THURSDAY THOUGHTS

This week was another short but filled with activity and lots of opportunities to get out of my usual comfort zone. I've been working on my "virtual" GDPR Audit offering to help companies with their compliance while maintaining social distancing. You will hear more about this in future weeks. I have also decided to offer an on line small business compliance session which I talk about below.

I can totally recommend getting out of your comfort zone whether this is visiting a different networking group or listening to an inspirational talk. There are loads on line to choose from. This week I went to Simply Networking which is run by the energetic Mark Greenwood and met a group of very interesting and friendly people. It is great to connect to new faces I think one of the big benefits of Zoom is that you can meet people from further afield without leaving your office.

I recommend you give "outside my comfort zone" a go – sometimes if you look away from the page you find the inspiration you were looking for on it!

GDPR is 2 years old

Did you know that GDPR is 2 Years Old? Since May 2018 across Europe more than 231 fines and sanctions have been levied and it will be interesting to see if there is an increase in the number of complaints in the last 12 months (last year's figure was 144,376). GDPR remains a strong framework and an excellent way of protecting people's fundamental right to keep their personal data private.

More needs to be done to support the national authorities charged with protecting our rights. The resourcing of the Data Protection Authorities across Europe remains a problem. Only 9/30 of them consider that they have adequate resourcing.

What are small businesses doing about GDPR 2 years on

In a recent survey of small businesses I found that just 42% of companies had started on their journey to GDPR compliance those who haven't fall into 3 categories:

- they know it applies but don't want to do anything wrong so are doing nothing.
- they don't think it applies to them – because they are too small.
- they think it's a "European" thing which will go away with BREXIT.

Sadly none of these approaches will stop a business from being fined for failure to comply with the regulation. Nor will it stop a fine for failure to register with the Information Commissioner.

Helping small businesses with their GDPR compliance

Because I have seen a recurring theme with small businesses I have decided to run an on line session "GDPR – Small Business Compliance" soon. Th-is will be aimed specifically at small businesses to help them understand what they must do about GDPR in order to be compliant. It will be a mix of practical hints and tips as well as guidance and support. If you want help with your GDPR journey you can always contact me using the following link: https://www.pppmanagement.co.uk/contact-

Do you think cybercriminals deliberately spell things wrong?

I read a really interesting post from Mike Ouwerkerk this week who used a Linked In poll to see if his network thought grammar or spelling mistakes in phishing emails were deliberate or if it was just that the originators couldn't spell.

Most thought it was the latter - 73% ticked the box "because the "muppets" can't spell". The chat in the post threw up some interesting ideas:

- If you receive an email that's trying to get you to click on something it needs to look convincing, mistakes in the text will be a good indicator that it isn't authentic.
- If you receive an email such as the "I have $1M dollars for you" which contains spelling mistakes and you notice the errors and don't respond the cybercriminals are less likely to bother with you in the future.
- If you receive an email such as the "I have $1M dollars for you" which contains spelling mistakes and you don't pick up on bad spelling or grammar and respond in some way you are a potential easy target, and they will focus on you (and no doubt share your details with others as "easy prey").

This week's top tip - check emails you aren't expecting for spelling and grammar, if there are mistakes don't respond.

Spreading the word about targeted advertising

It's really important that all sectors of the population get sound advice on keeping their personal data private. This week it was good to see that the Good Housekeeping magazine shared top tips to stop adverts following their readers around the internet. In easy to understand terms they explained what targeted advertising is and why after you look at something online you then see an advert for it on Facebook or Instagram.

The link to the article is below. It gives details of ways you can avoid this invasive marketing, telling readers how to:

- use "Incognito mode" on the computer when shopping.
- clear browsing data (on smartphones and tablets.
- stop adverts following them on Facebook and Google.
- stop Facebook using their online activities to personalise adverts.

https://www.goodhousekeeping.com/uk/consumer-advice/technology/amp32609843/stop-ads/?

The problem with location sharing

Did you know that just by allowing one app to share your location it is possible for the app owner to get a really detailed picture of your life. Where you live, where you work, things you're interested in, the routes you use to get home and even events/concerts/protests you have attended. Some of this data (depending on the app) can be used to sell you things, suggest content on your social media platforms but it can also be shared with law enforcement or whoever the platform decides it wants to share with. This article in the NY times is well worth a read:
https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

ICO advice on working from home – employers security checklist

As the demand for home working increases companies will have developed IT solutions to support their staff. It is really important to make sure that everyone is using these systems securely. The ICO has a selections of quick checks to help businesses identify some of the common IT vulnerabilities. The most important things to do are to:

- have clear policies, procedures and guidance for remote working.
- use the most up-to-date version of remote access solution.
- make sure staff use unique and complex passwords.
- use multi-factor authentication where possible.

The ICO also have guidance on Bring your own device (BYOD), Cloud storage, Remote desktop configuration, Remote applications and email. You can access their guidance here:

https://ico.org.uk/for-organisations/working-from-home/working-from-home-security-checklists-for-employers/?utm_source=linkedin&utm_medium=information%20commissioner%27s%20office&utm_term=17fc4399-0d55-4f44-930e-384ced45f2d0&utm_content=&utm_campaign=

Advice issued following EasyJet cyber incident

Following the announcement about the EasyJet cyberattack which compromised the email address and travel details of approximately 9 million customers (and the credit card details of 2,208 customers) Action Fraud and the National Cyber Security Centre have published advice for EasyJet customers. They are encouraging EasyJet customers to report any suspicious emails to the NCSC, using the Suspicious Email Reporting Service (SERS). Further advice and information can be found at it www.actionfraud.police.uk.