MONTH: JULY 2023

TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly update from Mark

With the increasing use of smartphones for work-related tasks, it's crucial to consider the security of the apps that your employees use on their phones. Many popular apps may not be adequately secured, leaving sensitive business data vulnerable to attacks.

To ensure the security of your business data, it's essential to take proactive measures such as implementing mobile device management (MDM) solutions that can manage app security on employee phones. Additionally, encouraging employees to be careful about the apps they download and app permissions can build security awareness.

If you want to learn more about improving mobile device security, contact us at mark@phrixus.com to schedule a chat.

Until then, stay safe,

Mark

DID YOU KNOW

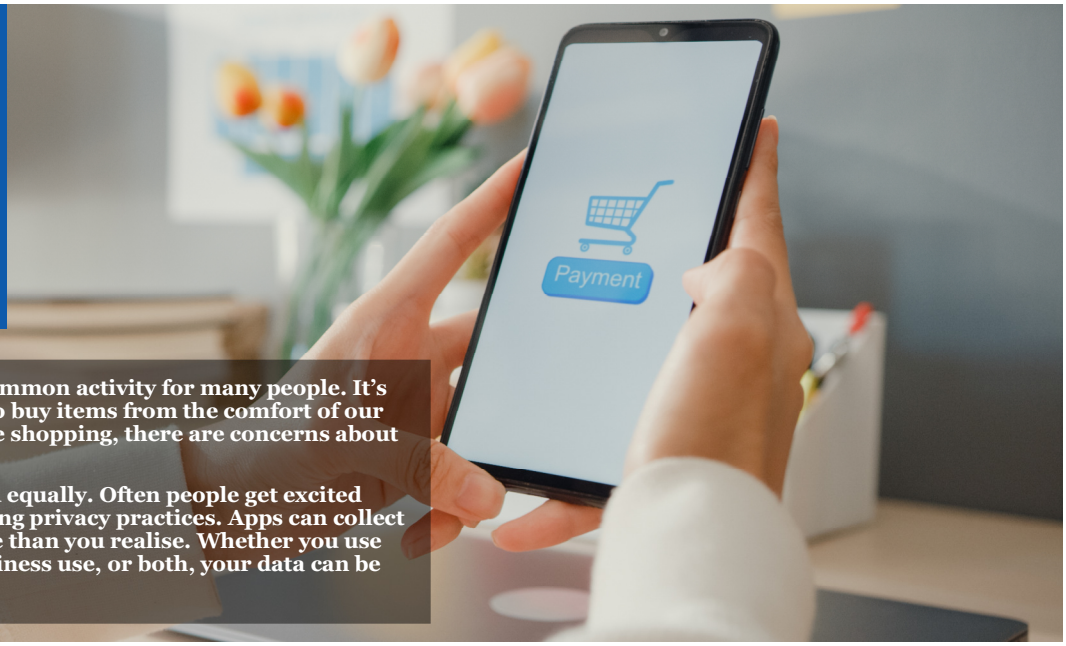
The first-ever email was sent in 1971 by computer engineer Ray Tomlinson.

Phrixus Technologies

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

02

IS YOUR ONLINE SHOPPING APP INVADING YOUR PRIVACY?



Online shopping has become a common activity for many people. It's convenient, easy, and allows us to buy items from the comfort of our homes. But with the rise of online shopping, there are concerns about privacy and security.

Not all shopping apps are created equally. Often people get excited and install an app without checking privacy practices. Apps can collect more data from your smartphone than you realise. Whether you use your phone for personal use, business use, or both, your data can be at risk. So can your privacy.

Shady Data Collection Practices from Popular Shopping App SHEIN

Recently, security experts found a popular shopping app spying on users' copy-and-paste activity. This app was tracking users' keystrokes, screenshots, and even their GPS location. This raises the question: Is your online shopping app invading your privacy?

SHEIN is the app in question, and it's a popular shopping app with millions of users. According to reports, researchers found the app collecting data from users' clipboards. This included any text that users copied and pasted. This means that if the user copied and pasted sensitive information, the app would have access to it.

Including things like passwords or credit card numbers.

Not only that but the app was also found to be tracking users' GPS location. SHEIN was also collecting data from device sensors, including the accelerometer and gyroscope. This means that the app was able to track users' movements. As well as collecting information about how they were using their device.

The app's developers claimed that the data collection was for "optimising user experience." A very vague explanation that's used by other app developers as well. The developers stated that the collected data was only used for internal purposes. But this explanation wasn't enough to please privacy experts. Those experts raised concerns about the app's data collection practices.

