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



**August 2024**

**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!"

## Is Your Digital Wallet Protected?

**Introduction**

Digital wallets have revolutionized the way we handle transactions, offering tremendous convenience and efficiency in our increasingly digital world. However, with this convenience comes the need for heightened security measures to safeguard your financial information.

As with any technology, digital wallets come with as many cutting-edge security capabilities as they do risks and pitfalls. Let's shed some light on the evolving landscape of financial technology.

**The Upsides of Digital Wallets**

All digital wallet platforms will employ advanced encryption techniques to secure user data. This effectively scrambles your credentials and financial information into unreadable "tokens" that need your password to unscramble. This ensures that personal and financial information is transmitted and stored securely. Since this process replaces sensitive data with unique tokens, it significantly reduces the risk of data breaches.

Many digital wallets additionally integrate multi-factor authentication requirements, which need you to provide multiple forms of ID before completing a transaction (or accessing any user information). This naturally makes it more challenging for threat actors to break in unauthorized. Typically, these MFA requirements will include a type of biometric authentication, such as fingerprint scans, facial recognition, voice identification, etc. This extra layer of security will significantly reduce the likelihood of unauthorized access.

*Continued on pg.2*

*Continued from pg.1*

If all else fails, remember that you can also turn on alerts for real-time notifications about every transaction made via a digital wallet. Thus, if someone is spending your money without your knowledge and authorization, you will be immediately notified and can take the next steps to secure your account and finances ASAP.

**The Downsides of Digital Wallets**

Unfortunately, the safety of your digital wallet doesn't necessarily rely solely on the technology itself. YOU also play a critical role in protecting your financial assets.

Think about it: The security of digital wallets is inherently tied to the security of the device they are installed on. Therefore, if your device is compromised, it could lead to unauthorized access to the digital wallet and potential financial losses. So, like always, your digital wallet is technically vulnerable to phishing and social engineering attacks. Malicious actors can trick users into providing sensitive information, such as login credentials, by posing as legitimate entities through emails, messages, or fake websites.

Then there is also the issue of standardization. Because all digital wallet providers are not held to one particular service or regulation, security measures can vary widely across all the different suppliers. Inconsistencies in protecting user data is a huge concern if you store multiple wallets on one device! A breach in one can mean a breach of the other, which ultimately puts *all* your financial information at risk.

Ultimately, the regulatory landscape for digital wallets is still evolving, and not all regions have comprehensive guidelines in place. Meanwhile, some users may not be fully aware of the security features available or may not take necessary precautions, leaving them susceptible to security threats. Research different providers before you choose a platform for your digital wallet and stay up to date on how to protect your finances no matter where you store them!

**Conclusion**

Digital wallets have transformed the way that modern society handles and considers our personal finances, by providing a convenient and efficient means of conducting transactions. While many services come with robust security features, it's up to US to remain vigilant and take proactive steps to protect our digital assets.

As the financial technology landscape continues to evolve, we must remain educated about the most prevalent threats to our personal data and hard-earned money. Ultimately, knowledge is the best defense against cybercriminals!

## 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-824/**
**Or Call Our Office At: 248-362-3800**

## Security Corner

**Falling For Financial Scams?**

What are some of the most common financial scams and how you can protect yourself and your money?

**Phishing**
This classic scam involves emails or texts that appear to be from legitimate sources like banks, credit card companies, or even government agencies. They often create a sense of urgency, making you panic thinking that you're being hunted by law enforcement or deeply in debt.

Once they have you, they'll ask you to wire money to their bank account or go to the nearest crypto ATM and send thousands of dollars. No matter how convincing, take a step back; legitimate organizations will NEVER ask you to send money via cryptocurrency, nor any other type of digital payments except through their official online portal.

**Vishing**
A form of phishing, *voice phishing* occurs over the phone. Aggressive calls claiming you owe money can be frightening. Don't give out personal information or agree to pay anything on the spot. Verify the debt with the original creditor directly, and always go through secure portals and legitimate websites.

Here's how you can stay cyber-safe and keep your finances secure!

- **Be skeptical:** If an offer seems too good to be true, it probably is.
- **Don't click on suspicious links:** Links in emails, texts, or social media posts can be gateways to malware or phishing sites.
- **Beware of unsolicited calls and emails:** Never give out personal information over the phone or email unless you are absolutely sure of the caller's or sender's identity.

For more information about financial scams, call us at 248-362-3800 or visit: https://tinyurl.com/mr4an9y8

## Tech Savvy Workspaces: How Technology Drives Office Productivity

Gone are the days of paper-laden desks and rows of filing cabinets. The modern office is a hub of innovation. Technology plays a starring role in this transformation.

Is your company leveraging technology as well as it could? This article dives into the ways technology fuels office productivity.

**Boosting Efficiency: Technology as a Time-Saving Ally**
The core benefit of technology in the office is its ability to save valuable time. Here are some key ways tech can help streamlines workflows:

**Automation Powerhouse**
Automating repetitive tasks frees up your team's time for creative thinking, strategic planning and complex problem-solving.

