TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

MONTHLY UPDATE FROM TONY

Is it time you took a break from technology?

Taking a step back from our devices can bring so many benefits; closer relationships, less stress, more motivation... I could go on. But it's not easy when you run a business, is it?

Fortunately, there are loads of tools available that can give you that time away from the things that are most distracting. Take social media, for example. Wow, it can suck you down a hole and steal literally hours from your week. What else could you be doing with that time?

Try Cold Turkey, an app for Microsoft 365 that allows you to block social media (and any other distractions) for an amount of time dictated by you. And there are alternatives for your smart phones - Screen Time on iOS allows you to block apps or give yourself time limits on each one.

There's also evidence to suggest that switching your phone's display to a grayscale can help you cut down on time spent on distracting apps.

Use that saved time doing something productive. Or something to help you unwind and see what a difference it can make.

Have you tried any of these ideas already? How did they work for you? We'd love to hear the tricks you use to cut down on your tech time, and the ways it has improved your life or business. Let us know!

Kind Regards,

Tony Baulch

Founder & Technical Director

DID YOU KNOW?

In 2010 fewer than 2 billion people in the world used the internet. As of January this year, 4.57 billion people around the world are online. That's 59% of the world's population.

Ashdown Solutions Limited

East Grinstead
West Sussex
RH19 4LZ
www.ashdownsolutions.co.uk
01342 363000

1

WHEN WAS YOUR LAST REVIEW?

Relax. We're not going into HR mode.

What we want to talk about is reviewing who in your business has access to which documents.

Do you know who has access to your documents?

Or can everyone access everything?

You may need to make some changes. You see, the more people that have access to your business documents, the less secure they are.

Let's imagine for a moment, that one of your people opens a very convincing email, supposedly from a supplier. The email contains a document to download, which they do, because it's from a supplier, right? They can trust it.

What your employee didn't notice was that the email signature was missing, or that the email address wasn't the same as it usually is. And the document they downloaded has now installed malware on their device.

They don't notice the malware because it all looked legit and nothing obvious has happened. They continue their working day unaware.

While they're working, the malware is working too, in the background. It's accessing and copying all of the data that your employee has access to.

You might get lucky and stop this malware before it enters your network and takes everything, but if your employee already has access to everything, well, it's gone. Although this isn't a malicious act on behalf of the employee, they've essentially caused a huge data breach that could kill your business.

And this scenario doesn't even need the malware to become a reality. One day a member of your team might decide they'd like to make a little money by stealing your valuable data. By giving everyone access to everything, you're making it too easy for them.

So, if you haven't already done this, I suggest that this week you make it a priority to sit down and work out who needs access to which files and documents and restrict access to absolutely everything.

Keep your own document detailing who has access to what. And update it whenever anyone joins the business or changes roles. This is also a great way of protecting your data when somebody leaves, because you can see exactly what you need to revoke access to.

If you already restrict access, when was the last time you reviewed it? Are people able to access files they no longer need? And are there people who could benefit from access to more documents to complete their role?

Yes, that's a lot to think about. But once you have a detailed document to work from, regular reviews are pretty simple and definitely worth your time.

Ransomware is **big** business. It's one of the fastest growing online crimes, and if you haven't already been targeted, it's likely you will be at some point in the future.

It's the computer crime where your data is encrypted so you can't access it, unless you pay the ransom fee.

The really scary part is that it's unlikely you'd realize you were under attack from ransomware until it was too late.

Cyber criminals hide in your network for between 60 to 100 days before they strike. During that time they're checking out your network, identifying vulnerabilities, and preparing what they need to hit you with the attack.

And they do all of this without leaving much of a footprint for you to discover.

Fortunately, there are a number of signs you can be on the lookout for, to identify an attack and stop it in its tracks. This is the most technical thing you will ever read from us; but it's important you know what to look out for.

2

ARE YOU ALREADY UNDER ATTACK?

OPEN RDP LINKS

What's an RDP link? How do you open or close one?

RDP - or Remote Desk Protocol - is Microsoft tech that allows a local PC to connect to a remote device. You'd use it if you've worked from home. And many people neglect to close their open RDP links when they've finished with the connection, allowing cyber criminals easy access.

Scan for open ports regularly and start using multi-factor authentication (where you generate a login code on another device) if you don't already.

UNFAMILIAR SOFTWARE

Noticed new software on your device lately? It's probably not an update.

Hackers typically gain access to one device, and then use particular software tools to access the entire network. Look out for anything you haven't noticed before, but particularly apps called Angry IP, Advanced Port Scanner, and Microsoft Process Explorer.

NEW ADMINISTRATORS

Noticed a new admin on your system? It's worth double checking that your IT team hasn't added the new person.

Cyber criminals will set themselves up as administrators so that they can download the tools they need to carry out their attack of your network. And to do this, as well as the software mentioned above, they may also use other software called Process Hacker, IOBitUninstaller, or PCHunter.

These are all pieces of software that your business may legitimately use, but they can be used to uninstall security.

DISABLED SOFTWARE

Of course, to carry out the perfect attack, your security software needs to be disabled. Some things called Active Controller and domain controllers will be disabled when the attack is imminent, and it's likely that your back-up will be corrupted too.

Ensure that someone is regularly checking that software is active, and your backup is working as it should be.

Remember, ransomware attacks are usually slow, so these things won't all appear at once. Vigilance is key here. Keep an eye out for anything unusual, and if you do spot something, no matter how minor, report it straight away. It could help stop a huge, costly attack on your business.