BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2211

Updated November 2026

"Suspicious Sign-In" Warnings — Real or Fake?

How to tell a genuine security alert from a scam designed to scare you

Plain-English account 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

Why These Warnings Exist at All 4

The Telltale Signs of a Fake 4

The One Safe Way to Check 5

If It Turns Out to Be Real 6

If It Was Just You 6

What Never to Do, No Matter What 7

The Text-Message and Pop-Up Versions 7

Reduce the Real Alerts You Get 8

Report the Fakes 8

Real Examples You Might See 9

Help the People You Care About 9

Why Slowing Down Is Your Best Defense 10

When to Call Bill 11

Everyday Cheat Sheet 12

A Note From Bill 13

Your Visit — and My Promise 14

SUMMARY

The 60-Second Version

A 'suspicious sign-in' warning is built to scare you, and scammers send fakes that look just like the real ones. You never have to guess: do not click anything in the message — instead, type the account's address yourself, sign in, and check its 'recent activity' or security page. If the alert is real, it shows there too, and you can change the password from the inside, sign out other devices, and turn on two-factor.

If it does not show up, it was a fake — report it as phishing and delete it. Fakes rely on urgency, links, and password requests; real companies never ask for your password or a code by email, and never cold-call you.

1 The Short Version

Real companies do send genuine alerts when they notice an unfamiliar sign-in — that part is a good and helpful feature. But scammers send look-alike warnings by the millions, counting on fear to make you click before you think. Both land in your inbox looking urgent and official.

You never have to guess. The one rule that keeps you safe is this: do not click the link or button in the message. Instead, open the account yourself by typing its address, and check from the inside. If something is truly wrong, you will see it there too.

- Genuine sign-in alerts are real and worth paying attention to — but so are the fakes.
- Never click a link or button inside the warning message itself.
- Check by going to the account directly, typing the address yourself.
- If it is real, you can secure the account from the inside; if fake, you lose nothing by ignoring it.

WATCH OUT

Think of it like a caller claiming to be your bank: you do not give details to whoever called you — you hang up and dial the number on your card. Online, the same wisdom applies: ignore the message's own link and go to the site yourself.

2 Why These Warnings Exist at All

It helps to know that genuine sign-in alerts are a safety feature, not a bad sign. Your email and other accounts watch for logins that look unusual and tell you, so you can act if it was not you.

- A sign-in from a new device, new browser, or new city can trigger a real alert.
- Even you traveling, or using a new phone, can set off a genuine warning.
- The alert gives you a chance to lock things down if it truly was not you.
- Scammers imitate this helpful feature precisely because people have learned to take it seriously.

GOOD TO KNOW

A real alert often turns out to be you — signing in from a new phone, a hotel, or a relative's computer. So a warning is not proof of a break-in; it is simply a prompt to check, calmly, whether that sign-in was yours.

3 The Telltale Signs of a Fake

While you should always verify by going to the site directly, scam warnings do share some giveaways. Spotting these can settle your nerves before you even check.

- Urgent threats: 'act within 24 hours or your account will be closed.'
- A sender address that is a jumble, or not the company's real domain.
- Greetings like 'Dear Customer' instead of your name, or clumsy wording.
- A big button begging you to 'verify now' or 'secure your account here'.
- A request to confirm your password, which no real company ever makes by email.

WATCH OUT

The surest tell of a fake is pressure plus a link. Real companies let you take your time and go to the site yourself; scammers need you to click their link right now, before the fear fades. Urgency is the weapon — slow down and it loses its power.

4 The One Safe Way to Check

Here is the method that works every time, for any warning, from any company. It never exposes you, because you go to the real place yourself rather than following the message.

1. Do not click anything in the message — not the link, not the button, not 'unsubscribe'.
2. Open your browser and type the company's address yourself (for example, gmail.com or your bank's site).
3. Sign in the way you normally do.
4. Look for a security or recent-activity section, which shows real alerts and recent sign-ins.
5. If the warning is genuine, it will appear there too; if it does not, the message was fake.

WATCH OUT

Most major accounts have a 'recent activity' or 'where you're signed in' page. Checking it directly not only confirms whether an alert is real — it also lets you sign out any device you do not recognize, right from the inside, safely.

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.

5 If It Turns Out to Be Real

Sometimes the check confirms a genuine unfamiliar sign-in. That is unsettling, but you are now in exactly the right place to handle it calmly and completely.

1. Change the account's password right away, from the inside where you already are.
2. Sign out all other devices or sessions, which the security page usually offers as one button.
3. Turn on two-factor if it is not already on, so a password alone is not enough.
4. Check that your recovery phone and email were not changed by whoever signed in.

> **GOOD TO KNOW**
>
> Changing your password from inside the account instantly boots out anyone else who was signed in. That one action does most of the work — the rest is tidying up and making sure they cannot get back in.

6 If It Was Just You

Very often the 'suspicious' sign-in was you all along — from a new phone, a trip, or a different browser. It is worth knowing so you do not worry over a false alarm.

- New phone or tablet? That is a new device, and a real alert is expected.
- Travelling? A sign-in from another city looks unfamiliar to the account.
- Used a relative's or library computer? That too can trigger a genuine warning.
- If you recognize the activity as yours, you can simply dismiss the alert.

> **WATCH OUT**
>
> When a real alert asks 'was this you?', you can safely say yes if you recognize it. Many accounts will then trust that device going forward and stop warning you about it — fewer false alarms later.

7 What Never to Do, No Matter What

A few actions are never safe in response to one of these messages, whether it turns out real or fake. Holding these lines protects you even if you cannot tell which it is.

