



AI-Written Scam Emails — Why Bad Grammar Is No Longer the Tell

Why phishing looks polished now — and the habits that still keep you safe.

————— **An Extended Guide · No. 1622 · 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. What Phishing Actually Is 5
- 3. How AI Changed the Game 6
- 4. The Habit That Still Works 7
- 5. Judge the Ask, Not the Appearance 7
- 6. The Most Common Disguises 8
- 7. The Links Are the Danger 9
- 8. Passwords, Codes, and Why They Matter 10
- 9. Turning On a Second Lock 10
- 10. Attachments You Didn't Expect 11
- 11. The Phone Call That Follows 12
- 12. If You Already Clicked 13
- 13. Reporting It — and Why It Helps 13
- 14. The Same Trick by Text Message 14
- 15. QR Codes Hidden in Messages 15
- 16. A Word on Business Email Scams 15
- 17. The Old Tells — Still Worth a Glance 16
- 18. Questions People Ask Me 17
- 19. Guarding Your Email Account Itself 18
- 20. Making It a Shared Family Rule 19

21. A Five-Minute Email Safety Setup 19

22. When to Just Call Me 20

23. 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

The old advice — 'scam emails are full of spelling mistakes' — no longer protects you. Scammers now use AI to write polished, convincing messages with correct grammar, real logos, and details about you. So we stop judging how an email looks and judge what it asks. If a message wants you to click a link, log in, pay, or share a code because something is urgent, you stop and verify through a channel you already trust — never through the email itself.

- 1 An email creates urgency: a problem, a package, a payment, a locked account.
- 2 Do not click links or call numbers inside the email.
- 3 Do not judge it by spelling — AI writes these cleanly now.
- 4 Go to the company yourself: a saved bookmark, the app, or a number off your card.
- 5 Confirm there before you do anything the email asked.

WATCH OUT

Perfect grammar is now a neutral sign, not a reassuring one. The real question is never 'does this read well?' It is 'is this email trying to rush me into clicking, paying, or logging in?'

1. Why I Wrote This One

The advice you memorized has quietly stopped working.

For most of my thirty-plus years helping folks in Portage County with their computers, I gave the same reliable advice about scam emails: look for the bad spelling, the broken grammar, the odd phrasing, and you will spot most of them. It was good advice for a long time. I am writing this guide because it has quietly stopped being true, and I do not want anyone relying on a rule that no longer protects them.

The reason is a new tool. Scammers now use artificial intelligence — the same kind of writing technology behind the helpful assistants you may have heard about — to write their emails for them. In seconds, a criminal who barely speaks English can produce a message in flawless, friendly, professional language, correctly spelled, perfectly punctuated, and even matched to your region or your bank. The clumsy tells we trained ourselves to catch are simply gone.

Here is the reassuring part, and I mean it. You do not need new technical skills to stay safe, and you do not need to examine every email like a detective. You need to shift your

attention from how a message looks to what it asks you to do, and to build one simple habit around that. We will go through why the emails changed, the habits that still work, the common disguises, and exactly what to do if you have already clicked. No fear, no jargon, no rush.

WATCH OUT

If you have grandchildren who tell you 'you can always spot a scam by the typos,' gently update them. That advice is now out of date, and they can get caught by it too.

2. What Phishing Actually Is

The plain-English name for the trick.

Phishing is simply a scam message designed to trick you into handing over something valuable — a password, a card number, a verification code, or money — usually by pretending to be a company or person you trust. The name is a play on 'fishing,' because the scammer casts out bait and waits for someone to bite. It arrives most often by email, but the same trick comes by text message and through social media too.

The bait is almost always a believable story plus a link or a request. You get an email that looks like it is from your bank, a delivery company, a streaming service, or a government office. It tells you there is a problem — a suspicious charge, a package stuck in customs, an account about to close — and it asks you to click a link, log in, confirm details, or make a quick payment to fix it. The link leads to a fake page built to capture whatever you type.

For years, the weak point in these scams was the writing. The criminals were often overseas and their English gave them away. Artificial intelligence closed that gap. Now the story is as polished as the design, which is why we have to defend ourselves at the level of what the message wants, not how well it is written. Understanding what phishing is for — getting you to act on the message itself — is what makes the safe habit obvious.

