TECH MONTHLY TALK

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

Monthly Update From Mark

It's a surprising statistic, but Microsoft estimates that mobile devices now do 80% of the workload in an office. Yeah, eighty percent!! They make up over half of the endpoints that a company must consider when planning network security.

But many organisations are still looking at computers first, servers second, then smartphones and tablets after that. As a result, there are a lot of risks out there when it comes to a lost or stolen device.

One lost tablet with access to sensitive customer or patient data can result in a major compliance violation if that info isn't protected. Not to mention the risk to your network if a hacker can plant ransomware that spreads from one device to another.

Just think about all the apps that a mobile device is persistently logged into. There's business email, cloud storage like Dropbox or OneDrive, and work apps like Zendesk, Salesforce, or Slack.

Oh, and all those stored browser passwords to websites and cloud accounts... these are also free game to a criminal with a stolen work device. How well protected are the mobile devices used at your business?

Are you worried about data exposure through smartphones and tablets? Need some help understanding what "endpoint device management" is all about? We'd love to chat. Drop me an email at mark@phrixus.com

Until then, stay safe,

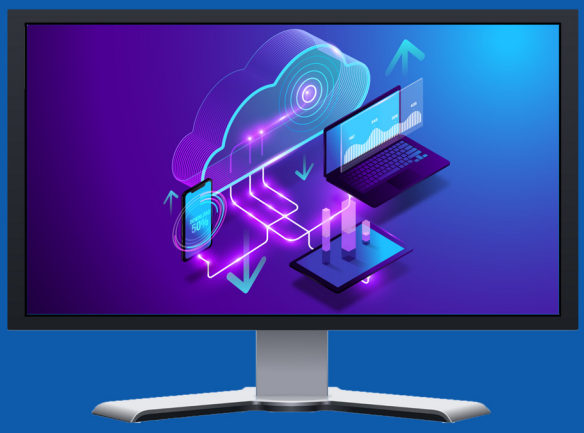
Mark

DID YOU KNOW?

Google's Android mascot is unofficially known as Bugdroid

Phrixus Technologies

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



02

HELPFUL TIPS FOR KEEPING YOUR SHARED CLOUD STORAGE ORGANISED

Cloud file storage revolutionised the way we handle documents. No more having to email files back and forth. No more wondering which person in the office has the most recent copy of a document.

But just like the storage on your computer's hard drive, cloud storage can also get messy. Files get saved in the wrong place and duplicate folders get created.

When employees are sharing the same cloud space it's hard to keep things organised. Storage can be difficult to keep efficient.

Disorganised cloud storage systems lead to problems. This includes having a hard time finding files. As well as spending a lot of extra time finding needed documents.

Has your office been suffering from messy cloud storage? Does it seem to get harder and harder to find what you need?

Here are several ways to tidy up cloud storage spaces and save time:

Use a Universal Folder Naming Structure

When people use different naming structures for folders, it's harder for everyone.

They often can't find what they need. It also leads to the creation of duplicate folders for the same thing.

Map out the hierarchy of folders and how to name each thing. For example, you might have "departments" as an outer folder and nest "projects" inside.

With everyone using the same naming system, it will be easier for everyone to find things. You also reduce the risk of having duplicate folders.

Keep File Structure to 2-3 Folders Deep

When you have too many folders nested, it can take forever to find a file. You feel like you must click down one rabbit hole after another. When people need to click into several folders, it discourages them from saving a file in the right place.

To avoid this issue, keep your file structure only two to three folders deep. This makes files easier to find and keeps your cloud storage more usable.

Use Folder Tags or Colors for Easier Recognition

Many cloud file systems allow you to use color tagging on folders. Using this can make a folder or group of folders instantly recognisable. This reduces the time it takes to find and store files .

Don't Create Folders for Fewer Than 10 Files

The more folders people have to click into to find a document, the more time it takes. Folders can quickly add up as employees create them, not knowing where a file should go.

Use a rule for your cloud storage that restricts folder creation to 10 files or more.

This avoids having tons of folders with less than a handful of files in them. Have someone that can act as a storage administrator as well. This can then be the person someone asks if they're not sure where to store a file.

