phrixus TECHNOLOGIES

MONTH: JUNE 2021

TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

Monthly update from Mark

This month we've learned that as well as the over 75s, the under 25s are the most likely age group to be hit by cyber-fraud.

That seems crazy. Because we perceive under 25s to be tech-savvy. After all, they've grown up with the internet, devices and social media.

But because all of this is second nature to them, they've become a lot more relaxed about their use of technology and the internet. And in turn, they're far more willing to share their personal data.

What does this mean for you? Do you employ many people under 25? And if they're more likely to fall for a phishing scam, for example, could they pose a threat to your organization and its data?

This shows that you really need to put a focus on cyber-security training for all your people; and maximise your cyber-security features too. You simply can't afford to assume that just because some of your team are younger, they're less likely to fall for a scam.

I recommend that you train all of your people regularly on cyber-security and the latest threats to look out for. The more aware you are, the less likely you are to make a very expensive mistake.

If you're looking for advice on cyber-security and training, we'd love to help. You can reach me at mark@phrixus.com or 02 9457 6416 [ext 401] Take a look on page 4 for more information.

Until then, stay safe,

Mark

WHAT'S INSIDE?

DID YOU KNOW?

Apple once tried to branch out into another sector?

In 1986 Apple had a line of clothing, imaginatively named 'The Apple Collection'. It was launched a year after Steve Jobs resigned as chairman of the company. It wasn't a hit, as you can imagine, but it did include the very first 'Apple Watch'!

Phrixus Technologies

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

NEWS FROM THE COALFACE

1

DO YOU HAVE A BUSINESS IT STRATEGY

As a business owner you already know the importance of strategy and planning.

Without it, you have no aim, no goals, and really, no direction.

While you probably spend a lot of time working on your strategy every month, quarter, or year, how much of that time is spent on your business's IT strategy?

If the answer is "not very much", it's time to change that.

Your business's IT is one of your most powerful, crucial tools in growing your business, keeping your team productive, and giving your customers a great impression of you.

It makes sense that you have a plan for how:

- **It will work for you now and in the future**
- **You will need it to grow with your business**
- **It can help take your business to the next level, faster**

If you've never created an IT strategy before, or it's been a while, here are a few of the key elements you need to include...

YOUR BUSINESS GOALS

Your IT infrastructure is there to work seamlessly alongside your business. It should complement everything you do, or plan to do, and make reaching your business goals a little easier.

Will you need additional tools to help your sales pipeline? Will it accommodate any future partnerships or acquisitions you plan to make? What about the different departments within your business; do their needs differ?

PEOPLE AND TIME CONSIDERATIONS

Who in your business is responsible for delivering your IT strategy? Will it be created and driven in-house, or will you outsource it to external experts? Internally, who needs to be involved, whether that's liaising with external experts, or overseeing elements of your plan?

And how long do you want to take to make these changes? As with any business plan, you need to take both long and short term goals into account. Do your plans rely on reaching a new level of turnover, or will they be based on your people adapting to the changes?

YOUR CURRENT INFRASTRUCTURE

How's it working for you right now? What would you change? What can't you manage without?

It's a great idea to speak to people in different departments about this, because what works for one team may be totally unhelpful for another. You can tailor your infrastructure to work well for everyone and keep all of your department feeling happy and motivated.

A TECHNOLOGY ROADMAP

This step may be a little more difficult that the others, but it is really worthwhile.

Think about your whole IT architecture here. Your hardware, software, and any other tools that you'll want to utilize. If you need assistance here, a good IT support partner will be able to make recommendations on the best of everything to fit your needs.

Break your roadmap down into departments and include everything that each will need. This will allow you to see how everything fits together.

NEW METRICS

While your infrastructure needs to be functional, it also has to be cost effective. What's the point in making all of these changes if it's not bringing a financial benefit to you?

Look at your current KPIs and forecast how these should improve with the changes you're making. Make sure they're realistic - change won't happen immediately. Allow some time for your people to adapt to the new tools. You can not only measure performance, but your KPIs should also help you to identify issues before your end users are affected.

