



Spotting a Fake Login Page

A calm, plain checklist for phishing

————— An Extended Guide · No. 1659 · PASSWORDS & SECURITY —————

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.

1. What a fake login page is	4
2. Why these scams work on careful people	4
3. The one habit that beats almost everything	5
4. Reading the web address	5
5. Lookalike addresses and the tricks they use	6
6. Let your password manager be the lookout	7
7. Urgency is the scammer's favorite tool	7
8. Phishing by email	8
9. Phishing by text message	9
10. Phishing by phone call	9
11. Fake pop-ups and search-result traps	10
12. Signing in: the safe routine	11
13. How passkeys sidestep the whole problem	11
14. Two-factor as your safety net	12
15. If you already typed your password	12
16. If you typed a payment card or more	13
17. Checking a link before you ever click	14
18. When a message is actually real	14
19. A special word on bank and brokerage sites	15
20. Helping a spouse or parent stay safe	15
21. Fakes that target one person	16

22. Why your email is the prize 17

23. Building the habits that last 17

24. Reporting a phish and warning others 18

25. A few myths worth clearing up 18

26. Putting it all together 19

27. Frequently asked questions 20

Your Spot-the-Fake Cheat Sheet 20

Plain-English Word List 21

A Picture to Follow Along 23

A Second Look 24

A Note From Bill 24

Your Visit — and My Promise 25

1. What a fake login page is

A convincing copy with one purpose: to catch your password.

A fake login page is exactly what it sounds like: a scammer's copy of a sign-in screen you trust — your bank, your email, Amazon, your account at a store. It can look perfect, right down to the logo and the colors. But it isn't the real site. It's a trap, and its single purpose is to catch your username and password the moment you type them.

The way it works is simple and sneaky. A scammer sends you a message with a link. You click, you see a familiar-looking sign-in page, you type your password out of habit — and in that instant, the password lands in the scammer's hands rather than logging you in. Often the fake page then shuffles you off to the real site so you never notice.

GOOD TO KNOW

This is the most common way ordinary people get their accounts stolen — not clever hacking, but a convincing copy and a moment of habit. The flip side is wonderful news: a few calm habits stop nearly all of it.

I help folks with this all the time, and I want you to leave this guide feeling calmer, not more fearful. The scammers rely on hurry and surprise. Slow down, and you win.

2. Why these scams work on careful people

It's not about being gullible — it's about being busy.

Let's clear something up right away, because it matters. Falling for a fake login page has nothing to do with being foolish or 'bad with computers.' These scams work on sharp, careful people every day. They succeed by catching you at a busy moment, with a message that looks routine and a request that seems reasonable.

The scammer's whole craft is making you act before you think. A message that looks like your bank, arriving when you're distracted, asking you to 'confirm' something — that's engineered to slip past careful judgment by not giving it time to engage. Knowing that is half the defense.

TIP

If you ever do get caught by one, be kind to yourself. It happens to professionals. What matters is acting quickly afterward, which this guide walks you through.

So the goal here isn't to make you suspicious of everything. It's to give you a couple of small, automatic habits that run in the background and catch the fakes without you having to be on high alert all day.

3. The one habit that beats almost everything

Reach the site yourself, don't follow the link.

If you take only one thing from this guide, make it this: never sign in by clicking a link someone sent you. Instead, reach the site yourself — type the address into your browser, or use a bookmark you saved. This single habit defeats the overwhelming majority of fake login pages, because the fake only reaches you through that link.

Think about it. The scammer's power is entirely in getting you to their copycat page. If you ignore their link and go to your bank the way you always do — your saved bookmark, or typing the name yourself — you simply never arrive at the fake. You land on the real site, every time.

- 1 Got an email or text urging you to sign in? Don't click its link.
- 2 Open your browser and type the company's address yourself, or tap your saved bookmark.
- 3 Sign in there, and see whether the thing the message mentioned is really waiting for you.

TIP

Make a bookmark for each site that matters — your bank, your email, Amazon. Then reaching the real site is one tap, and the temptation to click a risky link in a message just fades away.

4. Reading the web address

The single most reliable tell there is.