Temu Data Collection Practices Questioned

This isn't the first time people caught an app grabbing data without users' knowledge. Many popular apps collect data from their users, often for targeted advertising purposes.

The popularity of the shopping app Temu has been exploding recently. Since the app appeared in a Superbowl Ad in 2023, people have been flocking to it.

But Temu is another shopping app with questionable data collection practices. Some of the data that Temu collects includes:

- Your name, address, phone number
- Details you enter, like birthday, photo, and social profiles
- Your phone's operating system and version
- Your IPS address and GPS location (if enabled)
- Your browsing data

Tips to Protect Your Privacy When Using Shopping Apps

Know What You're Getting Into (Read the Privacy Policy)

Yes, it's hard to stop and read a long privacy policy. But, if you don't, you could end up sharing a lot more than you realise.

Turn Off Sharing Features

Turn off any data-sharing features you don't need in your phone's settings.

Such as location services. Most smartphones allow you to choose which apps you want to use it with.

Remove Apps You Don't Use

If you're not using the app regularly, remove it from your phone. Having unused apps on your phone is a big risk.

Research Apps Before You Download

It's easy to get caught up in a fad. You hear your friend talk about an app, and you want to check it out. But it pays to research before you download.

Shop on a Website Instead

You can limit the dangerous data collection of shopping apps by using a website instead. Most legitimate companies have an official website.

AnkerMake M5 3D Printer

The AnkerMake M5 3D Printer is a cutting-edge device that brings your creative ideas to life in three dimensions. It's like having a mini factory right at your fingertips!

It is a fantastic investment for anyone looking to explore the world of 3D printing. With its user-friendly interface, high-quality prints, and efficient design, it's the perfect tool to bring your creative visions to life.

Get yours at
https://www.ankermake.com/

03 HOW MICROSOFT 365 COPILOT IS GOING TO TRANSFORM M365 APPS

Microsoft is one of the biggest players in the office application field. It's at the forefront of introducing transformative technology. The company is about to transform Microsoft 365 in a huge way with its new Copilot app.

Microsoft 365 Copilot is a new tool designed to help users get the most out of their Microsoft 365 apps. This revolutionary tool is an intelligent, personalised assistant.

Let's take a closer look at Microsoft 365 Copilot and the key ways it's going to improve M365 apps and your business workflows.

What is Microsoft 365 Copilot?

Microsoft 365 Copilot is an AI-powered assistant. It helps users with their day-to-day tasks in M365 apps. It works across all M365 apps. This includes:

- Word
- Excel
- PowerPoint
- Outlook
- Teams
- and more

The tool is currently in testing and should be out sometime soon.

How Does Microsoft 365 Copilot Work?

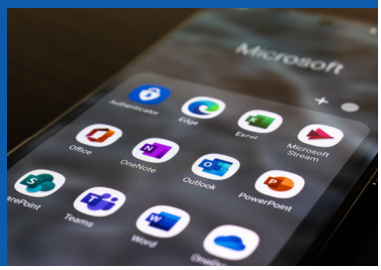
Microsoft 365 Copilot uses AI and machine learning to understand users' needs. It provides personalised help. It uses data from users' interactions with M365 apps. It learns a user's usage patterns and offers recommendations based on their preferences.

Say that you're working on a presentation in PowerPoint and struggling with design. Microsoft 365 Copilot can offer design suggestions based on your company's brand guidelines.

Microsoft 365 Copilot can also help users with common tasks. Tasks such as scheduling meetings and managing emails.

Benefits of Using Microsoft 365 Copilot

- Personalised Help - Microsoft 365 Copilot provides personalised help based on users' usage patterns and preferences.
- Time Saving - Microsoft 365 Copilot can help users save time on common tasks. Such as scheduling meetings and formatting documents. It can take on many information gathering tasks, like summarising meeting notes. Knowledge workers spend an average of 2.5 hours per day searching for information.
- Reduced Frustration – Microsoft 365 Copilot can help reduce frustration. It provides solutions when users are stuck on a task. The tool can also help users struggling with an Excel chart or table. Instead of having to figure out how to generate it, they can simply give a command to Copilot to do it for them.
- Improved Productivity – Microsoft Copilot handles tasks that go beyond what business apps have historically done. For example, you can use it in PowerPoint to create a presentation for you. Use a command such as, "Create a six-slide presentation based on (this) document." You can also tell it to find appropriate Microsoft stock photos and insert them.



04 LEARN HOW TO FIGHT BUSINESS EMAIL COMPROMISE

A significant cyber threat facing businesses today is Business Email Compromise (BEC). BEC attacks jumped 81% in 2022, and as many as 98% of employees fail to report the threat.

