6/11/20

THURSDAY THOUGHTS

The types of security risks that we all face came to the fore this week. Whether it is making sure that the files on USB drives you get rid of have been removed, or a salient lesson to protect our twitter accounts (Donald Trump) and laptops (Hunter Biden), the financial danger of using the same password on numerous accounts (do you really want to pay for someone else to eat at Nando's) and the problem with using default settings in the Internet of Things (using irrigation systems as an example).

Also featured, details on the ICO Marriot fine, how to successfully embed a culture of privacy by design and details of some free data protection webinars aimed at schools.

My "Blogs of the Week"
Neil Evans/ MyLife Digital – Open Letter to Data Brokers
NCSC Annual Review

Delete The Files On USB Drives Before You Sell Them

A Masters Degrees Student from Abertay University (Dundee) found that there were "deleted files" still on the majority of USB drives he purchased from an internet auction site. The files included contracts, bank statements and tax returns. Although the drives looked empty the researcher was able to recover information which included files named "passwords" and images with embedded location data from the drives using "publicly-available tools". Of the 100 drives only 32 had been properly wiped, 26 drives still contained partial files while 42 of the devices still contained every single file that had ever been placed on them. This serves as a salient warning to anyone planning to pass on or sell a USB drive. Make sure you use software to permanently wipe the drives or use a heavy hammer on the removed disk. You can read more here: https://www.bbc.co.uk/news/uk-scotland-tayside-central-54779322

Donald Trump's Twitter Account Hacked

It was reported that Donald Trump's Twitter account had been hacked by a Dutch security expert in October. Although this has not been confirmed by twitter or the Trump team it is a timely reminder to us all of the need for a secure password and two-step verification. Apparently the president's password was "maga2020!" (Trump's campaign slogan is Make America Great Again). Passwords that are obvious to us are simple for hackers to guess. I always recommend the use of three random words. The researcher used the twitter message service to tag the CIA, White House and FBI highlighting the fact that the account was not secure. Although he had no response from these messages, a day later two-step verification was activated on the account and two days later, the Secret Service got in touch. You can read more here: https://www.theguardian.com/us-news/2020/oct/22/trump-twitter-hacked-dutch-researcher-password

Hunter Biden Laptop Abandoned

Also in the news this week was a story that Hunter Biden's laptop was abandoned. This created a security nightmare when it was revealed that as well as containing personal drug and sex addiction information it also included security service details and telephone numbers for most of the Obama cabined. Apparently all secured with his password, Hunter02.

Nando's Customers – Online Accounts Hacked

Some online accounts of Nando's customers have been hacked following a credential stuffing attack. If you weren't aware already reusing username and password combinations across different accounts is a massive security "No No". Stolen credentials from data breaches are often used to try to gain access to multiple online accounts. In the case of Nando's the hackers placed large orders and ran up massive bills for the affected customers. You can take the following steps to protect yourself from attacks like this:

- Use separate passwords for important accounts
- Create strong passwords with three random words
- Consider saving your passwords in a browser
- Change your Nando's password

Smart Irrigation Systems Unprotected

Up to 100 smart irrigation systems for crops, tree plantations, cities, and building complexes were vulnerable to tampering after the companies that installed them did not change any of the default settings, including the administrator password.

Apple Security Updates

Apple has released a number of security updates to patch vulnerabilities that known to be being actively exploited allowing others to remotely execute arbitrary code and run malicious programs on apple products. The list of impacted devices includes iPhone 5s and later, iPod touch 6th and 7th generation, iPad Air, iPad mini 2 and later, and Apple Watch Series 1 and later. The fixes are available in versions iOS 12.4.9 and 14.2, iPad 14.2, watch 5.3.9, 6.2.9, and 7.1.

Marriot Fined £18.4M

The final figure for the Marriott hotel group fine for their data breach in 2018 is £18.4m. The breach made the news because the personal data of 339 million customers was compromised in a cyber-attack. The amount of the fine highlights the expectation that the ICO have that large organisations will put in place appropriately qualified personnel and systems to maintain a high level of security for their customer's data.

How To Successfully Embed A Culture Of Privacy By Design

We can all recognise the need to safeguard the storage and use of personal data. Especially in a world of smart technology and fast-emerging apps. Last month Tony DeBos (EY Global & EMEIA Data Protection and Privacy Leader) wrote a useful piece on how to embed a culture of privacy by design in an organisation. DeBoys stresses that the "strategy must be embraced by the whole organization and complemented by its culture and working processes" and gives five general steps organisations can take to get their staff thinking about Privacy by Design:

- Raise awareness and build your network
- Align with senior management and get their buy-in
- Understand the project's lifecycle, identify and be involved in key projects as early as possible
- Recognize the organization's capabilities and build upon them
- Define a roadmap for Privacy by Design

You can read the full article here: https://www.ey.com/en_gl/cybersecurity/how-to-successfully-embed-a-culture-of-privacy-by-design

Free Data Protection Webinars Aimed At Schools

The GDPR in Schools team have put together a selection of free data protection webinars to meet the needs of schools.. Topics in the next month include:

- Data breaches which occur every day – including some real examples of the breach's schools have encountered in the new world of online learning and working from home.
- The risks of cyberattacks - why schools are now in the sights of cybercriminals and the risks from a safeguarding perspective.
- Legal Labilities and responsibilities in data protection
- Data processing agreements
- SARs – when must you write a SAR or can you refuse
- Brexit – the implications of data transfer outside the UK

The details of the sessions are on their website https://www.gdpr.school/webinars .

Blogs of The Week

Neil Evans/ MyLife Digital – Open Letter to Data Brokers

Following on from the enforcement notice given to Experian last week the importance of concentrating on transparency and accountability has come to the fore. In an open letter from MyLifeDigital to data brokers the sector is urged to improve on their current "opaque" practices. Just like the rest of us data brokers should:

- Demonstrate ethical data processing practices
- Put individuals at the forefront of their processing
- Provide relevant information to individuals about their activities
- Enable individuals to make decisions regarding how they want their data to be used

You can read the whole blog piece here https://mylifedigital.co.uk/an-open-letter-to-data-brokers/

NCSC Annual Review

There have been some interesting developments over the last year so this year's NCSC's Annual Review is well worth a read. https://www.ncsc.gov.uk/news/annual-review-2020