The web address — the line at the top of your browser — is where a fake gives itself away. Scammers can copy a logo perfectly, but they can't use the real company's exact web address. So learning to read that address, even roughly, is the surest skill you can build.

The part to focus on is the core name right before the first single slash. For a real site, that's the company's plain name followed by its ending, like the bank's name and then.com. You're checking that this core name is exactly right — spelled correctly, with nothing odd

tacked on.

- Find the core name just before the first single slash.
- Check it's the company's real name, spelled exactly.
- Be wary of extra words, dashes, or a strange ending after the name.
- The lock symbol alone is not proof — fakes can have it too.

WATCH OUT

The little padlock symbol by the address only means the connection is private, not that the site is honest. Scammers' pages can show the padlock too. Read the name, not just the lock.

5. Lookalike addresses and the tricks they use

The small swaps that fool a quick glance.

Scammers are clever about building addresses that look almost right. Once you know their handful of tricks, they jump out at you. Here are the common ones to watch for.

- A swapped or extra letter — the company name with one letter changed or doubled.
- An extra word glued on — the real name plus '-secure' or '-verify' or '-support.'
- The real name buried in a longer address, as a word in the middle rather than the core name.
- An unusual ending — something other than the plain.com the company normally uses.
- A number standing in for a letter, like a zero for an 'o.'

The trickiest is the real name buried in the middle. A scammer might use an address where your bank's name appears, but the actual core name — the part just before the first single slash — belongs to the scammer. That's why you always look at that specific spot, not just whether the company's name appears somewhere.

GOOD TO KNOW

If reading addresses closely strains your eyes, that's all the more reason to lean on the 'type it yourself or use your bookmark' habit. It sidesteps the whole problem — you never see the fake address at all.

6. Let your password manager be the lookout

When it won't fill, that's a loud warning.

If you use a password manager, you have a quiet, tireless lookout working for you — and it's one of the best fake-page detectors there is. Here's why. A password manager remembers the exact web address where each of your passwords belongs. It will only offer to fill your password on that real address. On a fake page, it simply won't offer.

So when you land on what looks like your bank's sign-in, and your password manager stays silent instead of offering to fill it in as it always does, stop. That silence is the manager telling you, 'This isn't the address where your bank password lives.' It catches lookalike addresses that your eye might miss.

TIP

Train yourself to expect the auto-fill. When it's there, you're almost certainly on the real site. When it's missing on a page that should have it, treat that as a red flag and check the address carefully.

This is one more reason a password manager is worth having. Beyond strong, unique passwords, it doubles as a fake-page alarm that never gets tired or distracted. My guides on password managers walk through choosing and setting one up.

7. Urgency is the scammer's favorite tool

When a message rushes you, slow down.

Almost every phishing message has one thing in common: it tries to make you hurry. 'Your account will be closed in 24 hours.' 'Suspicious activity detected — verify now.' 'Your package couldn't be delivered, confirm immediately.' The urgency is the trick. It's designed to make you act before the careful part of your mind catches up.

Real companies rarely work this way. Your bank doesn't close your account in an hour over an email. The post office doesn't hold your package hostage over a text. When a message pushes you to act this instant, that pressure itself is the warning sign — more reliable, often, than any detail in the message.

TIP

Make urgency your trigger to slow down, not speed up. The moment a message says 'act now or else,' that's your cue to stop, set it aside, and reach the company yourself at your own pace.

Give yourself permission to be slow. Nothing genuine is lost by taking five minutes to go to the real site and check. And almost everything is lost by rushing into a fake one.

8. Phishing by email

The classic doorway, and how to read it.

Email is where phishing began and where much of it still lives. A phishing email dresses itself up as a message from a company you know, with their logo and tone, and a button or link inviting you to sign in or 'confirm.' The message may be about a payment, a locked account, a delivery, or a refund — whatever gets you to click.

- Check the real sender address, not just the friendly name — tap the name to reveal it.
 - Hover over a link, without clicking, to preview where it really goes.
 - Be suspicious of generic greetings like 'Dear Customer' from a company that knows your name.
 - Watch for odd phrasing or small spelling mistakes in an otherwise official-looking note.
- But here's the freeing part: you don't actually have to judge the email at all. Whatever it claims, the safe response is always the same — don't use its link; go to the company yourself and check. If the message was real, you'll find the matter waiting for you on the real site.

