

# TECH TALK

## MONTHLY

YOUR MONTHLY DOSE OF  
TECH & BUSINESS NEWS

### WHAT'S INSIDE?

- 02** WATCH OUT FOR RANSOMWARE PRETENDING TO BE A WINDOWS UPDATE!
- 03** SMART HOME SAFETY TIPS
- 04** WHAT IS MICROSOFT SALES COPILOT?
- 05** BIGGEST CYBERSECURITY MISTAKES
- 06** TECH TIP OF THE MONTH
- 07** "SECURE BY DESIGN" CYBERSECURITY PRACTICES



### Monthly update from Mark

As businesses increasingly rely on Software as a Service (SaaS) applications, the critical topic of cloud security takes center stage. There is a shared responsibility between account owners and cloud providers in safeguarding your SaaS apps. Many small businesses miss this key point.

The dynamic nature of cloud computing often blurs the lines of responsibility when it comes to protecting your cloud assets. Understanding the shared responsibilities between your organization and your chosen cloud provider is paramount to fortifying your digital fortress.

In a data-driven world, robust security is paramount. Need some help securing your cloud tools? Reach out to us at [mark@phrixus.com](mailto:mark@phrixus.com) to schedule a chat.

Until then, stay safe,

### DID YOU KNOW?

The name "Google" originated from a misspelling of "googol" which is a number equivalent to ten raised to the power of a hundred; a number so large that our minds can't even comprehend it.

### Phrixus Technologies

PO Box 266  
Berowra NSW 2081  
[phrixus.com](http://phrixus.com)  
02 9457 6416

## 02 WATCH OUT FOR RANSOMWARE PRETENDING TO BE A WINDOWS UPDATE!

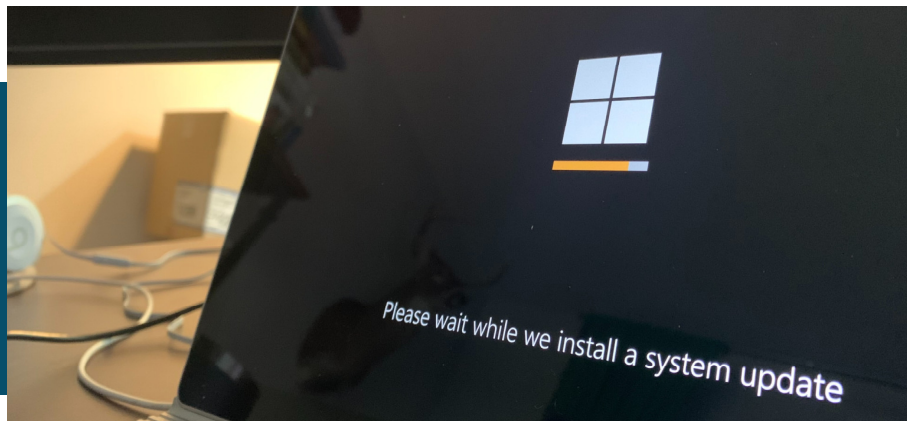
Imagine you're working away on your PC and see a Windows update prompt. Instead of ignoring it, you take action. But when you install what you think is a legitimate update, you're infected with ransomware.

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

### Backup Your Data

Regularly back up your important files. 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 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.

## 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/>



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 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.

**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.

**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.

## 04

## 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.

## 05

## 10 BIGGEST CYBER-SECURITY 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.

- Underestimating the threat
- Neglecting employee training
- Using weak passwords
- Ignoring software updates
- Lacking a data backup plan
- No formal security policies
- Ignoring mobile security
- Failing to regularly watch networks
- No Incident Response Plan
- Thinking they don't need Managed IT Services

## 06

## SUSTAINABLE TECH HABITS 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

## 07

## 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





## WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to your friends. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll gift them their free first month of service (for being a friend of yours) AND we'll gift you \$500 cash/gift voucher. Simply introduce me via email to [mark@phrixus.com](mailto:mark@phrixus.com) and I'll take it from there. I personally promise we'll look after their business with a high level of care and attention (just like we do with all our clients).



## NEED A LAUGH?

How does a computer get drunk?

It takes screenshots!

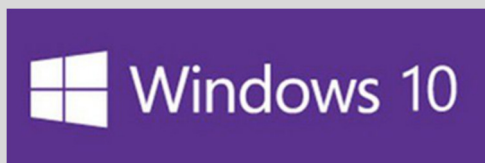


## TECHNOLOGY TRIVIA

The question this month is:

***What was the first ever domain name registered?***

## Windows 10 End of life



When Windows 10 was released Microsoft announced it would be the final Windows version with a number. Well things do change and Windows 10 will officially reach end of support in **October 2025**.

All systems supplied by Phrixus Technologies will now all be Windows 11, this operating system was released in October 2021 and almost all systems being shipped from new have this version installed. Microsoft have not yet announced the end of support date for Windows 11 but typically you should expect it to be supported for at least 10 years from its original release date.

Although there has not been any official announcement, the rumour mill is in full swing that Windows 12 is coming and it may even land on us as early as 2024. We should expect lots of AI support in the new version should the rumours be true and even a possibility it is on subscription or a free version with ads. Only time will tell and there is only one certainty—things change and evolve.

The first person to email me at

[mark@phrixus.com](mailto:mark@phrixus.com)

and give a correct answer gets a \$50 Amazon Gift Card!



*Each month you have a chance to win a \$50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!*

## Privacy Act Proposed Changes

Australian privacy laws are rules that are in place to protect your personal information and make sure it's handled responsibly. These laws apply to businesses, organisations, and sometimes even individuals who handle this information.

The Privacy Act of 1988 is expected to have some major changes in 2024 that will affect all Small Businesses. Currently SMBs with a turnover of less than \$3M are exempt from the act unless they handle sensitive financial or medical records.

The incoming change will scrap the \$3M threshold and every business will be included. Make sure you are prepared and increase your security and policies and procedures.