It may sound like a lot of work, but with a robust business IT strategy in place, you will soon start to wonder how you managed for so long without one. Need a hand? Just get in touch and we can help you get started.

2

ARE YOU AT RISK OF BEING SMISHED?

It’s safe to say we’ve all heard about phishing scams by now - if you haven’t, you’re not doing enough to protect your business from data theft.

But as with anything tech-related, things move on quickly.

Cyber-criminals will always try new and more powerful ways to trick you into giving away your data. And now they’re targeting our phones.

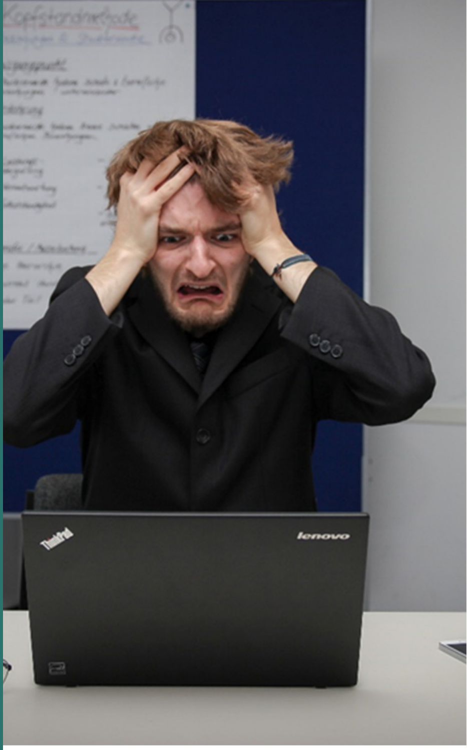
Ever received an SMS that you weren’t expecting, possibly from a well-known company? Maybe you received a notification that a courier attempted to deliver a package.

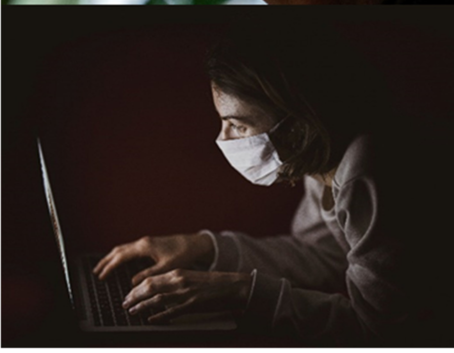
These kind of messages contain a link for you to click and rearrange delivery.

But when you click the link, you’re taken to a spoof page which steals your information as soon as you enter it.

This allows the scammer behind it to use those details to access your online accounts. Or gives them access to your device.

This is called smishing. The cell phone equivalent of phishing. You and your people need to be aware and ultra-vigilant.





What’s lead to this surge in smishing attempts? How successful it is.

98% of SMS messages are opened, and 45% are replied to. This is a much higher open rate than emails (which have an open rate of around 20%). So, it means a statistically higher success rate for the scammers behind the messages.

Beware of any unexpected SMS messages asking you to take an action by clicking a link or calling a number. If you’re unsure if it’s a genuine message, contact the company direct using the details on their website or any paperwork you have from them.

Make sure your whole team knows about this form of attack, too. If they’re using their smart phones to access work files then a smishing attempt to their personal device is also putting your business data at risk.

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.
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).

Staff Security Awareness Training

Old school Security Awareness Training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks. And require thorough ongoing training and testing.

Baseline Testing
Baseline testing can be provided to assess the Phish-prone percentage of your users through a simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See The Results
Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management.

Contact Mark for more information

NEED A LAUGH?

Whoever said that the definition of insanity is doing the same thing over and over again and expecting different results… has obviously never had to reboot a computer.

TECHNOLOGY TRIVIA

What is the origin of the word "spam" in the context of email spam?

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 being the first correct answer received last month.

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

Many thanks to everyone that supported Mark in donating to his Cancer Research fundraising page for the recent Barossa Valley half marathon training program that concluded on Sunday May 30th. Mark managed a personal best time at 1hr 50mins, raised $2,320 and ran 375KM since the end of February.

You can check the progress and donations are still open for a short while longer from the link below:

https://www.cantoo.org.au/fundraisers/markgiles