



AI Chatbot "Support Agents" That Are Really Scammers

Why that helpful 'support chat' or pop-up may be a scammer — and how to find real help.

————— An Extended Guide · No. 1636 · 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. The Fake Support Pop-Up 5

3. What Real Support Never Does 6

4. The Remote-Access Trap 7

5. The Fake Search-Result Number 8

6. The AI Chatbot Twist 9

7. The One Rule for Getting Help 9

8. The Refund and Overpayment Trick 10

9. Why It's So Effective 11

10. Finding Real Help Safely 12

11. A Word About Local, Honest Help 13

12. The Account 'Lockout' Version 14

13. Fake Apps and Download Traps 14

14. The Social-Media 'Support' Reply 15

15. A Steadying Word 16

16. If You Let Someone In 17

17. Helping a Loved One Who's Anxious 17

18. Questions People Ask Me 18

19. A Five-Minute Safety 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 pose as customer-support agents and AI chatbots — through pop-ups, fake phone numbers, fake 'help' websites, and ads — to get your money, your passwords, or control of your computer. Real support never contacts you first out of the blue, never needs your password or a verification code, never asks to take over your screen to 'fix' a surprise problem, and never wants payment in gift cards. To get help, you go to the company yourself through its official website or app — never a number or chat a pop-up, ad, or search result hands you.

- 1 A 'support agent,' chatbot, or pop-up offers to help with a problem.
- 2 It wants your password, a code, remote access to your screen, or payment.
- 3 Real support never needs those for a surprise problem.
- 4 Don't call the number or use the chat it gave you.
- 5 Reach the company yourself through its official site or app.

WATCH OUT

A scary pop-up saying your computer is infected and to 'call Microsoft/Apple support now' is always a scam. Real companies don't put a phone number in a pop-up warning.

1. Why I Wrote This One

Looking for help is where scammers wait.

In more than thirty years of helping folks across Portage County with their technology, I have noticed something a little heartbreaking: the very moment people most need help — when a device acts up, an account seems locked, or a scary message appears — is the moment scammers are most ready to pounce. They pose as the helpful support you are desperately looking for, and because you want help, your guard is down. This guide is about recognizing fake 'support' and finding the real thing safely.

What has made this worse is that 'support' now wears many faces, and artificial intelligence has made some of them very convincing. There are fake phone support lines, scary pop-ups urging you to call a number, fake 'help' websites that top search results, bogus chat windows, and lifelike AI chatbots that can carry on a natural, reassuring conversation while quietly steering you toward harm. The friendly agent helping you may not be a person at all, or may be a scammer wearing a trusted company's name.

The reassuring news is that real support and fake support behave in clearly different ways, and a few simple rules tell them apart every time. You do not have to be technical to stay safe; you just have to know how genuine help actually works and how scammers break those patterns. We will walk through the common fake-support traps, the behaviors that give them away, and — just as important — how to reach real help safely when you genuinely need it. No fear, and no judgment if a 'support' scam has already caught you.

WATCH OUT

The danger moment is when something's gone wrong and you're anxious for help. That's exactly when to slow down — because that's exactly when scammers are waiting.

2. The Fake Support Pop-Up

The scary warning that wants you to call.

One of the most common and alarming fake-support traps is the pop-up warning. You are browsing the web and suddenly your screen fills with a frightening message: your computer is infected, your accounts are at risk, you must not turn off the machine, and you need to call a support number immediately — often with alarming sounds, flashing warnings, and official-looking logos from a company like Microsoft or Apple. It is designed to panic you into calling the number on the screen.

Here is the plain truth: this is always a scam. Legitimate companies do not throw up a full-screen warning with a phone number telling you to call for support. Your computer's real security software does not work that way, and neither Microsoft, Apple, nor any real company monitors your personal browsing and pops up a number to call. The pop-up is a web page designed to look like a system alert, and the whole thing — the warning, the logos, the sounds — is fake, built for one purpose: to get you to call the scammers' number.