GOOD TO KNOW

Phishing by text is sometimes called 'smishing,' and by phone call 'vishing.' Different doors, same trick: a believable story that rushes you into clicking, paying, or sharing a code.

3. How AI Changed the Game

Polished, personalized, and produced in bulk.

It is worth understanding what the new tools actually do, because it explains why the old signs vanished. Artificial-intelligence writing tools can produce fluent, natural text on any topic in seconds. A scammer types a rough request — 'write a worried email from a bank about a suspicious charge, friendly and urgent' — and out comes a clean, convincing message. They can generate hundreds of variations, in any tone, aimed at any audience, without a single telltale error.

Worse, the messages can be personalized. Scammers buy or scrape lists that include your name, your town, sometimes which bank or service you use, pulled from past data breaches and public sources. Feed those details to the writing tool and the email greets you by name, mentions your area, and references the right company. A message that knows a few true things about you feels trustworthy, even though those details prove nothing — they were simply bought.

The same technology also builds the fake websites behind the links, clones company logos, and even powers chat 'support agents' and cloned voices for the phone follow-up. The whole production has leveled up. That sounds alarming, but it changes only one thing for you: you can no longer use quality as a filter. Everything else about staying safe — verify independently, never act on the message itself — works exactly as well as it always did, and we will lean on it hard.

WATCH OUT

A message that knows your name, town, or bank is not proof it is real. That information is cheaply bought and sold. Treat personal details as decoration on the bait, not as a badge of authenticity.

4. The Habit That Still Works

Verify independently — never through the message.

Here is the whole defense in one sentence: when a message asks you to do something, you never do it through the message — you go to the company yourself, through a channel you already trust, and confirm there. That is it. It does not matter how clean the writing is, how real the logo looks, or how urgent the story feels. The link, the phone number, the button in the email — none of those are the way you respond. You set the email aside and reach the company independently.

This works because it does not depend on your judging the email at all. The scammers pour all their new AI skill into making the message convincing. They cannot control the bookmark you saved, the app already on your phone, or the phone number printed on the back of your actual card. When you reach your bank through one of those, you step completely outside the scammer's reach. A real problem will be waiting for you there; a fake one simply will not exist.

So build the reflex. Message says there is a problem with your bank? Close it, and open your banking app or type your bank's address yourself, or call the number on your card. Message about a package? Go to the delivery company's real site or app and check your tracking. Message from a service about your account? Log in the way you always do, not through their link. Every time, the question is simply: how would I reach this company if the email did not exist? Then do that.

TIP

Keep a short list of bookmarks for the sites you use most — your bank, your email, your main shopping site. Reaching them by bookmark instead of by link kills most phishing on contact.

5. Judge the Ask, Not the Appearance

Train your attention on what the message wants.

Since you can no longer rely on spotting a fake by its look, point your attention at the request instead. Nearly every phishing message, however polished, asks for one of a small handful of things. When you see any of these, treat it as a reason to stop and verify independently, regardless of how professional the message appears.

- Click a link to 'verify,' 'confirm,' 'unlock,' 'reactivate,' or 'avoid closure' of an account.
- Log in to fix a problem — the link leads to a fake copy of a real login page.
- Pay, or update your payment details, often with urgency or a threat.
- Share a code, password, PIN, or card number by reply, form, or phone.
- Open an attachment you were not expecting — an 'invoice,' 'receipt,' or 'statement.'

Add urgency to any of these and the alarm should grow louder, not softer. Scams manufacture urgency — 'act within 24 hours,' 'your account will be closed,' 'final notice' — precisely to stop you from pausing to verify. A real company is rarely in such a frantic hurry, and will not punish you for taking a moment to check through official channels. The pressure to rush is itself one of the most reliable signs of a scam.

GOOD TO KNOW

Legitimate companies do send real emails about real problems. The difference is that a real one holds up when you verify independently — and never depends on you clicking the link inside it.

6. The Most Common Disguises

The costumes these emails wear most often.

Phishing emails impersonate whatever you are most likely to trust and act on quickly. Knowing the popular disguises helps you recognize the pattern even when the writing is flawless. None of these is a reason to panic — each is simply a reason to close the email and check with the real company yourself.

