TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly Update from Mark

Let's talk about why understanding those data sharing settings on apps and IoT gadgets is a big deal. It's like the gatekeeper for your personal info. If you're not on top of those settings, you might be unknowingly throwing open the doors to your private data. Think identity theft, unauthorised snooping, your data being sold, or who knows what.

Taking a minute to get what those settings are about means you get to decide who sees what. It's like having your own bouncer for your digital life. So, next time an app asks for permission, take a peek at what settings you're actually leaving on. It's your data – keep it on lockdown!

Would you like some help with good data privacy solutions or Cyber Security Training for your staff? Reach out to us at mark@phrixus.com to schedule a chat.

Until then, stay safe,

Mark

DID YOU KNOW

Domain name registration used to be free. Way back when people didn't realise how huge the internet would be, registering a domain name was free until 1995.

Phrixus Technologies

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

02 GAMERS BEWARE OF HACKERS!

Gamers haven't really been the focus of cybersecurity for a long time. You mostly hear about attacks on businesses. Or stolen personal data due to phishing attacks. But gamers are not safe from hackers targeting them.

As cyberattacks continue to escalate, gamers have become prime hacking targets. Malicious actors seek to exploit vulnerabilities in the digital realm. The gaming industry continues to expand. Also, more users immerse themselves in virtual worlds. As this happens, the risks associated with cyberattacks on gamers are on the rise.

Cyberattacks on young gamers increased by 57% in 2022.

Younger gamers playing games like Minecraft, Roblox, and Fortnite are particularly at risk. They're also often playing on their parents' devices. Data that holds the interest of hackers fills these devices.

The Gaming Boom and Cybersecurity Concerns

The exponential growth of the gaming industry has brought entertainment to millions. But it has also attracted the attention of cybercriminals looking for lucrative opportunities.

Hackers are deploying sophisticated techniques to compromise user accounts.

- **Stolen Credentials and In-Game Items**

What's one of the primary motivations behind these cyberattacks? It's the prospect of acquiring valuable in-game items, the account's credentials, and virtual goods, such as rare skins, weapons, or characters, that hold real-world value.

- **Ransom Attacks on Gaming Accounts**

Ransom attacks have become increasingly prevalent in the gaming world. In these instances, cybercriminals gain control of a user's account. They then demand a ransom for its release. Hackers often demand the ransom in untraceable cryptocurrency.

- **Disruption of Online Gaming Services**

Beyond individual attacks, hackers are now targeting gaming platforms. Their intent is to disrupt online services. They launch DDoS (Distributed Denial of Service) attacks to overwhelm servers. This renders them inaccessible to legitimate users.

Safeguarding Your Gaming Experience: Tips for Gamers

Here are some essential tips to enhance gaming cybersecurity.

Strengthen Your Passwords – Avoid using easily guessable passwords. Incorporate a mix of letters, numbers, and special characters. Regularly updating your passwords adds an extra layer of security.

Enable Multi-factor Authentication (MFA)

Multi-factor Authentication is a powerful tool that adds significantly to security. MFA users verify their identity through a secondary method such as a code sent to their mobile device. Enabling 2FA greatly reduces the risk of unauthorised access even if a hacker has compromised your password.

Stay Informed and Vigilant

Be aware of the latest cybersecurity threats targeting the gaming community. Stay informed about potential risks as well as new hacking techniques and security best practices. Additionally, be vigilant when clicking on links or downloading files. Keep your guard up when interacting with unknown users within gaming platforms.

Keep Software and Antivirus Programs Updated

Regularly update your gaming platform, antivirus software, and operating system. This will patch vulnerabilities and protect against known exploits. Cybersecurity is an ongoing process. Staying up to date is crucial in thwarting potential attacks.

Use a Virtual Private Network (VPN)

Consider using a Virtual Private Network (VPN) to encrypt your internet connection. This enhances your privacy. It also adds an extra layer of protection against potential DDoS attacks as well as other malicious activities.

Elgato Stream Deck XL

The Stream Deck XL is equipped with 32 customisable LCD keys, a feature that provides users with an unprecedented level of control and customisation. This vast array of buttons allows for a seamless and efficient operation.