If you ever see one of these, do not call the number, and do not let it rattle you. You can usually close it by closing the browser tab or window; if it will not close or seems to lock up your screen, you can restart the computer, which clears it. The pop-up cannot actually harm your computer by itself — its only power is to frighten you into calling. Once you know that, it loses its grip, and you can dismiss it with the calm it does not want you to have.

WATCH OUT

A pop-up with a phone number and 'your computer is infected, call now' is 100% a scam, every time. Don't call. Close the browser or restart — the pop-up itself can't hurt your computer.

3. What Real Support Never Does

The behaviors that unmask a scammer.

The most reliable way to tell fake support from real is to learn how genuine support behaves, because scammers consistently break these patterns. Real customer service, from any legitimate company, follows certain rules, and when 'support' violates them, you are dealing with a scammer, no matter how helpful or official they seem. Keep this short list of 'never' behaviors in mind and you can unmask most fake support instantly.

- Real support does not contact you first, out of the blue, about a problem you did not report.
- Real support does not put a phone number in a scary pop-up or a warning message.
- Real support does not ask for your password or a verification code — ever.
- Real support does not demand payment in gift cards, wire transfers, or cryptocurrency.
- Real support does not pressure you to act immediately or threaten dire consequences.
- Real support does not insist on taking remote control of your computer to fix a surprise problem it told you about.

Notice that these are about behavior, not technical details, so you do not need any expertise to apply them. When 'support' reaches out to you unprompted, wants your password or a code, demands gift cards, rushes you, or wants to take over your screen for a problem you did not know you had, the behavior itself is the giveaway. A genuine company helping you with a problem you reported, through a channel you chose, simply does not do these things.

GOOD TO KNOW

Judge support by behavior, not by how official it looks. Contacting you first, wanting a password or code, demanding gift cards, or rushing you all mean scammer — guaranteed.

4. The Remote-Access Trap

When 'let me fix it for you' hands over the keys.

A particularly dangerous move in tech-support scams is getting you to install software that lets the 'agent' see and control your computer remotely. It is framed as helpful — 'let me connect so I can fix this for you' or 'I'll just take a quick look at what's wrong.' Once you install the program and grant access, the scammer can see everything on your screen, open your files, watch you type passwords, and operate your computer as if sitting in front of it. You have handed a stranger the keys to your digital life.

With that control, scammers do real damage. They may pretend to 'find' problems to justify a fee, dig through your files for passwords and financial information, log into your bank while you watch, move money, install harmful software, or lock you out and demand a ransom. Some stage a fake 'refund' where they pretend to accidentally send you too much money and pressure you to repay the 'difference' in gift cards. The remote connection is the doorway to all of it.

So make this an absolute rule: you never let anyone who contacted you, or whom you reached through a pop-up, ad, or unverified number, take remote control of your computer. Legitimate support for a problem you genuinely reported, through an official channel, may occasionally use a remote session — but only when you initiated the contact through verified means and understand exactly what is happening. If a surprise 'agent' wants into your screen, the answer is always no, and the request itself confirms the scam.

WATCH OUT

Never let an unexpected 'support agent' take remote control of your computer. Granting screen access to a stranger hands them your files, passwords, and bank — it's the doorway to the whole scam.

5. The Fake Search-Result Number

When the 'support line' you looked up is a trap.

Here is a trap that catches careful people, because it springs even when you go looking for help the sensible way. You have a problem with a company — your bank, an airline, a streaming service, a software maker — so you search online for their customer-support phone number. Among the results, scammers plant fake support numbers and fake 'help' websites, dressed up to look official and often appearing high in the results through paid placement or trickery. You call what you think is the real company and reach a scammer instead.

This is insidious because you did initiate the contact, which normally is the safe move, yet you still landed on a scammer because the number itself was fake. The scammer, posing as the company's support, then runs the usual playbook: asks for your account details or password, offers to remote into your computer, or steers you toward a payment or gift cards. Because you believe you called the real company, you are inclined to trust and comply.

