JUNE 2024

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER

Out of sight, out of mind?

Having your employees work from home is the norm now. While there are lots of benefits to this new attitude to work, it's easy to overlook a crucial aspect of keeping operations secure.

Neglecting remote security can lead to some serious headaches down the line. Imagine this: Your employee's laptop gets breached because their home Wi-Fi network wasn't properly secured.

Or worse, a malware infection spreads from their kid's device to their work laptop, putting your entire network at risk. That's scary.

A little vigilance and some regular checks can prevent these risks, keeping your business and its data much safer.

So, let's talk about devices. Encourage your remote workers to treat their work devices like Fort Knox. That means regular updates, robust protective software, and using strong and unique passwords (password managers are your best friend for this). Remind them to avoid risky behaviours like downloading software from unofficial sources or clicking on suspicious links.

Next, address home networks. A weak Wi-Fi password is asking for trouble. Encourage your employees to set a strong password for their home network (again, a password manager can remove the hassle of this). While they're at it, remind them to enable encryption hide their network's SSID (Service Set Identifier) to add an extra layer of security.

It doesn't end there, it's not just about devices and networks – physical security matters too.

Use MFA to protect logins, a VPN (virtual private network) to protect your data, and remind your team to keep their work devices secure when they're not in use. Whether that means locking them away in a drawer or simply keeping them out of sight from prying eyes.

Regular checks are key to staying on top of security. Schedule routine audits of remote set-ups to ensure everything gets a thumbs up. This could include checking for software updates, reviewing network configurations, and providing regular security awareness training.

Want a hand with that? We can help – get in touch.

DID YOU KNOW...

Microsoft has a new email send limit?

Microsoft Exchange is cracking down on spam. Hooray! However, if your business sends bulk emails, it might affect you.

From January next year, Microsoft will allow **no more than 2,000 external recipients of bulk emails.** It's to prevent people abusing the service, which wasn't designed for bulk mailing.

Gregory Micallef Associates Ltd
Units 5 & 6 Brook Court, Blakeney Road, Beckenham. BR3 1HG.
Tel: 020 3327 1346 Email: hello@gmal.co.uk Website: www.gmal.co.uk

TechFacts

1. The internet weighs as much as a strawberry. That's according to physicist Russell Seitz. He says the combined weight of all the electrons in motion is about 50 grams.

2. The first computer bug was a real bug. In 1947, Grace Hopper and her team found a moth causing issues in their computer at Harvard University.

3. In 2015, the United Nations reported that a start-up in Kenya was converting human waste into clean, renewable energy. This energy, in turn, powered Wi-Fi routers in low-income areas.

Technology update

Install any website or web tool as an app in Windows 11

In Windows 11, you can install ANY website or web tool as a traditional app. They're known as Progressive Web Apps (or PWAs) and once installed, they'll appear on your Start menu like a normal app would. You can even pin apps to the Taskbar.

Why bother? PWAs use less resources than traditional apps, you'll always get the latest version without having to run an update first.

All you do is visit the site, click on Settings, select Apps, and click "Install this site as an app."

Easy.

INSPIRATIONAL QUOTE OF THE MONTH

"You build your own strategy. You don't define it by what another competitor is doing."

Ginni Rometty, CEO of IBM

June's fun tech quiz – June-o the answers to these?

1. The keyboard shortcut for copying information is Ctrl + C, but what's the shortcut to paste?
2. In 1999 Shigetaka Kurita invented what keyboard additions for phones that would get their own movie?
3. When a password is limited strictly to numbers, it's referred to as a PIN. What does that stand for?
4. What word is often abbreviated as Fn on a keyboard?
5. Which American tech company started with its founders' idea to rent out an air mattress in their San Francisco living room to travellers hoping to avoid the city's high cost of rent?

The answers are below.

1. Ctrl + V
2. Emojis
3. Personal Identification Number
4. Function
5. Airbnb

NEW TO

MICROSOFT

Microsoft Teams is becoming more inclusive

If you like to inject a little personality into your Teams chats, it's likely you use reactions from time to time. Until now, they've been a little restrictive.

This month, a small tweak is due to rollout which will allow people to select a skin tone for their reactions. Microsoft says, "This preference will be applied to all emojis reactions in chats, channels, and desktop/web meetings, allowing users to express themselves more authentically in conversations."

Think about recovery BEFORE the attack strikes

Let us set the scene. It's an ordinary Wednesday. You're minding your own business, getting things done, making boss decisions, then BAM... you get hit with a cyber attack.

Cue panic mode.

To put it simply, these attacks happen more often than you'd think, and guess who the favourite targets are? No, not big multinational companies – small to medium-sized businesses.

As for the consequences, we are talking financial losses, data loss, reputation damage, the whole nine yards.

However, it doesn't have to be that way. If you have a recovery plan in place you can turn a total nightmare into "an annoying inconvenience".

So, what should your recovery plan include? Well, first things first, prevention is key. Invest in solid cyber security measures like firewalls, antivirus software, DNS filters, MFA, regular security check-ups. Don't forget to educate your team about the importance of good cyber hygiene (things like using strong passwords not clicking suspicious links) – because human error is often the weakest link.

Next, have a game plan for when the inevitable happens. This means having clear protocols in place for how to respond to an attack, who to call, what steps will minimise the damage.

Let's talk backups. Backup repositories are the most targeted during an attack so it is crucial to have a regular, secure, and immutable backup solution in place that can be restored without fuss. Having secure backup and restoration capability is critical to cyber resiliency and can be a business life saver.

Finally, practice makes perfect! Test your recovery plan to make sure it's up to the job. After all, you don't want to wait until disaster strikes to realise your plan has more holes than a block of Swiss cheese.

Cyber attacks may be scary, but with a solid recovery plan in place, you can rest easy knowing your business is armed ready. Remember what they say: Fail to prepare, prepare to fail.

If you want help you with your recovery plan, backup solutions, or cyber security requirements, please get in touch.

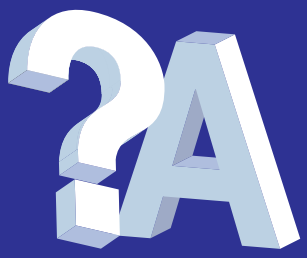
Business gadget of the month

Scan reader pen

This handy little pen can do loads. It can read aloud text that you scan with it, translate text written and spoken in different languages, record voice notes, and transcribe speech into text.

Handy if you travel or work with people in other countries. Also a useful tool for people with dyslexia.

£59.99 from Amazon.



Q: Should I move my business data to the cloud?

A: The cloud brings many benefits such as zero storage limits and automatic backup. However, it's important to choose the right provider. We can help – get in touch.

Q: How often should my team have cyber security training?

A: Since threats evolve at a rapid pace, regular training is important and must keep pace with the new methods of attack. Try to ensure security awareness training takes place at least once a month.

Q: Can we use Microsoft Teams as a phone system?

A: Yes. if you're already using Teams effectively, it could be a sensible solution. However, there may be other scalable and cost effective solutions that better fit your needs. Get in touch , we can help you.

This is how you can get in touch with us:

CALL: 020 3327 1346| **EMAIL:** hello@gmal.co.uk
WEBSITE: www.gmal.co.uk

GMA
GREGORY MICALLEF ASSOCIATES