TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

02 THERE'S NO SUCH THING AS A STUPID QUESTION

03 YOUR POCKED-SIZED SECURITY THREAT

MONTHLY UPDATE FROM TONY

As technology advances, it means we can access anything, anywhere, on any device. And that's great. We have the ability to work from anywhere in the world without worrying how to communicate or access info. It's all at our fingertips.

However, with the benefits comes a downside. Which is that we simply don't switch off.

Look at the last month. How often have you found yourself replying to a work email late at night? How many times have you had an 'I'll just get that done' moment outside of your regular working hours? How many calls have you received when you were spending time with family or friends, or trying to have a moment to yourself?

And because of this, we've become impatient waiting for responses. Gone are the days of getting back to someone in 3-5 business days. We want it now! And it's really frustrating when we do have to wait for something.

It's no surprise that there's been a huge rise in people burning out.

But slowly, some people are rebelling against this. And it's starting with a new email signature. Many businesses are asking their people to add a disclaimer to their email signature (or a human footer, as it's being called). Here's a great example...

TRULY HUMAN NOTICE: Getting this email out of normal working hours? We work at a digitally-enabled relentless pace, which can disrupt our ability to sleep enough, eat right, exercise, and spend time with the people that matter most. I am sending you this email at a time that works for me. I only expect you to respond to it when convenient to you.

Would you adopt this for your business? Do you already have a human footer on your email signature? I'd love to see it - send me an email to sales@ashdownsolutions.co.uk.

Until then, stay safe,

Tony Baulch

Founder & Technical Director

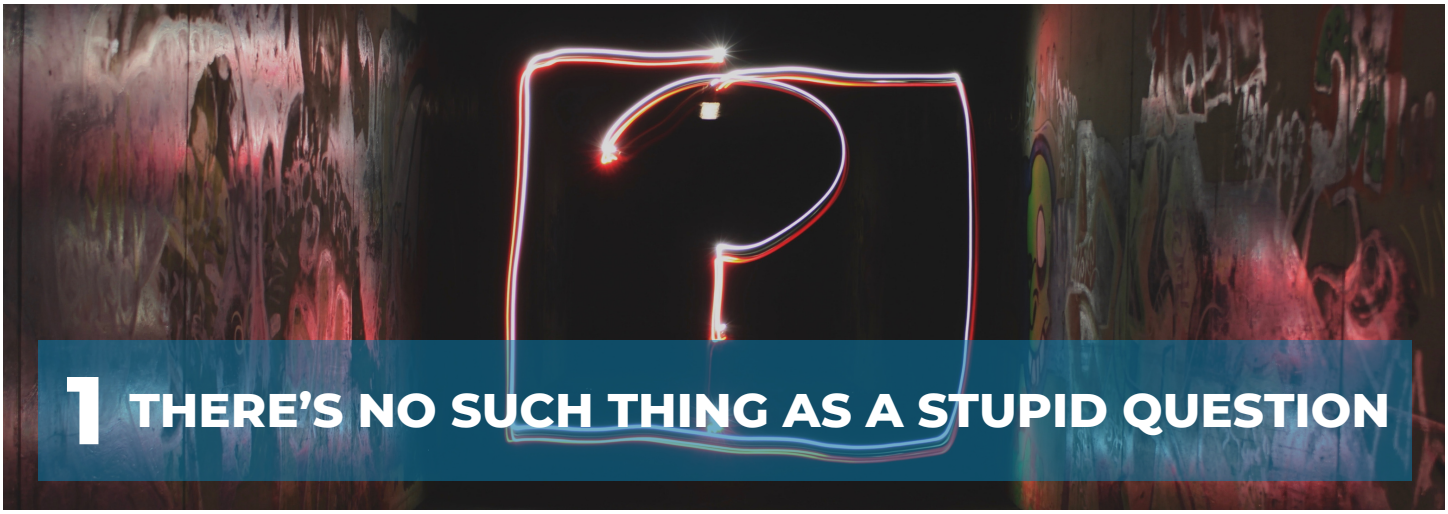
DID YOU KNOW?

