



COMPUTER TIES IT RESOURCE CENTER • EMPLOYEE QUICK GUIDE

Phishing & Suspicious Message Quick Guide

A desk reference for everybody who uses a computer at work. Print it, post it, hand it to new hires.

FILLABLE PDF

Type into any field, then save or print a copy.

EDITION

Version 1.1 • September 2026

QUESTIONS?

(517) 788-6393 • computer-ties.com

Attackers usually do not break in. They ask somebody to let them in, using a message that looks completely ordinary. You do not need to be technical to stop this. You need to recognize when a message is trying to hurry you, and you need to know it is always fine to stop and check.

The words you will hear, and what they actually mean

Phishing

A message impersonating someone you trust, designed to get a password out of you or get you to pay the wrong person.

Spear phishing

The same thing, aimed at you specifically, using real details about your job and your colleagues. Not a net thrown at a shoal. A single line, with your name on the hook.

Business email compromise (BEC)

Phishing aimed at money rather than passwords. Someone poses as a supplier, a director, or a payroll contact and changes where a payment goes. There is no attachment and no virus, which is why nothing catches it except a person stopping to check.

Smishing and vishing

The same tricks by text message and by phone call. Same script, different doorway.

MFA fatigue

Sending you sign-in approval prompts over and over until you tap approve just to make them stop. Someone leaning on your doorbell at 2am. Never approve a prompt you did not trigger.

1 Seven Signs a Message Deserves a Second Look

- ☐ **It is in a hurry.** Your account closes today, the invoice is overdue, the delivery is held, act within the hour.
The rush is the whole trick. It exists to stop you checking.
- ☐ **It asks for something unusual, and asks you to keep it quiet.** Buy gift cards, change where a payment goes, approve something, do not mention it to anyone yet.
A real request from your boss survives being checked out loud.
- ☐ **The sender is almost right.** A name you know with an email address you do not, a company name with one extra letter, a reply that is really a brand new message.
Look at the actual email address, not just the name displayed.



- ☐ **You were not expecting it.** An invoice, a shared file, a password reset, a delivery notice, a message from support.
Unexpected plus urgent is the most dangerous combination there is.
- ☐ **The link does not go where the words say.** Rest your mouse over it, or press and hold on a phone, and the real address appears.
Find the first single slash, then read the two words immediately before it. That is the real site. In [login.microsoft.com.account-verify.ru/signin](#) the real site is [account-verify.ru](#), and everything before it is decoration.
- ☐ **An attachment asks you to switch something on.** Enable editing, enable content, allow this to run.
That step exists to get past protections that were doing their job.
- ☐ **You get a sign-in code or prompt you did not ask for.**
This almost always means somebody already has your password and is trying to get past the second step.

2 The Usual Tricks, and What Gives Them Away

The message	What it is after	The giveaway
Your password expires today — click here to keep your account	Your password	Password changes start with you, not with an email.
A shared document from a colleague or a client	Your password, typed into a fake sign-in page	You are asked to sign in again to a page you only reached by clicking a link.
New bank details for an upcoming payment	Your money, sent to them instead	Any change to payment details, from anybody, ever.
A quick favor from the owner or a director	Gift cards, a transfer, or a change to somebody's pay	Sent from an outside address, and written to make checking feel awkward.
A pop-up or a phone call saying your computer is infected	Remote control of your computer	Nobody legitimate calls you about a virus you never reported.
Voicemail, fax, scan, or delivery notification	You to open a dangerous attachment or link	You were not expecting it, and it is oddly vague about the details.
A text about a parcel, a toll, or your bank	Your password or card details	A shortened link, the wrong delivery company, a number you do not recognize.

3 What To Do

You are not expected to work out what kind of attack it is. You only need to stop and check.

If	Then
It looks suspicious	Do not click, do not reply, do not open the attachment. Report it, then delete it.
You are not sure whether it is real	Check using a phone number or address you already had. Never use the contact details in the message itself, because those belong to whoever sent it.



If	Then
It involves money, bank details, or pay	Call a person you know on a number you already have and confirm out loud, before anything moves. Every time, no matter who it looks like it came from.
You clicked the link or opened the attachment	Tell somebody right away. Speed matters much more than being sure, and much more than feeling embarrassed.
You typed your password into a page you now doubt	Change that password immediately, then report it. Change it anywhere else you used the same one.
You approved a sign-in prompt you did not ask for	Report it right away, and assume somebody already knows your password.

Report it first, work out what it was afterwards

Every hour between the click and the report is an hour somebody else is using your access. An organization that finds out in ten minutes can usually contain it. An organization that finds out in ten days is dealing with wherever the intruder has got to since. Nobody at Computer Ties is going to make you feel foolish for reporting something that turns out to be nothing.

4

What Computer Ties Will Never Ask You For

- ☐ Your password. Not on the phone, not in an email, not during a remote session, not ever.
- ☐ A sign-in code, a code texted to your phone, or for you to approve a prompt on our behalf.
- ☐ Access to your computer when you were not expecting it.
We connect after you have contacted us, or when we have arranged it with you beforehand.
- ☐ Payment by gift card, cryptocurrency, or bank transfer.
- ☐ To install something we have not already talked to you about.

If somebody claiming to be Computer Ties asks for any of that

Hang up, or close the session, and call us on a number you already have: Help Desk **(517) 905-3168** or the office **(517) 788-6393**. Do not use a number the caller gave you. We would much rather take a call that turns out to be nothing.

5

Put This Where People Work

This works best pinned up where people actually sit, not emailed around as an attachment nobody opens twice. Organizations we work with usually post it in shared areas, include it in new-hire packets, and spend five minutes on it at a staff meeting once or twice a year.



■ Fill this in before you hand it out

Report suspicious messages to

Phone number or extension

Out of hours, contact

Last updated

About this guide

This is general awareness guidance for staff. It does not replace proper security training, and it does not replace your own organization's rules about reporting. If your organization is covered by HIPAA, CJIS, PCI DSS, or similar requirements, check what those require you to do.

Want your staff trained, not just warned?

Computer Ties provides security awareness training for organizations across southern Michigan, along with the email filtering and multifactor authentication that stop a good many of these messages reaching an inbox at all, and blunt the ones that do.

NEW PROJECTS AND PLANNING

(517) 788-6393

EXISTING CUSTOMER SUPPORT

(517) 905-3168

2903 West Michigan Avenue, Jackson, MI 49202 • computer-ties.com • Serving Jackson since 1990