The defense is to get support contact information from the company's own official source, not from a general search or an ad. Type the company's known web address directly, or use the contact details on your actual statement, card, product packaging, or the app you already have installed. Treat a phone number from a search result or an ad with caution, and favor numbers that come from the company's genuine site or your own documents. Reaching the company through a channel you can trust to be genuinely theirs is what keeps the 'I looked it up myself' move actually safe.

WATCH OUT

Scammers plant fake 'support' numbers and sites in search results and ads. Get support contact info from the company's official site or your own statement — not from a general search.

6. The AI Chatbot Twist

When the helpful 'assistant' isn't what it seems.

The newest wrinkle is the AI chatbot. Chat windows offering instant help are everywhere now, and many are legitimate tools that real companies use. But scammers also deploy fake chatbots — on bogus 'support' websites, in pop-ups, or through messaging — powered by AI that can hold a natural, reassuring, human-like conversation. The friendly 'agent' typing with you may be a scammer's bot, designed to build trust and then walk you into the same traps: your password, a code, remote access, or a payment.

There is also a subtler risk worth naming: people increasingly ask general AI assistants for help, including for things like a company's support number or how to fix an account problem. An AI can be genuinely useful, but it can also give a wrong or outdated number, or confidently state something incorrect, and scammers have even found ways to influence what some AI tools surface. So information from a chatbot or AI assistant, however confident and fluent, should be verified against the company's official source before you act on it, especially any phone number or link.

The rule that cuts through all of it is the same as before: do not trust a chat window or AI assistant that you did not reach through the company's own official channel, and never give any of them your password, codes, remote access, or payment. A real company's genuine chat support, reached through its official app or website, operates within the company's real safeguards. A chatbot you met through a pop-up, an ad, a fake site, or an unverified search result has no such safeguards, however human and helpful it seems to be.

GOOD TO KNOW

A fluent, friendly chatbot can be a scammer's bot — or a well-meaning AI giving a wrong number. Verify any support contact it offers against the company's official site before acting.

7. The One Rule for Getting Help

Always go to the company yourself.

Here is the whole defense in one sentence: when you need help, you go to the company yourself, through its official website, app, or a number from your own documents — and you never accept 'support' that came to you through a pop-up, ad, search result, chat window, or unsolicited call. That is it. You initiate the contact, through a channel you can trust to be genuinely the company's, and you ignore any 'help' that found you.

This works because it flips the direction of contact. Scammers need to reach you — through a pop-up, an ad, a planted number, an out-of-the-blue call — and their whole scheme depends on you accepting help that came to you. When you insist on initiating contact yourself, through the company's genuine channels, you cut off every one of those approaches. Real support is always reachable through the company's own official site, app, or the number on your card or statement, so you lose nothing by refusing the 'help' that found you.

In practice, build the instinct: a problem is never solved by calling a number from a pop-up, clicking 'help' in an ad, or trusting a chat you did not seek out. It is solved by closing all that, going to the source you trust — the company's real website you type yourself, its official app, the contact details on your actual paperwork — and reaching out from there. That one reflex, 'I go to them, they don't come to me,' protects you against the entire family of fake-support scams.

WATCH OUT

Make it a reflex: I go to the company, it doesn't come to me. Reach support through the official site, app, or your own statement — never a pop-up, ad, search number, or surprise call.

8. The Refund and Overpayment Trick

A common twist on fake support.

A frequent variation, often following a remote-access session, is the fake refund. The 'support agent' claims they owe you a refund — for an overcharge, a canceled service, a security issue — and offers to process it while connected to your computer. Then they stage a fake 'mistake': they pretend to accidentally refund far too much, showing a bank balance that appears to jump by thousands more than intended, and tearfully beg you to return the 'overpayment,' often in gift cards, or they will be fired or have to pay it themselves.

