TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly update from Mark

Have you ever wondered about the differences between malware and ransomware? These days, knowing how to spot each one is not just a matter of technical knowledge—it's a crucial aspect of cybersecurity.

From personal data protection to keeping business operations safe, knowing how to point out and defend against these digital threats is vital. But what does this mean for you and your sensitive data?

Recognising the signs of malware and ransomware could be the key to preventing devastating cyberattacks. Whether you're an individual user or managing enterprise-level systems, the ability to differentiate between these threats is essential.

Ready to enhance your cybersecurity knowledge and protect yourself from these evolving threats? Contact us at mark@phrixus.com to learn more about defense strategies against malware and ransomware.

Until then, stay safe,

Mark

DID YOU KNOW

The first commercially available USB flash drive provided 8mb of storage? Today you can buy USB flash drives with hundreds of gigabytes for cheap.

Phrixus Technologies

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

02
SPOTTING THE DIFFERENCE BETWEEN MALWARE AND RANSOMWARE

Bad software includes malware and ransomware. They can damage your computer or steal your data. It is critical to understand the difference between them to protect yourself and your business effectively.

This article will help you understand both types of threats.

What is Malware?

Malware is a general term that means "malicious software." This includes many types of harmful programs. Malware can do different bad things to your computer, such as corrupting files or stealing personal information.

Types of Malware

There are many types of malware. Here are some common ones:

- Viruses: These spread from one computer to another.
- Worms: They can copy themselves without your help.
- Trojans: They trick you into thinking they're good programs.
- Spyware: This type watches what you do on your computer.

What Malware Does

- Malware can cause a lot of problems. It might:
- Slow down your computer
- Delete your files
- Steal your personal info
- Use your computer to attack others

What is Ransomware?

Ransomware is a type of malware. It locks your files or your entire computer. Then it demands money to unlock them. It is a form of digital kidnapping of your data.

How Ransomware Works

1. Ransomware goes by a pretty basic pattern:
2. It infects your computer, normally through an e-mail or download.
3. It encrypts your files. This means it locks them with a secret code.
4. It displays a message. The message requests money to decrypt your files.
5. You may be provided with a key to unlock the files if you pay. In other cases, the attackers abscond with your money.

Types of Ransomware

There are primarily two types of ransomware:

- Locker ransomware: This locks the whole computer.
- Crypto ransomware: This only encrypts your files.

How are Malware and Ransomware Different?

Goals

- Malware: Harm your computer, steal data, or use your computer for attacks.
- Ransomware: Lock your files and demand payment.

Methods

- Malware: Works in secret. You might not know it's there.
- Ransomware: Shows up. It needs to make its presence known on your computer and demand money for its removal.

Effects

- Malware: There are several different effects malware can have on your computer.
- Ransomware: Computer or important files are always locked.

How Does It Get onto Your Computer?

Common Entry Points

- Through email attachments
- Via phony websites
- Via a USB drive with an infection
- From using outdated software

How Can You Protect Yourself?

- Keep your software up to date
- Use strong passwords
- Don't click on strange links or attachments
- Backup your files regularly

Why It Pays to Know the Difference

- Better Prevention. The more you know what you are against, the better your chance at taking the right steps to keep yourself safe.
- Faster Response. If you are under attack, knowing what type of threat it is helps you take quicker action.

We want to keep you secure in the face of all of cyberthreats. Contact us if you need more information.

TECHNOLOGY TRIVIA

The question this month is:

What is the name of the landscape wallpaper that was a default on Windows XP?

The first person to email me at **mark@phrixus.com** and give a correct answer gets a $50 Amazon Gift Card!

03 TOP 10 SECURITY TIPS FOR MOBILE APP USERS

Mobile applications have become an integral part of our lives. But they open us up to risks caused by fraudsters who may steal information or damage our phones.

How can you choose safe apps?

Only download from official stores.

Always download your apps from the App Store or Google Play.

Check app ratings and reviews.

Before you download an app, see what other people are saying about it.

What should you do before installing an app?

Read app permissions.

Apps frequently request permission to access certain parts of your phone. Consider whether they really need that information.

Update your phone's operating system.

Keep the software on your phone up to date. New updates frequently patch security vulnerabilities.

How can you protect your personal information?

Use strong passwords.

Make sure your password is difficult to guess. Do not use the same password for all apps. That way, if a person guesses one password, he or she cannot access all your apps.

Enable two-factor authentication.

Two-factor authentication means an additional step in order to log in. This will make it way harder for bad people to get into your accounts.

What should you be careful about when using apps?

Beware of public Wi-Fi.

Public Wi-Fi is never a safe space, it's not recommended to use it. Never use public Wi-Fi on important apps. Wait until you're on a safe network, like the apps for banking.

Log out of apps not in use.

Log out of apps whenever you're done using them. This is even more important when the apps hold personal information, such as banking or email apps. In case someone steals your phone, it's much harder for them to access such apps.

How do you protect your apps?

Update your apps.

Developers of applications usually fix security issues in updates. Keep updating your apps whenever newer versions get released. It will help in safeguarding your information.

Use app security features.

Lots of apps have additional security features, which may include fingerprint locks or face recognition. It's a good idea to switch these on if you can, as they help stop other people from using your apps and accessing your personal information.

What should you do to stay safe?

It's not hard to stay safe with mobile apps. Just be careful and think before you act. Only download apps you trust. Keep your phone and apps updated. Use strong passwords and extra security when you *can*.

Remember, safety is in your hands. And if ever you are confused with any app or anything on how to keep safe, don't hesitate to ask for help.

For more mobile app security tips, feel free to contact us today.