GOOD TO KNOW

Because your email is the master key to your other accounts, a phishing email aimed at your email password is especially dangerous. My guide on locking down your email pairs closely with this one.

9. Phishing by text message

The same trick, in your text messages.

Phishing by text message has its own nickname — 'smishing' — but it's the same trick in a different doorway. A text arrives with a short, urgent message and a link: a delivery problem, a toll you supposedly owe, a bank alert, a prize. Texts feel more personal and immediate than email, which is exactly why scammers like them.

Texts are also harder to inspect. The web address hides behind a short link, and there's no sender name to check — just a phone number that may be faked. So the 'reach the company yourself' habit matters here even more than with email. Don't tap the link; go to the company's app or type its address.

- Delivery and toll texts with links are overwhelmingly scams — check with the carrier or agency directly.
- Your bank's real texts don't ask you to sign in through a link.
- A link that's a jumble of letters, or uses a shortening service, deserves extra suspicion.

WATCH OUT

A text saying you owe a small toll or a delivery fee, with a link to pay, is one of the most widespread scams going in many areas. Never pay or sign in through such a link — go straight to the real agency or carrier yourself.

10. Phishing by phone call

When the scammer talks to you directly.

Phishing also comes by phone — sometimes called 'vishing,' for voice. A caller claims to be from your bank, a tech company, or even a government office. They sound professional and calm, and they steer the conversation toward getting you to confirm details, read back a code, or sign into something while they wait.

The golden rule with phone calls is this: a real company is fine with you hanging up and calling them back on a number you look up yourself. A scammer will fight that, because their whole scheme depends on keeping you on this call. So when in doubt, hang up and dial the number on the back of your card or the company's official site.

TIP

No legitimate company or agency will ever call and ask you to read back a security code that was just texted to you. That code is the key to your account. Reading it aloud hands it over. Hang up.

Be especially wary of a caller who tells you to keep the call secret, to buy gift cards, or to move money 'to keep it safe.' Those are never real instructions, no matter how official the caller sounds.

11. Fake pop-ups and search-result traps

Two more places fakes lie in wait.

Fake login pages don't only arrive by message. Two other doorways catch people, and they're worth knowing. The first is the alarming pop-up — a window that appears while you're browsing, warning that your computer is infected and urging you to call a number or sign in to 'fix' it. These are fakes, designed to frighten you into acting.

The second is the search-result trap. You search for your bank or a company's help line, and a result near the top — sometimes an advertisement — leads to a scammer's copycat page or a fake support number instead of the real one. Scammers pay to appear there precisely because people trust the top result.

- A pop-up claiming your computer is infected and giving a number to call is a scam — close the browser, don't call.
- When searching for a company, look past the ads and check the address before you click.
- Better still, use your saved bookmark instead of searching each time.

WATCH OUT

No real virus warning ever gives you a phone number to call. Those pop-ups exist only to connect you with a scammer. If one traps your browser, close the whole browser or restart the computer.

12. Signing in: the safe routine

A calm sequence you can make automatic.

Let's turn all of this into a short routine you can run without thinking — the sign-in equivalent of checking your mirrors before you change lanes. It takes a few seconds and catches nearly everything.

- 1 Pause — notice if a message is pushing you to hurry.
- 2 Reach the site yourself: type the address or use your bookmark.
- 3 Glance at the web address and confirm the core name is exactly right.
- 4 Expect your password manager to offer to fill — and be wary if it doesn't.
- 5 Sign in, and if a second-step code is requested, enter it only on that page you reached yourself.

Do this a few times and it becomes second nature, the way locking the front door is. You won't have to think it through each time — your hands will just reach for the bookmark, and your eye will flick to the address out of habit.

GOOD TO KNOW

The single most powerful line in that routine is 'reach the site yourself.' If you only ever remember that one, you'll sidestep the great majority of fakes.

13. How passkeys sidestep the whole problem

A sign-in that can't be phished.

