A QUICK SECURITY NOTE FROM YOUR TEAM AT SYSTECH

Think Before You Click.

A quick guide to the most common online tricks of 2026, and the simple habits that beat them.

A STORY YOU MIGHT RECOGNIZE

Tuesday morning. One email. One click. One bad day.

Picture a regular Tuesday. One of your staff, we will call her Sarah, is having coffee when an email lands. It looks like it is from DocuSign: you have a signed contract waiting. She clicks. A Microsoft login page comes up, and it looks completely normal. She types her password and gets the usual approval prompt on her phone. She approves it. The page reloads and simply sends her back to the login. A little odd. She tries again, and this time it works. She opens the document, finds it is nothing important, closes the tab, and moves on with her day.

Three weeks later, someone in another country has been quietly reading her email the entire time. They have set up forwarding rules. They have sent invoices to her clients with their own bank details attached. Sarah did nothing obviously wrong. There were no glaring red flags. So what actually happened? That is what this guide is here to explain.

WHY WE ARE SHARING THIS

Attackers changed their game. Antivirus alone will not catch this.

For years, the criminals tried to sneak software onto your computer: viruses, trojans, and malicious downloads. Antivirus stops most of that, so they changed tactics. Today they are not after your computer. They are after your accounts.

THE OLD WAY

They attacked the computer.

Viruses, malware, and suspicious downloads. Your antivirus saw them and blocked them. If something slipped through, we noticed it and cleaned it up.

THE NEW WAY

They trick you.

No virus. No suspicious file. Just a convincing email, a real-looking login page, or a helpful sounding message that gets you to hand over the keys yourself. Antivirus does not see a thing, because there is nothing to see.

THE ONE BIG IDEA

You are now the lock on the door.

Modern attackers cannot get past the technology anymore, so they go around it. They aim for the person sitting at the keyboard. That is not flattering, but it is empowering, because a few good habits from you stop most attacks before they ever start.

Notice

the moments that should give you pause.

Pause

for ten seconds before you click, approve, or paste.

Ask us

if anything feels off. We would rather hear from you ten times for nothing.

SIX MOMENTS THAT SHOULD MAKE YOU PAUSE

Each one looks normal. Here is what is really happening, and what to do instead.

1 The login that did not quite work the first time.

WHAT IT FEELS LIKE

You click a link in an email and a Microsoft or Google login appears. It looks completely normal. You type your password, approve the prompt on your phone, and the page simply reloads. You shrug, type your password again, and this time it works. The document you were after turns out to be nothing special, but at least you got there.

WHAT REALLY HAPPENED

That first login page was a fake, sitting between you and the real Microsoft. It passed everything you typed through to the real site, watched the login succeed, and stole the proof that you were signed in. Then it bounced you to the genuine site so the whole thing felt normal. The attacker is now signed in as you, on their own computer, and they no longer need your password.

WHAT TO DO INSTEAD

If a login page bounces you and asks you to sign in again, stop. Close the tab. Open a fresh browser tab, type the address yourself (for example, outlook.office.com), and go there directly. Then call us. That bounce is the giveaway.

2 “Click Allow to continue.”

WHAT IT FEELS LIKE

You click a link and land on a genuine Microsoft or Google page saying an app would like to access your email and files, and asking whether you allow it. The app name sounds reasonable, maybe Office Mail Sync or DocuViewer. The address looks right and the padlock is there, so you click Allow.

WHAT REALLY HAPPENED

Anyone can build an app and name it anything they like. By clicking Allow, you gave it permission to read your email and files for months to come. Even if you change your password tomorrow, the app keeps working. This is one of the only tricks that beats every kind of multi-factor authentication, because nothing is being broken. You handed over the keys yourself.

WHAT TO DO INSTEAD

Never click Allow on a consent screen you were not expecting. If you did not deliberately set out to connect a new app, the answer is no. When in doubt, close the tab and call us. We can tell you in about thirty seconds whether the request is real.

3 “Please enter this code to verify your account.”

WHAT IT FEELS LIKE

You get a Teams message or an email that looks like it is from us, or from Microsoft directly. It asks you to go to microsoft.com/devicelogin and enter a short code. The address really is Microsoft’s website. You go there, type the code, and sign in. The page tells you that you are verified. Done.

WHAT REALLY HAPPENED

The code came from the attacker, not from us. By typing it on the real Microsoft page and signing in, you connected the attacker’s session to your account. They are now signed in as you, on their computer, with full access. From where you sat, nothing looked wrong, because everything on the screen really was Microsoft.

THE ROCK-SOLID RULE

systech will never ask you to enter a code at microsoft.com/devicelogin. Not ever. If anyone asks you to do that, by email, chat, text, or phone, it is a scam. Full stop.

