THURSDAY THOUGHTS

Happy Thanksgiving! This Thursday thoughts focusses on keeping safe in the run up to the festive season. How to protect your data and ways you can be scammed. Included in this is how businesses are being scammed through "invoice hacking". I also have a super scary (and extreme) example of how easy it is for someone to take over your life.

Continuing on the Cookies theme of the last few weeks I have a description of how they are being used by the AdTech Industry on Charity websites (but this could just as well be your company website). It is a wakeup call for us all of what the "code" the AdTech Industry puts on our website, especially on sensitive pages, does behind the scenes in terms of profiling. To say that the AdTech Industry is in desperate need of further regulation is an understatement.

Also news of how one set of Hackers have taken a leaf out of Robin Hood's book and an exploration of whether you could cause a traffic jam over the internet. The usual fines and things to watch out for and for this week following the video theme I have replaced blog of the week with podcasts – I hope you like them!

My "Podcasts of the Week"
Data Privacy Podcast (hosted by Tom McNamara) – GDPR Records of Processing Activities
Debbie Reynolds - " Episode 3 of "The Data Diva" Talks Privacy Podcast

Protecting Your Data in the Run Up to Christmas

Many of us will be missing the human interactions that usually come with the Christmas Holiday Period. We will be doing more on line both from a sharing of information and shopping point of view. Here are some tips on how to protect yourself and your data:

- **Don't give sites your personal information** – when purchasing online or entering a competition, be aware of the information you provide. Ask if it is necessary for the vendor to have that information to complete the transaction if not only provide the minimum information required or checkout as a guest.
- **Don't overshare** – Be very careful about sharing where you are and who you are with. Post when you get home rather than immediately that way you can enjoy the moment and keep yourself and your property safe.
- **Don't rush through the online checkout** – be cautious of how you pay and consider the security controls on the merchant's website. Where possible use an external payment gateway, or Pay Pal.
- **Don't shop when you are stressed** – you are more likely to be scammed if you are stressed or overwhelmed.
- **Double check** – do not open an e-card or electronic gift card before you have checked with the gift giver. Be especially wary of .zip or .exe attachments or links.
- **Watch out for "Festive" Apps** – be mindful what your "Festive App" wants to access. Only use apps from reputable sources and check their reviews.

- **Websites** - be cautious on unfamiliar retail websites. Especially if they have products and services at extremely low prices. It is possible that they could be a scam website.

Gabriel Friedlander recently uploaded this video telling you how to keep safe when shopping on line https://youtu.be/uUhYuxAfRaI

How Many Ways Can You be Scammed Between Now and Jan 1

Happy Thanksgiving! But remember to be careful what you share, where you click and who you tell what you are doing. Holidays provide opportunities for scammers, trolls and the criminally minded who are out there looking for ways to take advantage of you, your community, AND your family. If you post asking for someone to look after your house while you are away it won't be just your contacts that see your post, similarly "all time good deals" will appear as if by magic to help you celebrate the events between now and the end of the year … and there are many!

Black Friday / Cyber Monday	Native American Heritage Day	St. Nicholas Day
Bodhi Day	Chanukah	Winter Solstice
Feast of Our Lady of Guadalupe	Christmas	Kwanzaa
New Year's Eve		

Invoice Hacking Scams

There has been an increase in the prevalence of Invoice Hacking Scams during COVID19. Businesses are being warned to call their suppliers and confirm invoice and bank account details before transferring large amounts of money. This is even more important if you have received an email from that supplier asking you to change the details of their bank account. Suppliers should also consider sending a text with every invoice they send so that the customer can expect the email. That way if there is a delay in transmission of the email the customer will know that there is a chance that the email has been hacked and the email intercepted. You can read one case study here: https://www.abc.net.au/news/2020-11-24/business-email-scam-tradies-computer-hacked-costs-51000/12817584

How Easy is it for Someone to Take Over Your Life

I found a video which explains how easy it is for someone to take over your life if you live it on line. It was achieved by just using Facebook, a phishing email and a phone call. It is really quite scary how easy it was! https://www.youtube.com/watch?v=Rn4Rupla11M&feature=emb_title

Cookies, Charities and The AdTech Industry

Recent research in the UK has highlighted that global for-profit advertising companies could be profiling users of charity websites much more extensively than the Charities or their supporters would have thought. Often this is most prevalent on pages dealing with topics like mental health, sexual violence, and disability. The research hopes to "shine a light on a practice that is, at best, morally opaque, and at worst, illegal and harmful". But who is at fault. Is it the AdTech Industry or the Charities. What is clear is that the AdTech Industry is in desperate need of further regulation. Much of the profiling happens on the server and the data supply chain is "muddied at best". However, it is the site owner's responsibility to understand what is and isn't loading on any given

page. This is a lesson for us all to take responsibility for the content on their websites (and not just the words that people read there). You can read more here https://proprivacy.com/privacy-news/exposing-the-hidden-data-ecosystem-of-the-uks-most-trusted-charities