- Your bank or card company: a 'suspicious charge,' 'locked account,' or 'verify your identity' alert.
- A delivery company: a package 'held,' a small 'redelivery fee,' or an address to confirm.
- A streaming or shopping service: 'payment failed,' 'update your card,' 'your subscription will end.'
- A tech company: 'unusual sign-in,' 'your storage is full,' 'confirm your account.'
- A government agency: taxes, benefits, Medicare, or Social Security 'issues' needing urgent action.
- An email or password 'security alert' urging you to log in right away.

Notice the pattern beneath the costumes: a trusted name, a problem, and a push to act now through the message. Once you see that shape, the specific disguise matters less. Whether it claims to be your bank or a delivery driver, the safe response is identical — do not act through the email, go to the real company yourself, and confirm. The costume is

just there to make you move fast.

WATCH OUT

Delivery-fee and 'confirm your address' texts and emails are everywhere. Real carriers rarely ask for a payment by text or email link. Check your tracking on the carrier's own app or site instead.

7. The Links Are the Danger

Why a single click can matter.

The heart of most phishing is the link, so it is worth understanding what a bad one does. A phishing link usually leads to a fake copy of a real login page — your bank, your email, a shopping site. It looks right down to the logo and colors. If you type your username and password into it, you have handed those straight to the scammer, who can then log into the real account. Some links instead try to install harmful software on your device simply by being opened.

The web address is sometimes a clue, but a fading one. Scammers register addresses that are near-copies of real ones — an extra word, a slightly different ending, a tiny misspelling. On a phone, the full address is often hidden, and AI helps criminals pick convincing names. You can sometimes catch a fake by looking carefully at the address, but like spelling, this is now a bonus check, not a reliable test. The safer rule is simply not to reach important sites through emailed links at all.

This is why 'go to the company yourself' is so powerful. If you never log in through a link that arrived in a message, a stolen password page has nothing to steal from you. You can look at a suspicious email, even read it with interest, and remain perfectly safe as long as you do not click through and type anything. The click, and what you type after it, is where the harm lives — so that is the step you simply skip.

WATCH OUT

On a computer, you can rest your mouse over a link (without clicking) to preview where it really goes. If the preview does not clearly match the real company, do not click — but when in doubt, just use your own bookmark instead.

8. Passwords, Codes, and Why They Matter

The crown jewels these emails are after.

A great deal of phishing exists to steal two specific things: your passwords and your one-time security codes. Your password opens an account; the six-digit code that a bank or service texts you is the second lock many accounts now use. Scammers know both, and a clever phishing message will try to collect them together, so the criminal can walk straight into your account past both locks.

The rule here is simple and absolute. No legitimate company will ever ask you to give them a verification code — the number they just texted you — by email, by reply, or over the phone. That code is for you to type into the real app or site, never to read aloud or send to anyone, not even someone claiming to be 'security' helping you. If anyone asks for that code, the request itself proves they are a scammer, no matter how official they sound.

The same goes for passwords and full card numbers. Real companies do not email you asking to confirm your password, and your bank already knows your card number. Any message or caller collecting these is fishing, not helping. If you treat your passwords and codes as things you type only into places you reached yourself — and never hand to anyone who contacted you — you close the single biggest door these scams try to walk through.

WATCH OUT

'Read me the code we just sent to confirm it's really you' is always a scam. The code is a lock meant to keep others out of your account — handing it over unlocks the door for them.

9. Turning On a Second Lock

The protection that survives a stolen password.

Because phishing is so good at stealing passwords, it helps enormously to have a second lock on your important accounts — a step beyond the password, often called two-step or two-factor verification. With it turned on, even a scammer who steals your password cannot get in without also having the one-time code, which is sent to your phone. It is one of the single best protections available, and most banks, email providers, and major services offer it for free.

The catch, and the reason the last chapter matters so much, is that phishing then shifts to trying to trick that code out of you. So the two habits work as a pair: turn on the second lock to protect against a stolen password, and never, ever give the code to anyone who contacts you. Together they make your accounts very hard to break into, even if a password leaks in some data breach you never hear about.

If setting up the second lock sounds fiddly, it is honestly a fifteen-minute job on each account, and it is exactly the kind of thing I am glad to help with. Email and banking are the two I would start with, because they are the keys to so much else. Once they are protected, a stolen password alone becomes far less dangerous, and you can breathe a little easier about the breaches that happen to everyone these days.