It integrates effortlessly with a wide range of platforms and tools.

The functionality is where the Stream Deck XL really shines. Switching scenes, launching media, adjusting audio – it's all at your fingertips.

03 TOP DATA BREACHES OF 2023: NUMBERS HIT AN ALLTIME HIGH

The battle against cyber threats is an ongoing challenge. Unfortunately, 2023 has proven to be a watershed year for data breaches. Data compromises surged to an all-time high in the U.S.

The last data breach record was set in 2021. That year, 1,862 organisations reported data compromises. Through September of 2023, that number was already over 2,100.

In Q3 of 2023, the top data breaches were:

- HCA Healthcare
- Maximus
- The Freecycle Network
- IBM Consulting
- CareSource
- Duolingo
- Tampa General Hospital
- PH Tech

Let's look at the main drivers of this increase.

1. The Size of the Surge – Data breaches in 2023 have reached unprecedented levels. The scale and frequency of these incidents emphasise the evolving sophistication of cyber threats as well as the challenges organisations face in safeguarding their digital assets.

2. Healthcare Sector Under Siege – Healthcare organisations are the custodians of highly sensitive patient information. As a result, they've become prime targets for cybercriminals.

3. Ransomware Reigns Supreme – Ransomware attacks continue to dominate the cybersecurity landscape. The sophistication of this threat has increased.

4. Supply Chain Vulnerabilities Exposed – Modern business ecosystems have an interconnected nature. This has made supply chains a focal point for cyberattacks. The compromise of a single entity within the supply chain can have cascading effects.

5. Emergence of Insider Threats – The rise of insider threats is adding a layer of complexity to cybersecurity. Organisations must distinguish between legitimate user activities and potential insider threats.

6. IoT Devices as Entry Points – The proliferation of Internet of Things (IoT) devices has expanded the attack surface. There's been an uptick in data breaches originating from compromised IoT devices.

7. Critical Infrastructure in the Crosshairs – Critical infrastructure has become a target of choice for cyber attackers.

8. The Role of Nation-State Actors – Nation-state actors are increasingly playing a role in sophisticated cyber campaigns. They use advanced techniques to compromise sensitive data and disrupt operations.

9. The Need for a Paradigm Shift in Cybersecurity –The surge in data breaches underscores the need to rethink cybersecurity strategies.

10. Collaboration and Information Sharing – Collaboration among organisations and information sharing within the cybersecurity community are critical. Threat intelligence sharing enables a collective defense against common adversaries.

04 5 WAYS TO LEVERAGE MICROSOFT 365'S NEW AI INNOVATIONS

Microsoft 365 has been adding some amazing AI innovations. They sit inside tools like Word, Excel, PowerPoint, Teams, and more. These smart Copilot features can enhance your experience and boost productivity.

Here are ways to take advantage of the benefits offered by Microsoft Copilot.

1. Speed Up Document Creation
Copilot provides intelligent suggestions, helping you articulate your thoughts more effectively. It speeds up the writing process. It also ensures that your content is clear, concise, and tailored to your audience.

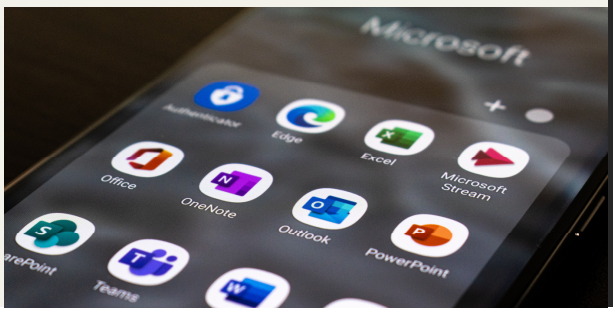
2. Enhance Your Teams Meeting Experience
Copilot in Teams can create coherent and context-aware responses. Such as a summary of meeting notes and an action item list.

3. Create PowerPoints with Ease
Become a "PowerPoint Master" with Copilot. The AI-infused features in PPT can create a slide deck for you based on text prompts, including the images.

4. Enjoy Smart Business Insights in Excel
Excel Ideas can automatically detect patterns and trends in your data. It will suggest charts, tables, and summaries that best suit your needs.

