BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2318

Updated November 2026

How to Spot an AI-Written Scam Email (It's Harder Now)

Bad grammar used to give scams away. Here's what to watch instead in 2026.

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

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech
(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

The 60-Second Version 3

The Short Version 3

Why the Old Advice Stopped Working 4

Judge the Request, Not the Writing 4

The Feelings That Should Make You Pause 5

Check Who It's Really From 6

Check Where a Link Really Goes 6

Attachments: When Not to Open 7

The New Trick: 'Reply' and 'Call Us' Scams 8

Turn On Your Email's Own Defenses 8

A Three-Question Gut Check 9

If You Clicked or Replied 10

Scams That Impersonate People You Know 10

Teach the Household the New Rules 11

When to Call Bill 11

Everyday Cheat Sheet 13

A Note From Bill 14

Your Visit — and My Promise 15

SUMMARY

The 60-Second Version

Scammers now use AI to write clean, polished emails, so good grammar no longer means an email is safe. Stop judging how a message is written and start judging what it asks you to do: click a link, open an attachment, send money, share a password, or call a number. Any of those, plus a sense of urgency, is the real warning sign.

Check a link's true destination by hovering on a computer or pressing and holding on a phone — or better, skip the email's link entirely and go to the company yourself. If you clicked or shared a password, change it right away, turn on two-step verification, and call your bank if money details were involved.

- Good grammar is no longer proof an email is safe.
- Judge the request and the rush, not the writing.
- Never use the email's own link or phone number — reach the company yourself.

1 The Short Version

For years we were told to spot scam emails by their bad spelling and clumsy grammar. That advice is now out of date. Scammers use AI writing tools to produce clean, polished, friendly emails in perfect English — so a well-written message is no longer a sign of safety. The reassuring part: the things that actually give a scam away were never really about grammar. They are about what the email wants you to do.

This guide retools your instincts for 2026. Instead of judging how an email is written, you'll judge what it asks for, how it pressures you, and where its links really go. Master a few of these, and a beautifully written scam is just as easy to catch as a clumsy one used to be.

- Good grammar no longer means an email is safe — AI writes scams cleanly now.
- Judge the request, not the writing: urgency, money, passwords, and links are the tells.

- Never click links or open attachments in an unexpected email — go to the company yourself.
- When in doubt, contact the company using a number or address you already have.

> **TIP**
> Here's the mindset shift in one line: stop asking 'is this well written?' and start asking 'what does this want me to do, and why the rush?' The second question catches scams the first one now misses.

2 Why the Old Advice Stopped Working

Scammers once wrote in broken English because many of them did not speak it well. The typos were an accident, not a strategy, and spotting them was a handy shortcut for the rest of us. Now AI writing assistants let anyone produce flawless, natural-sounding messages in any language, instantly.

So the typo shortcut is gone. Worse, a polished email can feel more trustworthy, which is exactly the problem. You have to retrain your eye away from the writing and toward the intent. The content of the trap hasn't changed — only the quality of the wrapping paper.

> **GOOD TO KNOW**
> Some scam emails are still sloppy, and sloppiness is still a red flag. But clean writing is no longer a green light. Treat good grammar as neutral — neither safe nor suspicious on its own.

3 Judge the Request, Not the Writing

Almost every scam email, however polished, is trying to get you to do one of a small handful of things. Learn this short list and you've learned the heart of it.

- Click a link and 'log in' or 'verify your account' — the link goes to a fake copy of a real site.
- Open an attachment — an 'invoice,' 'receipt,' or 'delivery label' that carries a virus.
- Send money, gift cards, or crypto — for a bill, a fine, a prize, or a stranded friend.
- Give up personal details — passwords, card numbers, your Social Security number, codes.
- Call a phone number in the email — leading to a fake 'support' line that talks you out of money.

> *The writing can be perfect. The request is where the scam lives. Change what you watch, and the quality of the prose stops fooling you.*

4 The Feelings That Should Make You Pause

AI can polish the words, but the emotional buttons it pushes are the same old ones. When an email makes you feel any of these, slow down — that feeling is the point.

