BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2324

Updated November 2026

Check If a Website Is Fake Before You Type Anything

A one-minute routine that spots copycat sites before they catch your password or card

Plain-English tech help from:
Bill's Home Tech
Portage County, Ohio

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 3
The Short Version 3
How You End Up on a Fake Site 4
Check the Web Address First 4
The Padlock Myth 5
Other Signs Something's Off 6
Look the Business Up Separately 6
Pop-Ups That Pretend to Be Warnings 7
Make Your Browser Help You 8
A One-Minute Routine 8
If You Already Typed Something In 9
Shopping Sites You've Never Heard Of 9
Keep Your Logins Locked Down 10
When to Call Bill 10
Everyday Cheat Sheet 12
A Note From Bill 13
Your Visit — and My Promise 14

SUMMARY

The 60-Second Version

Scammers build convincing copies of real websites to steal what you type, and they lure you there through links in emails, texts, ads, and QR codes. Your most reliable check is the web address: find the real name just before the '.com' and make sure it's exactly the company you expect — extra words, hyphens, or misspellings mean a fake.

Don't rely on the padlock symbol; it only means the connection is private, not that the site is honest, and fake sites have it too. Safest of all, reach your bank, email, and shopping sites by typing the address yourself or using an app, never by clicking a link someone sent. If you already typed something in, change that password right away, call your bank if money details were involved, and report the site at ReportFraud.ftc.gov.

- The real name sits just before the '.com' — read it carefully.
- The padlock proves privacy, not honesty — don't trust it alone.
- Reach important sites yourself, not through a sent link.

1 The Short Version

Fake websites are the backbone of modern scams. A scammer builds a near-perfect copy of your bank, a shopping site, or a government page, then lures you there through an email, a text, an ad, or a QR code. Everything looks right — the logo, the colors, the layout — but anything you type goes straight to the criminal. The encouraging part: you can check whether a site is real in under a minute, and the checks are easy to learn.

This guide gives you a short, reliable routine to run before you ever type a password, a card number, or personal details into any website. Do it once or twice and it becomes second nature — a quick glance that quietly protects everything you do online.

- Scammers build convincing copies of real sites to catch what you type.
- The web address (the part before '.com') is your most reliable tell.
- A padlock symbol means the connection is private — NOT that the site is honest.
- Safest of all: reach important sites yourself, not through a link someone sent.

WATCH OUT

The simplest protection isn't a check at all — it's a habit: get to your bank, email, and shopping accounts by typing the address yourself or using an app you installed, never by clicking a link in a message. Do that and most fake sites never get a chance.

2 How You End Up on a Fake Site

Nobody searches for a fake website — they're led there. Knowing the on-ramps helps you slow down at exactly the right moments.

- A link in an email or text claiming there's a problem with your account.
- An ad in a search result or social feed, sometimes above the real company's own listing.
- A QR code on a sign, flyer, or letter.
- A slightly misspelled address you typed or that auto-corrected — 'arnazon.com' instead of 'amazon.com.'

GOOD TO KNOW

Scammers sometimes buy ads so their fake site appears at the very top of search results, above the genuine company. The top result is not always the real one — look at the address, and when it matters, type it yourself.

3 Check the Web Address First

The web address is the hardest thing for a scammer to fake and the most reliable thing for you to check. The key is knowing which part to read.

1. Find the address bar at the top of your browser and look at the full address.

2. Read it right to left to find the real name: the part just before the first single slash '/', and specifically just before '.com', '.org', or '.gov'.
3. 'chase.com/login' is Chase. 'chase.secure-verify.com' is NOT Chase — the real name there is 'secure-verify.com'.
4. Watch for look-alikes: extra words, hyphens, misspellings, or odd endings like '.net' where you expect '.com'.
5. If the real name isn't exactly the company you expect, don't type anything.

> *The trusted name belongs right before the '.com'. If it's anywhere else in the address, it's decoration — and decoration is how fakes hide.*

4 The Padlock Myth

Many of us were taught that a little padlock in the address bar means a site is safe. That was never quite right, and today it's misleading. The padlock only means your connection to the site is private — that no one is eavesdropping between you and it. It says nothing about whether the site itself is honest.

Scammers can get that padlock on their fake sites easily and for free, so nearly all of them have one now. A padlock is like a sealed envelope: it keeps the letter private in transit, but it tells you nothing about whether the person who wrote it is trustworthy.

WATCH OUT

Do not treat the padlock as a sign of safety. A fake bank site can show a padlock just as easily as the real one. Judge the web address, not the padlock.

5 Other Signs Something's Off

Beyond the address, a few softer clues often give a fake site away. Any one of them is reason to stop and double-check.

- Prices that are too good to be true, or 'everything must go' urgency.
- Only odd payment options — gift cards, wire transfer, crypto, or 'friends and family' app payments.
- No real contact information, or a contact page with only a web form and no address or phone.
- Sloppy details: broken links, mismatched logos, or text that reads a little strangely.
- Pop-ups claiming your computer is infected and you must call a number or click to 'fix' it.

> **GOOD TO KNOW**
>
> A genuine store almost always offers normal, protected payment like a credit card. If a site will ONLY take gift cards, wire, or crypto, that alone is enough to walk away — those are the payments you can't get back.

6 Look the Business Up Separately

When you're unsure about a site — especially a shop you've never used — step away from it and check from the outside.

1. Open a new tab and search the company's name along with 'reviews,' 'scam,' or 'complaints.'
2. See whether the business has a real history — an established presence, not a site that appeared last week.
3. Find the company's phone number from a source other than the suspicious site, and call to confirm it's really them.
4. For a store, check whether a return address and policy actually exist and make sense.