4 The CAPTCHA that wants you to paste something.

WHAT IT FEELS LIKE

You are asked to do a quick human check that looks like the familiar “I am not a robot” box. After you click through it, the page tells you to copy the address from your browser’s address bar and paste it into a box, or to run a short command, to complete verification.

WHAT REALLY HAPPENED

That address in your bar contains a secret code created when you logged in. The CAPTCHA is fake, and its only job is to talk you into copying that code over to the attacker. The moment you paste, they have full access to your account. No real website ever needs you to copy something out of your address bar.

WHAT TO DO INSTEAD

If a verification page ever asks you to copy from your address bar, paste an address, run a command, or do anything beyond ticking a checkbox, close the tab right away. That is not how a CAPTCHA works.

5 Approval prompts that will not stop.

WHAT IT FEELS LIKE

Your phone keeps buzzing with approval requests from your authenticator app. You have not tried to log in anywhere. It is late, you are trying to sleep, and the prompts keep coming. After the eighth one, you tap Approve just to make them stop. Or maybe it happens by accident, half asleep.

WHAT REALLY HAPPENED

Someone already has your password, usually from a different website that was breached, where the same password was reused. They are trying to log in over and over, hoping you will approve a prompt to make the buzzing stop. Each prompt is your explicit permission for that login. One tap, even by accident, lets them in.

WHAT TO DO INSTEAD

Never approve a prompt you did not start yourself. If they keep coming, deny them, silence your phone, and call us. If you have already tapped Approve by accident, call us right away. We can fix it quickly. The longer it waits, the harder it gets.

6 An email from someone you know that is just a little off.

WHAT IT FEELS LIKE

An email arrives from your boss, a coworker, or a regular vendor. Real name, real signature, maybe even part of a real conversation from last week. They ask you to do something: click a link, review a document, pay an invoice with new bank details, or buy gift cards quickly. Maybe the wording is slightly off. Maybe it is urgent in a way they usually are not. Or maybe nothing seems wrong at all.

WHAT REALLY HAPPENED

Your coworker's or vendor's account was compromised earlier. The attacker is reading their mail and sending messages from their real address, using real signatures, real reply chains, and real context. It is the most convincing kind of phishing, because everything about it is real except for who is actually typing.

THE GOLDEN HABIT

Any unusual request involving money, login details, or sensitive files deserves a check through a different channel. Pick up the phone. Walk down the hall. Send a separate text. Two minutes of friction beats two weeks of cleanup.

BEFORE YOU CLICK, APPROVE, OR PASTE

Five questions. Ten seconds. Most attacks fall apart right here.

1. **Was I expecting this?**
   An email, a login screen, an approval prompt, a Teams message. If it showed up without warning, slow down.
2. **Is something being rushed?**
   Urgency is the oldest trick in the book. Real coworkers and real vendors almost never need it solved in the next ten minutes.
3. **Am I being asked to do something unusual?**
   Paste a code. Approve a prompt. Buy gift cards. Allow an app. If you have never done it before, ask first.
4. **Does this make me feel afraid or excited?**
   Both are flags. Attackers steer your emotions, because an emotional brain skips past the careful one.
5. **Would I rather ask, or apologize?**
   We would much rather hear from you for nothing than fix something afterward. There is no such thing as a dumb question here.

WHEN SOMETHING FEELS OFF

The shortest possible to-do list.

Stop.
Do not click, do not approve, do not paste. It can wait sixty seconds.

Do not delete it.
Leave the email, message, or window where it is. We may need to look at it.

Call us.
Or send a screenshot. We will tell you in a minute whether it is real.

Cleaning up early takes minutes. Cleaning up late takes weeks.

ABOUT YOUR TEAM AT SYSTECH

Here is what we will, and will never, ask you to do.

WE WILL NEVER

- ✗ Ask you to enter a code at microsoft.com/devicelogin
- ✗ Ask for your password, by phone, email, chat, or in person
- ✗ Ask you to read an approval code out loud or send it to us
- ✗ Send a “verify your account” link that needs your password
- ✗ Ask you to paste an address from your address bar somewhere else
- ✗ Pressure you to act fast, or before something gets locked

WE WILL

- ✓ Answer questions, even the ones that feel too small to ask
- ✓ Look at suspicious emails and tell you what you are seeing
- ✓ Walk you through a fix, and never blame you for asking
- ✓ Tell you the truth if we do not know yet, and follow up
- ✓ Reach you the way we always do, through familiar channels
- ✓ Treat “I think I clicked something” as routine, not embarrassing

THE WHOLE TALK, IN ONE LINE

Pause for ten seconds. Call us for the rest.

You do not need to recognize every trick. You only need to recognize the feeling of “huh, that is a little weird,” and pause long enough to ask. That one habit, multiplied across your whole team, makes your business a hard target.

Reach the systech helpdesk

541.696.5555, Option 1 | support@systech.io

Or simply reply to any ticket you already have open with us.