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

July 2025

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!"

What to Do If Your System Is Infected

Do you think a cyberattack could NEVER happen to you? In today's digital age, the threat of a system infection is actually a serious concern….for everybody.

Whether it's through malware, ransomware, or other malicious software, an infected system can lead to significant consequences.

The Dangers of Infected Systems

In 2024, data breaches reached a record high with over 1.5B records exposed. It's only a matter of time until your data is targeted too. If your system is compromised, you could be exposed to several key risks.

1. Loss or Damage of Files
   - One of the immediate impacts of a system infection is the potential loss, damage, or theft of your files. Important documents, photos, and other data can be corrupted or erased, leading to irreversible loss.
   - For example, in 2024, the BlackCat ansomware attack targeted several organizations, encrypting their files and demanding hefty ransoms for encryption keys.
2. Network Vulnerability
   - Hackers can exploit devices connected to the same network as the infected system. This means that not only is your device at risk, but any other devices sharing the network can also be compromised, leading to a broader security breach.

Continued on pg.2

Continued from pg.1

- A notable example from 2024 is the Emotet malware resurgence, which spread through phishing emails and compromised entire networks.

3. Exposure of Personal Information
   - Your Personally Identifiable Information (PII) can end up on the Dark Web. This includes sensitive data such as your social security number, credit card information, and other personal details that can be used for identity theft and other malicious activities.
   - The MOVEit Transfer data breach in 2024 exposed the personal information of millions of users, leading to significant risks of identity theft.

Infected systems are the foundation of cybercrime. It's the first step in their attack. First hackers exploit your device, then they started stealing data and planting malware.

How to Protect Your System

In 2024, ransomware attacks increased by 20% compared to the previous year, with over 70% of businesses reporting being targeted. To mitigate this and all other risks, it's crucial to take proactive steps toward protecting your systems!

- Install Reliable Antivirus Software: Ensure you have up-to-date antivirus software that can detect and remove threats.
- Regular Backups: Save your important files to an external drive or cloud storage, so you can retrieve copies if your data is lost or manipulated.
- Secure Your Network: Create strong, complex passwords and use encrypted networks to prevent unauthorized access and eavesdropping on privileged communications.
- Stay Informed: Learn about changes in the cyber-threat landscape and how to keep yourself safe online.

Conclusion

The average cost of a data breach in 2024 was estimated at $4.35M. Save yourself the money AND headache.

By staying vigilant and taking these precautions, you can significantly reduce the risk of your system becoming infected, thereby protecting your valuable data and personal information. Protecting your devices means protecting your PII.

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-725/
Or Call Our Office At: 248-362-3800

Security Corner

Are You Posting Too Much Information to Social Media?

How many social media profiles do you have right now? How often do you post on each of these pages?

With phones always in hand and the internet constantly abuzz, sharing moments from our daily lives on social media has become second nature. Unfortunately, constantly revealing our favorite hangout spots and activities can actually open the door to serious risks.

More Than Just a Post
Even the most seemingly innocent details, like your favorite hangout spots, pet's name, or birthday, can be used to craft convincing phishing scams or guess your passwords and security questions. Cybercriminals often piece together information from multiple posts to impersonate you or deceive your contacts into sending them money.

When Social Media Impacts Physical Safety
The risks involved in posting too much online stretch beyond the digital realm. Announcing your location in real time ("Just landed in Cancun!") can let unwanted visitors know when your house is empty. Burglars seek out easy victims with learnable routines.

To protect yourself, consider adopting a more cautious approach to social media!

- Avoid real-time location sharing. Post about your experiences after the fact
- Limit personal details. Refrain from sharing sensitive information like your address, travel plans, or answers to common security questions.

For more information about social media posting, call us at 248-362-3800 or visit: https://tinyurl.com/mr7hm8ek

Beyond The Password: Small Business Guide To Implementing Multi-Factor Authentication (MFA)

According to recent reports, nearly 43% of cyberattacks target small businesses, often exploiting weak security measures.

One of the most overlooked yet highly effective ways to protect your company is through Multi- Factor Authentication (MFA). This extra layer of security makes it significantly harder for hackers to gain access, even if they have your password.

What is Multi-Factor Authentication?

Multi Factor Authentication (MFA) is a security process that requires users to provide two or more distinct factors when logging into an account or system. The factors are something you know (like a password or PIN), something you have (like a mobile phone or smart card), and something you are (like fingerprints or facial recognition).