It is all an illusion. With remote access, scammers can make your on-screen bank balance appear to show money that is not really there — moving figures between your own accounts, or using fake web pages — so you believe you received an overpayment you did not. Feeling guilty and wanting to do right by the apologetic 'agent,' the victim sends real money or gift cards to cover a 'refund' that never actually happened. It preys on honesty and kindness, which makes it especially cruel.

The protection is to recognize the whole setup as a scam the moment it begins. No legitimate company gives refunds by remote-controlling your computer, and no honest refund process involves you repaying an 'accidental overpayment' in gift cards to help out a distressed agent. If anyone connected to your screen shows you an 'overpayment' and asks you to send some back, stop entirely, disconnect, and treat it as the scam it is. Your real bank balance is whatever your bank shows you when you log in independently, not what a remote 'agent' displays.

WATCH OUT

'I accidentally refunded you too much, please send the difference back in gift cards' is a classic scam. With remote access they fake the balance — the overpayment never happened.

9. Why It's So Effective

They catch you when you want help.

Fake-support scams are powerful for a specific reason: they catch you at the exact moment you are seeking help and are therefore most receptive to it. When your computer is misbehaving, your account seems locked, or a scary warning appears, you feel anxious and want the problem solved. A friendly, confident 'agent' who offers to fix it is a relief, and relief lowers your guard. The scammer is not fighting your suspicion; they are answering your plea, which is a much easier thing to do.

They also wear the authority of expertise. Many people feel uncertain about technology and defer to anyone who sounds knowledgeable about it. A calm 'agent' using technical terms, 'showing' you problems on your own screen, and speaking with confidence can easily lead someone who feels out of their depth. The scammer leverages that gap in confidence, positioning themselves as the expert you need and you as the layperson who should follow their lead.

Recognizing this removes the shame if you have been caught, and sharpens your guard going forward. Being fooled by fake support is not a sign of foolishness; it is the natural result of wanting help and trusting apparent expertise, both of which are reasonable. The fix is not to distrust all help, but to remember that genuine help is reached by going to the company yourself, and that the 'expert' who found you in your moment of need is exactly the one to doubt.

GOOD TO KNOW

These scams don't fight your suspicion — they answer your plea for help. Being caught isn't foolishness; it's wanting help and trusting apparent expertise. The fix is to go to the company yourself.

10. Finding Real Help Safely

How to actually get support you can trust.

Since the whole point is that you do sometimes need real help, let me be practical about how to get it safely. Knowing where to turn, in advance, means you are not scrambling and vulnerable when a problem hits. Here are the trustworthy ways to reach genuine support.

- Go to the company's official website by typing its known address yourself, and use the contact or support page there.
- Use the official app you installed from your phone's app store, which has the company's genuine support built in.
- Use the phone number on your actual card, statement, bill, or the product's packaging or manual.
- For your computer or phone itself, use the maker's official support site or, for Apple and others, their official stores and known support channels.
- For local, in-person help you can trust, turn to a known local technician — like me — rather than a voice that found you online.

The common thread is that you reach out through a channel whose authenticity you can trust, because you found it yourself from a reliable source, not because it was presented to you in your moment of need. Keep a short list of the real support numbers for the companies and services you rely on, from their official sources, so you have them ready. When a problem arises, that preparation turns a dangerous scramble into a calm, safe call to genuine help.

TIP

Keep a short list of real support numbers — from each company's official site or your statements — before you need them. Then a problem means a calm, safe call, not a risky scramble.

11. A Word About Local, Honest Help

Why a known local tech is different.

I want to say a word here about local, in-person help, because it is one of the safest and most reassuring ways to get technology problems solved — and, I will be honest, it is what I do. The difference between a known local technician and a voice that found you through a pop-up or an ad is everything: a local person is someone you can meet, whose business and reputation are rooted in your community, whom your neighbors know, and who will still be here next week. That accountability is a world apart from an anonymous online 'agent.'

A trustworthy local helper does not create fake emergencies, does not demand gift cards, does not need to frighten you into acting, and does not ask for your passwords or secretly take over your machine from afar. They explain what is actually wrong in plain language, let you watch and understand, charge fair and clear prices, and treat you with patience and respect. You can look them in the eye and ask questions, and they answer to you and to the community they serve.

