THURSDAY THOUGHTS

This week we have an interesting discussion on risk. This follows the Wentworth Golf Club cyber-attack where personal details of high-profile club members were stolen by hackers and yet the club only considers the loss of this information to be “low risk”. In the world of increased online working and socialising it is really important that we take time to check and double check something is genuine, whether a phishing attempt by SMS, COVID Vaccine emails or requests to make a payment to a different bank account. Its important to protect accounts with 2FA and have a good password. But we need to make sure that the way we authenticate a password reset is as good or better than the password itself.

Also in the news this week, the NCSC hosts its first-ever cyber security summit for Sports Clubs. Guidance on passwords, vulnerability scanning, housekeeping and protecting your personal data from your car as well as the latest round up of news, breaches and fines. This week some great videos for you.

Vlogs of the Week
Alex Dodgshon - 6 customer lock in strategies
Debbie Reynolds - The impact of Data Privacy on Marketing
Gabriel Friedlander - How Cyber Criminals Almost Got Away With Over $30 MILLION
Richard Merrygold – How to do a Gap Analysis

Wentworth Golf Cyber Attack

The Wentworth Golf Club cyber-attack presented an interesting discussion on risk this week. The membership details of high-profile club members were stolen by hackers - the details include names, dates of birth, home addresses, email addresses and landline numbers and the last four digits of bank accounts. But because the information stolen is insufficient to access any private account on the Wentworth portal the club considered the breach "low risk" and went on to say they were pleased to report that no ransomware request had been made. It makes one ask the question “Low risk to whom?”. Certainly not the data subjects who can now be stalked, targeted and “papped” by anyone the hackers have sold or shared the database with.

You should assess risk from the Data Subject’s point of view as well as from the businesses. So I await with interest the results of the comment from the ICO spokesperson "We received a data breach report from Wentworth Golf Club and will be assessing the information provided.”

Are Your Security Questions Leaving You Open to Attack

The best security tools and authentication systems are no use to you if they can be bypassed. You need to make sure that the way you authenticate a password reset is as good or better than the password itself. So if the answer is simple, the information is easy to find or it is so complicated you can never remember it then you should consider a different way. Here are 5 questions

- Can an attacker guess the answer?
- Can your user remember the answer?

- Is the answer used elsewhere
- Will the answer be long?
- Does this method require effort or cause stress?

Phishing, Spear Phishing and Whaling

We all recognise the term Phishing as a communication which contains a link that we are tempted to click on. It could be a SMS or email or even a post on social media. Those who fall for such attacks often find their passwords are compromised or their computer used as a Botnet. But what about spear phishing and whaling? They are also types of "phish" and they are more difficult to protect against. A phishing attack that targets a specific person is known as "Spear phishing". Often the email is crafted so that it contains sufficient personal information to make them click (think HMRC tax phishing campaigns at the beginning of each year). The next level up "Whaling" is a spear phishing attack on a "big phish". This can be a board member or an employee working in a particular area (e.g. vaccine developers).

COVID Vaccine Scams

There are growing reports of cyber criminals taking advantage of the COVID-19 vaccine roll-out. This was considered important enough to be covered on the One Show last night. The scam comes in the form of email or text and in one case a visit to an elderly lady in her home. What is common is that they ask victims for personal and financial information or to prove who they are by sending copies of personal documents (passport, driving license, bills or pay slips). None of these are required for the COVID Vaccine in the UK. If you live in UK and get a message like this remember: In UK the vaccine is **free,** the NHS **will never ask you** for your bank account or card details, the NHS **will never ask you** for your PIN or banking password, the NHS **will never arrive unannounced at your home** to administer the vaccine and most importantly the NHS **will never ask you to prove your identity**. If you received a scam email of any sort you can report it to the NCSC (report@phishing.gov.uk suspicious text messages can be forwarded to 7726).

Guidance

Passwords

In their latest guidance the NCSC reminded us that it is OK to writing passwords down on paper. As long as you keep that paper safe. Choosing an appropriate passwords as a keys to our online life is very important. The NCSC recommends using 3 random words or a password manager and that we use two factor authentication (2FA) to further protect our accounts. You will find all the latest guidance on the NCSC website (https://www.ncsc.gov.uk)

Vulnerability Scanning

If you are concerned that it is hard to keep up with critical vulnerabilities, software patching and configuration changes you may be considering using a vulnerability scanning service. There is so much choice and the solutions come in many shapes and sizes so selecting the right one for your business will be key. To help with the decision process the NCSC has produced new guidance on choosing and using a vulnerability scanner. Worth a look if you "own or make use of IT systems to communicate with other systems or people" i.e. most businesses or organisation. You will find the

guidance here: https://www.ncsc.gov.uk/blog-post/vulnerability-scanning-keeping-on-top-of-the-most-common-threats

Protecting Your Data From Your Car

Did you know that the data your car collects about you can be shared with automakers, rental agencies, police, & third parties? The newer your car is, the more data it probably collects. In addition to information on speed and acceleration, cars collect unique IDs of Bluetooth and Wi-Fi devices, call logs, contacts, text messages, when doors were open, locations you were in (and when/how often you were there). This means it can reveal when texts and calls were made and voice commands or web histories. This data can be accessed by police and others (e.g. criminals accessing live data from a target's car). If you rent a car and sync your phone to it you need to be wary. Don't let your smartphone sync with every car AND be sure to remove the data from the car when you have finished using it. If you use the car's navigation system, try using post codes and cross road rather than an entry entitled "home".