There's a newer way to sign in, called a passkey, that's genuinely immune to fake login pages — and it's worth knowing because it quietly removes the whole danger. A passkey replaces your typed password with your phone or computer's own unlock: your face, fingerprint, or PIN. Crucially, it's tied to the real site's exact address.

Because there's no password to type, there's nothing for a fake page to capture. And because the passkey only works on the genuine address it was made for, a scammer's copycat page simply can't use it — the passkey won't engage at all. It's the rare security upgrade that's also easier to use.

GOOD TO KNOW

This is one of the best reasons to adopt passkeys where they're offered. A password can be phished; a passkey essentially cannot. My passkeys guide walks through setting them up.

You don't have to switch everything over at once. Even adding a passkey to your most important accounts — your email, especially — takes a big target off the table.

14. Two-factor as your safety net

Why a second step softens a mistake.

Even careful folks slip up once in a while, and this is where the second step — two-factor — earns its keep. If you do type your password into a fake page, a scammer who has your password still can't get into your account without that second step. It's the net that catches you when the first line fails.

That said, be aware of one wrinkle: a sophisticated fake page may also ask for your second-step code, hoping you'll type it in too. This is why the 'reach the site yourself' habit still matters even with two-factor on — and why passkeys, which can't be phished at all, are stronger still.

- Two-factor greatly limits the damage of a stolen password.
- Never enter a code on a page you reached by clicking a link.
- An app-based or passkey second step is sturdier than a texted code.

TIP

Turn on two-factor everywhere it's offered, starting with your email and bank. Even if it isn't perfect against the cleverest fakes, it stops the ordinary ones cold.

15. If you already typed your password

A calm, clear order of operations.

Suppose the worst has happened — you realize, a moment too late, that you typed your password into a fake page. First, take a breath. This is fixable, and acting quickly makes it a small event rather than a big one. Here's the order.

- 1 Go to the real site yourself and change that password right away.
- 2 If you used that same password anywhere else, change it there too.
- 3 Turn on the second step (two-factor) if it wasn't already on.
- 4 Sign out all other devices if the site offers that option.
- 5 Watch the account closely, and contact the company if anything looks off.

Speed matters because you're racing the scammer to the account. Change the password before they can use it, and their stolen copy becomes worthless. If the account was your email, treat it as urgent — that's the master key to everything else.

WATCH OUT

If you also entered a card number or your Social Security number on the fake page, call your bank and consider a credit freeze. My guides on credit freezes and company breaches walk through those next steps.

16. If you typed a payment card or more

Extra steps when it's not just a password.

Sometimes a fake page asks for more than a password — a card number, your date of birth, even your Social Security number. If you entered those, a few extra steps are worth taking, calmly and in order. None of this is cause for panic; it's just closing the doors the information could open.

- Card number — call your bank's number on the back of the card, report it, and ask about a new card.
 - Social Security number — consider freezing your credit at all three bureaus, which is free.
 - Date of birth and address — these can't be changed, so lean on the freeze and on account alerts.
 - Watch your statements and set up transaction alerts so anything odd surfaces fast.
- The credit freeze is the strongest single move if your Social Security number was exposed, because it blocks anyone from opening new credit in your name. It's free by law, and I have a full guide devoted to it.

WATCH OUT

Report the scam at reportfraud.ftc.gov. It helps authorities track these schemes, and the site can also point you to the right recovery steps for your situation.

17. Checking a link before you ever click

How to peek at where a link really goes.

Sometimes you want to know where a link leads without committing to clicking it. There are safe ways to peek, and they're handy when a message is probably fine but you'd like to be sure. The habit of looking before you leap serves you well.

- On a computer, rest your mouse pointer over the link without clicking — the real address appears at the bottom corner of the screen.
- On a phone, press and hold the link gently — a preview of the address pops up, which you can then cancel.
- Read the core name just before the first single slash, as you would for any address.
- If the preview doesn't match the company it claims to be from, don't click.

That said, even this is optional. The safest path is still to ignore the link entirely and reach the company yourself. Peeking is a nice extra skill, but 'go there yourself' never fails.

GOOD TO KNOW

Shortened links, which hide the real address behind a short jumble, can't be read this way with confidence. Treat a shortened link in an unexpected message as something to avoid.