Promote the Slogan "Take Time to Save it Right"

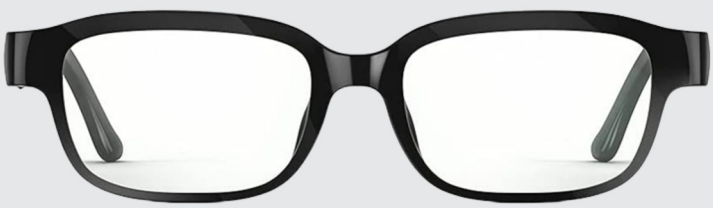
We're all guilty from time to time of saving to something general, like the desktop on a PC. We tell ourselves that we'll go back at some point and move the file where it should be.

This issue multiplies when you have many people sharing the same cloud storage space. Files that aren't where they belong add up fast.

This makes it harder for everyone to find things.

Promote the slogan "take time to save it right" among the staff. This means that they should take the extra few seconds to navigate where the file should be to save it. This keeps things from getting unmanageable. If you use a file structure that's only 2-3 folders deep, then this should be easier for everyone to abide by.

ECHO FRAMES



The Echo Frames are a sleek pair of unassuming black glasses. You would never guess that they have a fully capable Alexa speaker and microphone built into the sides.

They don't provide an AR experience though.

They work the same as a Bluetooth headset allowing you to give Alexa commands and listen to your Audible library on the go. They just happen to be mounted on some sleek eyeglass frames.

03 YOU NEED TO WATCH OUT FOR REPLY-CHAIN PHISHING ATTACKS

Phishing. It seems you can't read an article on cybersecurity without it coming up.

That's because phishing is still the number one delivery vehicle for cyberattacks.

80% of surveyed security professionals say that phishing campaigns have significantly increased post-pandemic.

Phishing not only continues to work, but it's also increasing in volume due to the move to remote teams.

Many employees are now working from home. They don't have the same network protections they had when working at the office.

One of the newest tactics is particularly hard to detect. It is the reply-chain phishing attack.

What is a Reply-Chain Phishing Attack?

You don't expect a phishing email tucked inside an ongoing email conversation between colleagues.

Most people are expecting phishing to come in as a new message, not a message included in an existing reply chain.

The reply-chain phishing attack is particularly insidious because it does exactly that. It inserts a convincing phishing email in the ongoing thread of an email reply chain.

How does a hacker gain access to the reply chain conversation? By hacking the email account of one of those people copied on the email chain.

The hacker can email from an email address that the other recipients recognise and trust. The attacker also gains the benefit of reading down through the chain of replies. This enables them to craft a response that looks like it fits.

They may see that everyone has been weighing in on a new product idea for a product called Superbug. So, they send a reply that says, "I've drafted up some thoughts on the new Superbug product, here's a link to see them."

The reply won't seem like a phishing email at all. It will be convincing because:

- It comes from an email address of a colleague. This address has already been participating in the email conversation.
- It may sound natural and reference items in the discussion.
- It may use personalisation. The email can call others by the names the hacker has seen in the reply chain.

Business Email Compromise is Increasing

Business email compromise (BEC) is so common that it now has its own acronym. Weak and unsecured passwords lead to email breaches. So do data breaches that reveal databases full of user logins.

Tips for Addressing Reply-Chain Phishing

Here are some ways that you can lessen the risk of reply-chain phishing in your organisation:

- Use a Business Password Manager
- Put Multi-Factor Controls on Email Accounts
- Teach Employees to be Aware

04 MICROSOFT PRODUCTIVITY SCORE OVERVIEW

Productivity can be challenging to track, no matter where employees are working. How do you know they're using their tools as effectively as possible? How can you enable them to adopt best practices?

You can't grade productivity simply by "clock in/clock out" times. In today's hybrid and mobile offices, the value and work product an employee brings is a better gauge. But you also must look at what may be getting in the way of great employees doing great work.

If your company uses Microsoft 365 then you have a tool you can use to find nuggets of productivity gold. This tool is Microsoft Productivity Score.

What Does Microsoft Productivity Score Do?

Microsoft Productivity Score looks at some core areas of your employees' workflow and gives you helpful insights that you can share with your staff. These insights help to boost their performance. It also includes hardware-related information.