So when you need real help and feel uncertain, consider reaching out to someone local and known rather than chasing support online, where the scammers lurk. For folks here in Portage County, that is exactly the role I try to fill — honest, patient, local help with no scare tactics and no surprises. Whether or not you call me, the principle holds: real help, especially in person, comes from known, accountable people, not from a voice or a chat that appeared on your screen uninvited.

GOOD TO KNOW

A known local tech is accountable to you and your community — no scare tactics, no gift cards, no secret screen access. That's a world apart from a voice that found you in a pop-up.

12. The Account 'Lockout' Version

'Your account is locked — contact support.'

A close cousin of the pop-up scam targets your online accounts. You receive an email, text, or on-screen message claiming your account — email, bank, a streaming service, a shopping site — has been locked, suspended, or compromised, and that you must contact support or verify your identity immediately to restore it. The message provides a helpful link or number, and a sense of urgency: act now or lose access, or your account will be deleted.

It is the same trick wearing an account-problem costume. The link leads to a fake login page that steals your password, or the number connects you to a fake support agent who 'helps' you by extracting your password, a verification code, or remote access. The lockout story is chosen because it is believable — accounts really do get locked sometimes — and because it creates urgency and fear of losing something you rely on. That believability is exactly what makes verifying essential.

The response is the familiar one: do not use the link or number in the message. If you are worried your account might really have an issue, go to that service the way you always do — its official app or a web address you type yourself — and check there. A genuine lockout will be apparent when you log in normally, and you can resolve it through the service's real support. The message that found you, with its convenient link and number, is the thing to ignore.

WATCH OUT

'Your account is locked, contact support here' with a link or number is a classic trap. Check by logging in the way you always do — never through the message's link or number.

13. Fake Apps and Download Traps

When the 'help' is a harmful program.

Some fake-support scams aim to get you to download and install software, which is its own danger. This might be framed as a 'support tool,' a 'security scanner,' a 'driver update,' or a program the 'agent' needs you to install so they can help. Once installed, the software may give the scammer remote access, steal your information, bombard you with more fake warnings, or hold your files for ransom. The download is the payload, dressed up as help.

Be especially wary of software offered by a pop-up, an ad, an unsolicited agent, or a search result rather than from an official source. Your computer and phone have official app stores and the device maker's official website; software from those sources is vetted, while a program an 'agent' urges you to download from a link is not. Scammers also create fake versions of real, well-known programs, so even a familiar name downloaded from the wrong place can be a trap.

The safe rule is to install software only from official sources you trust — your device's official app store, or the genuine website of the software maker that you navigated to yourself — and never because an unsolicited 'support agent' or a pop-up told you to. If you are unsure whether a program is legitimate or needed, that is a fine question for a trusted local technician before you install anything. When in doubt, do not download; an unneeded install is far easier to avoid than to undo.

WATCH OUT

Never install software because a pop-up or a surprise 'agent' told you to. Download only from your device's official app store or the maker's genuine site. The 'support tool' is often the trap.

14. The Social-Media 'Support' Reply

When you complain and a 'helper' slides in.

Here is a trap that catches people on social media. You post a complaint or a question to a company's page — 'my account won't work,' 'where's my order,' 'my payment failed' — and within minutes a reply or a private message arrives from what looks like the company's support, offering to help. It feels responsive and legitimate. But scammers monitor companies' public pages for exactly these complaints, then pounce with fake 'support' accounts that closely mimic the real one.

The fake support account, often with a near-identical name, logo, and a reassuring tone, then runs the usual playbook in private messages: asking for your account details, your password, a verification code, a payment, or directing you to a fake site or a remote-access tool. Because you reached out first, publicly, and help seemed to come promptly, the response feels trustworthy, even though the 'helper' is a scammer who simply saw your complaint.

