phrixus TECHNOLOGIES

MONTH: MAY 2024

TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly update from Mark

Imagine your top-secret business data, like customer records and internal company emails, are sitting out in the open. Just sitting there for hackers to have at them. If you're not using encryption, then this could be a reality. Encryption scrambles data so only those with the decryption key can access it.

Hackers might be lurking around, but with encryption, stolen data will just be gibberish to them. It's the same for emails, laptops, and anything else with sensitive info. Encryption throws up a shield and says, "Hands off my data!" It's not foolproof, but it makes things a whole lot tougher for anyone trying to steal your business's secret sauce.

Need some guidance leveraging encryption at your business? Reach out to us at mark@phrixus.com to schedule a chat.

Until then, stay safe,

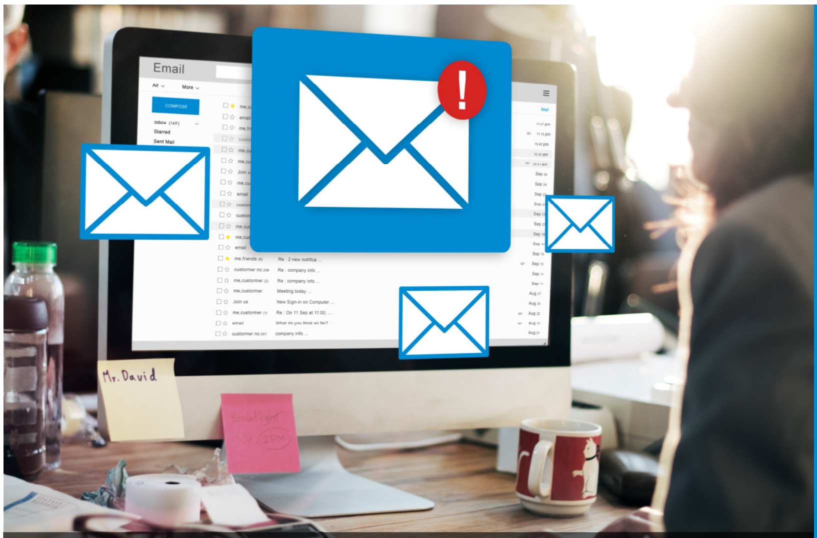
Mark

DID YOU KNOW?

The first-ever computer virus to spread via email, the "Morris Worm," infected thousands of computers in 1988.

Phrixus Technologies

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



02 GOOGLE & YAHOO'S NEW DMARC POLICY - WHY BUSINESSES NEED EMAIL AUTHENTICATION

Have you been hearing more about email authentication lately? There is a reason for that. It's the prevalence of phishing as a major security threat. Phishing continues as the main cause of data breaches and security incidents. This has been the case for many years.

A major shift in the email landscape is happening. The reason is to combat phishing scams. Email authentication is becoming a requirement for email service providers. It's crucial to your online presence and communication to pay attention to this shift.

Google and Yahoo are two of the world's largest email providers. They have implemented a new DMARC policy that took effect in February 2024. This policy essentially makes email authentication essential. It's targeted at businesses sending emails through Gmail and Yahoo Mail.

But what's DMARC, and why is it suddenly so important?

The Email Spoofing Problem

Imagine receiving an email seemingly from your bank. It requests urgent action. You click a link, enter your details, and boom – your information is compromised. The common name for this is email spoofing.

It's where scammers disguise their email addresses. They try to appear as legitimate individuals or organisations. Scammers spoof a business's email address. Then they email customers and vendors pretending to be that business.

These deceptive tactics can have devastating consequences on companies. These include:

- Financial losses
- Reputational damage
- Data breaches
- Loss of future business

Unfortunately, email spoofing is a growing problem. It makes email authentication a critical defense measure.

What is Email Authentication?

Email authentication is a way of verifying that your email is legitimate. This includes verifying the server sending the email. It also includes reporting back unauthorised uses of a company domain.

Email authentication uses three key protocols, and each has a specific job:

- SPF (Sender Policy Framework): Records the IP addresses authorised to send email for a domain.
- DKIM (DomainKeys Identified Mail): Allows domain owners to digitally "sign" emails, verifying legitimacy.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Gives instructions to a receiving email server including, what to do with the results of an SPF and DKIM check. It also alerts domain owners that their domain is being spoofed.

SPF and DKIM are protective steps. DMARC provides information critical to security enforcement. It helps keep scammers from using your domain name in spoofing attempts.

Why Google & Yahoo's New DMARC Policy Matters

Both Google and Yahoo have offered some level of spam filtering but didn't strictly enforce DMARC policies.