18. When a message is actually real

Not everything is a scam — how to tell calmly.

It's important to say this plainly: plenty of messages from companies are genuine. Your bank really does send statements; stores really do send receipts and shipping notes. The goal isn't to distrust every message — it's to have a safe way to act on the real ones without getting caught by the fake ones.

And the beautiful thing is that the safe habit works perfectly for real messages too. If your bank emails that there's a new statement, you don't need to decide whether the email is real. You just go to your bank the usual way — bookmark or typed address — and there's your statement, waiting. Real or fake, your response is identical and always safe.

WATCH OUT

This is why the 'reach it yourself' habit is so freeing: you never have to become a detective. You simply stop using links in messages to sign in, and the whole question of real-versus-fake stops mattering.

So don't let phishing make you anxious about every email. Let it make you calm — because you've got one simple move that handles them all.

19. A special word on bank and brokerage sites

The accounts scammers want most deserve extra care.

Your money accounts — bank, credit card, brokerage, retirement — are the biggest prizes for scammers, so they get the most convincing fakes. It's worth giving these a little extra care, because the stakes are higher and the copycats are at their best here.

- Use the bank's own app, or a bookmark you made yourself, never a link in a message.
- Turn on the strongest second step your bank offers.
- Turn on transaction alerts so you see activity as it happens.
- Know that your bank will never phone, email, or text asking you to 'verify' by giving a password or code.

If anything about a money account feels off — an unexpected message, a call, a page that doesn't look quite right — stop and contact the institution directly using the number on your card or statement. They would far rather take a cautious call than clean up a fraud.

WATCH OUT

A common, frightening scam is a call claiming to be your bank's 'fraud department,' warning of a charge and offering to 'protect' your money by moving it. Hang up and call the number on your card. Real fraud teams never move your money for you.

20. Helping a spouse or parent stay safe

Sharing the habit with the people you help.

If you look after technology for a spouse or an aging parent, teaching this one habit — reach the site yourself — is among the most protective things you can pass along. It doesn't require them to understand web addresses or spot clever fakes. It just asks them to stop using links in messages to sign in.

- Set up bookmarks on their devices for their bank, email, and key sites.
- Agree on a simple rule: 'If a message asks you to sign in, call me first.'
- Reassure them that it's always fine to pause and check — no real company minds.
- Make sure their accounts have a second step turned on as a safety net.

The 'call me first' agreement is powerful. It turns a lonely, pressured decision into a quick conversation, and it's often in that pause that a scam falls apart. Let them know you'd always rather get the call than hear about a loss later.

TIP

Consider being their go-to second opinion for anything that creates urgency. Many scams targeting seniors crumble the moment a trusted family member takes a look.

21. Fakes that target one person

When the scammer has done their homework.

Most phishing is sent out by the millions, hoping a few bite. But a smaller, nastier kind is aimed at one person — you, by name. The scammer may have learned a few true details about you from a breach or from social media, and they weave those into the message to make it feel personal and trustworthy.

A message like this might mention your real bank, your actual name, or a company you genuinely use. That accuracy is unsettling, and it's meant to be — it lowers your guard. But here's the reassuring part: your defense doesn't change one bit. No matter how personal the message, you still reach the company yourself rather than through its link.

- True details in a message don't make its link safe — they're often scraped from breaches.
- A message that knows your name and bank still gets the same treatment: go there yourself.
- Be extra wary of anything that follows up a real event, like a recent purchase.

GOOD TO KNOW

This is one more reason to keep your accounts locked down and your passwords unique — the less of your information floating around, the less material a scammer has to make a message feel personal.

22. Why your email is the prize

The one account a phisher most wants.

Of all the fake login pages out there, the ones impersonating your email provider deserve special caution. That's because your email is the master key to everything else you own — the place password resets for your other accounts land. A scammer who captures your email password can quietly reset your bank, your shopping accounts, and more.

So a message claiming your 'mailbox is full' or your 'email will be deactivated,' leading to a sign-in page, is a classic and dangerous phish. Treat any such message with the firmest version of the habit: never sign into your email through a link, only ever by typing the address or using your app.

