FROM THE MEHRUTHERM BLOG · CYBERSECURITY

That Urgent Phone Call Is Probably a Scam Too

Scammers don't only email. They call, or leave a pop-up telling you to call them, pretending to be your software company, your bank, or the government. Here's how to tell, and the one habit that stops nearly all of it.

November 9, 2026

The phone rings in the middle of a busy morning. The person on the line is calm and professional. They are from the company whose software runs your office, they say, and their systems have flagged a serious problem on one of your computers. They can fix it right now, if you'll just give them a few minutes of access.

Or there is no call at all, just a red screen that takes over the browser: a warning, a frozen page, maybe an alarm sound, and a number to call "before your files are locked." Or a voice message from your bank's fraud department, or the power company, or a government office, each with a reason you need to call back today.

Email scams get most of the attention, and we wrote a whole guide to those. But the same people work the phone just as hard, and a voice on the line carries an authority a strange email never quite manages. The good news is that the tells are nearly the same, and the single habit that defeats almost all of them takes about a minute.

The ask is still the tell

Strip away the uniform and every one of these calls is a request, and it is almost always one from a short list: let me onto your computer, read me the code that just texted you, confirm your account number, move some money, or buy gift cards and read me the numbers off the back.

So do the same thing you would do with a suspicious email: ignore how convincing the caller sounds and ask what they actually want you to do. If the answer involves access to your computer, a verification code, your account details, or a payment, treat the call as a scam until you have proven otherwise on

©2026 Mehrutherm LLC ·Creston, WA

your own terms. A real bank, a real software company, and a real government office will all survive you hanging up and checking.

"We've detected a virus on your computer"

No legitimate technology company watches your personal computer and calls you when something is wrong. They do not have your number, they do not know who you are, and they are not monitoring your machine. So a cold call claiming otherwise is a scam, every time, with no exceptions worth worrying about.

The pop-up version is the same scam in a different coat. A web page hijacks your screen, throws up alarming warnings and perhaps a siren, and tells you to call a number right now. Nothing is actually wrong with your computer. The page is just a loud picture built to frighten you into dialing. The fix is not to call the number. It is to close the browser, and if a tab will not close, restart the computer, after which the "emergency" is simply gone.

What they are after, once you call or let them in, is remote control of your machine, a payment for "support" you never needed, or both. The moment anyone you did not hire asks to connect to your computer, the call is over.

"This is your bank's fraud department"

The most convincing calls borrow a real institution: your bank, a card company, the power company, a county office, the Social Security people. The caller already "knows" a detail or two about you, speaks in the calm script of a real call center, and often shows a real-looking name or number on your screen.

That number proves nothing. The name and number that appear on an incoming call can be set to say anything, so a scam call can read as your bank's fraud line as easily as the real one can. It is a label the caller fills in, not a fact you can trust.

The real institutions these calls trade on do not actually need you to confirm a password, read back a one-time code, or move your money "somewhere safe" to protect it. That request, from anyone, is the scam itself. Government offices in particular do not call to demand immediate payment or threaten arrest. That is never how any of them work.

©2026 Mehrutherm LLC ·Creston, WA

Gift cards and odd payments are a dead giveaway

Watch what they ask you to pay with. Gift cards from the drugstore, a wire transfer, a payment app, cryptocurrency, a "refund" that first requires you to send money back: every one of these exists in the script because it is fast, hard to reverse, and hard to trace. No real fine, bill, fraud hold, or support charge is ever settled by reading gift-card numbers over the phone.

If a call steers you toward any of these, you do not need to work out the rest of the story. The payment method alone has told you everything.

Hang up and call a number you already had

Here is the habit that makes nearly all of these calls harmless: never act on a call you did not place. Hang up, find the real number yourself (on the back of your card, on a past bill, or on the organization's own website that you navigated to, not a number the caller gave you), and call that. If there is a genuine problem, it will still be there when you come in through the front door. If there is not, you just saved yourself.

This is the same move as going around a suspicious email instead of clicking its link. You never have to win the argument with the caller, because you stop talking to them and start again through a channel you trust.

KEY TAKEAWAYS

- These calls are the phone version of email scams, and the same thinking beats them: **the ask is the tell**, not how official the caller sounds.
- **No real technology company calls you about a virus**, and a scary pop-up telling you to call a number is just a web page trying to frighten you. Close it.
- **Caller ID can say anything.** A real-looking name or number is not proof of who is calling.
- **Gift cards, wire transfers, and crypto are the giveaway.** No legitimate bill is paid that way.
- The habit that ends almost all of it: **hang up and call back on a number you already had**, never one the caller provides.

©2026 Mehrutherm LLC ·Creston, WA

The call that targets your front desk

In a business or a town office, these calls often are not aimed at the owner. They are aimed at whoever answers the phone. A caller claiming to be from a vendor, from "the computer company," or even from the boss can talk a helpful employee into resetting a password, reading out an account detail, or changing where an invoice gets paid. It is the same trick as the fake-boss email, just spoken aloud, where it feels even harder to refuse.

The protection is a simple, boring rule everyone is allowed to follow without worrying they are being rude: any request that arrives by phone to grant access, share account information, or move or redirect money gets verified through a known contact before anyone acts. No employee should ever be in trouble for saying, "Let me call you right back." A workplace where that sentence is normal is one these callers cannot crack.

If you already answered

It happens to careful people, and the useful response is speed, not embarrassment. If you let someone onto your computer, disconnect it from the internet and get it to someone who can check it properly, then change your important passwords from a different device. If you shared a code or account details, call your bank and the real organization directly, using a number you look up yourself. If money moved, call the bank immediately, because the first hours are the ones that matter most. And tell whoever looks after your technology right away, so they can check what else the call may have touched.

The groundwork that prevents most of this is the same unglamorous set of cybersecurity basics and the plain checklist that blunt the email version. Strong sign-ins and a team that knows the playbook protect you no matter which way the scammer comes knocking.

DOESN'T THE NUMBER ON MY SCREEN PROVE WHO'S CALLING?

No. The name and number shown on an incoming call are set by whoever is placing it, and faking them is easy and common. A call that appears to come from your bank, a government office, or a local number can be anyone. Treat caller ID as a hint, never as proof, and verify by calling back a number you already trusted.

©2026 Mehrutherm LLC ·Creston, WA

What a scam caller can fake

- × A calm, professional voice and a real call-center script
- × A name and number on your screen that look official
- × A real detail or two about you or your business
- × A believable reason you have to act today
- × The logo and the alarm on a pop-up telling you to call

What a scam caller can't fake

- ✓ What you see when you call back a number you already had
- ✓ A real company actually monitoring your computer (none do)
- ✓ A legitimate bill that must be paid in gift cards
- ✓ Your bank genuinely needing your code or password
- ✓ Your right to hang up and check before doing anything

MEHRUTHERM · CRESTON, WA

Worried a call like this could get through to your team? Get in touch and we'll look at the sign-ins, the habits, and the simple rules that keep one of these calls from turning into a bad week, and walk your people through the handful of tells in plain English, no scare tactics.

mehrutherm.com/quote

©2026 Mehrutherm LLC ·Creston, WA