Thursday Thoughts – 27th May 2021

It's a right mix this week in Thursday Thoughts. We start with the warning ahead of a summer of sport and this weekend's all-English UEFA Champions League Final that sports fan's livestreams are notoriously insecure. Often using easily guessable passwords. So if you or your nearest and dearest are in that category please make sure you change the password to something more complex (and please don't use your favourite team or player's name). Also there is a warning of an increase in ransomware attacks on smaller businesses which can offer a route for the criminals into organisations further up the supply chain. If you have used FastTrack Reflex Recruitment recently you'll want to be on your guard for identity fraud as a result of their data breach.

As we return to the office I have some suggestions for those making important decisions on the tech they are using and how to protect their network as people come back into the office, it is also fortunate that this week the NCSC issued it's latest "the 10 Steps to cyber security", which will be helpful for those making those decisions. If you opted out of App tracking with your recent apple update you may be interested in how to avoid being tracked by Google Analytics across all websites. The Spanish Data Protection Commission who issued 5 fines this week and on the good news front a COVID-19 vaccine SMS scammer has been sent to jail for up to 4 years for sending fake text messages.

Blogs of the Week
Helen Calvert – The No Bullsh*t Guide To A Happier Life Podcast
Emily Overton – Open-source intelligence vs Privacy

Warnings For Sport Fans To Get Cyber Secure

The UK's cyber security experts are concerned that sports fans have not yet protected their online streaming accounts and are being encouraged to do so ahead of a summer of major events which starts this weekend with the all-English UEFA Champions League Final. With millions expected to livestream the final the NCSC is urging them to make sure that they take steps to secure their accounts which are notoriously easy to hack. Particularly if they use weak passwords (the list of previously compromised passwords include popular football team names liverpool (280,723), chelsea (216,667), arsenal (179,095), manutd (59,440) and everton (46,619). If an account has been breached a hacker can use the account holders' information to make unauthorised payments or harvest data to use for phishing emails and scam calls. You can find guidance here: https://www.ncsc.gov.uk/news/call-for-fans-to-get-cyber-secure-before-summer-of-sport

Cybercriminals Focus On Small Businesses

Traditionally, ransomware attacks have targeted larger organisations but we are seeing an increasing trend where small and medium-sized businesses are targeted. This is because many of these SMBs are vendors to larger enterprises and therefore can be a route into

their systems. You are after all only as safe as your weakest link and a cyber security focus throughout your supply chain is therefore key.

While regular system backups were once one of the key defences against a ransomware attack they are also no longer providing the protection that they once did. Ransomware has evolved and the criminals have learned that they can use the network access that they used to plant ransomware files to "exfiltrate data" which means they can "encrypt and exfiltrate" where they both encrypt the victims' files, steal them and threaten to sell or release the data if the victim doesn't pay the ransom. You can read more here: https://www-techradar-com.cdn.ampproject.org/c/s/www.techradar.com/amp/news/why-system-backups-no-longer-shield-against-ransomware

Personal Data leaked by FastTrack Reflex Recruitment

21,000 files were found to have been leaked by FastTrack Reflex exposing CVs which contained personal information from thousands of job applicants including personal IDs of applicants, including passports, citizen ID cards, driver's licenses, and skilled worker IDs. If you applied for a job through FastTrack Reflex Recruitment I strongly recommend you keep an eye out for potential scams and identity fraud.

The problems with Bringing the Tech Back on Site

As we slowly "get back to the new normal" businesses will be having some difficult conversations and making important decisions on the tech they are using and how to protect their network as people come back into the office. There are 3 real choices that we will all face; to bring everyone back in, some form of hybrid working and to keep remote working.

All will require IT departments and business owners to think carefully about cyber security in ways they may never have done before. This is in addition to their health and safety and operational concerns. The main issue will be addressing the question of just how "safe" the tech they plan to bring back onto their network is. Whether staff were using one of your desktop systems or a laptop it is possible their computer could bring a "virus" back to work that is just as deadly to the business as COVID was to the humans in it. Before these computers connect to the network you will want to make sure you have scanned them for viruses and carried out any remedial work such as updating the software, network connections and virus guards.