So treat unsolicited 'support' replies and messages on social media with caution, even when you did post a complaint. Check that any account contacting you is the company's genuine, verified one, and better still, take the matter to the company's official support channel — its real website or app — rather than continuing in social-media messages with whoever replied. A real company's verified support will still be reachable through its official channels; a scammer watching the page will not.

WATCH OUT

Complain on a company's social page and a 'support' account may message you in minutes — often a scammer watching for complaints. Verify it's the real account, or take it to the official site instead.

15. A Steadying Word

Confident about getting help.

I do not want this guide to leave you afraid to seek help when you need it, because getting help with technology is normal, necessary, and nothing to dread. The goal is not to make you distrust all support, but to make you confident in reaching the real kind safely. With one simple reflex — I go to the company myself, through channels I trust — you can get all the help you need while sidestepping the scammers who lurk where help is sought.

Keep the danger in its proper, narrow place. The problem is not support itself, but 'support' that comes to you uninvited through a pop-up, an ad, a planted number, a surprise call, or an unsolicited message. Genuine help, reached through official channels or a known local technician, is safe and good. So you need not hesitate to solve your technology problems; you need only solve them by going to trustworthy sources, not by accepting the help that finds you in your moment of need.

And remember that honest help is close at hand. Whether it is a company's official support, reached the safe way, or a trusted local person you can look in the eye, you are not at the mercy of the scammers. For folks here in Portage County, I am glad to be that honest, patient, local help, with no scare tactics and no surprises. Reach out anytime a 'support' situation feels off, or before you act on one — a quick call can save you from a costly mistake, and that is exactly what I am here for.

GOOD TO KNOW

Getting help with technology is normal and fine — just reach the real kind. One reflex, 'I go to the company myself,' lets you get all the help you need while sidestepping the scammers.

16. If You Let Someone In

Steps if you gave remote access or info.

If you realize you let a fake support agent into your computer, or gave them information or money, act promptly and calmly — there is a clear set of steps, and taking them quickly limits the harm. There is no shame here; these scams are built to exploit the moment you most want help. The priority is to cut off the scammer's access, secure your accounts, and protect your money.

- 1 Disconnect the computer from the internet right away (turn off Wi-Fi or unplug it) to cut remote access.
- 2 From a different, trusted device, change the passwords on your important accounts — email and bank first — and turn on the second lock.
- 3 If you paid or shared card or bank details, call your bank or card company now, say it was a scam, and ask them to stop or reverse it; report gift cards to the card company fast.
- 4 Have the computer checked and cleaned by a trustworthy local technician, and the remote-access software removed, before using it for anything sensitive.
- 5 Write down what happened, watch your accounts closely, and report it (FTC, and FBI for larger losses).

WATCH OUT

Assume a scammer who had remote access saw your saved passwords. Change them from a clean device, and don't use the affected computer for banking until it's been checked.

17. Helping a Loved One Who's Anxious

Support that doesn't shame.

Fake-support scams hit hardest those who feel least confident with technology, so a loved one who is anxious about devices may be especially vulnerable — and may also be reluctant to admit a problem for fear of seeming incapable. If you are helping such a person, your patience and lack of judgment matter enormously. The goal is to be the safe, trusted helper they turn to instead of the scary pop-up or the voice online.

Teach the simple truths that defuse these scams: real companies never pop up a number to call, never ask for passwords, never take over your screen uninvited, and never want gift cards. Write these on a card by the computer. Most powerfully, make the open-door promise: 'If something goes wrong with your computer or an account, or a scary message pops up, just call me first — I'll help you, no judgment, and we'll find the real help together.' Being their first call short-circuits the whole scam.

Set them up for safety in advance: save the real support numbers and your own number where they can find them, and make sure they know that closing a pop-up or restarting the computer is safe and that the pop-up cannot really hurt the machine. Reassure them, often, that needing help with technology is completely normal and nothing to be embarrassed about, and that the honest helpers — you, a trusted local tech — are only a call away. Confidence that safe help exists is what keeps them from grabbing the dangerous kind.

