



TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

Why Following the Rules
Isn't the Same as Being
SecurePage 1

FREE: Business Owner's
Guide To IT Support Services
And Fees Page 2

Security Corner: What To
Do In The First Hour Of A
Cyber AttackPage 3

QR Code Scams: What
Are They And How To
Spot Them.....Page 3

Still On Windows 10?
Here's Why It's A Risk.....Page 4

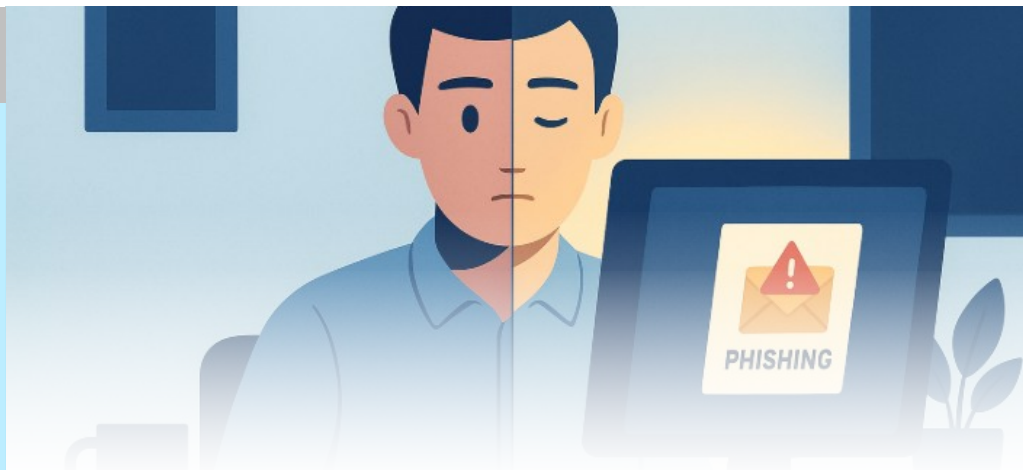
Passkeys: The Login That
Can't Be Phished.....Page 4

August 2026



Kim Nielsen,
CISSP, CCSA
President &
Chief Technology
Strategist at
Computer
Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"



Why Following the Rules Isn't the Same as Being Secure

In every workplace, cybersecurity awareness begins with a laundry list of rules: *Avoid unknown links. Never share passwords. Don't plug in unapproved devices.*

These rules exist for a reason, of course. They form the foundation of how we protect company data and everybody in the office.

Unfortunately, *security rules are only as strong as the people following them.* In other words, your boss can lay out a ten-page manual about cyber hygiene, but it doesn't matter if nobody reads it.

When complying with safety rules turns into muscle memory (i.e. clicking through training modules, checking the "*I've read this policy*" box without actually doing so) we risk losing the most important part of the process: *Awareness.*

The Illusion of "Doing It Right"

It's easy to assume that if you follow every policy, you're automatically safe from all cyberattacks. Most breaches today don't happen because someone *broke* the rules, however; they happen because someone *stopped thinking* about why those rules exist.

Take the 2023 MGM Resorts breach as an example. Attackers didn't need to hack into servers or exploit code. By simply impersonating an employee on a phone call, the hackers convinced IT support to reset their credentials, and from there, everything unraveled.

The staff didn't ignore procedure; they just trusted the wrong person at the wrong moment. The case serves as a powerful reminder that security isn't just about rule-following. You need to stay alert and pause when something

Continued on pg.2

Continued from pg.1

suspicious comes up. A moment of forethought can save months of recuperation and stress after a breach.

When Routine Becomes Risk

Cybersecurity fatigue is real. After hearing the same reminders year after year, even the most diligent employees can slip into autopilot. Maybe you start approving login prompts without reading them, or you skip setting up MFA because you're busy. Perhaps you even reuse a password more than once instead of logging yourself back into a secure Password Manager.

It's human nature. Unfortunately, attackers count on it.