GOOD TO KNOW

Turning on a second lock for your email first is wise — your email is the master key that can reset passwords everywhere else. Protect it, and you protect the whole chain.

10. Attachments You Didn't Expect

The quiet danger of 'just open this file.'

Not all phishing is about links and logins. Some messages carry an attachment — an 'invoice,' a 'receipt,' a 'statement,' a 'delivery label,' a 'resume' — and the whole goal is to get you to open it. Opening the wrong attachment can install harmful software that steals your passwords, locks up your files for ransom, or quietly watches what you type. The message will give you a plausible reason it matters and a nudge of urgency to open it now.

The safe habit mirrors the others: do not open attachments you were not expecting, especially from senders you do not know or that arrive with a pushy story. If an email claims to be an invoice from a company you do business with, do not open the file to check — instead, contact that company through a number or site you already have and ask whether it is real. An unexpected attachment is one of the few things worth being quite strict about, because a single click can do real harm.

Be especially wary of attachments that ask you to 'enable content,' 'enable editing,' or turn off a safety warning to view them. Those prompts are often exactly how the harmful part gets permission to run. A real document rarely needs you to override your computer's warnings. If a file is fighting your device's safety features to open, let the device win and

delete the message.

WATCH OUT

An unexpected file plus 'enable content to view' is a classic trap. Legitimate documents do not need you to switch off your computer's protections to be read.

11. The Phone Call That Follows

Phishing often has a spoken sequel.

Modern scams rarely stay in one channel. A phishing email may be followed by a phone call, or a 'please call this number' message, with the same AI tools now cloning voices and staffing fake support lines. The call reinforces the email's story: 'We emailed you about suspicious activity; I'm calling to help you secure your account.' The combination of a written message and a live, friendly voice is powerful, and it is designed to walk you straight past your defenses.

The same rule covers the call. You do not trust a phone number that came from the email, and you do not trust a caller just because they reference the email you received — they sent it. If you are worried there might be a real problem, you hang up and call the company back on a number you already have, from your card, your statement, or the company's official site. The spoken sequel changes nothing about the safe habit: verify independently, on a channel you chose.

Be especially alert if a caller wants to 'help' by having you install software, share your screen, or read back a code. Those are the same crown jewels the email was after, now requested out loud by a warm, patient voice. No legitimate company support call needs remote control of your computer or your one-time codes to fix an account problem. If that is asked, it confirms a scam, and the right move is to hang up and verify independently.

WATCH OUT

Email plus a follow-up call referencing that email is a one-two punch. The caller knowing about the email is not proof they are real — they are the ones who sent it.

12. If You Already Clicked

Calm, quick steps to limit the damage.

If you clicked a link and realized afterward, or typed something into a page you now doubt, take a breath — you can still limit the harm, and acting promptly helps a lot. Clicking a link alone is usually less dangerous than what you did next, so the steps depend on how far it went. Either way, there is no shame here; these are built to catch careful people, and you caught yourself, which is exactly right.

- 1 If you entered a password, change it right away on the real site — and anywhere else you used the same one.
- 2 Turn on the second lock (two-step verification) on that account if it is not already on.
- 3 If you entered card or bank details, call your bank or card company now and tell them it was a scam.
- 4 If you opened an attachment or installed something, disconnect from the internet and get the device checked.
- 5 Watch your accounts and statements closely for the next while, and report the phishing (see the next chapter).

GOOD TO KNOW

Changing a reused password everywhere matters: scammers try a stolen password on your other accounts. If email, bank, and shopping all shared one password, change them all.

13. Reporting It — and Why It Helps

A few minutes that protect other people.

Reporting a phishing message helps shut down the fake sites and warns others, and it is quick. You do not need to have lost anything to report; flagging the attempt is valuable. Most email programs have a 'report phishing' or 'report junk' button, which both removes the message and teaches your email to catch similar ones. Beyond that, a couple of official reports put the scam on the radar of the people who fight it.

