phrixus TECHNOLOGIES

LOCAL BUSINESS AWARDS 2021 WINNER HORNSBY KU-RING-GAI

MONTH: MARCH 2024

TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly Update From Mark

Employees, unintentionally, can become one of your company's biggest cyber threats. It's not about them being evil geniuses; it's more like accidentally clicking on that shady email link or leaving their password on a Post-it. We've all been there, right?

But seriously, it's crucial to remember that the folks on your payroll can be the first line of defense or the Achilles' heel. A bit of cybersecurity training goes a long way. Help them spot the phishing emails, show them the ropes on strong passwords, and let them know it's cool to double-check things. It's like having your crew trained to be the cyber superheroes your business needs. Because in this digital age, your employees are basically the gatekeepers of your digital fortress. Keep 'em sharp!

Need some help with employee security awareness training? Reach out to us at mark@phrixus.com to schedule a chat.

Until then, stay safe,

Mark

DID YOU KNOW ?

There are approximately 3.5 billion Google searches per day. 7.2% of this traffic comes from people searching the term 'Google'.

PHRIXUS TECHNOLOGIES

PO Box 266
Berowra NSW 2081
phrixus.com
02 9457 6416

02

ARE YOUR SMART HOME DEVICES SPYING ON YOU?

The integration of smart home devices has become synonymous with modern living. They offer convenience, efficiency, and connectivity at our fingertips.

But a recent study has raised concerns about the darker side of these smart gadgets. It suggests that our beloved smart home devices may be spying on us.

It's natural these days to invite these devices into your home. Yet there is also the need to scrutinise their privacy implications.

The Silent Observers in Our Homes

Smart home devices can range from voice-activated assistants to connected cameras and thermostats. They have woven themselves seamlessly into the fabric of our daily lives.

These gadgets promise to make our homes smarter and more responsive to our needs. But a study by consumer advocate group ***Which?*** raises unsettling questions. What is the extent to which they may be eavesdropping on our most private moments?

The study examined the data practices of popular smart home devices.

Key Findings from the Study

The study scrutinised several popular smart home devices such as smart TVs, doorbell cameras, and thermostats.

Widespread Data Sharing

A significant number of smart home devices share user data with third-party entities. This data exchange is often unbeknownst to users. It raises concerns about the extent to which companies are sharing our personal data as well as doing so without explicit consent.

Potential for Eavesdropping

Voice-activated devices, like Alexa, are common. Smart speakers and assistants were found to be particularly susceptible to potential eavesdropping. The study revealed some eyebrowraising information. There were instances where these devices recorded and transmitted unintentional audio data.

Lack of Transparency

One of the most disturbing aspects highlighted by the study is the lack of transparency. Data practices are often obscured under mountains of text. Many smart home device manufacturers fail to provide clear and comprehensive information.

Security Vulnerabilities

The study also identified security vulnerabilities in certain smart home devices. This highlights the risk of unauthorised access to sensitive information. Inadequate security measures could potentially expose users to cyber threats.

Navigating the Smart Home Landscape Safely

Here are the key steps to navigate the smart home landscape safely.

1. Research Device Privacy Policies
Before purchasing a smart home device, carefully review the manufacturer's privacy policy.

2. Optimise Privacy Settings
Take advantage of privacy settings offered by smart home devices. Many devices allow users to customise privacy preferences.

3. Regularly Update Firmware
Ensure that your smart home devices have the latest firmware updates.

4. Use Strong Passwords
Put in place strong, unique passwords for each smart home device. Avoid using default passwords.

5. Consider Offline Alternatives
Research whether you can achieve certain smart home functionalities with offline alternatives. If you can, opt for devices that operate offline or have limited connectivity.

6. Limit Voice-Activated Features
If privacy is a top concern, consider limiting or disabling voice-activated features. This reduces the likelihood of inadvertent audio recordings and potential eavesdropping.

7. Regularly Audit Connected Devices
Periodically review the smart home devices connected to your network. Seeing just how many there are may surprise you. Remove any devices that are no longer in use or that lack adequate security measures. Keep a lean and secure smart home ecosystem to mitigate your risk.

