TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly update from Mark

Did you know your data could be lurking in the shadows of the internet? Dark web monitoring promises to shine a light on hidden threats, but is it really worth the hype?

There are tons of cybersecurity tools out there, but dark web monitoring stands out as a hands-free way to protect your identity.

The truth is, what you don't know can hurt you. Your personal information could be up for grabs without you knowing, leaving you open to identity theft, financial fraud, and more.

Want to learn more about dark web monitoring? Reach out to us at mark@phrixus.com to schedule a chat.

Until then, stay safe,

Mark

DID YOU KNOW

The first webcam was invented in 1991 by Cambridge University scientists to monitor coffee

Phrixus Technologies

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

Threat Exposure Management (TEM) is an important cybersecurity tool. It helps organisations find and fix weak spots in their digital systems. TEM outsmarts hackers before they break into your network.

02 WHAT IS THREAT EXPOSURE MANAGEMENT (TEM) AND WHY YOU NEED IT?

Importance of TEM

Cyber attacks keep getting worse. Hackers always find new ways to break in. TEM helps businesses spot problems before they become big issues.

TEM allows you to:

- Find weak points in your network
- Fix issues quickly
- Reduce your risk of cyber attacks

How TEM Works

TEM uses special software to scan your entire network. It finds places hackers could attack and helps you fix these weak spots.

Continuous Monitoring

TEM keeps looking all the time. This way, you can find new problems as soon as they appear.

Risk Assessment

TEM finds which weak spots are the most dangerous. This helps you fix the most important ones first.

Main Parts of a TEM Program

Asset Discovery

This finds all devices and software on your network. You can't protect what you don't know about!

Vulnerability Scanning

This looks for open weak spots in your system. It's like checking for unlocked doors in your house.

Threat Intelligence

This provides insights into new hacker techniques, helping you stay informed about what to watch out for.

Remediation Planning

Once you find the vulnerabilities, you need a plan to fix them. TEM helps you make good choices on how to patch these spots.

Benefits of TEM for Your Business

Better Security

Finding and fixing weak spots makes your whole system much safer and more resilient.

Cost Savings

Stopping an attack before it happens can save you a lot of money. Dealing with the aftermaths of cyberattacks often comes with expensive costs.

Peace of Mind

With TEM, continuous monitoring ensures your system is always under watch. This can help you worry less about cyber attacks.

What to Look for in a TEM Solution

A good TEM tool should:

- Be user-friendly, ensuring that all team members, regardless of their technical expertise, can easily navigate and utilise the tool.
- Provide immediate results, enabling quick and effective decision-making to address potential threats as soon as they are detected.
- Integrate seamlessly with your existing security infrastructure, enhancing overall protection by working in harmony with other security tools and systems.
- Generate clear and comprehensible reports, presenting findings in an easily digestible format that facilitates understanding and action by all stakeholders.

Getting Started with TEM

- Check your current security setup to understand your existing vulnerabilities and areas for improvement.
- Find a TEM tool that fits your needs, ensuring it aligns with your security goals and integrates well with your current systems.
- Set up the tool and start scanning your environment.
- Make a plan to fix the weak spots you find, prioritising the most critical issues.
- Keep scanning and improve your security continuously, regularly updating your strategies and tools to stay ahead of emerging threats.

Want to learn more about how TEM can help your company? Contact us today for help staying safe in the digital world.

TICKTIME CUBE

Ticktime Cube is your ultimate time manager to boost your efficiency and productivity.

The TickTime Cube is a single task countdown timer with a built-in Pomodoro mode. Just flip it and the timer will restart for you.

The timer comes with a selection of preset countdown times, but you can also set a custom time of 99 minutes and 59 seconds or less or use the stopwatch feature to count up.

It's a fun way to keep track of your time.

03 10 TIPS FOR A SEAMLESS SMART HOME EXPERIENCE

Smart homes make life easier. But setting one up can be tricky. Here's how to make a smooth smart home system.

What is a Smart Home?

A smart home uses technology to control many parts of life. This includes turning lights on and off and unlocking doors. You can control these devices with your voice or smartphone. These devices often connect over the internet and talk to each other.

Why Should I Make My Home Smart?

Smart homes save you time and energy. They can also make your home safer. Lastly, they are fun to use. Just say it and watch it happen!

How do I build my smart home?

Choose Your Hub

The hub acts as the brain of your smart home. It helps devices talk to each other. Common hubs include the Amazon Echo and the Google Nest.

Choose Compatible Devices

Your devices should work with your hub. When buying, look for phrases like "Works with Alexa" or "Google Home compatible".

Set Up Your Network

You need a strong Wi-Fi network. You might need to change your router. Some smart devices work best on their own network.

What are some must-have smart devices?

Smart lights

These let you control your lights with your voice or phone. You can change colors and set schedules too.

Smart thermostat

This device learns your schedule and adjusts the temperature to save energy. You can control it remotely from anywhere.

Smart locks

These let you lock and unlock your doors with your phone. You can also share digital keys with guests.

How can I get my devices to work together?

Use routines

Routines let you control many devices with one command. Say, "Good morning," and you can turn on the lights and start your coffee maker.

Group your devices

Put devices in the same room into groups. This lets you control all of them at once.

How Do I Keep My Smart Home Safe?

