1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

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

What's Inside

April 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!"

How Everyday Work Habits Leak More Data Than You Think

Most people imagine data breaches as elite hackers breaking into corporate networks, but in reality, a surprising amount of sensitive information leaks out through simple, ordinary behaviors that even *you* might perform in the office.

That's right. Those screenshots, AI prompts, file-sharing shortcuts, and even the way we communicate online with others can lead to accidental leaks of private information.

Although none of it feels risky in the moment, in reality, these small actions can add up and expose far more than we realize.

Hidden Risks in Everyday Actions

Be mindful about…

- **Screenshots:** A quick screenshot seems harmless…until you notice the open tabs, internal tools, client names, or even a colleague's phone number visible at the top. That one image, shared in Slack or emailed to a vendor, can unintentionally reveal internal systems or confidential information.
- **AI Prompts**: Generative AI tools are incredibly helpful, but many people don't realize that sharing client details, contract language, confidential documents, or internal conversations in their prompts may expose data to third-party systems. Some tools store inputs for training unless enterprise protections are enabled, and once a third-party has access to private information, you can't hide it again.
- **File-Sharing Shortcuts**: Sharing a document "quickly" often means using personal cloud accounts, opening link settings so that "anyone with the link can view", or forwarding files to a personal inbox so that you can

Continued on pg.2

Continued from pg.1

work remotely. *Every shortcut creates new copies of sensitive data that your IT team can't see, track, or secure.*

- **Collaborative Platforms**: Unsecured workplace group chats may make communication fast, *but they also turn casual messages into permanent records*. Forwarded attachments, screenshots of customer information, or even typing, *"Hey, can you send me Mr. Johnson's termination papers?"* in the wrong channel can expose data unintentionally. Always use platforms with end-to-end encryption and ensure you're chatting with the right persons

Staying safe doesn't mean working slower. It just means working more intentionally.

Case Study: 2024 Cyjax Exposure

In 2024, threat intelligence firm Cyjax discovered thousands of sensitive internal documents indexed by public search engines. Affected data included financial reports, passwords, HR data, and internal source code.

The cause wasn't a breach or a hack. Instead, employees *unknowingly* synced work files to their personal cloud storage while using mobile devices and home computers. The services backed up everything automatically, and public search engines did the rest.

It's a perfect example of how everyday convenience can turn into widespread exposure — without you ever meaning to share it.

How to Share Smarter (and Safer)

Online collaboration is a touchstone of the modern workplace, so we have to understand how to exchange information *securely*.

- **Double-check screenshots** before sending. Crop or blur anything sensitive.
- **Never paste confidential info into AI tools** unless approved by your company.
- **Use work-approved cloud storage** instead of personal accounts.
- **Set file permissions deliberately**, not by default.

Conclusion

Most data exposure doesn't come from cybercriminal geniuses. Often, risks come from tiny oversights that slip through during a busy day. By staying aware of what you *might* be sharing unintentionally, you strengthen your organization's security in ways that technology can't on its own.

Security isn't just about firewalls and antivirus. It's about everyday awareness — and the small, everyday choices that protect the information we never meant to share.

Security Corner

What Is Piggybacking?
Not all security breaches involve malware, phishing emails, or hacked passwords. Some start with a simple act of courtesy. Piggybacking can be a physical security risk, where an unauthorized person gains access to a restricted area by following someone who does have permission.

How Does Piggybacking Happen?
These threats happen when someone uses another person's access to enter a secured space without proper authorization. Common examples include:

- Holding a secured door open for somebody behind you
- Logging into a system using someone else's credentials
- Allowing a visitor to enter restricted areas without escort
- Remaining logged in on a shared or public device

Why Is Piggybacking So Effective?
Digital piggybacking is especially dangerous because it leaves fewer visible signs. A shared login or can provide access to systems, data, and tools for long periods of time without raising suspicion.

How to Prevent Physical and Digital Piggybacking
Consistent habits help prevent risks to your data. Don't share your badge, usernames, passwords or other access tokens. Lock your devices when you step away from them, even if it's only for a moment. If you use a shared system, then always remember to log out after using it.