5. Save Time in Outlook with AI Help
Use Copilot in Outlook to summarise the key points of an email to save yourself reading time. It can also help write emails and suggest responses to emails in your inbox.

As we embrace the era of intelligent productivity, M365 becomes more powerful. Its new AI innovations pave the way for a more efficient work environment. By incorporating these capabilities into your daily workflow, you're staying competitive.



05 WAYS TO SHOW THE TANGIBLE VALUE OF CYBERSECURITY

The benefits of cybersecurity are often indirect and preventive in nature. This differs from tangible assets with direct revenue-generating capabilities.

Success is often measured by incidents that do not occur. This complicates efforts to attribute a clear monetary value. As a result, companies grapple with finding certain metrics.

Below are several ways to translate successful cybersecurity measures into tangible value.

- Quantifying Risk Reduction
- Measuring Incident Response Time
- Financial Impact Analysis
- Monitoring Compliance Metrics
- Employee Training Effectiveness
- User Awareness Metrics
- Technology ROI
- Data Protection Metrics
- Vendor Risk Management Metrics

06 9 TIPS FOR SETTING UP AI RULES FOR YOUR STAFF

Artificial intelligence (AI) is a powerful tool. It can enhance the productivity, efficiency, and creativity of your staff. But AI also comes with some challenges and risks. Businesses need to address and manage these to use AI effectively.

Here are some tips for setting up AI rules for your staff. These tips can help you harness the benefits of AI while avoiding the pitfalls.

1. Define the scope and purpose of AI use.
2. Establish ethical principles and guidelines.
3. Involve stakeholders in the decision-making process.
4. Assign roles and responsibilities.
5. Provide training and support.
6. Ensure data security and privacy.
7. Put a feedback loop in place.
8. Review and update your AI rules regularly.
9. Encourage a growth mindset.

07 HOW SMALL BUSINESS CAN APPROACH WORKFORCE TECHNOLOGY MODERNISATION

Technology plays a pivotal role in driving efficiency, productivity, and competitiveness. For small businesses, workforce technology modernisation is both an opportunity and a challenge.

Embracing modern technology can empower small businesses. It can help them thrive in a digital era. Important benefits include improved employee retention and decreased cybersecurity risk not to mention the productivity and time-saving advantages.

Here are some steps to get your small business get started.

- Assess Your Current Technology Landscape
- Align Technology Goals with Business Objectives
- Focus on Cloud Adoption
- Invest in Collaborative Tools
- Look at Cybersecurity Measures
- Embrace Mobile-Friendly Solutions
- Look at Remote Work Options
- Consider Automation for Efficiency
- Provide Ongoing Training and Support
- Watch and Adapt to Evolving Technologies

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).

Scam of the Month

Jean was at work looking at the latest financial report when she received a phone call. The call was from an unknown number, but Jean often gets calls from potential clients, so she answered. To her surprise, it was her daughter Kenzie's voice on the other line. Kensie sounded scared and said she was in trouble. She said she needed a few thousand dollars wired to an account or else she would go to jail. She told her mom she would explain more later. Jean panicked and wanted to make sure her daughter was safe, so she wired the money immediately. Later she tried to call the number back but there was no answer. She called Kenzie's normal phone number and Kenzie answered. When Jean asked her what happened, Kenzie was confused. She was never in any trouble and never asked for money. Jean realized it was a scam. Plus, the wallet she transferred the money into turned it to cryptocurrency, so it was not traceable.

Did you spot the red flags?

NEED A LAUGH?

What is the computer's favorite snack to eat?

Microchips!

TECHNOLOGY TRIVIA

The question this month is:

What does the acronym CAPTCHA stand for?

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!

Is your main home email account attached to your telco/ISP?

With TPG closing down their email system last September you have a 1 year grace to move all your email services to a fixed email provider before it is gone forever. This will also include those with Ozemail and iiNet email addresses.

Telstra and Optus are likely to follow the same path and Telstra have already stopped providing new Bigpond addresses.

For those of you that have had these addresses for decades, they are likely linked with many of your essential home services and banking.

It is recommended to never rely of these addressing systems from the Telco and instead use a stable service such as a Microsoft Outlook.com or a Gmail account.