- Use strong passwords. Give all your devices strong, unique passwords.
- Keep software updated. Update your devices with new software. This keeps them safe from hackers.

What if I have problems with my smart home?

- Check your network: Poor Wi-Fi causes many issues. Make sure your network is strong and stable.
- Restart your devices: Sometimes, you can fix problems by simply turning things off and then on again.
- Call for help: Don't be afraid to ask for support when you get stuck.

Smart homes are great, but they take some work to set up. Follow these tips to make the process smooth.

Need help making your home smarter? Contact us to make your home work just how you want it to.

04 HOW PASSWORD MANAGERS PROTECT YOUR ACCOUNTS

A password manager keeps all your passwords in one place. Think of it as a digital safe for your login information.

You only need to remember one password, the master password. This master password lets you access all your other passwords.

Types of Password Managers

- Apps you download on your phone or computer
- Tools that work in your web browser
- Some offer both options

Why Use a Password Manager?

- It Helps You Create Strong Passwords. Password managers generate long, random passwords that are hard to crack.
- It Remembers Your Passwords. With a password manager, you don't need to memorise many passwords. The tool does this for you.
- It Keeps Your Passwords Safe. Password managers use high-level security to protect your data. Even if someone hacks the password manager company, they can't read your information.

Features of Password Managers

- Password Generation: Good password managers can create tough, unique passwords for you.
- Auto-Fill: Many password managers can fill in your login information on websites. This saves time and avoids typos.
- Secure Notes: Some password managers let you store credit card numbers or important documents.
- Password Sharing: Some tools let you share passwords safely with family or coworkers.

How to Choose a Password Manager

- Find one with strong encryption and two-factor authentication.
- The manager should be easy for you to understand and use.
- Make sure it works on all your devices.
- Research the features you want and the price you can afford.

Consider using a password manager today to improve your online security. If you need help choosing or setting up a password manager, contact us today.

05 INNOVATIVE SOLUTIONS TO IOT DEVICE SECURITY

The Internet of Things is growing day by day. More devices are connecting to the internet. And with that growth comes new security risks.

Here are some new ways to keep your IoT devices safe.

- Use strong passwords. Always change the default password.
- Always update software. This closes the security gaps in the software.
- Encrypt your data. This scrambles data so others cannot read it.
- Develop an IoT security policy. Establish regulations relating to the use and security of IoT devices.
- Implement network segmentation. Isolate the IoT devices from other networks.
- Do research before buying. Choose devices from companies that take security seriously.
- Secure your home network. Enable network encryption.
- Think twice about what you connect. Only connect devices you need.

06 HOW IS YOUR CYBER HYGIENE? ESSENTIAL TIPS FOR 2025

- **Improve your passwords.** Passwords are like keys to your online home.
- **Update your software.** Updating your software is like getting a flu shot.
- **Implement two factor authentication.** It's like putting two locks on your door.
- **Be careful on public Wi-Fi.** It's like yelling in a crowded place.
- **Identify phishing scams.** It's like a fake fisherman trying to catch you.
- **Back up your data.** It's like making copies of your important papers.
- **Review privacy settings.** Your privacy settings are like curtains on your windows.
- **Teach your family about cybersecurity.** This is for everyone in your family. It's like teaching kids to look both ways.

07 DO YOU REALLY NEED DARK WEB MONITORING?

Dark web monitoring looks for your information on the dark web. It can find stolen passwords or credit card numbers. This helps you know if someone stole your data.

But is dark web monitoring really necessary? Here are the most important benefits to consider:

- **Identity and business** protection. It helps you know if someone stole your personal or business data. You can then change passwords and protect yourself.
- **AI monitoring to spot patterns that people might miss.** AI helps them search faster and better.
- **Real-time alerts when your information is stolen.** The tools send an alert right away when they find your information.
- **Protection for passwords, credit card numbers, social security numbers, and more.** This enables you take quick, specific actions.

Dark web monitoring is an easy way to protect your information. It watches when you can't. If you want to stay safe online, it's a good tool to have.

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).

The Windows 10 clock is ticking

With Windows 10 support ending on 14th October 2025, it's time to act and plan to replace or upgrade your old Windows 10 systems

What staying on Windows 10 Means after October 14th

What Steps you can take.

1. **Identify Vulnerable Devices:** Which of your systems can't support Windows 11?
2. **Plan the Upgrade Path:** From licenses to hardware, get a head start before the last-minute scramble.
3. **Secure Your Business:** Ensure you have the tools to stay protected and productive.

Take Advantage of our offers: Explore our hand-picked selection of desktops and laptops, and secure stock now at exceptional prices.

If you have not had a recent IT strategic review, contact Mark to schedule it in ASAP.

NEED A LAUGH?

Why shouldn't you use "beef stew" as a computer password?

It's not stroganoff.

TECHNOLOGY TRIVIA

The question this month is:

What year was the QR code invented?

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 365 CoPilot

Until now Microsoft 365 CoPilot has only been available to purchase annual up front for $538.

From January 2025 this will be available to purchase with monthly payments and annual commitment too giving more flexibility and allowing more businesses to deploy it to more staff. There are a few steps to take to make sure your organisation and data is ready for this technology. A CoPilot readiness assessment should be carried out and some data hygiene may be required.

We are having the CoPilot discussion with all our clients but if you need any help in planning this please reach out.