TIP

Be your loved one's first call for tech trouble: 'Scary message? Call me first, no judgment.' Being the safe, known helper is what keeps them away from the scammer posing as one.

18. Questions People Ask Me

The ones that come up again and again.

A pop-up says my computer is infected and to call Microsoft — is it ever real? No, never. Microsoft, Apple, and other real companies do not put phone numbers in pop-up warnings or monitor your browsing to alert you. It is always a scam. Don't call; close the browser or restart, and the pop-up is gone.

But I called the number myself after searching — doesn't that make it safe? Not necessarily. Scammers plant fake support numbers in search results and ads, so even a number you 'looked up' can be fake. Get support contact info from the company's official website (typed yourself) or your own statement, not from a general search.

The agent was so knowledgeable and helpful — surely they were real? Scammers are trained to sound confident and helpful, and that is part of the trap, not proof of legitimacy. Judge support by behavior — did it contact you first, want your password or screen, demand gift cards? — not by how expert and friendly it seems.

Is it ever okay to let support control my screen? Only when you initiated the contact through the company's genuine official channel, understand exactly what's happening, and trust the source. Never for a problem a pop-up or surprise caller told you about. When in doubt, say no and get local, in-person help instead.

19. A Five-Minute Safety Setup

Be ready before something goes wrong.

A little preparation makes fake-support scams easy to sidestep, because you will know exactly where to turn when a problem hits instead of scrambling. Do these once and you are well protected, and far calmer the next time something goes wrong with a device or an account.

- 1 Make a short list of real support numbers — from each company's official site or your statements — and keep it by the computer.
- 2 Write the key rule on a card: 'Real support never pops up a number, never wants my password or screen, never wants gift cards.'
- 3 Know that closing the browser or restarting clears a scary pop-up — it can't really hurt your computer.
- 4 Decide, as a rule, that you reach companies yourself and never accept support that found you.
- 5 Pick a trusted local tech (and keep my number) for in-person help you can rely on.

GOOD TO KNOW

The strongest 'setting' is the reflex: I go to the company, it doesn't come to me. Plus knowing a scary pop-up is harmless and a real local helper is a call away.

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://www.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](https://www.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 a 'support agent' or chatbot offering to help with a tech or account problem 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.

Real help never reaches out to you first, never needs your passwords or your screen, and never wants gift cards. Reach companies through their own official channels, and call me whenever a 'support' offer feels off. I am a phone call away, and glad to be the honest help on your side.

CHEAT SHEET

Everyday Cheat Sheet

The one rule

Go to the company yourself for help — official site, app, or the number on your statement. Never accept 'support' that found you via pop-up, ad, search result, chat, or surprise call.

Always a scam

- A pop-up with a number saying 'call support now.'
- Support that contacted you first about a problem.
- Anyone asking for your password or a code.
- 'Let me take control of your screen' for a surprise issue.
- Payment or a 'refund repayment' in gift cards.

Get real help safely

- 1 Close the pop-up or restart — it can't hurt your PC.

- 2 Type the company's official web address yourself.
- 3 Use the number on your card, bill, or official app.
- 4 Never let a surprise 'agent' into your screen.
- 5 For in-person help, use a known local tech — call Bill.

WATCH OUT

'I accidentally refunded you too much — send the difference in gift cards' is a scam; the overpayment is faked with screen access. And real support never pops up a number to call.

AT A GLANCE

A Picture to Follow Along

The Faces of Fake Support

They wait where you go looking for help.



Real help never finds you - you go to the company yourself.

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

AT A GLANCE

A Second Look

How to Get Help Safely

Flip the direction: you reach them, not the reverse.

- 1 A problem or scary message appears
- 2 Don't call a pop-up, ad, or search-result number
- 3 Don't give a password, code, or screen access
- 4 Close the pop-up or restart - it can't hurt your PC
- 5 Go to the company's official site, app, or your statement
- 6 Or call a known local tech for in-person help

Real support never contacts you first or wants gift cards.

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.