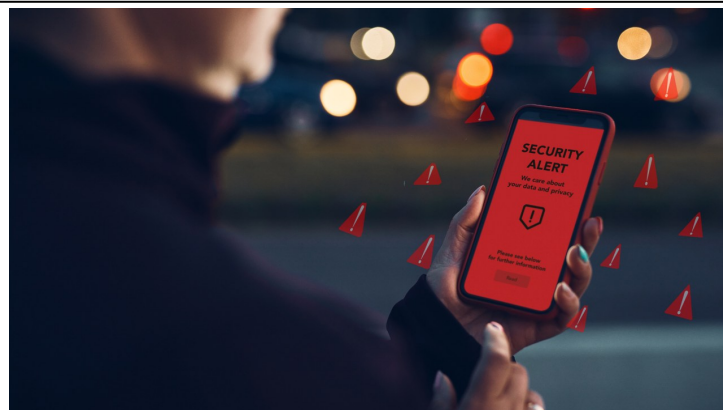
Social engineers, phishers and other hackers all thrive on routine. They know when employees are busiest, most distracted, and least likely to question a familiar-looking email, and that's exactly when they strike.

Turning Compliance Into Awareness

So how do we stay secure *and* engaged? It's about transforming rule-following into mindful habits, ones that are rooted in understanding, instead of feeling of pure obligation.

Here are a few simple ways to start:

- **Ask "why," not just "what."** Every policy has a reason. The more you understand that reason, the easier it is to recognize when something feels off.
- **Pause before you click.** Even if an email looks familiar, give it two seconds of critical thought. Tiny pauses prevent massive breaches.



- **Speak up.** If something doesn't feel right, trust your gut. Security teams would rather investigate a false alarm than a real incident.
- **Stay curious.** Cyber threats evolve constantly. Keep learning, because even small refreshers help you spot new tactics faster.

Conclusion

Cybersecurity isn't just an IT problem, and it's not just about checking boxes. It's a living practice that depends on each of us to stay aware, question interactions that feel unusual, and remember *why* the rules matter.

The moment we stop paying attention, even the best defenses can fall apart.

So next time you get that "verify your login" prompt or a suspicious email, don't just follow the rulebook, but think about *why* it's there. That two-second pause could save your company hours of recovery time.

Free Cyber Risk Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now



At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber risk audit to uncover any loopholes that may exist in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these risk problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are exposed to various threats in a number of areas.

Claim Your FREE Assessment Today At:

<https://www.cti-mi.com/cyber-security-audit-826/>

Or Call Our Office At: 248-362-3800

Get More Free Tips, Tools and Services At Our Website: <http://www.cti-mi.com>
(248) 362-3800

Security Corner

What To Do In The First Hour Of A Cyber Attack

If your business is hit by a cyberattack, the first hour decides how bad it gets. The instinct is to start fixing things, and that's usually what makes it worse. Work through these five steps instead.

1. Disconnect the affected devices from the network. Unplug the network cable and turn off Wi-Fi so the problem can't spread to other computers or your backups. Try not to power the machine off, because that can wipe evidence of what happened.
2. Call your IT provider, by phone. Don't email, in case the attacker is watching your inbox. If you have cyber insurance, call them next, since many policies want their incident team involved early.
3. Leave the evidence alone. Don't wipe, reinstall, or tidy up the affected machines yet. Screenshots are fine, but keep the originals.
4. If money was sent, call your bank immediately. Ask them to recall the transfer. With wire fraud, the first few hours make the biggest difference.
5. Reset passwords from a clean device, and turn on MFA. Start with email and admin accounts, using a device you know isn't affected.

Then report it: in the US to the FBI's IC3. The FBI doesn't recommend paying, and it's a decision to make with law enforcement and your insurer, not in the first panicked hour.

For more information about this topic, call us at 248-362-3800.

QR Code Scams: What Are They And How To Spot Them

QR codes are part of everyday business now. You scan them for menus, payments, Wi-Fi, and shared files. Scammers know that, and they've started hiding their links inside QR codes to get past the security that would normally catch a bad link in an email.

