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 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 Life Encrypted?

Introduction

Imagine you have a secret message you want to send to your friend, but don't want anyone else to read it. If they have the "key" to reading it, then only the intended recipient can decipher what you are you are trying to say.

Encryption is like that secret code you and your friend create to lock the message, making it look like gibberish to anyone else who finds it. Instead of coming up with your own secret codes, though, technology scrambles data into unreadable "tokens" to keep YOUR data safer.

What Is Encryption

Your original message, called "plaintext," gets transformed into a confusing mess, known as "ciphertext." Think of it as replacing each letter with a symbol or number based on a secret code.

This scrambling happens using complex math algorithms. Just like a physical lock needs a key, unlocking the encrypted message requires a special "decryption key." This key is like the password to your secret code, and only you and your friend (or authorized recipient) have it.

The recipient uses the decryption key to unscramble the ciphertext back into the original plaintext message. Voila! They can now read your secret message!

Why Do We Rely on Encryption

When do you encounter encryption techniques? Probably more often than you think!

Continued from pg.1

Encryption is hidden behind the scenes in many everyday activities, from the websites you visit to the messaging apps that you use.

When you see “https” in your browser address bar, it means the website is using *encryption* to protect your information like passwords and credit card details. That S at the end stands for *secure*, and that means that your device’s communication with that website has a Secure Sockets Layer (SSL) Certificate. That means the data that you enter into that site is scrambled and safe.

Many digital communication platforms rely on encryption, too! Your messaging apps use it to keep your conversations private, like WhatsApp and Signal. ***End-to-end encryption*** adds even more security, by securing your communications in transit and when it gets to the recipient’s device. All of this keeps your conversations more private!

Some email services even offer encryption options, which is very important professionally and for transmitting *personally identifiable information* (PII). Rental application needs to check your credit history? Send the information securely. New job needs your Social Security Number? Make sure the communication is encrypted!

Conclusion

Encryption plays a crucial role in protecting our privacy and security in the digital world. By scrambling data, it makes it much harder for hackers and other unauthorized individuals to steal or misuse our information. For additional security, consider a VPN. **Virtual Private Networks** use encryption to create a secure tunnel for your internet traffic, protecting your online activity from prying eyes.

So, the next time you see “https” or use a secure messaging app, remember the invisible encryption shield working in the background to keep your information safe!

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

IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

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-924/

Security Corner

Don't Text Back To A Pretext!

62% of the world's population is texting on a regular basis.

While that comes with convenience (and cyber-risks) of its own, it's not just *texting* that you have to worry about…it's ***pretexting!***

What is Pretexting?

Pretexting is a deceptive practice where individuals or entities obtain sensitive information from unsuspecting victims by pretending to be someone they are not. This fraudulent tactic is often employed to gain access to personal financial information.

By impersonating trusted entities like bank representatives, scammers can manipulate individuals into divulging confidential details such as account numbers, Social Security numbers, and login information.

Protecting Ourselves from Pretexts

To combat pretexting, financial institutions have implemented robust security measures, including employee training, advanced authentication systems, and data encryption. The evolving nature of these scams, however, necessitates ongoing vigilance and adaptation by both financial institutions and consumers to stay ahead of cybercriminals.

Conclusion

Pretexting is coming back in style. This year has shown twice the influx of pretexting attacks than last year, and we know that cyber-attackers are getting smarter with how they use our social media to learn about our daily habits—which makes us easier targets for scams like pretexting.

For more information about pretexting, call us at 248-362-3800 or visit: https://tinyurl.com/3dwjhyx4

Windows 10: The Final Countdown– It's Time To Upgrade Your PC

Windows 10 has served us well. But its time is running out. Microsoft plans to end support for Windows 10 on October 14, 2025. This means no more security updates, patches, or support.

It's time to upgrade to Windows 11. This is especially true for business users with many systems to check and upgrade. This change isn't just about getting new features. It's about ensuring your PC stays secure, fast, and capable.