04 IS IT TIME FOR A DEVICE UPGRADE? CHECK FOR THESE 7 SIGNS

Technology is fast, and in no time, our gadgets get outdated. It is quite tricky to determine when an upgrade is needed. Here are the seven main signs that it is time to get a new gadget.

- Is Your Device Slow and Laggy? Slow performance is a major indicator. If your device takes an eternity to boot up, that might be a sign to get an upgrade.
- How's Your Battery Life? Battery problems are a clear upgrade sign. If your device dies quickly, it's a red flag. Needing to charge multiple times a day is not normal. A healthy device should last most of the day on one charge.
- Is Your Storage Always Full? Running out of space all the time? That's a good indication that an upgrade is due. It is frustrating when you can't install new apps. Constantly deleting photos and files is a pain. More storage is one great reason to upgrade.
- Are You Missing Out on New Features? New devices boast cool new features. If your device can't get the latest updates, you're missing out. Newer models often boast better cameras and screens. They also have faster processors and more memory.
- How Old Is Your Device? Age plays a huge factor in device performance. Most smartphones last around 2-3 years, and laptops, perhaps 3-5 years. Older devices struggle with new software and apps.
- Are Repairs Costing Too Much? If the repair costs are high, upgrading may be wiser. Sometimes, the repair costs are almost equal to a new device. In such cases, it is often better to buy a new one.
- Does Your Device Support the Latest Software? Older devices often can't run new software. This may be a security risk and also means you miss new features. Consider upgrading if your device can't update to the latest OS.

Ready for a Fresh Start?

Don't wrestle with an older, slower device; upgrade to one that will serve you much better. If you need help upgrading, contact us today.

05 8 CONSIDERATION BEFORE BUYING USED TECHNOLOGY

Here are a few things to consider before purchasing used tech:

- Is the device still supported? Older devices may not receive updates.
- How old is the device? Check when it originally hit the market.
- What's the battery life like? Try to get a rough idea about the battery health.
- Are there any visible damages? Search for cracks, dents, and water damage.
- Does it come with all accessories? Missing items could mean additional purchases.
- What's the return policy? See if you can take it back if something goes wrong.
- How does the price compare? Compare it with new and used alternatives to make sure you're getting the best deal.
- Can you test it before buying? It's always a good idea to try a device before you buy.

06 HOW MUCH DEVICE STORAGE DO YOUR REALLY NEED?

Device storage dictates how many applications, photos, and files you can retain on your device. This guide will help you figure out how much storage is actually needed.

- Basic users: 64GB is perfect for email, social media, and light photo taking.
- Average users: For people who take lots of photos and use many apps, 128GB to 256GB works to cover many apps, photo libraries, and some video storage.
- Power users: If you work with large files or store lots of media, you need 512GB or more. This is for video editing, large game libraries, and huge photo collections.
- Professional users: 1TB or more is common for 4K video production, large datasets, and professional photo editing.

07 ALL ABOUT THE NEW U.S. CYBER TRUST MARK

The Cyber Trust Mark is a new smart device label created by the US government to prove that a device is safe.

You may see a shield with the "U.S. Cyber Trust Mark" when device shopping. Here are the key details:

- **Devices must go through testing to ensure they meet requirements.** Companies send their devices for testing and if a device passes, it gets the mark.
- **Any device with the label is safe to use.** The Cyber Trust Mark makes shopping simpler. We may simply look for the mark to know which devices are safe.
- **If a device doesn't have the mark, that doesn't mean it's not safe.** In this case, you should look into its safety features.
- **It will be implemented right away, so you may see it during your next shopping trip.** The government wants stores to start using it immediately.

Stay Safe and Smart

The Cyber Trust Mark helps us in making informed choices; it's an easy way to know what devices are safe.

If you have any questions about device safety, don't be afraid to ask. We're here to help keep you secure.

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 more you refer the more we will reward you!

Guide to understanding domain registrations and DNS hosting

We often receive questions surrounding the confusion of domain registration, DNS hosting, web hosting and email hosting. To simplify this as best as possible, lets compare it to a car:

1 **Domain registration**—a car needs to be registered with the Roads and Maritime Authority. A domain name has to be registered with a domain registrar, of which there are many and we use TPP Wholesale to register and renew your domain names.

2 **DNS Hosting or DNS Management**—This has to be included with all domain names much like a car having to have CTP insurance. It can often be hosted with the domain registrar, Microsoft or another domain management service. Be VERY careful in not allowing web developers access to this as they often will break other essential services such as email.

3 **Email hosting**—In most of our clients' cases this is hosted with Microsoft in Exchange Online but also can be Google Business mail. This can be equated to having fully comprehensive insurance and is essential for Businesses to have.

4 **Web hosting**—This is where your website is hosted, in most cases should be at your web developers preferential hosting platform and WordPress is the most popular. This needs constant maintenance in security updates, being backed up and content updates. Consider this similar to breakdown assistance. Not all businesses have much of a web presence but many will have.

NEED A LAUGH?

What happens when a hard drive gets into a fight?

It asks for backup.

Security Permissions and local admin restrictions

Some of you may have observed a recent security enforcement where your primary login account on your system has been restricted from having elevated permissions and the ability to install applications.

This measure is implemented to prevent the inadvertent execution of malicious content.
This ultimately safeguards individuals as malicious content evolves in sophistication, causing more individuals to fall victim unknowingly.

Although this condition is not new, it is now being enforced to comply with recommended best security practices to protect your data and your business.
It has always been a requirement agreed upon by everyone in our Service Agreements.

We are enhancing our security measures and extending them to all our clients in preparation for SMB1001:2025 Cyber Security framework requirements.