the channels helps you stay alert in them. The most common is social media, where scam stores buy ads promoting their unbelievable deals, slipping them into your feed alongside legitimate ones. These ads can look entirely normal and professional, and appearing on a major platform does not mean anyone verified the store — scam ads routinely slip onto the biggest sites.

Search results are another avenue. Scammers use various techniques, including paid placement, to get their fake stores to appear prominently when you search for a product or a deal, so a high search ranking is not a guarantee of legitimacy. And links to fake stores arrive by email, text, and social-media messages too, sometimes promoting a sale, sometimes impersonating a known retailer. Any of these channels can deliver you to a convincing fake if you click through and shop.

The practical response is to be especially cautious about stores you reach by clicking an ad, a search result, or a link, as opposed to stores you go to deliberately. When an ad or a deal catches your eye, rather than buying through it, note the product and the brand, then go find it the safe way — at a retailer you know, reached through its own site or app. Treating 'stores that found me' with more suspicion than 'stores I went to' is a simple, powerful filter that keeps most fake-store traffic from ever reaching your wallet.

WATCH OUT

A scam store appearing in your social feed or high in search results isn't vetted by anyone — scam ads slip onto major platforms constantly. Be extra cautious with any store you reach by clicking an ad or link.

12. The Counterfeit-Goods Problem

When something does arrive, but it's fake.

Not every fake-store experience ends in receiving nothing; sometimes an item arrives, but it is a counterfeit or a cheap substitute far from what you ordered. You order a brand-name product and receive a knockoff; you order a quality item and get a flimsy, worthless version; you order one thing and get something else entirely. The store got your money, and you got something nearly valueless, which is its own form of the scam.

Counterfeits are not just a disappointment; they can be unsafe. Fake electronics and chargers can be fire or shock hazards, counterfeit health and beauty products can contain harmful ingredients, and knockoff safety equipment may not protect you as the real thing would. So the harm from a counterfeit can go beyond wasted money to genuine risk, which is one more reason to buy brand-name and safety-sensitive items from trusted, authorized sellers rather than from unknown stores offering suspiciously cheap deals.

If a counterfeit arrives, your credit card is again your friend: you can dispute the charge for receiving an item materially different from what was advertised, and document the

discrepancy with photos. You can also report counterfeit sellers to the platform and the real brand, which works to shut such sellers down. But the best protection remains prevention — buying from authorized, reputable sellers — because chasing a refund for a counterfeit from a fly-by-night store is far harder than simply avoiding it, and no refund undoes the risk a dangerous counterfeit can pose.

WATCH OUT

Counterfeit electronics, chargers, and health products aren't just a waste of money — they can be genuinely unsafe. Buy brand-name and safety items from trusted, authorized sellers.

13. The Fake Order and Delivery Texts

Scams that ride on your real shopping.

Closely related to fake stores are scams that exploit the fact that you shop online, arriving as fake order confirmations and delivery notifications. You get a text or email about a package 'held' for a small fee, an 'order problem' needing you to confirm details, a 'delivery' that failed and must be rescheduled, or a charge for an order you do not recognize with a link to 'dispute' it. These ride on the normal flow of online shopping to seem plausible, especially if you are actually expecting a package.

The goal is the usual one: to get you to click a link and enter payment or personal details on a fake page, or to call a fake support number. The 'small redelivery fee' is a classic, as is the 'confirm your details to release your package' request. Because so many of us have packages in transit much of the time, a delivery notification does not raise suspicion the way an out-of-the-blue message might, which is exactly why scammers use this framing.

The defense is to never act through these messages. Do not tap links in unexpected delivery or order texts and emails; instead, check your orders and deliveries the way you always do — in the retailer's own app or site, or the shipping carrier's official app, reached yourself. A real package issue will show up there. A real retailer does not charge surprise fees by text link to release a delivery. Treating every delivery and order message as something to verify independently, rather than act on, closes this door completely.

WATCH OUT

'Your package is held, pay a small fee' and 'confirm your order details' texts are scams riding on your real shopping. Check orders and deliveries in the retailer's or carrier's own app — never the link.

14. Protecting Your Details at Checkout

Safe habits for entering payment info.