Why You Need to Upgrade Now

- **Security Concerns:** No more updates mean no more security patches. Upgrading to Windows 11 ensures you are always receiving the latest security updates
- **Enhanced Performance:** Windows 11 is designed to be faster and more efficient. It optimizes your hardware, providing better performance.
- **Improved Features:** The redesigned Start Menu and Taskbar offer a fresh, modern look. Snap Layouts and Snap Groups help you organize your workspace. Virtual Desktops allow you to create different desktops for different tasks. These enhance productivity and make your PC experience more enjoyable.

Benefits of Upgrading to Windows 11

- **Better User Interface:** Windows 11 offers a cleaner UI with a simplified Taskbar.
- **Improved Multitasking:** You can easily organize open windows, switch between tasks and create separate desktops.
- **Integrated Microsoft Teams:** Quickly start a chat or video call directly from the Taskbar.

What Are the Risks of Waiting to Upgrade?

- **Increased Vulnerability**: Waiting to upgrade increases your vulnerability. As the end-of-support date approaches, the risk of security threats grows. Upgrading now minimizes this risk.
- **Potential Compatibility Issues**: New applications and updates may not be compatible. By upgrading now, you ensure compatibility with the latest software.
- **Business Disruption**: Starting an upgrade for your office now gives time for a smooth rollout.

How to Upgrade

- **Check Compatibility:** Check if your PC meets the requirements using the PC Health Check tool.
- **Backup Your Data:** Avoid losing important files during the upgrade process.
- **Follow Upgrade Instructions:** This may involve downloading the installation file and running the setup.
- **Seek Professional Help:** If you're unsure about upgrading, seek the help of tech experts.

The countdown to the end of Windows 10 has begun. Ensure your PC stays protected and up to date. Don't wait until the last minute!

Unmasking The True Price Of IT Downtime

Imagine this: you walk into your office on a busy Monday morning, ready to tackle the week. But something's wrong. Computers are unresponsive. Phones are silent. The internet is a ghost town. Your business has come to a grinding halt – victim of an IT outage.

It's a scenario every business owner fears. But beyond the initial frustration are expenses you may not immediately see. IT downtime carries hidden costs that can significantly impact your bottom line. Let's peel back the layers and expose the true price of IT outages.

The Immediate Impact: Lost Productivity

When IT systems go down, your employees are effectively sidelined. Sales can't be processed. Emails pile up.

Customer Impact: Frustration and Lost Trust

An IT outage isn't just an internal inconvenience. It directly impacts your customers. Frustrated customers can't place orders or access their accounts.

Reputational Damage: A Hit to Your Brand Image

IT outages can tarnish your brand image. Customers expect businesses to be reliable and readily accessible.

Hidden Costs: Beyond the Obvious

The financial impact of IT downtime extends beyond lost productivity and sales. It includes:

- Employee Demoralization
- Emergency Repairs
- Data Loss or Corruption
- Compliance Issues

SPEAK THE MAGIC WORDS TO ENTER
FORGOT YOUR MAGIC WORDS? SAY YOUR EMAIL
ANDERSON

Investing in Uptime: Building Business Resilience

IT downtime is a threat every business faces. By knowing the true cost and taking proactive measures, you can significantly reduce the risk.

8 Tips For Safeguarding Your Gadgets While Traveling

Traveling with technology has become a necessity. Whether for work, communication, or entertainment, we rely heavily on our devices. But traveling exposes these gadgets to various risks. Theft, damage, and loss are common concerns.

We've put together some helpful tips to mitigate the risk of any tech mishaps on your next trip.

1. Use Protective Cases
2. Leverage Tracking Apps
3. Keep Devices Close
4. Use Strong Passwords
5. Be Cautious with Public Wi-Fi
6. Back Up Your Data
7. Be Mindful of Your Surroundings
8. Use Anti-Theft Accessories