MONTH: JUNE 2022

TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

02 TOP 5 CYBERSECURITY MISTAKES THAT LEAVE YOUR DATA AT RISK

03 UNIFIED COMMUNICATIONS

04 BOOSTING VOIP SECURITY

05 PHISHING ATTACK TRENDS

06 TECH TIP OF THE MONTH

07 4 THINGS YOU SHOULD NEVER DO ON A WORK COMPUTER

Monthly update from Mark

In today's landscape of smart devices and computers in our pocket you would think that we've nailed the whole cybersecurity thing right?

But every day more and more people are tricked into visiting malicious websites, giving up personal information through social engineering and getting their re-used passwords compromised.

As unbelievable as it may sound, it's not only our senior citizens falling prey to these cyber-criminals, it's our younger generations as well. You would expect people 25 and under to be more tech savvy, and that's precisely the problem, they think so too.

And that's a problem for the modern workplace which is filled with college graduates and employees under 30 years old. And while their older counterparts tend to be more wary about sharing data, all it takes is one key login to bring down an entire network, and by consequence, the entire business.

But you're OK right? You have the fancy firewalls and antivirus with all the bells and whistles. But what about Security Awareness Training? Oh, you have that during employee onboarding? That's awesome! But what about the rest of the time?

Security Awareness Training needs to be a year-long endeavour and you need to keep your employees (and yourself) on their toes to make sure that they actually remember and apply what they learned when they read the employee manual when they started.

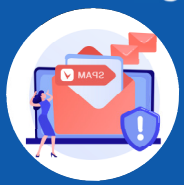
Call me on 02 9457 6416 Ext 401 or email me at mgiles@phrixus.com to find out more.

Have an outstanding month

Mark

DID YOU KNOW?

The origin of the word "spam" in the context of email originated from a Monty Python skit from the 70s



Phrixus Technologies

PO Box 266

Berowra NSW 2081

Phrixus.com

02 9457 6416

TOP 5 CYBERSECURITY MISTAKES THAT LEAVE YOUR DATA AT RISK

02

The global damage of cybercrime has risen to an average of $11 million USD per minute, which is a cost of $190,000 each second. 60% of small and mid-sized companies that have a data breach end up closing their doors within six months because they can't afford the costs.

The costs of falling victim to a cyberattack can include loss of business, downtime/productivity losses, reparation costs for customers that have had data stolen, and more. Many of the most damaging breaches are due to common cybersecurity mistakes that companies and their employees make.

Here are several of the most common missteps when it comes to basic IT security best practices.

Not Implementing Muti-Factor Authentication (MFA)

Credential theft has become the top cause of data breaches around the world, according to IBM Security.

MFA reduces fraudulent sign-in attempts by a staggering 99.9%.

Ignoring the Use of Shadow IT

Shadow IT is the use of cloud applications by employees for business data that haven't been approved and may not even be known about by a company.

Shadow IT use leaves companies at risk for several reasons:

- Data may be used in a non-secure application
- Data isn't included in company backup strategies
- If the employee leaves, the data could be lost
- The app being used might not meet company compliance requirements

It's important to have cloud use policies in place that spell out for employees the applications that can and cannot be used for work.

Thinking You're Fine With Only an Antivirus

No matter how small your business is, a simple antivirus application is not enough to keep you protected. In fact, many of today's threats don't use a malicious file at all.

Phishing emails will contain commands sent to legitimate PC systems that aren't flagged as a virus or malware. Phishing also overwhelmingly uses links these days rather than file attachments to send users to malicious sites. Those links won't get caught by simple antivirus solutions.

You need to have a multi-layered strategy in place that includes things like:

- Next-gen anti-malware (uses AI and machine learning)
- Next-gen firewall
- Email filtering
- DNS filtering
- Automated application and cloud security policies
- Cloud access monitoring

Not Having Device Management In Place

A majority of companies around the world have had employees working remotely from home since the pandemic. However, device management for those remote employee devices as well as smartphones used for business hasn't always been put in place.