Since a fake store's goal may be to steal your payment and personal details at checkout, a few habits protect that sensitive moment. First, only enter your card and personal information on stores you have reason to trust, reached the safe way, since the checkout page is precisely where a fake store harvests what it wants. If you are not confident the store is legitimate, do not reach the point of entering your details at all.

Give only the information a purchase genuinely requires, and be wary of a store asking for more than makes sense — a store does not need your Social Security number, your date of birth, or excessive personal details to sell you a product, and requests for such information are a warning sign. Using your credit card rather than a debit card or bank details limits what is exposed, and some banks and cards offer virtual or single-use card numbers for online shopping, which add a layer of protection by keeping your real number off unfamiliar sites.

It also helps to watch your card and bank statements regularly for charges you do not recognize, since a stolen card number may be used quietly. Catching an unauthorized charge early lets you dispute it and get a new card number promptly, limiting the damage. Between shopping only at trusted stores, paying by credit card, giving only necessary information, and keeping an eye on your statements, you make the checkout moment — the scammer's prime target — a safe one.

WATCH OUT

A store asking for your Social Security number, date of birth, or excessive personal details to sell a product is a warning sign. A purchase needs your payment and shipping info — not your life story.

15. Why It Works on Savvy People

Not gullibility — good fakes and good deals.

Falling for a fake store is not a sign of being naive or a poor shopper; it happens to savvy, experienced online shoppers, and understanding why removes any shame. The fakes are simply very good now, thanks to AI — professional sites, realistic photos, convincing reviews — so the usual judgment of 'this looks legitimate' no longer reliably distinguishes real from fake. A careful person applying sensible instincts can still be fooled, because the fakes are built to pass exactly those instincts.

The lure of a great deal also plays on a universal human tendency. We all love a bargain and feel a little thrill at finding one, and scammers engineer their fake deals to trigger that excitement and the fear of missing out. That emotional pull can momentarily override caution in anyone, which is why the too-good-to-be-true deal is such an effective hook. It is not a failure of intelligence to be tempted by an amazing price; it is human nature, deliberately exploited.

So if you have been caught by a fake store, set aside any embarrassment; you encountered a convincing fake and a tempting deal, both engineered to fool careful people. The useful response is to recover what you can, protect your card, and carry the simple habits forward. And the lesson is not to distrust all online shopping, which is overwhelmingly fine at trusted retailers, but to bring extra care to the edges — the unknown stores and the too-good deals — where the fakes live.

GOOD TO KNOW

Fake stores fool savvy shoppers because AI makes the fakes genuinely convincing and the deals genuinely tempting. Being caught isn't gullibility — it's human nature, deliberately exploited.

16. If You've Been Scammed by a Store

Steps to recover and protect yourself.

If you have paid a fake store and received nothing, got a counterfeit, or suspect your details were stolen, act promptly — and if you paid by credit card, your odds of recovery are good. There is no shame in being caught by a convincing fake; the priority now is to recover your money and protect your accounts.

- 1 Contact your credit card company right away, explain the situation, and dispute the charge; they can often refund you and issue a new card number.
- 2 If you paid by debit card, call your bank immediately to dispute and protect your account; act fast.
- 3 If you paid by wire, gift card, or crypto, contact that provider at once, though recovery is harder — still try.
- 4 Watch your statements closely for any further unauthorized charges, and get a new card number if your details may be compromised.
- 5 Report the fake store to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud), the platform where you saw the ad, and the real brand if it was impersonated.

GOOD TO KNOW

If you paid a fake store by credit card, you can usually dispute the charge and recover your money. This is the biggest reason to make a credit card your default for online shopping.

17. A Word on Marketplace Sellers

Person-to-person selling has its own traps.

Beyond fake storefronts, a lot of online buying and selling now happens person-to-person, on marketplaces and classifieds and in buy-sell groups, and these carry their own scams worth a brief word. Here the 'store' is an individual seller or buyer, and AI helps scammers craft convincing listings, photos, and messages. The deals that are too good to be true apply just the same: a sought-after item priced far below reason, from a seller urging you to act fast, is a classic marketplace trap.