03 EXAMPLES OF HOW A DATA BREACH CAN COST YOUR BUSINESS FOR YEARS

The repercussions of a data breach extend far beyond the immediate aftermath. They often haunt businesses for years. Only 51% of data breach costs occur within the first year of an incident. The other 49% happen in year two and beyond.

The Unseen Costs of a Data Breach

Introduction to the First American Title Insurance Co. Case

The 2019 cybersecurity breach at First American serves as a stark illustration. It reminds us of the far-reaching consequences of a data breach. In this case, the New York Department of Financial Services (NYDFS) imposed a $1 million fine. Cybersecurity sites announced the fine in the fall of 2023. The company's fine was for failing to safeguard sensitive consumer information. This is one example of how costs can come long after an initial breach.

Lingering Impacts of a Data Breach

• Financial Repercussions

The financial toll of a data breach is significant. Immediate costs include things like:

- Breach detection
- Containment
- Customer notification

Beyond those, businesses face long-term expenses. These relate to legal battles, regulatory fines, and reparations.

• Reputation Damage

The impact on a business's reputation is arguably the most enduring consequence. Customers lose trust in a company's ability to protect their sensitive information. This loss of trust can result in a decline in customer retention. As well as acquisition difficulties and long-lasting damage to the brand image.

• Regulatory Scrutiny

Regulatory bodies increasingly hold businesses accountable for safeguarding consumer data. A data breach triggers regulatory scrutiny. This may lead to fines and ongoing compliance requirements.

• Operational Disruption

The aftermath of a data breach disrupts normal business operations. Companies must take remediation efforts and put in place enhanced security measures. These can divert resources away from core business functions.

• Customer Churn and Acquisition Challenges

A data breach often leads to customer churn. Individuals lose confidence in the business's ability to protect their data. Acquiring new customers becomes challenging. Potential clients are wary of associating with a brand that has suffered a breach. The prolonged effects on customer acquisition can hinder the company's growth as well as its market competitiveness.

A Cautionary Tale for Businesses Everywhere

The repercussions of a data breach extend far beyond the immediate incident. They can impact the financial health and reputation of a business for years as well as its regulatory standing.

04 ONLINE SECURITY: ADDRESSING THE DANGERS OF BROWSER EXTENSIONS

Browser extensions have become as common as mobile apps. People tend to download many and use few. These extensions offer users extra functionalities and customisation options.

While browser extensions enhance the browsing experience, they also pose a danger which can mean significant risks to online security and privacy.

Key Risks Posed by Browser Extensions

• Privacy Intrusions
Many browser extensions request broad permissions. If abused, they can compromise user privacy. Some of these include accessing browsing history and monitoring keystrokes.

• Malicious Intent
There are many extensions developed with genuine intentions. But some extensions harbor malicious code. This code can exploit users for financial gain or other malicious purposes.

• Outdated or Abandoned Extensions
Extensions that are no longer maintained or updated pose a significant security risk. Outdated extensions may have unresolved vulnerabilities.

• Phishing and Social Engineering
Some malicious extensions engage in phishing attacks. These attacks can trick users into divulging sensitive information.

Mitigating the Risks: Best Practices for Browser Extension Security

- Stick to official marketplaces.
- Review permissions carefully.
- Keep extensions updated.
- Limit the number of extensions you install.
- Use security software.
- Educate Yourself.
- Report Suspicious Extensions.
- Regularly audit your extensions.

05 7 AI TRENDS THAT ARE SWEEPING THE CYBERSECURITY REALM

As cyber threats grow in sophistication, traditional measures face challenges in keeping pace. This is where AI steps in. It offers a dynamic and adaptive approach to cybersecurity.

Machine learning algorithms, neural networks, and other AI technologies analyse vast datasets. They do this at unprecedented speeds.

The integration of AI in cybersecurity doesn't replace human expertise. It enhances it.

