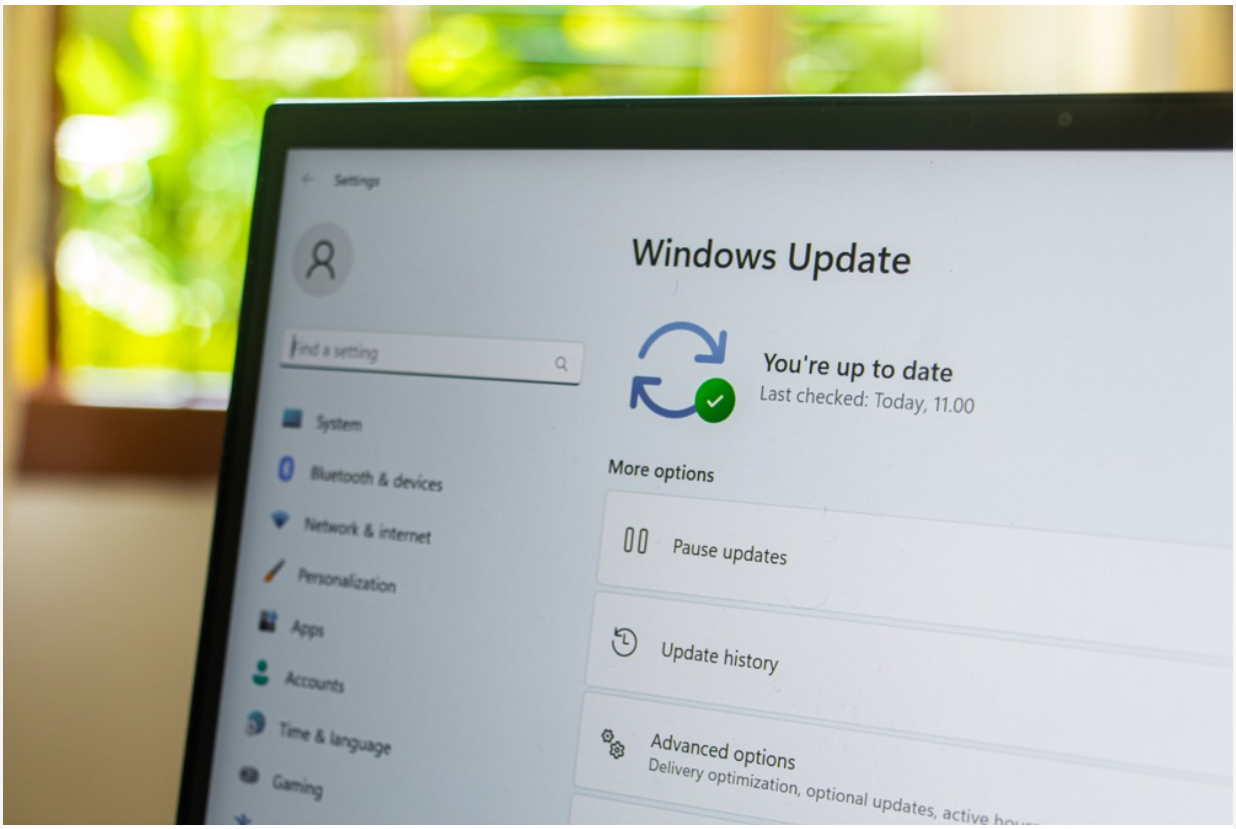
TECHNICAL FRAMEWORK
MANAGED IT & CYBERSECURITY

(970) 372-4940
info@techframework.com
https://techframework.com



Watch Out for Ransomware Pretending to Be a Windows Update!

TECH INSIDER
November 2023

Corporate

- Watch Out for Ransomware Pretending to Be a Windows Update!
- What is Microsoft Sales Copilot & What Does It Do?
- 10 Biggest Cybersecurity Mistakes of Small Companies
- Sustainable Tech Habits That Are a Win for Your Bottom Line
- Secure by Design Cybersecurity Practices

Personal & Home-Office

- TickTime Cube
- Keep Your Smart Home From Turning Against You

Websites

- 6 Reasons Why Website Maintenance is Important

CORPORATE

Watch Out for Ransomware Pretending to Be a Windows Update!

Imagine you're working away on your PC and see a Windows update prompt. Instead of ignoring it, you take action. But when you install what you think is a legitimate update, you're infected with ransomware.

Cybercriminals are constantly devising new ways to infiltrate systems. They encrypt valuable data, leaving victims with difficult choices. One such variant that has emerged recently is the "Big Head" ransomware.