A device management application in place, like Intune in Microsoft 365 can help manage this.

Not Providing Adequate Training to Employees

An astonishing 95% of cybersecurity breaches are caused by human error.

Employee IT security awareness training should be done throughout the year, not just annually or during an onboarding process.

Some ways to infuse cybersecurity training into your company culture include:

- Short training videos
- IT security posters
- Webinars
- Team training sessions
- Cybersecurity tips in company newsletters

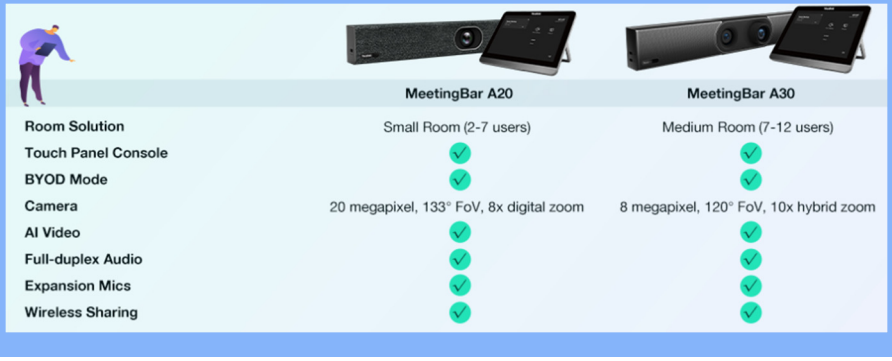
Video Conferencing

Yealink Meeting Bar A20 and A30

The All in One Meeting Bars for huddle and small spaces with integrated AI-powered camera, 8 MEMS microphone array and speaker. Includes the CTP18 collaboration touch panel.

A20 $2,420 inc GST

A30 $3,185 inc GST



03 UNIFIED COMMUNICATIONS KEY FEATURES

1. Mobility

When connected to unified communications, all employees can stay connected at all times and from all locations.

It doesn't matter whether they're working from home, vacationing on a remote island, or sitting in the office.

They'll still be able to chat, receive calls, and more.

2. Unified Messaging

This allows employees to handle different message types using a single tool. They can easily switch communication modes, depending on their needs.

3. Conferencing

Whenever you need conferencing tools, you'll have them in the palm of your hand. You can allow a group of teammates or customers from outside your organisation to connect and speak via video or audio from different locations.

4. Fax Support

Faxes received through unified communications appear as email attachments. This way, users can also receive faxes on their desktops and smartphones.

5. Presence

This feature lets other users know each other's status. That means you'll be able to see when someone is online (Active), busy (Do Not Disturb), or away (Out of the Office).

What Is Unified Communications?

It's a ready-to-use system that allows for seamless communication in numerous ways such as phone, video, screen sharing, chat and file management.

The system operates as a cloud, making it easily accessible to all team members with access to the internet.

But why should anyone consider switching to unified communications?

There are several reasons, but this is the most crucial:

Business leaders who adopt it would be able to impact their business every day and make it seamless for employees to interact with each other.

That said, we'll list 5 of the key features of this concept to help you better understand how it can help you scale your business.

04 BOOSTING VOIP SECURITY

Given the variety of threats imposed by attackers on VoIP systems, it's necessary to optimise your VoIP security ASAP.

Here are 6 valuable tips to get you started.

Tip #1. Set Up a Firewall

If spam or a threat comes your way, the firewall will identify and gain control over it, shielding your system shielded from the attack. A good set-up will allow the data packets you send to travel unhindered.

Tip #2. Use Strong Passwords

Use randomly generated passwords consisting of at least 12 characters including numbers, upper- and lower-case letters and symbols. Most VoIP phones come with pre-set passwords, often available publicly, change these immediately.

Tip #3. Restrict Calling

Many VoIP attacks happen due to toll fraud. So, if your business runs locally, there's no need to have the international call option enabled. You should also block 1-900 numbers to avoid toll fraud.