- Urgency: 'your account will be closed in 24 hours,' 'act immediately.'
- Fear: 'suspicious activity detected,' 'you owe back taxes,' 'your package is held.'
- Greed or hope: 'you've won,' 'you're owed a refund,' 'claim your reward.'
- Authority: a message that looks like it's from your bank, the IRS, Amazon, or Medicare.

WATCH OUT

The IRS, Social Security, Medicare, and your bank do not demand immediate payment or passwords by email, and they never ask for gift cards. An email that claims otherwise is a scam no matter how official it looks.

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 Check Who It's Really From

A scam email can show a friendly, familiar name, but the actual email address behind it often tells a different story. It takes a moment to look, and it is one of the most reliable checks there is.

1. Look at the sender's full email address, not just the display name. On a phone, tap the sender name to expand it.
2. Be suspicious of addresses that use a slightly-off domain, like 'amazon-support.net' instead of 'amazon.com.'
3. Remember that even a correct-looking address can be faked, so a right-looking sender is not full proof.
4. If the address is hidden or odd, treat the whole message as suspect.

GOOD TO KNOW

Because a sender address can be spoofed, treat a suspicious address as a clear red flag but a normal-looking one as only mild reassurance. The link and the request still matter more than the sender line.

6 Check Where a Link Really Goes

The single most useful habit is to see a link's true destination before you ever click. Scam links hide behind friendly words like 'Verify now' or a shortened address.

1. On a computer, rest your mouse pointer over the link without clicking; the real web address appears at the bottom of the screen or in a small box.

2. On a phone or tablet, press and HOLD the link (don't tap) until a preview of the real address pops up, then let go without opening it.
3. Read the main part of the address carefully — the words just before '.com' are what matters, like 'yourbank.com' versus 'yourbank.secure-login.com.'
4. If the real destination isn't the company's normal website, don't go there.

WATCH OUT

The safest habit of all: don't use the email's link at all. Open your browser and type the company's address yourself, or use the app you already have. That way it doesn't matter where the email's link pointed.

7 Attachments: When Not to Open

A surprise attachment is one of the most dangerous parts of a scam email, because opening it can quietly install harmful software. Treat unexpected attachments with real caution.

- Don't open attachments you weren't expecting, even if the email seems to be from someone you know.
- Be especially wary of 'invoice,' 'receipt,' 'shipping label,' and 'resume' files from strangers.
- A file that asks you to 'enable editing,' 'enable macros,' or 'enable content' to see it is a classic trap — don't.
- If a known company really sent you a document, you can usually find it by logging into your account directly instead.

GOOD TO KNOW

When a friend's email has only a vague line like 'check this out' and a link or file, their account may be hacked. A quick text or call to them — 'did you really send this?' — settles it.

8 The New Trick: 'Reply' and 'Call Us' Scams

Because clean writing lets scammers sound like real customer service, a growing style skips the obvious bad link. Instead it gives you a phone number to call or invites you to reply, then a smooth 'agent' does the rest by voice.

- A fake receipt for something you didn't buy, with 'call this number to cancel' — the number is the scam.
- A 'your subscription renewed for $499' email designed to make you call in a panic.
- A polite request to 'reply to confirm your details,' which starts a back-and-forth that wears you down.

> **WATCH OUT**
> If an email about a charge worries you, don't call the number in the email. Look up the company's real number yourself, or check the account directly. The phone number in a scam email leads straight to the scammer.

9 Turn On Your Email's Own Defenses

Your email service already filters a lot of junk, and a few settings make it work harder for you. These help whether you use Gmail, Outlook, iCloud, or Yahoo.

1. Leave your spam filter on, and glance in the spam folder occasionally rather than turning it off.
2. Use the 'Report spam' or 'Report phishing' button on bad messages — it trains the filter and protects others.
3. Be cautious about unsubscribing from obvious spam you never signed up for; a reply or click can confirm your address is live.
4. Keep your email password strong and unique, and turn on two-step verification so a stolen password alone isn't enough.