What is Business Email Compromise (BEC)?

BEC is a type of scam in which criminals use email fraud to target victims. These victims include both businesses and individuals. They especially target those who perform wire transfer payments.

BEC attacks are usually well-crafted and sophisticated, making it difficult to identify them. The attacker first researches the target organisation and its employees online. They gain knowledge about the company's operations, suppliers, customers, and business partners.

The scammer pretends to be a high-level executive or business partner. Scammers send emails to employees, customers, or vendors.

These emails request them to make payments or transfer funds in some form.

The email will often contain a sense of urgency, compelling the recipient to act quickly. The attacker may also use social engineering tactics. Such as posing as a trusted contact or creating a fake website that mimics the company's site. These tactics make the email seem more legitimate.

According to the FBI, BEC scams cost businesses about $2.4 billion in 2021.

These scams can cause severe financial damage to businesses and individuals. They can also harm their reputations.

How to Fight Business Email Compromise

BEC scams can be challenging to prevent. But there are measures businesses and individuals can take to cut the risk of falling victim to them.

- Educate Employees
- Enable Email Authentication
- Deploy a Payment Verification Processes
- Check Financial Transactions
- Establish a Response Plan
- Use Anti-phishing Software

05 SMALL BUSINESS TIPS TO GET READY FOR THE UNEXPECTED

What would you do if your business suffered a ransomware attack tomorrow? Do you have a contingency plan in case of any disasters? The unexpected can happen anytime, and small businesses can get hit particularly hard.

Here are 10 helpful tips to get ready for anything:

1. Create a Contingency Plan
2. Maintain Adequate Insurance Coverage
3. Diversify Your Revenue Streams
4. Build Strong Relationships with Suppliers
5. Keep Cash Reserves
6. Build Strong Outsourcing Relationships
7. Check Your Financials Regularly
8. Invest in Technology
9. Train Employees for Emergencies
10. Stay Up to Date on Regulatory Requirements

06 BEST PRACTICES FOR SECURING YOUR HOME NETWORK

In today's world, technology is ubiquitous, and connectivity is a must. Securing your home network has become more critical than ever. A secure home network is essential for protecting your personal data from hackers.

From phishing to smishing (SMS phishing), it's getting harder to avoid a breach.

The National Security Agency (NSA) has provided some best practices for securing your home network:

- Change Default Passwords and Usernames
- Enable Encryption
- Update Firmware
- Enable a Firewall
- Disable Unused Services
- Secure Wi-Fi Network
- Use Strong Passwords
- Create a Guest Network
- Limit Physical Access

07 HOW TO USE THREAT MODELING TO REDUCE YOUR CYBERSECURITY RISK

Today's offices are digitally sophisticated. Just about every activity relies on some type of technology and data sharing. Hackers can breach these systems from several entry points. This includes computers, smartphones, cloud applications, and network infrastructure.

It's estimated that cybercriminals can penetrate 93% of company networks.

One approach that can help organisations fight these intrusions is threat modeling. Threat modeling is a process used in cybersecurity. It involves identifying potential threats and vulnerabilities to an organisation's assets and systems.

Here are the steps businesses can follow to conduct a threat model:

- Identify Assets That Need Protection
- Identify Potential Threats
- Assess Likelihood and Impact
- Prioritise Risk Management Strategies
- Continuously Review and Update the Model

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 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).

Phrixus Technologies supporting the Can Too Foundation and raising funds for Cancer Research

As many of you have been aware Mark has been supporting the Can Too Foundation with raising funds for essential Cancer Research through the half marathon training programs.
He always said he would NEVER run a full 42Km marathon but that has now changed. Due to some amount of peer pressure and thinking he can run that distance once in his lifetime he will be participating in the Sydney Marathon this September and is in full swing with the training program now in week 9 of 20. If anyone would like to donate to this great cause please do so by visiting:

https://www.cantoo.org.au/fundraisers/markgiles/blackmores-marathon-2023

Many thanks for your generous donations

NEED A LAUGH?

Why was the computer cold at the office?

Because it left its Windows open!

TECHNOLOGY TRIVIA

The question this month is:

Who invented the first digital camera?

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!

Client Security and Privileged Information

We are sometimes contacted by unknown third party providers of our clients requesting information about your network and IT security. Please remember it is our security policy that we will not engage in these requests and will provide no information to them. All communication regarding these requests has to come from the main authorised IT contacts for our clients. This also includes completing any insurance or compliance forms. We provide the reports and information regularly so you already have the information to hand, we can assist but are not able to complete these forms for you.

Client security is our priority, many thanks for understanding.