Hackers and Robin Hood

Just when you thought 2020 couldn't get odder comes the news that a hacker group have been trying to make donations to charity. "Darkside" are better known for hacking into computer systems, blocking access to critical data and then leaking it online while at the same time demanding a ransom from its victim. However, they posted receipts on the dark web showing that they were trying to give $10,000 to charities(one supporting children and the other clean water). This is but a small portion of their "earnings" and the charities are ones most of us would support. But It does make you ask what judgement would be made by the supporters of these charities if it came to light the source of such a "donation". You can read more here: https://www.marketplace.org/2020/11/18/cyber-crooks-seek-to-provide-charitable-donations/

Could you Really Cause a Traffic Jam over the Internet

According to a recent research paper you can make a tesla apply its brakes suddenly if you insert play short clips of pedestrians on digital billboards beside the road. In order for the clips to be picked "seen" by the Tesla cameras the clips need to be less than 0.5 seconds long (almost imperceptible to passing humans). Let's see if we see a spate of these internet connected billboards being taken over by actors remotely inserting random clips and causing tailbacks. You can read more here: https://www.nassiben.com/phantoms

ICO fines Ticketmaster UK Limited £1.25million

The ICO has fined Ticketmaster UK Limited £1.25million for failing to protect customers' payment details. The ICO assessed that Ticketmaster had "failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page." The case "straddles" the before and after GDPR period (Feb-Jun 2018).

Ticketmaster were subject to a data breach (names, payment card numbers, expiry dates and CVV numbers) which potentially affected 9.4million customers throughout Europe including 1.5million in the UK. As a result of the breach, 60,000 Barclays Bank customers and 6,000 Monzo Bank customers suffered fraudulent use of their cards. The ICO found that Ticketmaster failed to:

- Assess the risks of using a chat-bot on its payment page
- Identify and implement appropriate security measures to negate the risks
- Identify the source of suggested fraudulent activity in a timely manner

If you had a Ticketmaster account in 2018 then I would double check your passwords and check out haveibeenpwned.com.

You can read the ICO summary here: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-

details/?utm_source=linkedin&utm_medium=information+commissioner%27s+office&utm_term=66939fc7-ad24-466c-a74d-aba85a8de984&utm_content=&utm_campaign=

and the full judgement here: https://ico.org.uk/media/action-weve-taken/mpns/2618599/ticketmaster-uk-limited-mpn.pdf

Spanish DPA fine Security Company for NOT Having a DPO

Conseguridad SL (a private security company in Spain) set up a video surveillance system to record activity on their premises. But the company failed to appoint a data protection officer. The lack of the DPO meant that individuals could not exercise their rights under GDPR (right of access) because there was no one to ask. Because the national legislation specified that DPO is required if a private security company processes personal data on a large scale the Spanish DPA fined Conseguridad SL €50,000 for violating of Article 37(1)(b) of GDPR. You can read more here: https://gdprhub.eu/index.php?title=AEPD_-_PS/00251/2020&mtc=today

Things to Watch

Dell and CISCO move to "as-a-Service"

Dell, CISCO and other companies have announced that they will move their product catalogue to an "as a Service" offer. This should provide customers greater flexibility in procurement and maintenance but requires them to trust the companies more. It will be interesting to see how this pans out. You can read more here: https://www.crn.com/news/data-center/dell-to-make-all-offerings-as-a-service-says-michael-dell

Possible Update of the Computer Misuse Act

The UK Prime Minister was asked to look at reforming the Computer Misuse Act by a group of British infosec companies last year. Many feel that the act "has failed to keep pace with technological and market developments". In particular the companies want to see statutory defences for professionals who are trying (ethically) to detect and prevent crime. One to watch!

Blogs of The Week – Podcast Special

For a change this week I have 2 Podcasts in the Blog of the Week spot. Sometimes it's nice to stop and listen!

Data Privacy Podcast – GDPR Records of Processing Activities

This Data Privacy Podcast (hosted by Tom McNamara) discusses the Records of Processing Activities (ROPA). The guest is Laura de Vries from Cuccibu. If you want to know what the ROPA includes, who needs to do one, and the best approach to completing it. This is a great place to start. https://dataprivacypod.com/laura-de-vries-how-to-create-a-gdpr-records-of-processing-activities/

Debbie Reynolds - " Episode 3 of "The Data Diva" Talks Privacy Podcast

This is an excellent and wide-ranging interview from Debbie Reynolds with Allen Woods covering such a variety of cyber topics. If you want to know about cookies, data storage, contracts, adequacy and Schrems II amongst others they are all covered in an engaging and natural conversation. Well worth a listen! https://www.debbiereynoldsconsulting.com/podcast/e3-allen-woods