GOOD TO KNOW

Reporting a message as phishing does more than delete it — it teaches your email provider's filters to catch similar ones for everybody. It's a small civic good that takes one tap.

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 A Three-Question Gut Check

When any email makes you uneasy, run it through three quick questions before you touch a thing. If the answer to any is troubling, stop and verify through a channel you trust.

- Was I expecting this? A surprise 'account problem' or 'package' email deserves suspicion.
- What does it want me to do? Clicking, paying, calling, or sharing details are all reasons to slow down.
- Why the rush? Real organizations give you time; manufactured urgency is a scam's signature.

> *Expecting it? What does it want? Why the rush? Three questions beat a thousand clever words.*

11 If You Clicked or Replied

If you clicked a link, entered a password, or replied with details, don't panic — quick action limits the damage, and you're far from alone.

1. If you entered a password, change it right away on the real site, and change it anywhere else you used the same one.
2. Turn on two-step verification for that account if it isn't already on.
3. If you shared card or bank details, call your bank or card company to watch for and stop fraud.
4. Run a scan with your device's built-in security, and watch for odd activity in the days ahead.
5. If you gave up a lot — Social Security number, many accounts — visit IdentityTheft.gov for a step-by-step recovery plan.

> **WATCH OUT**
>
> Clicking one bad link is rarely a catastrophe, especially if you act quickly. If you're not sure what you exposed or what to change first, call me and we'll sort it out together, calmly and in the right order.

12 Scams That Impersonate People You Know

Some of the most convincing emails appear to come from a person, not a company — your boss, your pastor, a family member, a club you belong to. AI makes these sound natural and personal, which is unsettling but still beatable with the same habits.

- A 'quick favor' email asking you to buy gift cards for someone and 'you'll be paid back' — a classic, now polished.
- A note from a 'friend' who's traveling and suddenly stranded and needs money.
- A message from a familiar name whose account was hacked, sent to everyone they know.
- An email that matches a real relationship but asks for something out of character.

WATCH OUT

When an email from someone you know asks for money, gift cards, or urgent secrecy, confirm by voice on a number you already have before doing anything. A real friend won't mind the check; a scammer is counting on you skipping it.

13 Teach the Household the New Rules

Because the grammar shortcut is gone, it helps to make sure everyone at home has the updated instincts, not the old ones. A short, friendly refresher does the trick.

1. Share the headline: a well-written email is no longer a safe email.
2. Agree on the family habit of never using links or phone numbers from inside an email.
3. Show each other the hover-and-check and press-and-hold tricks once, so they feel familiar.
4. Reassure everyone that clicking one bad link is fixable and nothing to be ashamed of.

GOOD TO KNOW

The people who get fooled least are the ones who talk about scams openly at home. Treating it as a normal safety topic, like checking the stove, takes away a scammer's favorite tool: your embarrassment.

14 When to Call Bill

Email is where a huge share of scams begin, and the rules changed when AI learned to write. If you'd like your defenses brought up to date — or you just want someone to glance at a suspicious message before you act — that's an easy, welcome call.

I'll help you tune your spam and phishing filters, set strong passwords with two-step verification so a stolen password isn't enough, and teach you the hover-and-check habit on your own computer and phone. If you think you clicked something you

shouldn't have, I'll help you change the right things in the right order and make sure nothing's been left open.

- You want a quick look at an email before you click, reply, or call a number in it.
- You'd like your spam filters, passwords, and two-step verification set up properly.
- You clicked a link or shared details and want to close any gaps.
- You'd like to learn the link-checking habit hands-on, on your own devices.

CHEAT SHEET

Everyday Cheat Sheet

Keep this by the computer. When an email feels off, run down this list.

I want to...	Do this...
Judge an email	Ignore the grammar — judge the request and the urgency
Check the sender	Expand the full address; a slightly-off domain is a red flag
Check a link safely	Hover (computer) or press-and-hold (phone) to see the real address
Stay safest	Don't use the email's link — go to the company yourself
Handle scary charges	Don't call the number in the email; look it up yourself
If you clicked	Change the password, turn on two-step, call your bank if needed
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.