- Starting in February 2024, the new rule took place. Businesses sending over 5,000 emails daily must have DMARC implemented.
- Both companies also have policies for those sending fewer emails. These relate to SPF and DKIM authentication.

Look for email authentication requirements to continue. You need to pay attention to ensure the smooth delivery of your business email.

The Benefits of Implementing DMARC:

- Protects your brand reputation
- Improves email deliverability
- Provides valuable insights

Product of the Month

Kensington SD1700P - Mobile docking station

Kensington SD1700P USB-C Dual 4K Mobile Dock

With wireless QI Charging, 100W Pass-through

https://shop.phrixus.com/products/kensington-sd1700p-usb-c-dual-4k-portable-dock-2090721

03 BEWARE OF DEEPFAKES! LEARN TO SPOT THE DIFFERENT TYPES

Have you ever seen a video of your favorite celebrity saying something outrageous? Then later, you find out it was completely fabricated?

Welcome to the world of deepfakes. This is a rapidly evolving technology that uses artificial intelligence to create synthetic media. They can appear real but are actually manipulated. Bad actors can use deepfakes to spread misinformation. They are also used in phishing attacks.

So, what are the different types of deepfakes, and how can you spot them?

FACE-SWAPPING DEEPFAKES

This is the most common type. Here, the face of one person is seamlessly superimposed onto another's body in a video.

Here's how to spot them:

- Look for inconsistencies: Pay close attention to lighting, skin tones, and facial expressions. Look for subtle glitches.
- Check the source: Where did you encounter the video? Be cautious of unverified sources and unknown channels.
- Listen closely: Does the voice sound natural? Incongruences in voice tone, pitch, or accent can be giveaways.

DEEPFAKE AUDIO

This type involves generating synthetic voice recordings. They mimic a specific person's speech patterns and intonations. Scammers can use these to create fake audio messages.

Here's how to spot them:

- Focus on the audio quality: Deepfake audio can sound slightly robotic or unnatural. Pay attention to unusual pauses or a strange emphasis.
- Compare the content: Does the content of the audio message align with what the person would say? Consider if the content seems out of character or contradicts known facts.
- Seek verification: Is there any independent evidence to support the claims made? If not, approach it with healthy skepticism.

TEXT-BASED DEEPFAKES

This is an emerging type of deepfake. It uses AI to generate written content such as social media posts, articles, or emails. They mimic the writing style of a specific person or publication. These can be particularly dangerous.

Here's how to spot them:

- Read critically: Pay attention to the writing style, vocabulary, and tone.
- Check factual accuracy: Verify the information presented in the text against reliable sources.
- Be wary of emotional triggers: Be cautious of content that evokes strong emotions.

DEEPFAKE VIDEOS WITH OBJECT MANIPULATION

This type uses AI to manipulate objects within real video footage.

Here's how to spot them:

- Observe physics and movement: Pay attention to how objects move in the video.
- Seek original footage: If possible, try to find the original source of the video footage.

04 10 MOST COMMON SMART HOME ISSUES

Back when you were a kid, living in a "smart home" probably sounded futuristic. While we don't have flying cars, we do have video telephones and voice-activated lights.

But even the most advanced technology can have analog problems. Hackers can get past weak passwords. Bad connections can turn advanced into basic pretty quickly.

Have you run into any issues with your smart home gadgets?

Here are some of the most frequent problems and solutions.

1. Connectivity Woes
Restart your router and your devices. If that doesn't work, ensure you've positioned your router centrally. Or invest in a Wi-Fi extender for better coverage.

2. Device Unresponsiveness
Try turning it off and back on. Also check for software updates on your devices.

3. Battery Drain
Adjust settings to reduce power consumption. Disable features you don't use.

4. Incompatibility Issues
Check to ensure your devices are compatible with each other. Build your devices around your smart home platform. Review the manufacturer's specifications thoroughly to avoid compatibility headaches.

5. Security Concerns
Use strong and unique passwords for all your devices and accounts. Enable two-factor authentication wherever available.

6. App Troubles
Try logging out and logging back in to refresh the connection. If issues persist, uninstall and reinstall the app.

7. Automation Gone Wrong
Review rules and test individually.

8. Limited Range
Move your devices closer to the hub or router for better communication.

9. Ghost Activity
Investigate causes and change passwords.

10. Feeling Overwhelmed
Don't hesitate to consult your device manuals and online resources or get an expert help.

05 5 DATA SECURITY TRENDS TO PREPARE FOR IN 2024

With cyber threats evolving at an alarming pace, staying ahead of the curve is crucial. It's a must for safeguarding sensitive information.