- Use your email's 'report phishing' or 'report spam' button on the message itself.
- Forward suspicious emails to the Anti-Phishing Working Group at reportphishing@apwg.org, and scam texts to 7726 (SPAM).
- Report the scam to the Federal Trade Commission at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud).
- For losses or serious cases, report to the FBI at [ic3.gov](https://www.ic3.gov) and the Ohio Attorney General at 800-282-0515.

I have a separate, step-by-step guide on reporting scams to the FTC, the FBI, and the Ohio Attorney General, with exactly what to include. If any of this feels like a chore or a puzzle, that is a perfect thing to call me about — I am glad to sit down and help you report it properly, and to make sure your accounts are locked up tight afterward.

14. The Same Trick by Text Message

Smishing: phishing that buzzes in your pocket.

Phishing is not only an email problem. The exact same con arrives by text message, where it is sometimes called smishing, and texts can be even more effective because they feel personal and urgent and the full web address is usually hidden on a small screen. You get a short message about a package, a toll, a bank alert, or a 'suspicious login,' with a link to tap. AI writes these cleanly too, so the old 'it reads foreign' tell is gone from texts as well.

The habit transfers without a single change. A text asking you to tap a link, pay a small fee, or confirm details gets the same treatment as an email: you do not tap, and you reach the company yourself through its app, your bookmark, or the number on your card. If a text says your package needs a redelivery fee, open the carrier's own app and check your tracking there. If it claims to be your bank, open your banking app. The text is just another door with the same lock on your side.

A few text-specific notes help. You can report scam texts by forwarding them to 7726, which spells SPAM on the keypad, and your phone carrier uses those reports to block numbers. Do not reply 'STOP' to a scam text — with a real company that unsubscribes you, but with a scammer it simply confirms your number is live and worth targeting more. Just delete it, and report it if you like. Never tap a link in a text you did not expect, however ordinary the story sounds.

WATCH OUT

'Your package is held, pay a small redelivery fee' and 'you have an unpaid toll' are two of the most common scam texts right now. Carriers and toll agencies do not collect fees by surprise text link.

15. QR Codes Hidden in Messages

A newer twist that skips the suspicious link.

A newer wrinkle worth knowing is the scam QR code — those square, boxy patterns you scan with your phone's camera. Scammers now put them in emails, letters, and even printed flyers, because a QR code hides its destination completely. You cannot read a web address in a pattern of squares, so the usual advice to check a link before clicking does not help. You point your camera, it opens a website, and you may have no idea where you have landed.

These show up in emails claiming to be from a bank or service ('scan to verify your account'), on fake parking or toll notices, and on stickers placed over real codes on parking meters and menus. The destination is a fake login or payment page, exactly like a phishing link, just delivered through your camera instead of a tap. Because the address is invisible until you have already arrived, a scam QR code can be even sneakier than a scam link.

The rule, happily, is the same one: do not use a QR code from a message, email, or unexpected notice to reach anything involving your account or your money. If your bank or a service seems to want you to scan a code, reach them your usual way instead — your app or bookmark — and sort it out there. A QR code is just another emailed link in disguise, and it earns exactly the same 'go to the company myself' response.

GOOD TO KNOW

I have a separate guide just on QR-code scams, covering the stickers on parking meters and menus. Ask me for it if you scan codes out and about.

16. A Word on Business Email Scams

If you run a shop or help with one, read this.

If you own a small business, help with the books, or handle money for a church or club, there is a version of this aimed squarely at you, and AI has made it sharper. A scammer impersonates a boss, a vendor, or a familiar contact and emails a believable request: pay this invoice, update our bank details for the next payment, buy some gift cards for a client, wire this urgently. The writing is polished, the tone matches the real person, and the timing often lands when you are busy.

The defense is the same habit in work clothes. Any request to send money, change payment details, or buy gift cards gets verified through a known, separate channel before you act — you call the boss or vendor on their real number, not the one in the email, and confirm out loud. A real colleague will never mind the check. Scammers rely on the awkwardness of double-checking a 'boss,' so make it normal policy that nobody is offended by a confirmation call.

Pay special attention to any email about changed bank details for a vendor you pay regularly. 'Our account has changed, please use these new details' is a classic and costly scam. The rule is ironclad: never change payment details based on an email alone. Confirm the change by calling the vendor on a number you already had on file, every single time, no exceptions. That one habit prevents the most expensive version of this scam.