Do Cybercriminals Deliberately Spell Things Wrong

This week as I prepared a training session I was reminded of a post last year by Mike Ouwerkerk asking if grammar or spelling mistakes in phishing emails were deliberate or if it was just that the originators couldn't spell (73% of respondents thought the latter was correct). In many conversations afterwards the simple advice to check emails for spelling and grammar and if there are mistakes don't trust it has helped many take their first steps in protecting themselves. This is because:

- Genuine businesses take time with their emails so if a message asks you to click on a link there are unlikely to be spelling mistakes in the text.
- If you ignore a message which contains spelling mistakes the cybercriminals are less likely to bother with you in the future.
- Conversely if you receive an email 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 are more likely to focus on you.

Targeted Advertising

Following the latest apple update where users are automatically unsubscribed from tracking by the apps on their phones I was pleased to find a link on the ICO page to opt out of being tracked by Google Analytics across all websites (https://ico.org.uk/Global/cookies). As well as using a search engine such as Duck Go this is a simple way to avoid seeing an advert on social media for a product you have viewed online. Simple advice on how to:

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

Can be found on the National Cyber Security Centre website (https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely).

How Organisations Can Protect Themselves In Cyberspace

The NCSC have reissued their "the 10 Steps to cyber security" which will be very timely advice for organisations as they return to work. Although it is aimed at medium to large organisations, those who have a member of staff to manage the organisation's cyber security it can be used by all (smaller organisations may wish to start with the NCSC Small Business Guide). The 10 steps is a summary of NCSC advice, with links to more detailed guidance and it can be used with their very helpful "Cyber Security Toolkit for Boards". If you are looking for something to help those leading the organisation have the "right" discussions about cyber security I recommend you check it out. The 10 Steps include:

Risk management	Engagement and training
Asset management	Architecture and configuration
Vulnerability management	Identity and access management
Data security	Logging and monitoring
Incident management	Supply chain security

Fines

Spanish Data Protection Authority Issues 5 Fines In A Week

It was a busy week for the Spanish Data Protection Commission (5 fines in one week). A restaurant shared details of a complaint with other guests and was fined €6000, another company was fined €4000 for excessive video surveillance, Vodafone Espana were fined

€100000 for failure to screen marketing calls against the "Robinson list", a company MD was fined €1500 for failing to inform a data subject that he was collecting data and a physician was fined for €3000 for copying patients files so he could offer them services at his new clinic.

UK ICO Fines Amex £90,000 – For Sending Unsolicited Marketing Emails

The Information Commissioner's Office received complaints from Amex customers who were getting marketing emails even though they had having opted out. Between June 2018 and May 2019 Amex sent over 50 million servicing emails to customers including more than 4 million marketing emails, designed to encourage customers to make purchases (viewed by the ICO as a deliberate action for financial gain). Moreover the company did not review its marketing model after it received customer complaints. Andy Curry, ICO Head of Investigations said ***"I would encourage all companies to revisit their procedures and familiarise themselves with the differences between a service email and a marketing email, and ensure their email communications with customers are compliant"***.

Prison Sentence For COVID-19 Vaccine SMS scammer

A criminal received a 4-year jail sentence for sending fake SMS messages pretending to be from the NHS, banks, and other commercial organisations. The scam included setting up bogus websites based on the GOV.UK domain, which claimed the information was needed to "verify" individuals and their entitlement to receive a vaccine.

Blog and Podcast of the Week

Helen Calvert – The No Bullsh*t Guide To A Happier Life Podcast

I was lucky enough to attend Helen's podcast launch this week and was delighted to listen to the first two of her podcasts afterwards. Episode 2 was all about how we can reach your own optimum productivity. When was the last time you took stock of what it is you need to function properly? Helen shares her own experiences and explains why identifying what it is we need to be at our best, is important, as well as some reasons why we need to get rid of any guilt when we say no and how important it is to ask for help. I'll be coming back every fortnight! You can listen here: https://www.clear-day.co.uk/category/podcast/

Emily Overton – Open-Source Intelligence Vs Privacy

This is a great ethics blog about the impact of open-source intelligence (OSINT) on Privacy. OSINT is the methodology for collecting, analysing, and making decisions about data obtained from publicly available sources. Emily (AKA RM Girl) believes it is all about the purpose for which you are gathering the information (who you are, why you're doing it and what you plan to do with it) and I am inclined to agree. She asks herself if she would be happy with it if she was the data subject and if not she doesn't do it. A great case of do as you would be done by. Asking such questions as: should you be doing it, will it get you in trouble and are your motivations sinister can help guide you through the ethics maze. You can read the blog here: https://rmgirl.co.uk/2021/05/24/osint-vs-privacy-infringement-and-good-uses/