**Cloud-Based Collaboration:** Cloud storage platforms allow teams to access and share documents seamlessly, ensuring everyone is working on the latest iteration and eliminating frustrations.

**Enhancing Accuracy: Technology Mitigates Errors:** Technology saves time. It also reduces errors that can derail projects and waste valuable resources. Here are some ways you can leverage tech to do this.

**Data Accuracy Champions:** Spreadsheet formulas eliminate the risk of human error in manual data entry. Project management software tracks deadlines and dependencies. These tools provide a single source of truth for project information.

**Fostering Teamwork: Technology Bridges the Communication Gap**
Technology empowers effective communication and collaboration, essential for a productive team environment. Here's how it can do that:

**Remote Work Enablement**
Cloud-based tools and video conferencing apps allow teams to collaborate regardless of location, fostering a diverse workforce.

**Knowledge Sharing Made Easy**
Internal wikis and knowledge sharing platforms allow teams to create a repository of company knowledge.

**Project Management Made Simple**
Collaborative project management tools have many features that ensures everyone is on the same page, ensuring smooth project execution.

**Creating a Tech-Savvy Workspace: Considerations for Implementation**
Successful implementation requires careful consideration:

**Choose the Right Tools:** Choose tools that integrate seamlessly with your systems and workflows.

**Cybersecurity is Paramount:** As your reliance on technology increases, so does the need for robust cybersecurity.

**Change Management.** Prepare to manage change within your team. The extra help getting over road bumps makes a world of difference.

## 6 Important Considerations Before Buying Smart Home Tech

Smart homes seem like something straight out of a sci-fi movie. They have lights that respond to your voice commands and thermostats that auto-adjust. Not to mention robot vacuums that clean your floors while you relax or are away from home.

It's all very tempting. But before you rush out and buy the newest gadget, there are some crucial considerations. Here are 7 essential things to ask yourself before diving headfirst into any new smart home tech.

1. Does it solve a real problem?
2. Is it compatible with other devices?
3. Is your Wi-Fi up to the challenge?
4. Privacy concerns deserve attention
5. Security matters: Protect your smart home
6. Start small and scale up

## Essential Security Practices For Remote Workers

The rise of remote work has redefined the modern workplace. Gone are the days of rigid office schedules and long commutes. With this flexibility comes a new set of cybersecurity threats.

Here are some essential security practices for remote teams. You'll learn how to keep company data safe and secure, no matter your location.

- Secure your home Wi-Fi network
- Use strong, unique passwords for all accounts
- Protect devices with updates & anti-malware
- Use safe browsing practices
- Engage in cybersecurity awareness training

## AI Data Breaches Are Rising– Here Is How To Protect Your Company

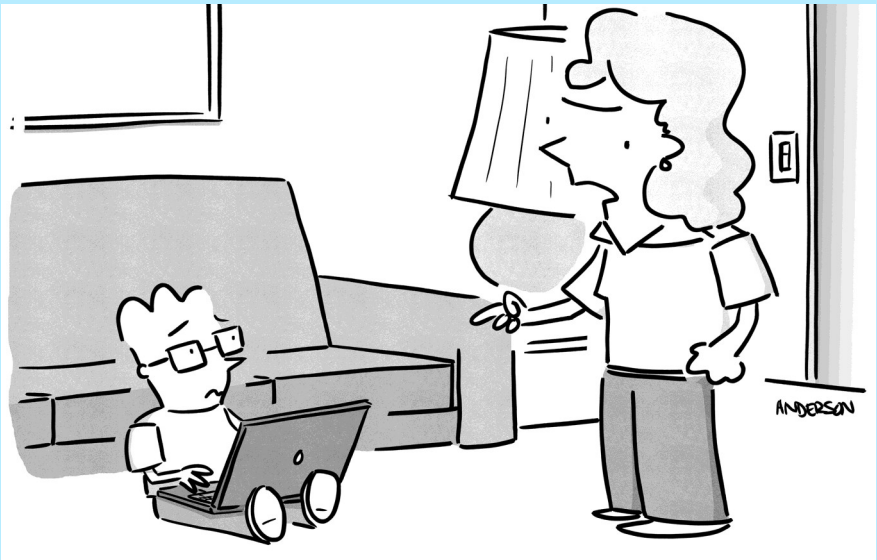
AI is rapidly transforming industries. It offers businesses innovative solutions and automation capabilities. But with this progress comes a growing concern: AI data breaches.

A recent study on AI security breaches found that in the last year, 77% of businesses have experienced a breach of their AI. This poses a significant threat to organizations.

The good news is that there are steps you can take to mitigate your risk:

- Data Governance
- Security by Design
- Threat Modeling
- Employee Training
- Security Patch Management
- Security Testing

**Stay Informed.** Keep yourself updated on the latest AI security threats by subscribing to reliable publications and seeking out workshops on AI and security.




"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back