Several patterns recur. A seller asks you to pay outside the platform's protected system — by wire, gift card, a payment app to a stranger, or a deposit to 'hold' an item — which removes your protection and is a strong red flag. A buyer 'accidentally' overpays and asks for the difference back, which is a scam built on a fake or reversible payment. A listing for a rental, a vehicle, or a pet asks for money before you have seen the real thing, and the item does not exist. In each, money is requested before any genuine, verifiable exchange.

The protections are sensible and simple. Favor local, in-person transactions where you can see the item and, for safety, meet in a public place or a police-department 'safe exchange' spot. Keep payments within the platform's protected system where one exists, and be very wary of any request to pay off-platform or by untraceable methods. Never send money for an item, deposit, or 'shipping' before you have verified it is real, and treat overpayment and 'pay to hold it' requests as scams. Used carefully, these marketplaces are useful; the

caution is for deals and requests that ask you to pay before anything real has changed hands.

WATCH OUT

On marketplaces, a request to pay off-platform (wire, gift card, app to a stranger) or a buyer who 'overpays' and wants the difference back is a scam. Keep it local, in-platform, and verify before you pay.

18. Questions People Ask Me

The ones that come up again and again.

The store had hundreds of great reviews — doesn't that prove it's real? No. AI can generate hundreds of believable fake reviews in minutes, and a store controls what appears on its own pages. Weigh independent reviews and reputation from outside the store far more than the praise on its own site.

The ad was on a major social-media platform — isn't it vetted? No. Scam stores advertise on the biggest platforms all the time, and the platform does not verify that advertisers are honest. Seeing an ad somewhere reputable is not a guarantee; judge the store itself, and prefer going to it the safe way rather than through the ad.

Is it safe to shop at small or unknown online stores at all? It can be, with care: check the store independently (search its name plus 'reviews' or 'scam,' check the BBB), make sure it takes credit cards, and pay by credit card for protection. Many small shops are perfectly legitimate — the caution is for unknown stores with too-good deals, especially those that found you via an ad.

How do I know I'm on the real brand's site and not a fake? Reach brands by typing their known web address yourself or using their official app, not by clicking an ad, link, or search result. Watch the web address for tiny misspellings or odd endings. When you go to a brand through a channel you control, lookalike sites can't intercept you.

19. A Five-Minute Safe-Shopping Setup

Habits that let you shop with confidence.

A few simple habits, adopted once, let you enjoy online shopping with confidence while sidestepping fake stores and stolen details. None of it is restrictive; it is just a sensible way to shop that keeps your money and information safe. Make these your defaults and most of the risk simply falls away.

- 1 Shop mainly at retailers you already know and trust, reached through their own site or app.
- 2 Pay by credit card for the strong protection it gives if anything goes wrong.
- 3 Be suspicious of deals too good to be true, and of pressure to buy right now.
- 4 Check any unfamiliar store independently (search 'name + scam/reviews,' check the BBB) before buying.
- 5 Reach brands by typing their address or using their app — not through ads, links, or search results.
- 6 Give only necessary information at checkout, and watch your statements for charges you don't recognize.

GOOD TO KNOW

If you do just two things: shop at retailers you already know, and pay by credit card. Those two habits handle the great majority of online-shopping risk.

20. Reporting It — and Why It Helps

A few minutes that protect the next person.

Reporting a scam can feel pointless once the money is gone, but it genuinely matters. Reports help investigators link cases together, give platforms and phone carriers the evidence to shut fakes down, and warn others before they are caught. You do not need to have lost money to report — flagging an attempt is valuable too. It takes only a few minutes, and it turns a bad experience into something that helps your neighbors.

- Report to the Federal Trade Commission at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov), the national clearinghouse for scams. You can also call 1-877-382-4357.
- Report online or financial crime to the FBI at ic3.gov, their internet-crime complaint center — especially for larger losses or cryptocurrency.
- Contact the Ohio Attorney General's consumer protection team at 800-282-0515 or through ohioattorneygeneral.gov.

- If your identity may be exposed, visit [IdentityTheft.gov](https://www.identitytheft.gov) for a step-by-step recovery plan.
- Report spam texts by forwarding them to 7726 (SPAM), and use the 'report' button inside apps and email.