WATCH OUT

For shopping sites you don't know, paying with a credit card (not a debit card or app) adds a layer of protection, because card companies can dispute fraudulent charges. It's a good habit even on sites you trust.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

7 Pop-Ups That Pretend to Be Warnings

A whole family of fakes isn't a website you went to, but a scary pop-up that ambushes you — flashing warnings that your computer is infected, with a number to call or a button to click. These are fake, every time.

- Real virus protection does not fill your screen with alarms and a phone number to call.
- The goal is to get you to call 'support' (a scammer) or click to install something harmful.
- They often freeze the page or play a loud alert to panic you.

1. Don't call the number, don't click the pop-up, and don't let it rush you.
2. Close the browser tab or window; if it won't close, shut the whole browser down.
3. If the screen seems stuck, restart the computer — the pop-up is almost always just a web page.
4. If a 'technician' is already on the line, hang up, and never let anyone remotely control your computer.

WATCH OUT

Never let someone you reached through a pop-up or unexpected call take remote control of your computer. That's how they lock you out or empty accounts. If this is happening, hang up and call me instead.

8 Make Your Browser Help You

Your web browser has built-in protections that warn you about known dangerous sites, if they're switched on and up to date.

- Keep your browser updated — updates include fresh lists of known scam sites.
- Leave 'safe browsing' or 'fraudulent website warning' features turned on in your browser's settings.
- Save your real banking and shopping sites as bookmarks, and use those instead of searching each time.
- Let your browser or password manager fill saved passwords — if it doesn't offer to on a 'familiar' site, that site may be a fake.

> **GOOD TO KNOW**
>
> A password manager quietly doubles as a fake-site detector: it only offers to fill your password on the exact site where you saved it. If you're on 'your bank' and it stays silent, the address probably isn't really your bank.

9 A One-Minute Routine

Put it all together and checking a site takes less than a minute. Run this before typing anything sensitive.

1. Read the address: is the real name, just before '.com', exactly who you expect?
2. Ignore the padlock — it proves nothing about honesty.
3. Ask how you got here: a link someone sent is riskier than an address you typed.
4. If anything's off, stop, and reach the site yourself by typing the address or using the app.

> *Read the address, ignore the padlock, question the link. One minute, and the fakes fall away.*

10 If You Already Typed Something In

If you entered details on a site you now doubt, move quickly and gently — this catches careful people too.

1. If you entered a password, change it on the real site at once, and anywhere you reused it.
2. Turn on two-step verification so a stolen password alone can't get in.
3. If you shared card or bank details, call your bank or card company to watch for and block fraud.
4. If you shared a lot of personal information, visit IdentityTheft.gov for a tailored recovery plan.
5. Report the fake site to the FTC at ReportFraud.ftc.gov.

> **WATCH OUT**
>
> If you're unsure what you exposed or which account to secure first, call me. We'll go through it in the right order so nothing's left open, and I'll make sure your real accounts are locked down tight.

11 Shopping Sites You've Never Heard Of

A big share of fake sites are fake stores — dazzling ads for deals that are too good to be true, often on social media. A few extra checks protect both your money and your disappointment.

1. Search the store's name with 'reviews' and 'scam' before buying anything.
2. Be wary of a brand-new site with impossibly low prices on popular items.
3. Look for a real address, phone number, and a sensible return policy.
4. Pay with a credit card, which can dispute fraud, rather than a debit card, app, or gift card.
5. If the deal and the urgency both feel high, slow down — real bargains rarely vanish in an hour.

WATCH OUT

A fake store may take your money and send nothing, or send a cheap knock-off. Paying by credit card is your safety net, because the card company can reverse a fraudulent or undelivered charge in a way that gift cards and apps cannot.

12 Keep Your Logins Locked Down

Even careful people land on a fake site now and then, so it pays to make a single stolen password as harmless as possible. Two habits do most of the work.

- Use a different password for each important account, so one leak doesn't unlock the rest.
- Turn on two-step verification, so a stolen password alone can't get in without a code only you have.
- Let a password manager remember them for you — it's safer than reusing one you can memorize.
- Never share the one-time codes your bank or email texts you; no real company will ask for them.

GOOD TO KNOW

Two-step verification is the single most powerful protection against stolen passwords. Even if a fake site captures your password, the thief is stopped cold at the step that asks for the code only you receive.

13 When to Call Bill

Telling a real website from a fake one is a skill, and like any skill it's easier learned with someone beside you the first time. If you'd like to feel confident every time you log in or shop, that's a friendly, practical visit.

I'll set up bookmarks and apps for your important sites so you're not searching and clicking links, turn on your browser's safety features, help you with a password

manager that doubles as a fake-site detector, and practice the address-reading check until it's second nature. And if a fake site has already caught you, I'll help you close every gap.

- You want your banking and shopping sites bookmarked and your browser's protections on.
- You'd like to practice spotting a real web address versus a look-alike.
- A scary pop-up is on your screen or a 'technician' wants to control your computer.
- You typed details into a site you now suspect was fake.

CHEAT SHEET

Everyday Cheat Sheet

Keep this by the computer. Run this before typing anything sensitive.

I want to...	Do this...
Check a site fast	Read the address — is the real name just before '.com' who you expect?
Avoid a classic trap	Ignore the padlock; it proves privacy, not honesty
Stay safest	Reach your bank/shops by typed address or app, not a link
Judge an unknown store	Only odd payments (gift card, wire, crypto) = walk away
Handle a scary pop-up	Don't call or click; close the browser; never allow remote control
If you typed details	Change the password, call your bank, report at ReportFraud.ftc.gov
Get help	Call Bill: (330) 200-8042

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

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

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.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · 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.