WATCH OUT

'Our bank details have changed — please update them' is a red flag whenever it arrives by email. Always confirm a payment-detail change by phone, using a number you already had, before paying a cent.

17. The Old Tells — Still Worth a Glance

Clues that sometimes catch a lazier fake.

While I never want you leaning on them, some old-fashioned clues do still catch the weaker, lazier phishing attempts, and noticing one can confirm your instincts. Just remember that a sharp, AI-written scam will show none of these, so a clean-looking email proves nothing. Use them as a small bonus, never as your test.

- A sender address that does not match the real company, especially after the @ sign.
- A greeting that is oddly generic ('Dear Customer') or oddly specific in a way that feels bought.
- A link preview or web address that is a near-copy of the real one, with extra words or odd endings.
- Pressure and threats: 'act now,' 'final notice,' 'account will be closed today.'
- A request for a payment method that is hard to reverse — gift cards, wire, or cryptocurrency.

If one of these jumps out, trust it and delete the message. But if an email looks flawless, treat it with the very same caution, because flawless is now easy to produce. The safe habit — verify independently, never act through the message — does not care whether the

fake was sloppy or perfect, and that is exactly why it keeps working while the old spelling test fails.

GOOD TO KNOW

The sender's address and the real link destination are harder to fake than the words, so they remain modestly useful clues — but your bookmark is still safer than any amount of squinting at an address.

18. Questions People Ask Me

The ones that come up again and again.

The email had my correct name and knew which bank I use — isn't that proof it's real? No. That information is routinely bought, leaked in data breaches, and scraped from public sources, then fed into the writing tool. A few true details are decoration on the bait, not proof of honesty. Verify through the bank itself regardless.

Is it dangerous just to open an email? Opening a plain email to read it is almost always safe. The danger comes from clicking links, opening attachments, and typing information into pages the email sends you to. You can read a suspicious email with interest and stay perfectly safe, as long as you do not act on it.

How can I tell a real bank email from a fake one now? Honestly, you often cannot tell by looking, and that is the whole point of this guide. So do not try to judge by appearance. Go to your bank yourself — app, bookmark, or the number on your card — and check. If the problem is real, it will be there too.

What if I'm not sure and don't want to bother anyone? Then call me. There is never a charge to ask whether an email is a scam, and I would much rather spend two minutes reassuring you than have you click something you shouldn't. 'I wasn't sure' is exactly the right time to ask.

19. Guarding Your Email Account Itself

Your inbox is the master key — protect it first.

It is worth pausing on why your email account matters more than almost any other. Your inbox is the master key to your digital life. If a scammer gets into your email, they can click 'forgot password' on your bank, your shopping sites, and your social media, receive the reset links right there in your inbox, and quietly take over account after account. That is why so much phishing is aimed at your email password specifically, and why protecting the inbox is the single most valuable thing you can do.

Protect it with the same two habits, applied with extra care. Turn on the second lock — two-step verification — for your email before anything else, so a stolen password alone cannot open it. And be especially suspicious of any message claiming to be from your email provider about 'unusual activity' or 'storage full, verify now.' Those are favorite disguises precisely because they lead you to type your email password into a fake page, handing over the master key.

Check now and then for signs someone has been inside: unfamiliar sent messages, rules that forward or delete your mail, or security alerts you did not expect. If you ever suspect your email has been compromised, change its password immediately from a device you trust, turn on the second lock, and review its security settings. If that feels daunting, it is exactly the kind of thing to call me about — securing an email account is quick with a hand, and it protects everything downstream.

TIP

If you do only one thing after reading this guide, put the second lock on your email. It is the key that can unlock everything else, so it deserves the strongest protection you have.

20. Making It a Shared Family Rule

A habit spreads best when the whole house holds it.

These habits are easiest to keep when they belong to the whole household rather than to one careful person. Phishing reaches everyone — spouses, grandchildren, the person who handles the bills — and a single click by any one of them can cause trouble. When the family agrees on the same simple rule, there is no weak link, and no one feels singled out as the one who 'needs watching.' It becomes just how your family does things, like locking the back door.