The Big Head Ransomware Deception

Big Head ransomware presents victims with a convincing and fake Windows update alert. Attackers design this fake alert to trick users. They think that their computer is undergoing a legitimate Windows update. The message may appear in a pop-up window or as a notification. The deception goes even further.

The ransomware uses a forged Microsoft digital signature. The attack fools the victim into thinking it's a legitimate Windows update. They then unknowingly download and execute the ransomware onto their system. From there, the ransomware proceeds to encrypt the victim's files. Victims see a message demanding a ransom payment in exchange for the decryption key.

Here are some strategies to safeguard yourself from ransomware attacks like Big Head:

Keep Software and Systems Updated

Big Head ransomware leverages the appearance of Windows updates. One way to be sure you're installing a real update is to automate.

Verify the Authenticity of Update

Genuine Windows updates will come directly from Microsoft's official

Use an external storage device or a secure cloud backup service. Backups of your data can allow you to restore your files without paying a ransom.

Use Robust Security Software

Install reputable antivirus and anti-malware software on your computer.

Educate Yourself and Others

Stay informed about the latest ransomware threats and tactics. Educate yourself and your colleagues or family members.

Use Email Security Measures

Put in place robust email security measures. Be cautious about opening email attachments or clicking on links.

Enable Firewall and Network Security

Activate your computer's firewall. Use network security solutions to prevent unauthorized access to your network and devices.

Disable Auto-Run Features

Configure your computer to disable auto-run functionality for external drives.

Be Wary of Pop-Up Alerts

Exercise caution when encountering pop-up alerts especially those that ask you to download or install software. Verify the legitimacy of such alerts before taking any action.

Keep an Eye on Your System

Keep an eye on your computer's performance and any unusual activity. If you notice anything suspicious, investigate immediately.

Have a Response Plan

In the unfortunate event of a

website or through your IT service provider or Windows Update settings.

Backup Your Data

Regularly back up your important files.

ransomware attack, have a response plan in place. Know how to disconnect from the network. Report the incident to your IT department or a cybersecurity professional. Avoid paying the ransom if possible.

PERSONAL & HOME-OFFICE

TickTime Cube

The Ticktime cube is a digital countdown timer that's as easy to use as a light switch. It's a stylish, user-friendly gadget that helps you manage your time to help boost your efficiency and productivity.

It's perfect for any tasks that needs a timer. It also comes in a variety of cool colors to match your style or mood.

Get yours at https://www.ticktime.store/

PERSONAL & HOME-OFFICE

Keep Your Smart Home From Turning Against You

Smart homes offer unparalleled convenience and efficiency. But as we embrace the convenience, it's essential to consider the potential risks.

Recent headlines have shed light on the vulnerabilities of smart home technology. Such as the story in the New York Post's article titled "Locked Out & Hacked: When Smart Homes Turn on Owners."

The article describes smart home nightmares. Including the new owner of a smart home that unexpectedly got locked in. The prior owner had left
preprogrammed settings. Suddenly at 11:30 p.m., the home told him it was time to go to bed and locked every door in the house.

Another technology victim was a woman terrorized by lights and sounds at home. Her ex-partner was maliciously manipulating the smart technology.

As homes get smarter, how can you avoid a similar experience? We'll

4. Regularly Update Firmware – Firmware updates are essential for fixing security vulnerabilities in your smart devices. Make it a habit to check and apply firmware updates regularly.

5. Vet Your Devices – Look for products that have a history of prompt updates and robust security features. Avoid purchasing devices from obscure or untrusted brands.

6. Isolate Sensitive Devices – Consider segregating your most sensitive devices onto a separate network, if possible.

7. Review App Permissions – Smart home apps often request access to various permissions on your devices. Before granting these, scrutinize what data the app is trying to access.

8. Be Cautious with Voice Assistants – Review your voice assistant's privacy settings. Be cautious about what information you share with them.

explore some key strategies to protect your home and your privacy.

Smart Home Safety Tips You Need to Use

1. Secure Your Network – The foundation of any smart home is its network. Just as you wouldn't leave your front door wide open, you shouldn't neglect Wi-Fi security.

2. Strengthen Device Passwords – Avoid using easily guessable information like "123456" or "password." Use a combination of upper and lower-case letters, numbers, and symbols.

3. Enable Two-Factor Authentication (2FA) – Many smart home device manufacturers offer 2FA as an extra layer of security. This helps keep unwanted people out.

9. Check Your Devices Regularly – Regularly check the status and activity of your smart devices. Look for any unusual behavior.

10. Understand Your Device's Data Usage – Review your smart device's privacy policy. Understand how it uses your data.

11. Stay Informed – Finally, stay informed about the latest developments in smart home security. Subscribe to security newsletters.