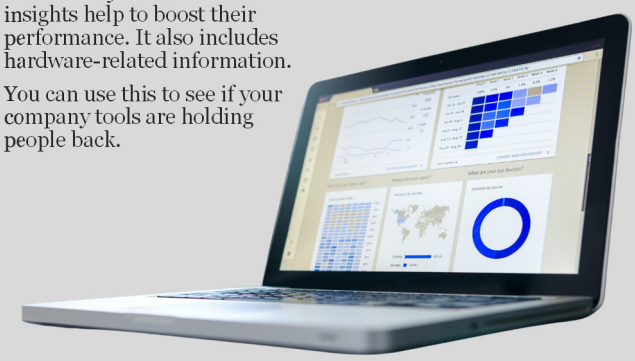
You can use this to see if your company tools are holding people back.

How Productivity Score Helps Your Company

- Automatic Metrics Tracking
- Insights to Understand the Data
- Recommended Actions to Take

MS Productivity Score looks at the following areas.

- People Experiences
  - Communication
  - Content collaboration
  - Mobility
  - Meetings
  - Teamwork
- Technology Experiences
  - Endpoint analytics (You need Intune for these)
  - Network connectivity
  - Microsoft 365 apps health
- Special Reports



05 REDUCE RISK WHEN YOU LOSE A MOBILE DEVICE

Few things invoke instant panic like a missing smartphone or laptop. These devices hold a good part of our lives. This includes files, personal financials, apps, passwords, pictures, videos, and so much more.

The things you do in the minutes after missing a device are critical. This is the case whether it's a personal or business device. The faster you act, the less chance there is for exposure of sensitive data.

Steps to Take Immediately After Missing Your Device

- Activate a "Lock My Device" Feature
- Report the Device Missing to Your Company
- Log Out & Revoke Access to SaaS Tools
- Log Out & Revoke Access to Cloud Storage
- Activate "Wipe My Device" Feature

06 TECHNOLOGY TOOLS YOU SHOULD UNINSTALL

While older technology may still run fine on your systems that doesn't mean that it's okay to use. One of the biggest dangers of using outdated technology is that it can lead to a data breach.

Outdated software and hardware no longer receive vital security updates. No security patches means a device is a sitting duck for a cybersecurity breach.

Get Rid of This Tech Now If You're Still Using It

- Internet Explorer
- Adobe Flash
- Windows 7 and Earlier
- macOS 10.14 Mojave and Earlier
- Oracle 18c Database
- Microsoft SQL Server 2014 (losing support in 2024)

07 6 IMPORTANT IT POLICIES ANY SIZE COMPANY SHOULD IMPLEMENT

Many smaller businesses make the mistake of skipping policies. They feel that things don't need to be so formal.

But this way of thinking causes issues for business owners.
Employees aren't mind readers.

Things that you think are obvious, might not be to them.

IT policies are an important part of your IT security and technology management.

Here are some of the most important to have in place.

1. Password Security Policy
2. Acceptable Use Policy (AUP)
3. Cloud & App Use Policy
4. Bring Your Own Device (BYOD) Policy
5. Wi-Fi Use Policy
6. Social Media Use Policy

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).

NEED A LAUGH?

Machetes are extremely tech savvy

They can hack anything!

TECHNOLOGY TRIVIA

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!

The question this month is:

What is the most commonly used password?

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

LOCAL BUSINESS AWARDS 2022 FINALIST HORNSBY KU-RING-GAI

AUSTRALIAN SMALL BUSINESS CHAMPION AWARDS 2022 FINALIST

Following on from winning this award last year we are delighted to have reached the finalist stage in the local business awards again this year. It is a great achievement and recognition for our team to have been nominated and to reach this stage of the awards again.

We will let you know how we go when the awards are announced on October 19th.

Many thanks to all of you that voted for us.

We have also reached the finalist stage of the National Business Champion awards for Information Technology, the awards night for this are announced on Friday 2nd September.

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

Mark has once again joined the Can Too half marathon training program in preparation for the Sydney half marathon on Sept 18th.

All money raised for the Can Too Foundation supports community cancer prevention programs and cancer research.

All donations gratefully received to help me reach my goal target:

https://www.cantoo.org.au/fundraiser/markgiles/blackmores-half-marathon-2022

Many thanks for your support.