satswana

Company registered number 09329065 www.satswana.com

Spring Council Update

Contents

1 Hack of Council Website

We do not often get totally new issues within our Council business, but when an authority received a complaint from one of their correspondents it revealed something that we were totally unaware of – and are now bringing it to your attention, as it could very easily happen to you!

Because the subject had come up within Council business the letter, with all personal details and the address redacted, had been published along with the Minutes on the website. At least, that is what the officers thought.

As it happened there were no real negative consequences, but a researcher who was interested in the subject sought to get in touch with the correspondent, and knew that if he took a copy of the Word Document from the website and pasted it into a blank document that the original address and name would appear! The researcher was totally open in what he had done, but the correspondent was very annoyed at her personal data being compromised.

From the technical data protection angle we determined that because "there was no arising risk to persons" that the breach did not have to be reported to the ICO, but it was nevertheless very embarrassing.

What we learned is that you have to completely delete any personal data from any Word Document that you reproduce and publish – and then take a further copy without the data on it at all.

We are much wiser now!

.

2 Wifi on your phone?

Naturally enough when we are at home or at our place of work we will stay logged onto wifi, but recent reports have identified the dangers of leaving it on when you travel elsewhere

since you may connect to a rogue source that has anything other than your interests at heart!

This is especially true when it comes to coffee bars or similar public spaces. Possibly we can all recall the joy of finding an unprotected source that we can log onto and update our email, but now that we know it could be an exploiter then it is clearly unsafe to do so. If you travel a lot an alternative is to buy a dongle that connects to the GSM network – yes you have to pay, but data lasts a long time just downloading email.

So the recommendation is to turn wifi off when you are not at a secure location. You will find there is an added benefit from a battery that lasts longer, since the phone will not be hunting for a signal all the time!

3 Using a "Sandbox"

Originally a military term where a box of sand was used to contain (hopefully!) the explosion of a grenade or such like that had become unstable; the word has been adopted to describe a safe environment in which you can test files without blowing up your PC.

Windows 10 Pro offers a version but it has to be turned on by searching for "Turn Windows features on and off" and should be restricted to competent users who will establish that it creates a unique virtual machine that is apart from the rest of the PC.

A specific use is to check an unknown or unrecognised USB stick, since it is a favourite criminal trick to leave one lying on the ground for the unsuspecting to pick up. The natural action then is to try and locate the owner by checking the content – then wham, you have a virus! Open it in a sandbox please.

4 It can happen to anybody

The announcement below was viewed with a certain amount of schadenfreude by most who read it, a Regulator having to report itself to a Regulator!

https://www.fca.org.uk/news/statements/fca-data-breach

It does demonstrate how easy it can be to make a mistake, and how perfection cannot be legislated for.

5 The most successful fraud

Before you read on, please think to yourself what the most successful online fraud might be, we would bet that many would think that it was credit card cloning or faking bank documents, something like that. Thus I am sure you will be surprised to learn that Business Email Compromise (combined with email spoofing) is by far the leader, harvesting a value for a criminal that is 30 times larger than credit card fraud.

Our advice has to be never to trust any online request for payment, even if it appears to come from "the Clerk who has rushed on holiday and forgotten to pay a critical invoice". An infiltrated email account will be monitored, perhaps for years, waiting for the opportunity, knowing when the Clerk has gone on leave, learning the style in which an email is written. The hackers are capable and patient professionals. You must assume the request is faked until you have proved otherwise – and if you cannot contact the person to do so, wait until you can!

Also never accept instructions to change bank account details, that request is almost always a red flag. Check and double check before doing so – and delay anyway. The person you talked to on the phone to confirm the instruction may have had a knife at their throat. Yes, it can be that dangerous.

6 References

For a period of time, we had to disclose what was said in a reference under a Subject Access Request. Not so under DPA 2018, what you say is now protected from disclosure

Under the Data Protection Act 1998, references given by an organisation were exempt from disclosure on receipt of a SAR.

The exemption only applied to references given by the organisation. This meant that the exemption could only be used by the provider of the reference, and not a recipient.

The Data Protection Act 2018 has removed this distinction so that any reference provided in confidence is exempt from disclosure under a SAR. This means that if an organisation receives a subject access request, confidential employment references about the individual making the request, whether created by that organisation or received from a third party, will be exempt from disclosure.

7 Face recognition technology

We are keeping an eye on this in the belief that it is likely to play a major role in the use of artificial intelligence as essentially it is "intelligent" CCTV – in that you not only can see a person, you know who they are, and that can be managed by a program.

There was a very negative report regarding the use of the technology to identify criminals in London that, if true, just means that the supplier is dreadful. It is a very different story in China, where – as a consequence of Coronavirus – they can now identify people when masked. Cynics may say that they can also then track democracy activists in Hong Kong – they are claiming 99.9% accuracy, that being the feared "big brother" aspect.

However, the flip side is that in Wuhan they felt safer because "outsiders were identified coming into an isolation area, and they could stop those from leaving who were infected. One fears it is a privacy debate that has already been lost – not least because history would indicate that once something is technologically possible, then it will be adopted. And Cressida Dick (Metropolitan Police Commissioner) pointed out that many of the people

objecting to the use of facial recognition were the same people who were happy to allow Facebook to use their image to connect with friends.

Intelligent recognition technology will have to be deployed and will become ever smarter in recognising risks. You may consider that an appalling invasion of privacy, but you will not be able to come up with an alternative that is as effective. Please take a seat Mr Orwell.

Gosh, did we forget to mention that the Wuhan cameras also had infrared technology to take temperatures so that they could identify sick people?

8 Disposing of computers

Did you know that within the second hand computer market (and indeed any intelligent device) there is a thriving trade in scanning disks and memory for any residual personal information – particularly stored login details?

It is not enough to simply erase your personal files as this does not actually delete the data; it just deletes the index to it, so that it cannot be found by the program that was using it.

The only way to guarantee that data has been removed is to overwrite the drive, and there are specialist firms that can do this for you, but you can do it yourself. Other machines and Macs have similar options, but with a Windows (we hope you are all on Windows 10 by now) machine first go to Settings. Select the Update and Security area. Select Recovery, then Reset this PC, choose the option to “remove everything”. During the reset you will be presented with the option “Remove files and clean the drive” which fills all but the section containing the system with digital noise, it may take an hour or two.

Make sure you have taken copies of any data you need in future, there is no way back!

9 Chess anybody?

Garry Kasparov, possibly the greatest player in history, has complained that he is the first knowledge worker whose job has been threatened by a machine!