AI Trends Sweeping the Cybersecurity Realm

1. Predictive Threat Intelligence
2. Behavioral Analytics
3. Autonomous Security Systems
4. Explainable AI (XAI)
5. Cloud Security Augmentation
6. Deception Technology
7. Zero Trust Architecture

06 THE NEWEST FEATURES OF MICROSOFT EDGE

Microsoft Edge continues to redefine user experiences. This is due to Microsoft's commitment to innovation. The latest updates bring a host of features. These are designed to enhance productivity, security, and browsing satisfaction.

It is now the third most popular browser worldwide.

From personalised workspaces to a built-in VPN, Microsoft Edge is not just a browser. It's a comprehensive toolkit for users navigating the digital landscape.

Here are newest Features of Microsoft Edge:

- Workspaces to organise browser session focuses
- Built-in Edge Secure Network VPN
- Autofill for more webform fields
- Web Capture
- Copilot (AI)
- Read Aloud

07 HOW SMALL BUSINESSES ARE UNLOCKING GROWTH WITH GENERATIVE AI

Staying ahead in business often means embracing cutting-edge technologies. New tools can unlock new avenues for growth. Especially for small businesses. SMBs are often looking for affordable ways to gain a competitive advantage.

One such transformative force is Generative Artificial Intelligence (GenAI). This is a technology that goes beyond automation and the AI we used to know. It can create content, solutions, and possibilities before unimaginable.

The landscape of small business marketing is evolving rapidly. The integration of AI technologies is reshaping strategies for growth. Small businesses are turning to GenAI to enhance their marketing efforts.

How Are Small Businesses Using GenAI?

- Image & content creation and personalisation
- Enhanced customer experience
- Data analysis and decision-making
- Innovative product development
- Efficient social media management

WE LOVE REFERRALS

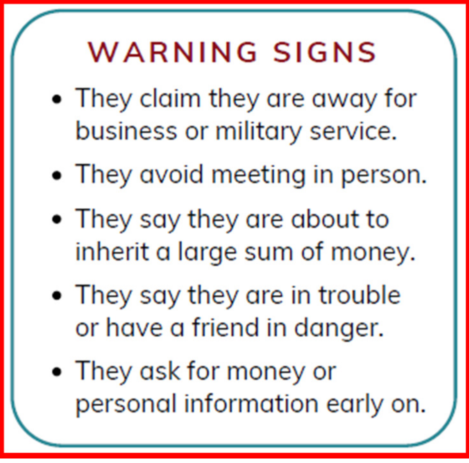
The greatest gift anyone can give us is a referral to your friends. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend's business 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** 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).

Spotlight on Romance Scams

What are they?

Romance scams occur when a scammer creates a profile on a dating or social media site. They typically use fake pictures and move the relationship along quickly, claiming they are in love. After gaining the person's trust, the scammer tries to move the conversation away from the platform and ask for money. With the rise of deepfake technology, scammers can now even mimic voices and make convincing videos using another person's identity.



WARNING SIGNS

- They claim they are away for business or military service.
- They avoid meeting in person.
- They say they are about to inherit a large sum of money.
- They say they are in trouble or have a friend in danger.
- They ask for money or personal information early on.

NEED A LAUGH?

What kind of books grow on trees?

Apple MacBooks

TECHNOLOGY TRIVIA

The question this month is:

What computer and printer giant was founded in 1939 in Palo, Alto, CA? It is sometimes better known by the two-letter acronym based on its founders names.

The first person to email me at **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!

Microsoft Copilot

There has been a lot of talk about AI and now Microsoft have released Copilot for small business 6 months earlier than planned within its M365 stack.

Copilot is like having a super-smart writing buddy by your side. It's an **AI companion** that helps you with all sorts of tasks, from writing code to creating stories, poems, and more. Imagine having a friendly digital sidekick that assists you in your creative endeavours!

It is very early to start to adopt the technology within your M365 tenancy at this stage however as there are many security implications to consider as to what data it can retrieve. Lots of planning is required with data hygiene and access controls to be implemented