Tip #4. Encourage Your Team to Report Suspicious Behavior

You should hold periodical Cybersecurity Training to keep your environment safe at all times. Train your employees how to spot unusual network activity and report suspicious behavior.

Tip #5. Deactivate Web Interface Use

Unless it's absolutely necessary for you to use the web interface, be sure to secure it very strictly. It's enough for a single phone user falling prey to leave the whole system exposed to an external party. All your data can be stolen in text format as a result.

Tip #6. Use a VPN for Remote Workers

Virtual Private Networks (VPNs) are great software that encrypts traffic regardless of your employee's location. You can set up such a network for your remote staff to prevent data leaks and breaches. A well configured VPN won't degrade the call quality.

05 PHISHING ATTACK TRENDS

In 2020, 75% of companies around the world experienced a phishing attack.

Phishing remains one of the biggest dangers to your business's health and wellbeing because it's the main delivery method for all types of cyberattacks.

One phishing email can be responsible for a company succumbing to ransomware and having to face costly downtime.

It can also lead a user to unknowingly hand over the credentials to a company email account that the hacker then uses to send targeted attacks to customers.

Phishing takes advantage of human error, and some phishing emails use sophisticated tactics to fool the recipient into divulging information or infecting a network with malware.

Mobile phishing threats skyrocketed by 161% in 2021.

06 GOOGLE SEARCH TIPS

One way you can save time on your personal and work-related searches is to learn some "secret" Google search tips.

These help you narrow down your search results and improve productivity by helping you find the information you need faster.

- Search a Specific Website Using "site:" Type in the search bar site:(site url) (keyword)
- Find Flight Information Without Leaving Google Just type in the flight number and the name of the airlines, for example, type in the search bar American AA 1977
- Look for Document Types Using "filetype:" Type in the search bar filetype: (type) (keyword)
- Get Rid of Results You Don't Want Using "-(keyword)" Type in the search bar (keyword) -(keyword)
- Locate Similar Sites Using "related:" Type in the search bar related:https://website.com

07 THINGS YOU SHOULD NEVER DO ON A WORK COMPUTER

Save Your Personal Passwords in the Browser

If your company's network is compromised the malicious actors can leverage your passwords to access your cloud accounts.

Store Personal Data

This bad habit and leaves you wide open to:

- Loss of your files
- Your personal files being company-accessible

Visit Sketchy Websites

You should never visit any website on your work computer that you wouldn't be comfortable visiting with your boss looking over your shoulder.

Allow Friends or Family to Use It

Allowing anyone else to use your work computer could constitute a compliance breach of data protection regulations that your company needs to adhere to.

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:

Who launched the very first website?

The first person to email me at **mark@phrixus.com** and give a correct answer gets a $50 Amazon Gift Card!
Well done to Gary for the first answer received last month— Star Wars

Email and inbox management

We are adding this tip back as a reminder to all users of email as we have seen too many mailboxes blow out to unmanageable sizes and have to purchase additional licenses to work around the issue. It is each persons responsibility to manage their own mailbox.

Email and Outlook are a communication tool and was never intended to be a storage system, some tips and limits to consider are:

1. Mailbox management—strive for zero inbox and sent items. Emails you need to keep should be filed into a subfolder and delete anything unimportant.
2. Save large attachments into Sharepoint or on your server and remove them from the email
3. Empty your deleted items and junk folder daily
4. For quick messaging with your team, use the chat function in Teams/Slack/Google Chat instead of email

Most mailboxes have a 50Gb limit on the hosted server, Outlook is limited to a maximum 10,000 folders, 100,000 items per folder and 5,000 calendar items. If you are getting even close to these limits you will experience performance issues especially when accessing on an older slow system and on a slow internet connection.

The Phrixus Online Store

With the end of financial year approaching, please make sure if you need any IT products invoiced before the end of June, place your orders ASAP either from our online store or by contacting our staff for a quote to be sent.
All our clients should have a login for this and many have ordered from here over the past few years. If you haven't yet checked it out, login here:

https://shop.phrixus.com