What a QR code scam is

A QR code scam, sometimes called "quishing," swaps a written link for a QR code. You scan it with your phone, it opens a web page, and you land on a fake login or payment screen built to steal your details. The QR code is only the way the scammer gets you there. The page on the other end is the same kind of fake you'd see in any phishing attack, made to look like Microsoft 365, your bank., or any other important site.

Why QR code scams get past your security

Two things make these scams effective. First, the malicious link is hidden inside an image. Most email security tools scan the text of a message for known bad links. A QR code is a picture, so the link inside it is not text the filter can read. The UK's National Cyber Security Centre points out that not all phishing-detection tools scan images, which is the reason criminals started using QR codes to disguise their links in the first place.

Second, scanning a code moves you onto your phone. Your work computer probably has web filtering, endpoint protection, and DNS controls that block known bad sites. Your personal phone usually has none of that. So, the moment you scan, you step outside the protection your business pays for, often without realizing it happened.

Common QR scams to watch for

- A fake "scan to keep your account active" email, often from "Microsoft" or "IT."
- A QR code inside a PDF invoice, with a "scan to pay" prompt that sends your money to the scammer.
- A sticker placed over a real QR code on a parking meter or payment terminal.

How common are QR code scams?

The volume is climbing fast. In its report on email threats for the first quarter of 2026, Microsoft said it detected around 8.3 billion email-based phishing threats in those three months.

QR code phishing rose 146% across the quarter, from 7.6 million attacks in January to 18.7 million in March. By the end of the quarter it had reached its highest monthly volume in at least a year.

Microsoft also found that most of these attacks arrived as PDF attachments, growing from 65% of QR code attacks in January to 70% in March.

How to protect your business from QR code scams

Protecting yourself against Quishing comes down to a few habits:

- Treat a QR code in an email with the same caution as a strange link,
- Before you act, check the web address your phone previews when you scan. If it isn't the site you expected, close it.
- When in doubt, skip the code and go to the site directly by typing the address yourself.
- Tell your team what these look like, with a real example, because most people have never been warned about this.

What to do if someone already scanned one

If you or someone on your team scanned a QR code and entered details on the page that opened:

1. Change the password for that account right away.
2. Confirm multi-factor authentication is turned on for the account.
3. Tell whoever manages your IT, so they can check for unusual sign-ins.
4. If card or banking details were entered, call the bank and watch the account closely.

Acting quickly limits what an attacker can do with the details they captured.

■ Still On Windows 10? Here's Why It's A Risk

Windows 10 stopped getting security updates in October 2025. The computers still work, which is why it's easy to leave them, but every new flaw found now stays unpatched. That makes those machines easier to attack and can cause problems with compliance and your cyber insurance.

Here's how to move off it:

1. List every computer still running Windows 10.
2. Check which ones can upgrade to Windows 11 (free if the hardware qualifies) using Microsoft's free PC Health Check app.

3. Upgrade the ones that qualify. The upgrade keeps your files and programs in place.
4. For the rest, choose between paid Extended Security Updates as a shot-term bridge or replacing the PC.

Your IT provider can run this inventory quickly and tell you the best option for each machine.

■ Passkeys: The Login That Can't Be Phished

People reuse passwords, write them down, and type them into fake login pages. Passkeys replace them: you sign in with the same fingerprint, face, or

PIN you use to unlock your phone, and there's no password for anyone to steal, guess, or phish.

- Why they're safer: nothing to phish, nothing for a hacker to steal in a breach, and nothing to reuse or forget.
- Where they work: Microsoft, Google, and Apple accounts, plus a growing list of banks and business tools.
- Included with Microsoft 365 at no extra cost.
- They're faster: A passkey sign-in takes about 3 seconds, against 69 for a password plus a code.
- Two types: a synced passkey is backed up to your account and works across your devices, while a device-bound passkey stays on one device or a physical security key.
- Start with your most sensitive accounts: administrators, finance, and anyone who can move money.
- Let everyone else add a passkey alongside their password at first.
- Give each person a backup, like a second device or a security key, so a lost phone doesn't lock anyone out.
- Keep passwords for the few systems that don't support passkeys yet.