If there was a computer as powerful as the human brain, it would be able to do 38 thousand trillion operations per second; and hold more than 3,580 terabytes of memory.

Ashdown Solutions Limited

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

NEWS FROM THE COALFACE



1 THERE'S NO SUCH THING AS A STUPID QUESTION

OK, it might be sensible to hold some of the questions back in certain situations.

But the one time you should ask anything and everything is when you're looking for a new IT support partner (or any other outsourced service, for that matter).

When you're trusting a large element of your business to another company, you want to be certain that you're making the right decision in choosing them.

If you're looking for a new IT support provider, these are some of the tricky questions we suggest you ask...

The answers to these questions can really tell you a lot about a company. So ask the difficult questions. Learn as much as you can about any new partner for your business. Because you want to make sure they're a great fit for you.

Do you specialize in an industry?	Do they have the right knowledge of your sector to be able to provide you with the right solutions? If they do specialize, how will they translate their service to your business? Will it be a good match? Are they used to working with businesses the same size as yours, or do they usually work with smaller or larger companies?
What's your retention rate?	Are they going to do what they say they're going to do? Or do their clients soon become disillusioned and look for a better service elsewhere? What's the main reason that clients leave them?
How much of your revenue comes from fixing issues vs preventing them?	We know things can't always be anticipated – especially when it comes to IT problems. However, it's really important to choose an IT service partner who will work proactively to prevent as many issues as possible. If their work is primarily reactive, they're missing some big steps in their service.
Who will be responsible for my account?	You want to know who you're working with, and if they're a good fit for your business. But it's important to know if you'll have a dedicated account manager, or if issues are simply passed to the person with the lowest workload at that particular time. A level of continuity when it comes to your IT support can mean that problems are resolved faster, simply because someone is familiar with your set-up.
What's the biggest disaster you've ever had?	Not a trick question! It can tell you a lot about the business to know how they dealt with a huge problem. Was it something they already had a procedure for? If not, have they created procedures in case something like that happens again? The biggest warning sign is a company that tells you they've never had a huge disaster - unless they're brand new, that can't be true.

2

YOUR POCKED-SIZED SECURITY THREAT

You guessed it. I'm talking about phones.

How many people in your business have a company-issued phone, or use their own to access company data like emails, client information, or documents? It's probably a high number, right?

And your phone is a big risk to your data security. Smishing attacks (that's the text message equivalent of a phishing email) increased 328% in 2020 and will probably significantly rise again this year.

That's because it's a goldmine for cyber criminals. 98% of text messages are read and 45% are responded to. So a smishing text is likely to yield good results for crims.

Once your phone is infected, malware can monitor your calls and messages, download and delete your data, and if a phone is connected to your business network, the infection might even spread.

60% of interaction with corporate data happens via a mobile device.

Malware aside, mobile devices are more prone to loss and theft, which could see them easily falling into the wrong hands.

So with all that in mind, what steps are you taking to keep phones protected from threats like cyber-attacks and data theft?

First and foremost, you need to educate your people on the dangers that smart phones pose. Make sure they know how to spot a smishing attempt, and not to click or respond to anything that raises a red flag. Encourage everyone to block any numbers sending bad texts, and even consider installing a spam blocking app on all devices.

If your people are in any doubt as to whether a message is genuine or not, ask them to clarify with their contact with a phone call. Don't respond to a message if there is any doubt over its authenticity!

Make sure that everyone uses multi-factor authentication or biometrics to unlock handsets. And set up encryption and the ability to remotely wipe data if a device be lost or stolen.

Everyone in your business should also know exactly what they have to do if they think they've tapped on a potentially dangerous link, downloaded something they shouldn't have, or lost a device. Create a protocol that details who needs to be informed and in what timeframe, the information that needs to be given, and how it's escalated. The sooner a potential breach is reported, the more can be done to quickly rectify the situation and protect your data.

As usual, if you need any further help or advise on keeping all of your devices safe and secure, give us a call.