- Never type your password into a page you reached by clicking the message.
- Never read a verification code to anyone who calls or messages you.
- Never call a phone number printed inside the warning message.
- Never let someone 'from support' take remote control of your computer.

WATCH OUT

Scammers sometimes follow a fake email with a phone call, or put a 'support number' right in the message. Any number you did not look up yourself is suspect. Use only contact details from the company's real website or the back of your card.

8 The Text-Message and Pop-Up Versions

These warnings do not only come by email. Texts and sudden pop-ups use the same fear, and the same safe method defuses them all.

- A text saying 'unusual login, tap here' is checked the same way — go to the site yourself.
- A pop-up while browsing that screams about your account is almost always fake.
- A full-screen 'security warning' with a phone number is a scam; restart to clear it.
- The rule never changes: verify from the real site, never from the message.

GOOD TO KNOW

Pop-ups that appear while you are just browsing the web almost never come from your actual account — accounts send alerts to your email or app, not as web pop-ups. A browser pop-up shouting about your account is a near-certain fake.

9 Reduce the Real Alerts You Get

You can cut down on genuine-but-unnecessary alerts by letting your accounts recognize your own devices. Fewer real alerts also makes the occasional fake stand out more clearly.

- Say 'yes, trust this device' on your own private phone and computer.
- Keep your main devices signed in rather than logging in fresh each time.
- Use an authenticator app, which generates its own alerts you can trust.
- Update your recovery details so alerts reach you, not an old address.

TIP

The fewer false alarms you get, the sharper your instincts stay for the real thing. Trusting your own devices quiets the routine noise, so a genuinely odd alert — or an obvious fake — is easier to notice.

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.

10 Report the Fakes

Reporting a scam message is quick and does a small public good, helping the email provider catch the next batch. It also cleans up your own inbox.

1. In Gmail, Outlook, or Apple Mail, use the 'Report junk' or 'Report phishing' option.
2. This both removes the message and teaches the provider to block similar ones.
3. Do not reply to the scammer, even to tell them off — a reply confirms your address is live.
4. Then simply delete it and carry on.

GOOD TO KNOW

Reporting phishing is more useful than just deleting, because it trains the filters that protect everyone. It takes a single tap, and over time it means fewer of these frightening messages reach you at all.

11 Real Examples You Might See

It helps to picture the common shapes these messages take, so a new one feels familiar rather than frightening. The wording varies, but the playbook is always the same.

- 'We detected a sign-in from Russia. If this wasn't you, verify here.' — go to the site yourself instead.
- 'Your Apple Account has been locked. Confirm your details to unlock.' — Apple does not lock accounts by email link.
- 'Unusual activity on your Amazon account — click to secure.' — open Amazon directly and check your orders.
- 'Your mailbox is full and will be closed — verify to keep it.' — a classic fake; your provider warns you inside the account.

GOOD TO KNOW

Notice the pattern: a scary claim, a demand to act now, and a convenient button. Once you see that shape, you can recognize a fake in seconds — and the safe response is identical every time, so you never have to analyze the details.

12 Help the People You Care About

These scams lean hardest on people who are newer to this, so sharing the one simple rule is a real kindness. It is the same rule that keeps you safe.

- Teach the one rule: never click the message — go to the site yourself.
- Offer to be the person they call before clicking anything worrying.

- Remind them no real company asks for a password or code by email or phone.
- Reassure them that asking first is smart, never a bother.

> **TIP**
>
> Being someone's 'check with me first' person is one of the most protective things you can offer. A ten-second phone call before they click has stopped countless scams cold — and it is far easier than cleaning up afterward.

13 Why Slowing Down Is Your Best Defense

Every one of these scams depends on one thing: getting you to act before you think. The warning is loud, the clock is ticking, the button is right there. The single habit that defeats all of them is simply to slow down.

A real company is perfectly happy for you to close the message, open a browser, and come to them in your own time — nothing bad happens from waiting five minutes. A scammer, by contrast, needs you in the next thirty seconds, because the moment you pause to check, their trick falls apart. So when a message makes your pulse quicken, let that feeling be your cue to slow down, not speed up.

- Urgency is manufactured — real deadlines are rare, and real companies give you time.
- Closing the message and checking later costs you nothing if it is genuine.
- The pause itself is what protects you, because scams cannot survive a calm second look.
- When in doubt, sleep on it or call someone you trust before acting.

> *If a message is rushing you, that pressure is the scam — not the deadline.*

14 When to Call Bill

Telling a real warning from a fake gets easier with practice, and this guide gives you a method that works every time. But these messages are built to rattle you, and when one arrives about your email or your bank, a second opinion is worth a great deal.

I am always glad to look at a worrying message with you before you touch it, tell you plainly whether it is genuine, and — if it is — secure the account properly from the inside. There is no such thing as a silly question here; checking is exactly the right instinct.

- You are not sure whether a warning is real and do not want to risk clicking.
- The check suggests the sign-in was genuinely someone else.
- You already clicked a link or entered details and now feel uneasy.
- A pop-up or caller is pressuring you and you want it handled calmly.

CHEAT SHEET

Everyday Cheat Sheet

Keep this by the computer for the next scary-looking alert.

I want to...	Do this...
Check if it's real	Don't click the message — type the site's address yourself and sign in
See the truth	Look at the account's 'recent activity' / 'security' page
Spot a fake	Watch for urgency, a link/button, 'Dear Customer', or a password request
Handle a real one	Change password from inside, sign out other devices, turn on two-factor
Handle a fake	Report junk/phishing, don't reply, delete it
Never, ever	Click the link, call its number, or read a code to anyone
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.