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

September 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!"

Why You Should Never Pay A Ransomware Fee

How much do you really know about ransomware?

It's one of the most rampant threats to our private data today, and the damage to our systems can be catastrophic if we don't have the proper cyber-defenses in place. Secure and reliable backup systems can be integral to recovering from such an attack.

Unfortunately, the threat of damage, loss, or theft of your data can cause people to act without thinking. So, while you may have learned how to spot and avoid ransomware attacks, or what to do when your data is illegally encrypted, how much do you really know about why you shouldn't pay those ransom fees?

How Ransomware Steals Your Money

First, let's delve a little bit into how hackers use this malware to steal your data and then extort you for money.

These threat actors either trick you with social engineering or hack their way directly into your systems. Once inside your network, they find your most lucrative files like personally identifiable information or confidential records. By stealing and encrypting your data, these hackers effectively scramble your files into unreadable tokens that you need their special decryption key to unlock.

Continued on pg.2

Continued from pg.1

This is where good backups come in. If you have reputable storage systems that you regularly check for functionality, you should be able to restore the most recent versions of your data from the backup database. Unfortunately, without a reliable way to gain back data, some people can feel pressured into paying the ransom, *which averages to about $2M per attack.*

Whether or not you pay the fee, the threat actor is likely to charge a double extortion fee to stop them from releasing your private data to the public or selling it on the Dark Web.

Why You Shouldn't Pay the Ransom

Remember, you have no guarantee that the threat actor will follow through on their word. It's pretty safe to assume that a criminal that's stolen your data isn't trustworthy!

Even when companies pay the hacker to decrypt and restore their data, 92% of organizations still can't restore all of their data. Whether you pay the double extortion fee too, they could and likely will still sell your information on the dark web.

No matter how much you give them, bad actors that attack with ransomware are most likely to run off with your data and money!

In good news, society is becoming better at warding off ransomware. According to the latest research, more than 70% of ransomware targets don't pay the ransom — and yes, that's good news! That means we're learning that paying these fees only causes more problems.

Conclusion

Studies indicate that there are about 1.7M ransomware attacks every day. Even the most introductory-level threat actor can buy full-service malware kits on the Dark Web to weaponize against you!

The widespread proliferation of these dangerous cyber-threats is the very reason that we need to hone our security awareness and learn best practices for incident response!

While we can't stop every threat, we can avoid paying high fees and minimize the overall risk to our systems post-breach. By ensuring our backup systems are ready to jump in and save us, and by not paying the very ransomware hackers who threaten and steal from us, we can better protect our financial and digital safety!

Free Executive Guide Download: The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim your FREE copy today at
https://www.cti-mi.com/itbuyersguide-925/

Security Corner

What Are The Risks to Your Cloud Data?

Cloud storage provides robust backup and recovery options, securing data so that you can restore files, even in the case of hardware failure or other types of disasters.

While remote storage protects your data from physical attacks or damage, your cloud data can also be hacked.

How Do Hackers Exploit Cloud Storage?

Some common ways that threat actors can compromise cloud data include:

- Weak or reused passwords. Attackers can exploit weak or reused passwords through brute force attacks or phishing scams.
- Data breaches. Even with strong security measures, people still fall victim to data breaches that expose sensitive information.

Protecting Your Cloud Data

To best safeguard your files, you should understand and implement some of these best practices for cloud data security.

Your cloud data storage should include encryption services, which scrambles your data into unreadable tokens without the login.

You should also implement multi-factor authentication when you login to reduce the risk of unauthorized access by cyber criminals.

By following these practices, you can significantly enhance the security of your cloud data.

For more information about cloud data storage, call us at 248-362-3800 or visit: https://tinyurl.com/njsn9hc3

Is Your Smart Office A Security Risk? What Small Businesses Need To Know About IoT

Your office thermostat, conference room speaker, and smart badge reader are convenient, but they're also doors into your network. With more devices than ever in play, keeping track can be tough, and it only takes one weak link to put your entire system at risk.

Here's a practical guide designed for small teams getting ready to work with connected tech.

Steps To Manage IoT Security Risks for Small Businesses

Know What You've Got

- Walk through the office and note each gadget.
- Record model names and who uses them

Change Default Passwords Immediately

- Change every password to something strong and unique
- Store passwords securely where your team can consistently access them

Segment Your Network

- Create separate Wi-Fi or VLAN sections for IoT gear
- Block IoT devices from accessing sensitive servers
- Use guest networks where possible

Keep Firmware and Software Updated

- Check for updates monthly
- Automate updates when possible
- Replace devices that are no longer supported

Set Up a Response Plan

- Who to contact when devices act weird
- How you'll isolate a problematic device

Limit What Each Device Can Do

- Turn off unused features and remote access
- Block internet access where not needed
- Restrict device functions to exact roles only

Watch for Devices That Creep In

- Have a simple approval step for new devices
- Ask questions: "Does it need office Wi-Fi? Does it store data?"
- Reject or block any gear that can't be secured

Encrypt Sensitive Data

- Check device settings for encryption options
- Use encrypted storage systems on your network

Reevaluate Regularly

- Reassess passwords, network segments, and firmware
- Replace devices that don't meet today's standards

Why This Actually Matters

Smart devices simplify work but can pose risks if not properly secured. More businesses are experiencing cyberattacks through their IoT devices than ever before, and these attacks are rising rapidly.

Protecting your systems isn't about expensive high-tech solutions; it's about taking simple, smart steps.

These simple steps can protect your business without getting in the way. Plus, with the right IT support, staying ahead of threats is simpler than you might expect.

Your Office Is Smart, Your Security Should Be Too

With the right IT partner who understands the unique challenges small businesses face, you can take steps to protect what matters.

Ready to get serious about IoT security? Contact us today and partner with a team that protects small offices, without the big-business complexity.

4 Simple Ways To Keep Your Business Data Clean

Data is everywhere, and if you are not utilizing it to your advantage, you are missing out. It is found in emails, customer profiles, inventory systems, or basically throughout your entire workflow. But relying on outdated or inaccurate information can lead to confusion, slow down your team, and ultimately cost you a lot of money.

Follow these simple steps to help you keep everything clean and running smoothly.

1. Decide What Info Actually Matters: Identify the key data that keeps your business running smoothly, like customer contacts, order details, or payment terms. Then, create simple guidelines your team can easily follow.

2. Show Your Team the Right Way to Do It: Most data errors occur when people aren't sure what's expected of them. Rather than overwhelming your team with lengthy manuals, provide a simple, clear guide. It makes a big difference in maintaining consistency.

3. Tidy Things Up Often: Don't wait too long to clean up your data. A quick monthly review helps you spot duplicates, fix mistakes, and update old info before it creates bigger issues.

4. Keep Your Documentation Updated: Things change fast with new systems, tools, and teams. That's why it helps to keep a simple note on where your data comes from, who handles it, and how it should be used.

6 Smart Tips To Boost Your WiFi

1. Upgrade Your Hardware: Invest in equipment that can handle today's demands and grow with you down the line.

2. Give Priority to What Matters Most: Prioritize important traffic like video and phone calls.

3. Divide Your Networks: By dividing your network into segments, you reduce congestion and boost security.

4. Balance Server Load: Shared workload across servers keeps systems running smoothly during busy times.

5. Watch for Threats Before They Slow You Down: Keep an eye out for unusual activity that might be slowing down your network.

6. Build in a Backup Plan: Having a backup internet connection means your team can keep working.