FROM THE MEHRUTHERM BLOG · CYBERSECURITY

How to Tell if That Email Is a Scam

Scam emails don't have typos anymore, and the logos are perfect. Here's how to actually tell the real thing from the fake, and what to do if you already clicked.

Himanshu Mehru · Founder, Mehrutherm

July 18, 2026

The email says your Microsoft password expires today. Or that a package couldn't be delivered. Or it's an invoice from a supplier you actually use, or a note from your bank about a charge, or a quick favor from the boss. The logo is right, the colors are right, the wording sounds exactly like every real email that company has ever sent you.

You may have heard the old advice: look for bad grammar and clumsy spelling. That advice is dead. The people sending these use the same AI writing tools everyone else does now, and the messages come out fluent, polished, and personal. The fakes aren't sloppy anymore, which means you need tells that don't depend on the scammer being bad at their job.

The good news: those tells exist, they don't require any technical skill, and there are only a handful to remember.

KEY TAKEAWAYS

- This kind of scam email is called **phishing**, and that's the last time we'll need the word. What matters is how to spot one.
- **Everything you can see can be faked**: the logo, the sender's name, the writing style, the footer. So the look of an email proves nothing.
- **The ask is the tell.** Sooner or later, every scam asks you to click, log in, pay, or hand something over. That moment is where to focus.
- **Urgency is the weapon.** Deadlines, threats, and "right now" exist to make you act before you think.
- The habit that beats all of it: **never respond through the email itself. Go around it**, using a login, bookmark, or phone number you already had.

©2026 Mehrutherm LLC ·Creston, WA

The Ask Is the Tell

Strip away the design and every scam email is a request, and it's always one of the same few: click this link and sign in. Open this attachment. Pay this invoice. Buy gift cards and send the codes. Read me back the verification code that just texted you. Update the bank account we pay you with.

So skip the cosmetics and ask one question: what does this email want me to do? If the answer involves your password, your money, a code, or a change to payment details, treat it as a scam until proven otherwise, no matter how legitimate it looks. Real companies mostly don't ask for those things by email, and the real ones that do will survive you taking ten minutes to verify.

Everything Visible Can Be Faked

The name in the "From" line is just a label, and the sender types whatever they want there. "Microsoft Support" can be typed by anyone. Look at the actual address behind the name, and then look closely, because near-miss addresses are the whole game: `support@micros0ft-billing.com`, `accounts@rnicrosoft.com`, `yourbank-security.net`. Close enough to pass a glance, which is all most emails ever get.

And even a perfect-looking address isn't a guarantee, because addresses themselves can be forged, and a scammer who has broken into a real person's account sends from the genuine article. That's why the sender check can only ever vote "suspicious," never "safe." The ask still rules.

Hover Before You Click

Links wear disguises too. The text can say `chase.com` while the link underneath goes somewhere else entirely. On a computer, rest your mouse on a link without clicking and the true destination appears in the corner of the window or in a small pop-up. On a phone, press and hold the link and the real address shows up. If what's underneath doesn't match what's written, you're done; that's the whole verdict.

Attachments deserve the same reflex. An invoice or "shared document" you weren't expecting is a classic delivery vehicle, and opening it can be all it takes. Weren't expecting it? Don't open it, verify it.

©2026 Mehrutherm LLC ·Creston, WA

Urgency Is the Weapon

Notice how often these emails come with a clock. Your account closes in 24 hours. The invoice is overdue and going to collections. The delivery gets returned today. The boss needs it before the meeting. Some even threaten: pay or the power gets shut off, respond or there's a warrant.

The time pressure isn't decoration; it's the mechanism. A person who slows down starts noticing things, so the email is built to keep you from slowing down. Flip that around and you get a reliable rule: the more urgent an email insists it is, the more time you should take with it. Real organizations move slower than their impostors, send paper, and call. Panic is a signature of the fake.

The Email From the Boss

The most expensive version of all this doesn't have a link or an attachment at all. It's a short, plausible note that appears to come from the owner, the pastor, the mayor, or the clerk: "Are you at your desk? I need you to handle a payment." Or from a vendor you really do pay: "We've changed banks, here's the new account for future invoices." Small businesses, churches, and town halls around here see exactly these, because scammers read websites and minutes and know who signs the checks.

One rule shuts this down completely: any request to move money or change payment details gets verified by voice, on a number you already had, before anything happens. Not by replying to the email, and not by calling a number the email helpfully provides, because both of those just connect you to the scammer. It's a thirty-second phone call, and no legitimate boss or vendor will ever fault you for making it.

When in Doubt, Go Around

Here's the habit that makes almost every scam email harmless: never act through the email. If "your bank" flags a charge, don't touch the link; open a new browser tab, log in the way you always do, and look. If "Microsoft" says your password expires, sign in from your bookmark. If a vendor sends a surprise invoice, call the number in your records. The real situation, if there is one, will be waiting inside the real account.

Going around costs a minute or two. It also means you never actually have to win the guessing game, because you never play it.

©2026 Mehrutherm LLC ·Creston, WA

If You Already Clicked

It happens, including to careful people, including to people who read guides like this one. What matters now is speed, not blame.

If you typed a password into a page you reached from the email, change that password right now, along with anywhere else you'd reused it, and make sure multi-factor authentication is turned on. If money moved or bank details were involved, call the bank immediately; the first hours matter. And tell whoever looks after your technology right away, because the sooner someone's checking what else the click touched, the smaller this stays. The costliest scams aren't the ones somebody fell for; they're the ones somebody sat on out of embarrassment.

DOESN'T THE SPAM FILTER CATCH THESE?

It catches the mass-produced junk, which is why your inbox isn't drowning. But messages written for you specifically, referencing your real vendors or your actual boss, are precisely the ones that sail through. A filter is a screen door, not a guard. (Funny enough, we've also written about the opposite problem: your own legitimate email landing in other people's spam.)

What a scammer can fake

- ✕ The logo, layout, and colors, pixel-perfect
- ✕ The sender's display name and writing style
- ✕ A footer with a real address and phone number
- ✕ A login page identical to the real one
- ✕ Urgency, authority, and a plausible story

What a scammer can't fake

- ✓ What your account shows when you log in from your own bookmark
- ✓ The phone number you already had on file
- ✓ Your boss's voice on a thirty-second call
- ✓ The true destination a link shows when you hover
- ✓ Your willingness to slow down

Spotting scams one inbox at a time is the last line of defense, not the first. The layers in front of it, the fundamentals and a worked-through checklist, catch most trouble before a human ever has to judge an email, and for towns, that same groundwork is what your insurer now expects anyway.

©2026 Mehrutherm LLC ·Creston, WA

MEHRUTHERM · CRESTON, WA

Want your team to see this coming? Get in touch. We'll set up the protections that stop most of these emails from arriving at all, and walk your people through the handful of habits in this guide, in plain English, no scare tactics.

mehrutherm.com/quote

©2026 Mehrutherm LLC ·Creston, WA