Data security threats are becoming more sophisticated and prevalent. The landscape must change to keep up.

Here are some key areas to watch.

1. The Rise of the Machines: AI and Machine Learning in Security

2. Battling the Ever-Evolving Threat: Ransomware

3. Shifting Strategies: Earlier Data Governance and Security Action

4. Building a Fortress: Zero Trust Security and Multi-Factor Authentication

5. When Things Get Personal: Biometric Data Protection

06 HOW TO PROPERLY DEPLOY IOT ON A BUSINESS NETWORK

The Internet of Things (IoT) is no longer a futuristic concept. It's rapidly transforming industries and reshaping how businesses operate. IoT is a blanket term to describe smart devices that are internet enabled. One example is smart sensors monitoring production lines. Connected thermostats optimising energy consumption is another.

Here are the steps you need to properly deploy IoT on a Business Network:

Step 1: Define Your Goals and Needs

Step 2: Select the Right Devices and Network Infrastructure

Step 3: Focus on Security Throughout the Journey

Step 4: Deployment and Ongoing Management

Step 5: Continuous Learning and Improvement

07 INTRODUCING THE NEW MICROSOFT PLANNER

Calendars, task lists, and project planning are important business tools. Many people use Microsoft's apps to power these processes including Planner, Microsoft To Do, and Project for the web.

These tools help keep processes on track and enable task accountability. But they're separate apps. Switching between apps can be cumbersome. It adds more complexity to a workflow.

On average, employees switch between 22 different apps 350 times per day. This puts a big dent in productivity and efficiency.

Microsoft is working to solve that. It is rolling out a brand-new version of Microsoft Planner in 2024. The new Planner is packed with exciting features designed to simplify your project management journey.

Here are some of the key features:

- Combines the functions of Planner, To Do, and Project for the web
- Enhanced Collaboration
- AI-Powered Insights with Copilot
- Scaling with Your Needs
- Pre-Built Templates
- Integrates with Teams, Power BI, Viva, and more

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).

Plan for mass email sending limits

Microsoft have announced that, beginning in January 2025, Exchange Online will begin enforcing an external recipient rate limit of 2,000 recipients in 24 hours.
"Exchange Online does not support bulk or high-volume transactional email. We have not enforced limiting of bulk email until now, but we plan on doing so with the introduction of an External Recipient Rate (ERR) limit." The ERR limit is being introduced to help reduce unfair usage and abuse of Exchange Online resources.
What about the Recipient Rate Limit?
Exchange Online enforces a Recipient Rate limit of 10,000 recipients. The 2,000 ERR limit will become a sub-limit within this 10,000 Recipient Rate limit. There is no change to the Recipient Rate limit. If you send to less than 2,000 external recipients in a 24 hour period, you will still be able to send to 10,000 total recipients.
How will this change happen?
The new ERR limit will be introduced in 2 phases:
Phase 1 - Starting Jan 1, 2025, the limit will apply to cloud-hosted mailboxes of all newly created tenants.
Phase 2 - Between July and December 2025, we will start applying the limit to cloud-hosted mailboxes of existing tenants.
What are the options for customers who have business needs that exceed the ERR limit?
If you have a cloud-hosted mailbox that needs to exceed the ERR limit, you can move to Azure Communication Services for Email, which is designed specifically for high volume email sent to recipients external to your tenant. Or you use a bulk email sending platform such as MailGun or Mail Chimp

NEED A LAUGH?

Why do vampires use Linux?...

Because they don't like Windows in their house.

TECHNOLOGY TRIVIA

The question this month is:

In 1999 Shigetaka Kurita invented what keyboard additions for cell phones that would eventually replace emoticons and even get their own movie?

The first person to email me at
mark@phrixus.com
and give a correct answer gets a $50 Amazon Gift Card!
Well done to Sonifex for winning last month

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!

End of Financial Year Deals

As we approach the end of the financial year we have negotiated some special deals with our distributors for our most popular desktop and 14" Laptop systems:

HP ProBook 440 G10, 14" FHD Screen, Intel i5-1334U, 16GB DDR4 RAM, 512GB @ $1,499 exc GST (normally $1,640)

Lenovo desktop
Lenovo ThinkCentre M70Q G3 Tiny, Intel i5-12400T, 16GB DDR4 RAM, 512GB NVMe SSD, Keyboard+Mouse, Wireless AX+Bluetooth, 3 Year Onsite Warranty – 130 units in stock @ $999 exc GST (Normally $1,060 exc GST)

Please contact us to secure these before they expire on June 30 2024 using deal code Phrixus25