Thursday Thoughts – 6th May 2021

Happy Password day!

Rather unsurprisingly this week's Thursday Thoughts has a password focus. What a strong password looks like, considerations for small businesses when setting up a password protection policy. A step up from passwords is 2 factor authentication. Something Google has just announced it is going to start automatically enrolling users in. I say this a lot – If you haven't set up 2FA on your accounts please do so. That way the criminals are less likely to be able to get your data or steal your business social media account. A light-hearted way of getting the password message across is the Rachel Tobac sea shanty on twitter. If you do nothing else share it with someone who doesn't yet understand why they need separate passwords for their accounts

Also this week was the ICO's Data Protection Practitioners' Conference which was held on line for the first time and was attended by more than 3,000 data protection professionals. It offered some great insights into the work of the ICO and emerging best practice from DPOs around the UK. Especially of interest for those subject to FOI requests were examples of best practice in particular the suggestion that as a proactive measure.

For those with new second hand tech the NCSC recently published advice on setting up second hand devices which will be useful. I've also included a case study of how Ransomware got into a bio research institute (spoiler alert it was not phishing this time).

Blogs and Videos of the Week
NCSC - Passwords, passwords everywhere
Rob Arnold/Saurabh Gupta/Avishai Ostrin - Holistically protecting your Salesforce data

Passwords

The experts recommend that each password you use is "strong" and "separate". But what does this mean in practice.

The aim is to stop others accessing your personal accounts and walking off with personal information, such as your bank details, address or date of birth. The idea is that by having separate passwords for your accounts that if a cybercriminal gets into one account they cannot access another.

The NCSC recommend that you use three random words. It needs to be memorable too so use words that are memorable to you and don't forget that our social media accounts can give away vital clues. Particularly you should never use the following as a password:

- Current partner's name
- Child's name
- Other family members' name

- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team

Every year a list of the Top 1000 most commonly used passwords is published on line. This is extracted from the 2020 list:

Most used Passwords	Names	Premier League football teams	Musicians	Fictional characters
123456	ashley	liverpool	blink182	superman
123456789	michael	chelsea	50cent	naruto
qwerty	daniel	arsenal	eminem	tigger
password	jessica	manutd	metallica	pokemon
1111111	charlie	everton	slipknot	batman

There is a great sea shanty from Rachel Tobac that explores the risks of having the same password across platforms. https://twitter.com/RachelTobac

Passwords for sole traders and small businesses

For small business owners the risk of someone accessing an account through poor password management could be catastrophic. Most commonly it is our emails accounts that can contain sensitive information about customers, our own business or contracts and invoices. The NCSC publish a small business guide which is a great starting point. For business with staff other suggestions include screening passwords against the most commonly used list mentioned above, or having a policy that devices should be turned off when the not in use and that passwords are not kept next to the device or in camera shot of a video call … and certainly not on a post it note on the screen.

ICO's Data Protection Practitioners' Conference 2021 was

The ICO's Data Protection Practitioners' Conference 2021 was held this week, which was attended on line by about 3,000 data protection professionals. It afforded insights into the work of the ICO and emerging best practice from DPOs around the UK. Especially of interest for those subject to FOI requests were examples of best practice in particular the suggestion

that as a proactive measure businesses develop a series of FAQs/Top Tips on their websites. This way they can answer most of the common FOI topics in a proactive way rather than wait for the inevitable request. Other news from the day is that the ICO is working on bespoke UK standard contractual clauses (SCCs) for international data transfers, the importance of data ethics and some practical tools to help businesses to decide when and how to share data.

Firefox for Android gets critical update to block cookie-stealing hole

Firefox's latest android update is to stop attackers being able to access private browser data from website X while the user is on a "booby-trapped" website. Browsers are supposed to have a process that locks down locally-saved web data so that it can only be read back in later on by the same website that saved it in the first place. If you have an android and you use Firefox get the patch downloaded.

Case Study – How Ransomware got into a bio research institute

The unnamed biomolecular facility in Europe lost at least a week's worth of research through the actions of one student. Ransomware had made its way onto the facility's network when the student concerned on posted on a forum details of his hunt for a free version of a data visualization software tool (which usually costs hundreds of pounds/euros). The student selected a cracked software version which triggered Windows Defender so the student disabled defender as well as their firewall. The resulting Trojan was downloaded which harvested the student's access credentials to the biomolecular institute's network and once in the institute ransomware was deployed. You can read the full details here. https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/ryuk-ransomware-finds-foothold-in-bio-research-institute-through-a-student-who-wouldnt-pay-for-software/

NCSC advice on how to set up (and use) second-hand devices for online home learning

Last month the NCSC published further advice for families who have access to a second-hand laptop, tablet, or smartphone. In particular there is guidance on how to reset the second-hand device before you start using it, how to start afresh with a clean installation of Windows 10 and the need to keep devices up to date. Of course also included in the advice is the use of strong passwords, 2FA and, particularly relevant for home learning, using video conferencing safely and setting up (and using) second-hand devices for online home learning. The NCSC advice can be found here: https://www.ncsc.gov.uk/blog-post/home-learning-advice-for-parents-and-carers

Google plans to automatically enrol users in two-step verification

Google's contribution on "World Password Day" is a plan to enable two-step verification on Gmail. Users are being prompted today to enrol in two-step verification but soon it will be automatically enrolling users and making their accounts safer.

Videos and Blogs of the Week

NCSC - Passwords, passwords everywhere

This blog from NCSC will help you to make your password policies simpler and help users to choose a 'good' one. One of the suggestions is to use a "password deny lists" in other words a list of passwords commonly found in data breaches. For example the password '123456' was found 23 million times in breaches listed on the haveibeenpwned website. You can read the full post here: https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere

Rob Arnold/Saurabh Gupta/Avishai Ostrin - Holistically protecting your Salesforce data

This is a really informative conversation between a CISO, a DPO and an Architect. Each providing their own perspective on how to protect the data gathered as part of the business. It is an in-depth discussion of the balancing act that organisations have to achieve between the privacy of customers, what the regulator wants and pressure to be competitive. I recommend it as well worth a listen, especially to understand the difference between a data incident and a data breach and the tools at our disposal to mitigate the risks so and therefore minimise the impact (I am a fan of Avishai's bucket approach). Some helpful tools offered at the end for salesforce users too. Here's the link: https://www.youtube.com/watch?v=yBMq0F3GWEY&t=775s