Have a short, friendly conversation and agree on the essentials together: nobody clicks links or opens surprise attachments from messages; everybody reaches companies through their own apps and bookmarks; no one ever shares a verification code with anyone; and anyone can forward a questionable message to the family, or to me, for a quick sanity check with zero embarrassment. Framing it as a shared rule, not a warning to the 'vulnerable' member, is what makes it stick.

Update the younger members too, kindly. Many still believe scams are easy to spot by their typos, and that outdated confidence can get them caught. Let them teach you the newest apps while you teach them that polished no longer means safe. A family that talks openly about the strange messages it receives, without judgment, is remarkably hard to scam, because the first person to notice something odd simply says so, and everyone benefits.

GOOD TO KNOW

The strongest anti-phishing tool in any home is a family that feels free to ask 'does this look right to you?' without fear of being teased for asking.

21. A Five-Minute Email Safety Setup

Small settings that do a lot of quiet work.

A little setup now makes your inbox safer every day without any ongoing effort. None of this is complicated, and most of it is a one-time job you can do yourself or with a hand. Think of it as locking the doors and windows once, so you are not checking every latch each night.

- 1 Turn on the second lock (two-step verification) for your email and your bank, starting with email.

- 2 Save bookmarks for the handful of sites you use most, so you never reach them by emailed link.
- 3 Learn where your email's 'report phishing' or 'report junk' button is, and use it.
- 4 Make sure your devices install their updates, which quietly patch the holes bad attachments use.
- 5 Pick strong, separate passwords for your most important accounts — a password manager makes this easy.

TIP

If this list feels like a lot, do just the first two. The second lock on your email, plus bookmarks for your bank, together block the great majority of what phishing is trying to do.

22. When to Just Call Me

A two-minute check beats a day of worry.

If an email has you second-guessing yourself — you are not sure if it is real, you half-clicked something, or you just want a calm second opinion before you do anything — please call me. There is never a charge to ask, and never any judgment. Forwarding me a suspicious email, or reading it to me over the phone, takes two minutes and can save you a great deal of worry or worse. That is genuinely what I am here for.

If you would like a hand in person, I come to homes across Portage County. I can set up the second lock on your email and bank, clean up and organize your bookmarks, check a device after a worrying click, and show you the simple habits until they feel like second nature. We will go at your pace, with no pressure and no rushing, and you will come away feeling steadier about your inbox.

GOOD TO KNOW

The best time to call is before you click or reply. A quick 'does this look right to you, Bill?' is one of my favorite kinds of call to get.

23. Contact Card & a Warm Close

Keep this page by the computer even if you file the rest away.

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: 'is this email a scam?' 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.

Here is the one line to carry away: stop judging scam emails by how they look, because AI writes them perfectly now, and start judging what they ask. Whenever a message wants you to click, log in, pay, or share a code, set it aside and reach the company yourself, the way you always would. Do that, and the finest fake in the world has nowhere to send you. And if you are ever unsure, I am a phone call away and glad to take a look.

CHEAT SHEET

Everyday Cheat Sheet

The one rule

Never act through a message. Go to the company yourself — a saved bookmark, the app, or the number on your card — and confirm there.

What the email is really after

- A click to 'verify,' 'unlock,' or 'reactivate.'
- Your password typed into a fake login page.
- A one-time code — never give it to anyone.
- A payment or updated card details.
- An unexpected attachment you're urged to open.

Habits that still work

- 1 Judge the ask, not the spelling.
- 2 Reach the company by bookmark, app, or card number.
- 3 Turn on a second lock for email and bank.
- 4 Never share a verification code with anyone.
- 5 Unsure? Forward it to Bill before you click.

WATCH OUT

Perfect grammar is now meaningless. 'Our bank details changed — update them' and 'read me the code' are both scams, however polished the message looks.

AT A GLANCE

A Picture to Follow Along

Why the Old Test Fails

AI removed the clumsy clues we used to rely on.



You can't judge it by looks - judge what it asks you to do.

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

AT A GLANCE

A Second Look

The Habit That Still Works

Never act through the message - verify on your own channel.

- 1 An email creates a problem and urgency
- 2 Don't click the link or call its number
- 3 Ask: how would I reach this company anyway?
- 4 Use your bookmark, app, or the card's number
- 5 Confirm there before you act
- 6 Never share a password or one-time code

A real problem waits for you there; a fake one won't exist.

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.