Microsoft Recommends Security House Cleaning

Microsoft's director of identity security has urged customers tighten up permissions and use multi-factor authentication to prevent future attacks. This is the first time I have seen Microsoft recommend organizations adopt a "zero trust mentality". You can read more here: https://www.zdnet.com/article/microsoft-how-zero-trust-can-protect-against-sophisticated-hacking-attacks/

Guidance On Data Breach Notification

The EDPB has issued a public consultation on its proposed data breach notification guidelines. The guidelines should help data controllers manage data breaches and understand the factors it should take into account in any risk assessment. The public consultation ends on March 2nd.

Best Antivirus Software In 2021

If you are looking for new antivirus software to keep you and your data safe from malware and viruses. There is a guide here: https://www.zdnet.com/article/best-antivirus/

News

Billions in Bitcoin Inaccessible in Lost Wallets

Approximately $220 million in Bitcoin will be sitting in "wallets" which are permanently lost or inaccessible. Simply because the person controlling it has either lost the password or the hard drive on which it was stored has been disposed of or reformatted.

Kenyan Data Protection Taskforce

The Kenyan government has set up a Data Protection Taskforce which will be chaired by Data Commissioner Kassait. The taskforce will set up a data protection committee, establish data protection regulations and "sensitize the public" to the new regulations.

Police Records Accidentally Wiped

Hundreds of thousands of police records were prematurely deleted. Apparently as a result of a coding error which was not picked up at the testing stage before the software was run. Police are working "round the clock" to rectify the error. However assurances have been given that criminals

will not get away with anything. Multiple records are held on the same individuals on the same crimes on other profiling systems and if necessary officials can re-submit the entries manually.

Sports clubs summit on cyber security

It was great to hear that the NCSC has hosted its first-ever cyber security summit for Sports Clubs. Over 180 representatives attended from a range of clubs and organisations (including the Premier League, EFL, rugby and cricket clubs. The sports industry continues to be a high-value target. They receive more than double the average number of cyber-attacks each year than other UK businesses. The majority of organisations suffer at least one attack each year.

'Shaping a Safer Digital Future'

The European Data Protection Supervisor has produced a new brochure to tell the public what it does. The brochure contains a snapshot of the EDPS 2020-2024 Strategy and is available in French and German: https://edps.europa.eu/sites/edp/files/publication/21-01-20_edps_brochures_en.pdf

SCCs

There have been joint opinions on standard contractual clauses (SCCs). One for contracts between controllers and processors and the other for the transfer of personal data to third countries.

TikTok – Really a Data Collection Engine

The saying goes is something is free then you are the product. A coder recently reverse-engineered the TikTok Android app to find out just how it works. Their analysis of what they found is that TikTok is a data collection engine rather than a social network. The App came under fire at the end of 2019 and throughout 2020 because it was a form of "legitimate spyware." We should all be wary of our use of technology - search engines are not educational charities and social media platforms are there because they want to support us socialising. You can read more here: https://www.digitalmusicnews.com/2021/01/18/tiktok-source-code-leak/

Fines

Facebook And Other Big Tech Companies Facing More Lawsuits

There has been much irritation with Facebook's attempts to work around the requirement to comply with GDPR. A court case in Belgium could change how GDPR is enforced. If the Court of Justice of the European Union (CJEU) follows the advice from Advocate General Michal Bobek, then the national privacy authorities in any EU country may take action against a company, even if the firm has its main EU office elsewhere in the bloc. Giants such as Facebook, Google, Twitter, and Oracle who have not been prosecuted up until now (mainly because their EU headquarters are in Ireland and the Irish authority is under resourced) could then face more cases in the courts.

Leaks and Cyber Attacks

Capcom releases update on their ransomware attack

Capcom report that up to 390,000 people could have had their personal information stolen in last year's ransomware attack. Fortunately, credit card details were not part of the information stolen by hackers.

SolarWinds cyber-attackers also breached Malwarebytes internal emails

Malwarebytes confirmed this week that some internal emails were accessed by the same group as SolarWinds. Not as the result of a SolarWinds compromise, but via Microsoft Office 365 and Azure.

Blogs of the Week

Alex Dodgshon - 6 customer lock in strategies

In this blog Alex recommends "Digging a wider moat to lock in your customers". Few of us achieve the status of being a monopoly without competition but the simple strategies with real examples from Alex show how we can defend ourselves from competitors who want to take our customers away. You will read about ideas such as why it is important to demonstrate expertise, creating an "Army of Raving Fans" and Becoming a Verb. Here is the link: https://www.uscita.co.uk/customer-lock-in/

Debbie Reynolds - The impact of Data Privacy on Marketing

In this episode Debbie talks to Beth Winters about the impact of data privacy on marketing, consent versus notice, data privacy policies, types of data privacy technologies, keeping track of CCPA and CPRA data and compliance issues. You can see the video here: https://www.debbiereynoldsconsulting.com/podcast/e11-beth-winters

Gabriel Friedlander - How Cyber Criminals Almost Got Away With Over $30 MILLION

In a salient (and succinct) video Gabriel discusses a targeted attack where the criminals had access to the company's email and were therefore able to intercept emails. Look for signs, like, does the style of the email feel different from previous emails you received from that particular person. If something changes always call and verify. Watch this video: https://youtu.be/Q37i4P7SKA0

Richard Merrygold – How to do a Gap Analysis

In this edition of the Data Protection Diaries for those who can't afford to pay someone to do it for them Richard explains that a gap analysis doesn't have to be a complicated, time-consuming or annoying activity. If you want to know what a good gap analysis looks like and how to do one this is a video for you: https://www.youtube.com/watch?v=B5IwGV0oR2Y&feature=youtu.be