WATCH OUT

Fake 'your email is full / verify your account' pages are among the most valuable to scammers, because your inbox unlocks the rest. Reach your email only the way you always do, never through a message's link.

If you take one account and make it bulletproof, make it your email — a strong unique password, a second step, and ideally a passkey. My guide on locking down your email walks through all of it.

23. Building the habits that last

Small routines that quietly protect you for good.

The best protection against fake login pages isn't vigilance — staying alert is tiring and can't last. It's a few small habits that run on their own, so you're protected even on a distracted, busy day. Let's gather them in one place.

- Bookmark the sites that matter, and sign in through those.
- Use a password manager, and treat its silence as a warning.
- Turn on a second step everywhere, and add passkeys where offered.
- Let urgency be your cue to slow down, never to hurry.
- Never give a password or code to someone who contacted you.

None of these asks you to be an expert or to inspect every message. They quietly stack up into a strong defense that works whether you're paying close attention or not. That's exactly what good security should feel like — mostly invisible.

GOOD TO KNOW

Habits beat knowledge here. Knowing about phishing helps, but the bookmark you actually use and the manager that actually guards you are what stop the fakes in practice.

24. Reporting a phish and warning others

A small kindness that trips up the scammers.

When you spot a phishing message, a minute of reporting it does real good. It helps providers block the scam for everyone else, and warning the people you know can spare a friend a bad afternoon. You don't have to make a project of it — a couple of easy actions are plenty.

- In most email apps, use the 'Report phishing' or 'Report junk' option rather than just deleting.
 - Forward suspicious texts to your carrier by sending them to 7726, which spells SPAM.
 - Report scams to the Federal Trade Commission at reportfraud.ftc.gov.
 - Tell a friend or family member if you see a scam going around — a quick heads-up helps.
- Reporting also helps the real company. Banks and big services run teams that take down fake pages impersonating them, and your report can be the tip that gets a copycat site shut down before it catches someone else.

TIP

If a fake page impersonated a specific company, let that company know through its real website. Many have a dedicated address for forwarding phishing attempts, and they genuinely want to hear about it.

25. A few myths worth clearing up

Beliefs that give false comfort or needless fear.

A handful of common beliefs about fake pages are off the mark, and sorting them out keeps you from either false comfort or needless worry.

- 'The padlock means it's safe.' No — it only means the connection is private. Fakes can show it too.
- 'It looked exactly like the real site, so it must be real.' Looks are easy to copy; the address and your habits are what count.

- 'Only careless people get phished.' Not so — it catches careful people during busy moments.
- 'If I have antivirus, I'm covered.' Helpful, but it can't stop you typing a password into a convincing fake.

The common thread is that appearances and single gadgets aren't the defense. Your habits are — reaching sites yourself, reading the address, trusting your password manager's silence, refusing to be rushed.

TIP

When someone tells you a page 'looked totally real,' gently steer them to the real question: how did you get there, and was the address exactly right? That's where the truth lives.

26. Putting it all together

The whole defense on one breath.

Let's bring it home. A fake login page is a scammer's copy of a site you trust, built to catch your password. You defeat nearly all of them with one habit — reach the site yourself instead of clicking a link — backed by a few small helpers.

- 1 Reach sites yourself: type the address or use your bookmark.
- 2 Read the web address and confirm the core name is exactly right.
- 3 Let your password manager's silence warn you off a fake.
- 4 Treat urgency as a reason to slow down.
- 5 Keep a second step on, and add passkeys where you can.
- 6 If you slip, change the password fast and watch the account.

That's the whole defense. No gadget to buy, no expertise required — just a calm habit or two that quietly keep your passwords where they belong.

GOOD TO KNOW

If a message ever has you unsure, you don't have to decide alone. It's always free to pause and ask someone you trust — or to call me and we'll look at it together.

27. Frequently asked questions

Quick answers to the things people ask most.

How can I tell a fake login page from the real one? The surest way is to reach the site yourself and check the web address. A password manager that won't auto-fill is another strong clue.

Does the padlock symbol mean a site is safe? No. It only means the connection is private. Scammers' pages can have the padlock too — read the address name.