WEBSITES

6 Reasons Why Website Maintenance is Important

Maintaining a website is crucial for several reasons:

1. Security: Regular maintenance helps protect a website from cyber threats like hacking, malware, and viruses. Keeping software and plugins updated is essential for closing security vulnerabilities.

2. Performance Optimization: Regular updates and checks can improve the speed and efficiency of your website. This includes optimizing images, updating code, and ensuring that all elements of the site are functioning as intended.

3. Search Engine Optimization (SEO): Search engines favor websites that are regularly updated with fresh content. Regular maintenance can also ensure that SEO practices are up to date, which can improve your site's visibility and ranking.

4. User Experience: A well-maintained website offers a better user experience. Broken links, outdated content, and slow loading times can frustrate users and drive them away.

5. Data Backup: Regular backups are a critical part of website maintenance. They ensure that in the event of a problem, such as data loss or a cyber-attack, you can restore your website to its previous state.

6. Keeping Up with Trends: The digital landscape is constantly evolving. Regular maintenance allows you to implement new technologies, design trends, and user preferences, ensuring that your website remains modern and relevant.

Contact us today to learn more about our website maintenance services.

CONTACT US

CORPORATE

What is Microsoft Sales Copilot & What Does It Do?

Microsoft is a pioneer in the tech industry and this new AI era. Its newest innovation is Microsoft Sales Copilot.

It represents a significant leap forward in leveraging AI and machine learning. It's designed specifically to enhance sales processes and customer engagement.

This groundbreaking tool is built on the foundation of Dynamics 365 Customer Insights. This is Microsoft's platform for unifying customer data and delivering actionable insights.

WHAT CAN MICROSOFT SALES COPILOT DO?

Personalized Customer Insights

Personalized customer insights is one of the core features of Microsoft Sales Copilot. It analyzes a wide range of data sources. This includes:

- Customer behavior
- Buying history
- Customer interactions

By aggregating and processing this data, Sales Copilot saves salespeople time.

AI-Driven Recommendations

The tool can suggest things like:

- The most appropriate communication channels
- Timing for follow-ups
- Tailored, client-specific content recommendations

Enhanced Collaboration

Sales Copilot improves collaboration among team members. It keeps sales teams aligned in the approach to engaging with customers.

Predictive Analytics

The tool analyzes historical data and customer behavior patterns. This allows it to predict future customer actions and trends.

Seamless Integration

Sales Copilot seamlessly integrates with other Microsoft tools and services. This creates a unified ecosystem. This integration allows for a smooth flow of data between applications.

CORPORATE

10 Biggest Cybersecurity

CORPORATE

Sustainable Tech Habits

Mistakes of Small Companies

Cybercriminals can launch very sophisticated attacks. But it's often lax cybersecurity practices that enable most breaches.

Small business owners often don't prioritize cybersecurity measures. They may be just fully focused on growing the company.

Below are some of the biggest reasons small businesses fall victim to cyberattacks.

1. Underestimating the threat
2. Neglecting employee training
3. Using weak passwords
4. Ignoring software updates
5. Lacking a data backup plan
6. No formal security policies
7. Ignoring mobile security
8. Failing to regularly watch networks
9. No Incident Response Plan
10. Thinking they don't need Managed IT Services

That Are a Win for Your Bottom Line

Below are several sustainable tech habits you can adopt:

- Energy-efficient hardware and appliances
- Virtualization and cloud computing
- Remote work and telecommuting
- Renewable energy sources
- E-waste recycling programs
- Optimize data centers
- Green web hosting
- Paperless office
- Eco-friendly office supplies
- Software optimization
- Remote monitoring and control
- Green transportation policies
- Sustainable data practices
- Green IT certification
- Employee education and engagement
- Supply chain sustainability
- Lifecycle assessments
- Green marketing

CORPORATE

Secure by Design Cybersecurity Practices

Cybersecurity has become a critical foundation upon which many aspects of business rely. The frequency and sophistication of cyberattacks continue to increase. It's essential to shift from a reactive to a proactive cybersecurity approach, such as "**Secure by Design**."

Secure by Design integrates security measures into the very foundation of a system, app, or device. It does this from the start. It's about considering security as a fundamental aspect of the development process.

Key principles of Secure by Design include:

- Risk Assessment
- Standard Framework
- Least Privilege
- Defense in Depth
- Regular Updates
- User Education

Why Secure-by-Design Matters?

- Proactive Security
- Cost Savings
- Regulatory Compliance
- Reputation Management
- Future-Proofing
- Minimizing Attack Surfaces


Technical Framework
maintains an A+ rating
with the BBB
A+
BBB

FORT COLLINS AREA
CHAMBER
OF COMMERCE

GREELEY AREA
CHAMBER OF
COMMERCE