I wrote a separate, step-by-step guide on reporting to the FTC, the FBI, and the Ohio Attorney General, with exactly what to write down and what to expect afterward. If the reporting steps feel like a lot, that is a perfect thing to call me about. I am glad to sit with you and help you file, so that your report actually reaches the people who can use it.

GOOD TO KNOW

You will usually not hear back from a report, and that is normal. Your report still joins a bigger picture that helps investigators and warns others, even when nothing lands in your own inbox.

21. When to Just Call Me

A calm second opinion costs you nothing.

If something about an online store, deal, or product reviews you're unsure about has you second-guessing yourself, or you just want a steady second opinion before you do anything, please call me. There is never a charge to ask a scam question, and never any judgment. I would far rather spend a few minutes on the phone talking it through with you than hear later that something cost you money or worry. That is genuinely what I am here for, and it is some of the most satisfying work I do.

If you would like a hand in person, I come to homes all across Portage County. I can help you check something safely, tighten up your accounts and passwords after a close call, set your devices and routine so these scams have a harder time reaching you, and walk your whole family through a simple plan. We go at your pace, with no pressure and no rushing, and you come away feeling steadier.

GOOD TO KNOW

The best time to call is before you act — before you click, pay, or share anything. A quick 'does this seem right to you, Bill?' is one of my favorite kinds of call to get.

22. Contact Card & a Warm Close

Keep this page where you can find it again.

Bill's Home Tech — your local tech, Bill Davis, owner and only tech. Phone or text: (330) 200-8042. Email: bill@billshometech.com. Web: billshometech.com. Service area: Atwater, Ravenna, Kent, Streetsboro, Aurora, Rootstown, Mantua, Garrettsville, Windham, Edinburg, Suffield — all of Portage County, Ohio.

- Free phone call: any scam question or close call, always free, with no judgment and no rushing.
- In-home scam-check visit: \$99 flat for the first visit, with a 30-day follow-up included.
- Remote help by screen-share, for when you would rather not wait for a visit.

A little caution lets you enjoy all the convenience of online shopping while keeping your money and your details safe. Shop at stores you trust, pay by credit card, and call me anytime a deal or a site seems off. I am a phone call away, and glad to help you shop with confidence.

CHEAT SHEET

Everyday Cheat Sheet

The one rule

Buy from retailers you already know, reached through their own site or app, and pay by credit card. Treat unknown stores and too-good deals with real caution.

Red flags

- A price too good to be true, with 'buy now' pressure.
- A store you've never heard of advertising amazing deals.
- Glowing reviews only on the store's own site.
- A web address with misspellings or odd endings.
- Only wire, gift card, crypto, or bank-transfer payment.

Shop safely

- 1 Check unknown stores independently ('name + scam/reviews,' BBB).
- 2 Reach brands by typing their address or using their app.
- 3 Pay by credit card, never wire/gift card/crypto.
- 4 Give only necessary info; watch your statements.
- 5 Scammed? Dispute the credit-card charge right away.

WATCH OUT

AI fakes the store and the reviews perfectly now. Judge by the price, independent reputation, and how they want you to pay — not by how professional the site looks.

AT A GLANCE

A Picture to Follow Along

The Fake-Store Trap

AI builds the whole convincing facade in minutes.



Judge by price, reputation, and payment - not by the polish.

Illustration - a schematic; details vary by device and setup.

AT A GLANCE

A Second Look

Shop Online Safely

A few habits keep your money and details safe.

- 1 Tempted by a deal or an unfamiliar store?
- 2 Be suspicious if it's too good to be true
- 3 Check the store independently ('name + scam')
- 4 Reach brands by typing the address or using the app
- 5 Pay by credit card - never wire, gift card, or crypto
- 6 Give only necessary info; watch your statements

A credit card lets you dispute and recover if something goes wrong.

Illustration - a schematic; details vary by device and setup.

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.



HOW I CAN HELP

Your Visit — and My Promise

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full \$99. No questions, no awkwardness. That's how I'd want to be treated.

Call or text **(330) 200-8042** · Book a visit: **billshometech.com/book** · **bill@billshometech.com**

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.