I clicked a link but didn't type anything — am I in trouble? Usually not. The danger is typing your password or details. If you only clicked and closed it, you're very likely fine.

What's the best single protection? Reach sites yourself instead of using links in messages. Passkeys, where offered, are immune to fake pages entirely.

I typed my password into a fake page — now what? Go to the real site yourself, change that password at once, change it anywhere you reused it, and turn on a second step.

TIP

If any of this feels like one step too many, that's exactly the kind of thing I can sit down and walk through with you — in person or remotely — in under an hour.

CHEAT SHEET

Your Spot-the-Fake Cheat Sheet

Keep this page by the computer. It's everything you need to catch a fake login page before you hand over a password.

The three-second check (every time)

- 1 Stop — don't let a message rush you.
- 2 Read the web address, especially the part just before the first single slash.
- 3 Reach the site yourself — type it, or use your own saved bookmark.
- 4 Only then sign in.

Warning signs you're on a fake

- A link in an email or text sent you there.
- The web address is misspelled or has extra words.
- Your password manager won't offer to fill the login.

- The page threatens that your account closes unless you act now.
- It asks for more than usual — card number, Social Security number, codes.

If you already typed your password

- 1 Don't panic — act, in order.
- 2 Go to the real site yourself and change that password.
- 3 Change it anywhere else you reused it.
- 4 Turn on the second step (two-factor) if it isn't on.
- 5 Watch the account, and call the company if anything looks wrong.
- 6 Need a hand? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Phishing — A scam that tricks you into typing your password or details on a fake page or into a fake message. Said like 'fishing.'

Fake login page — A scammer's copy of a trusted site's sign-in screen, built to capture your username and password as you type them.

Web address (URL) — The line at the top of the browser that names the site you're on, such as the bank's name followed by.com.

Domain — The core name in a web address — the part just before.com or.org. Reading it carefully is the surest way to spot a fake.

Lookalike domain — A web address built to resemble a real one, using a swapped letter, extra word, or odd ending to fool a quick glance.

Password manager — An app that stores your logins and fills them in. It only fills on the real site, so a refusal to fill is a warning.

Two-factor (2FA) — A second step after your password. It limits the damage if a password is ever stolen on a fake page.

Smishing — Phishing that arrives by text message rather than email. Same trick, different doorway.

Vishing — Phishing done by phone call — a 'voice' version — where a caller tries to talk you into giving up details or codes.

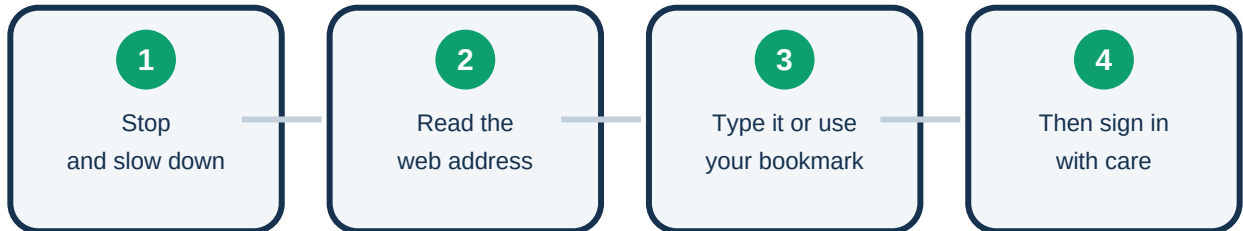
Spoofing — Faking the sender name, phone number, or look of a message so it appears to come from someone you trust.

AT A GLANCE

A Picture to Follow Along

The Three-Second Check

Before you type a password, run this every time.



Reaching a site yourself beats trusting any link you were sent.

Illustration - a calm habit that defeats almost every fake login page.

AT A GLANCE

A Second Look

Real Sign-In vs. Fake Page

The tells that separate the genuine from the counterfeit.

Real Sign-In	Fake Page
You went there Address is exact Manager auto-fills No pressure	A link sent you Address is off Manager won't fill Urgent threats

When the address is wrong or the manager won't fill, don't type.

Illustration - the warning signs usually appear together.

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.