How to Implement Multi-Factor Authentication in Your Business

Implementing Multi-Factor Authentication (MFA) is an important step toward enhancing your business' security. While it may seem like a complex process, it's actually more manageable than it appears, especially when broken down into clear steps. Below is a simple guide to help you get started with MFA implementation in your business:

- **Assess Your Current Security Infrastructure.** Conduct a thorough review of your existing security systems and identify which accounts, applications, and systems need MFA the most. Prioritize the most sensitive areas of your business.
- **Choose the Right MFA Solution.** Choosing the right one for your business depends on your size, needs, and budget. Some popular options that can cater to small businesses include:
  - Google Authenticator
  - Duo Security
  - Okta
  - Authy

When selecting an MFA provider, consider factors like ease of use, cost-effectiveness, and scalability as your business grows.

- **Implement MFA Across All Critical Systems.** Once you've chosen an MFA provider, it's time to implement it across your business. Here are the steps to take:

  Step 1: Set Up MFA for Your Core Applications: Prioritize applications that store or access sensitive information, such as email platforms, file storage, etc.

  Step 2. Enable MFA for Your Team: Make MFA mandatory for all employees, ensuring it's used across all accounts.

  Step 3. Provide Training and Support: Offer clear instructions and training on how to set it up and use it.

  Step 4. Test Your MFA System Regularly. After implementation, it's essential to test your MFA system regularly to ensure it's functioning properly. Periodic testing allows you to spot any vulnerabilities, resolve potential issues, and ensure all employees are following best practices.

If you're ready to take your business's security to the next level, or if you need help implementing MFA, feel free to contact us. We're here to help you secure your business and protect what matters most.

Common Pitfalls When Choosing Cloud Storage

- **Ignoring Security and Compliance Requirements:** Always evaluate a provider's security certifications and data encryption methods.
- **Choosing Based on Price Alone:** Weigh costs against features, customer support, and the ability to grow with your business.
- **Overlooking Integration with Existing Tools:** Ensure the cloud storage solution integrates seamlessly with your current ecosystem.
- **Underestimating Scalability Needs:** Look for storage providers that offer flexible plans, tiered storage, and enterprise-ready infrastructure.
- **Neglecting Backup and Redundancy:** Storing data in the cloud doesn't automatically mean it's backed up. Look for providers with built-in backup and redundancy features.

Simple And Effective Backup And Recovery Plan

Every business runs on data: customer information, financial records, communications, product files, and more. Yet data security is often in the bottom of the to-do list.

Unsure where to start? Here are simple, effective backup and recovery plans that every small business can use:

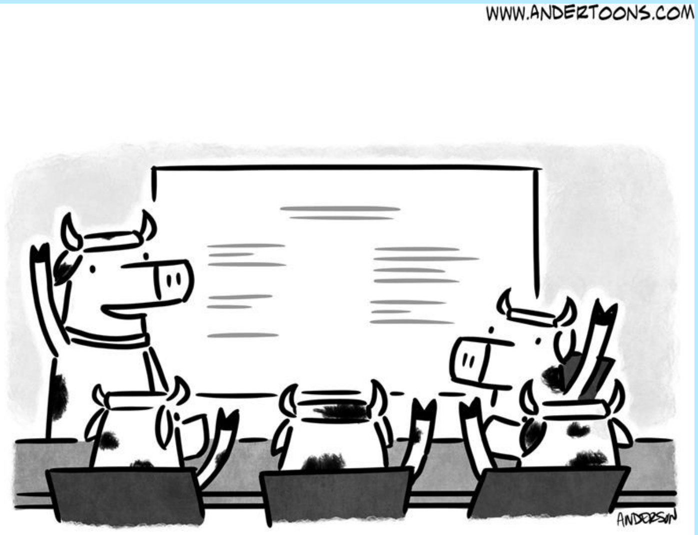
1. Know Your Storage Limits
2. Use a Cloud Service
3. Automate Your Backup Schedule
4. Test Your Recovery Plan
5. Keep a Local Backup for Fast Access
6. Educate Your Team
7. Keep Multiple Backup Versions
8. Monitor and Maintain Your Backups
9. Consider a Hybrid Backup Strategy

Advanced Remote Work Security Strategies

A secure remote workplace in 2025 is not defined by perimeter defenses. It's layered, intelligent, and adaptable systems. Here are some critical upgrades and strategic shifts your business should adopt now to keep your remote team secure.

- Embrace Zero Trust Architecture
- Deploy Endpoint Detection and Response (EDR) Solutions
- Strengthen Secure Access with VPN
- Cultivate a Security-First Culture
- Implement Data Loss Prevention (DLP) Measures
- Use Automation and AI for Faster, Smarter Threat Response
- Run Regular Security Reviews and Simulations.

These advanced tactics not only keep your systems safe but also ensure business continuity, regulatory compliance, and peace of mind.



"Another unanimous vote! Man I love the herd mentality!"