Conclusion
From offices to healthcare facilities, data centers, and shared workspaces, piggybacking remains one of the most overlooked ways attackers bypass security controls.

For more information about this topic, call us at 248-362-3800 or visit: **https://tinyurl.com/yu448jbh**

The MFA Level-Up: Why SMS Codes Are No Longer Enough (And What To Use Instead)

For years, enabling Multi-Factor Authentication (MFA) has been a cornerstone of account and device security. While MFA remains essential, the threat landscape has evolved, making some older methods less effective.

The most common form of MFA, four- or six-digit codes sent via SMS, is convenient and familiar, and it's certainly better than relying on passwords alone. However, SMS is an outdated technology, and cybercriminals have developed reliable ways to bypass it. For organizations handling sensitive data, SMS-based MFA is no longer sufficient. It's time to adopt the next generation of phishing-resistant MFA to stay ahead of today's attackers.

Why Phishing-Resistant MFA Is the New Gold Standard

To prevent these attacks, it's essential to remove the human element from authentication by using phishing-resistant MFA. This approach relies on secure cryptographic protocols that tie login attempts to specific domains.

One of the more prominent standards used for such authentication is Fast Identity Online 2 (FIDO2) open standard, that uses passkeys created using public key cryptography linking a specific device to a domain. Even if a user is unknowingly tricked into clicking a phishing link, their authenticator application will not release the credentials because the domain does not match the specific record.

Implementing Hardware Security Keys

Hardware security keys are physical devices resembling a USB drive, which can be plugged into computer or tapped against a mobile device. You simply insert the key into the computer or touch a button, and the key performs a cryptographic handshake with the service. This method is quite secure since there are no codes to type, and attackers can't steal your key over the internet. Unless they physically steal the key, they cannot access your account.

Mobile Authentication Apps and Push Notifications

If physical keys are not feasible, mobile authenticator apps such as Microsoft or Google Authenticator are a step up from SMS MFA. These apps generate codes locally on the device, eliminating the risk of SIM swapping or SMS interception since the codes are not sent over a cellular network.

There are still risks. For example, attackers may flood a user's phone with repeated login approval requests, causing a frustrated or confused user to "approve" just to stop the notifications. Modern authenticator apps address this with "number matching," requiring the user to enter a number shown on their login screen into the app. This ensures the person is physically present at their computer.

Passkeys: The Future of Authentication

Modern systems are embracing passkeys, digital credentials stored on a device and protected by biometrics. Passkeys are phishing-resistant and can be synchronized across your ecosystem, such as iCloud Keychain or Google Password Manager. They offer the security of a hardware key with the convenience of a device that you already carry.

5 Security Layers Your Small Business Is Likely Missing (And How To Add Them)

If your security stack has grown organically over time, these are the gaps that often show up first.

• Phishing-resistant authentication: enforce strong MFA everywhere, then tighten admin and remote access first.

• Device trust and usage policies: define what a compliant device is, and what happens when it isn't.

• Email and user risk controls: reduce exposure by default with filtering, warnings, and easy reporting.

• Continuous vulnerability and patch coverage: measure patch latency and include third-party apps.

• Detection and response readiness: define what gets escalated, document runbooks, and practice containment steps.

• Recovery that's proven: run restore drills and define recovery priorities before you need them.

• Governance that sticks: publish clear "approved" standards and make exceptions time-bound and owned.

When you strengthen these five layers, you turn your business' security into a repeatable, measurable baseline you can be confident in.

"The poster is more aspirational."

The Essential Checklist For Securing Company Laptops At Home

Remote work security gets easier when the basics are standardized. Use this quick checklist as a minimum Baseline for your company:

- Lock the screen every time you step away.
- Store work laptops securely when not in use.
- Don't share work laptops with family members or guests.
- Use strong sign-ins and MFA on work accounts, with no exceptions for admins.
- Patch fast: enable automatic updates and restart when prompted.
- Secure home Wi-Fi like it's part of the office.
- Keep security tools switched on (firewall + endpoint protection).
- Keep work data in approved work storage, not your personal cloud.