THURSDAY THOUGHTS

First this week some good news. Zoom is offering unlimited time on their basic service for schools and colleges for free during the pandemic. I also celebrate a little-known cyber fact about Hollywood actress Hedy Lamarr. There is also the usual updates on recent fines, a hospital in Cork for disposing of hard copies of medical data in a public recycling centre and the airline IBERIA for failing to allow users to reject all cookies when surfing its website. There has been a potential data leak which if true has the potential to affect millions of Agoda, Expedia, Booking.com and Hotels.com clients.

I also explore password audit tools, why we should move away from telephone-based multi-factor authentication, the risks of clicking on links and double clicking on pictures. There's an update on how many cyber attacks the UK has seen in the last 12 months (more than 200 of them related to COVID19) and some news of the "Tianfu Cup" where hackers come together in an international competition to see if they can hack commonly used software.

My "Blogs of the Week"
NCSC - Secure Remote Access for Critical Infrastructure
Andy Graham – MHFA999- My 5 Favourite Mental Health Apps

Schools get unlimited time on Zoom for Free

Many schools may not yet be aware that Zoom will remove the 40 min time limit on their free basic accounts. Zoom have temporarily removed the 40-minute time limit on free Basic accounts for primary and secondary schools affected by the Coronavirus.

Celebrating Hedy Lamarr - actress, mathematician and inventor

This week would have been actress Hedy Lamarr's 106th birthday. Many are not aware that as well as being a Hollywood actress she was also a mathematician and inventor. She co-invented a device that helped make possible the development of GPS, Bluetooth, and Wi-Fi technology and the frequency hopping used in radios.

Cork hospital fined €65k

The importance of proper procedures for the destruction/disposal of personal data cannot be understated. On 4 Nov it was reported that Cork University Maternity Hospital had been fined €65k after patient data was found by a member of the public in a public recycling centre. A large number of documents were found which related to 78 people and included sensitive health data about six of them (including medical histories and future planned programmes of care). In addition to the fine the DPC (the Irish equivalent of the ICO) ordered the hospital to bring its systems for processing and disposing of patients' information "into compliance" with GDPR standards and issued the executive with a formal reprimand regarding same.

Website users Should have control over cookies

This week the Airline Iberia was fined €30000 for not allowing users to reject all cookies when surfing its website. I also saw a series of blogs about the Formula 1 website and it's cookie policy. If you haven't yet got the cookies on your website sorted then I urge you to look at it. The fine for Iberia should be seen as enough of a warning of the potential consequences.

Hotel Booking Firm Leaks Guest Data

A software provider has potentially exposed the personal data of millions of hotel guests around the world after a cloud database belonging to the Spanish developer Prestige Software was found to be unprotected. The platform in question enables hotels to automate their availability on booking websites like Agoda, Expedia, Booking.com and Hotels.com. Over 10 million individual log files, dating back to 2013 including full names, email addresses, national ID numbers, phone numbers and even card details (card number, holder's name, CVV and expiration date). There is no evidence that the information has been used by cyber criminals but this cannot be guaranteed. You can read more here: https://beebom.com/credit-card-data-booking-sites-data-breach/

Password Security

Password security is more important than ever and there are some types of dangerous passwords that can expose organization to great risk. Many larger organisations are therefore turning to password audit tools which scan their active directory, identifying password-related vulnerabilities. The information gathered compares passwords to lists commonly found on websites like haveibeenpwned.com and those listed as having been breached on the dark web. It then produces a report for the business of any vulnerable passwords that are in use as well as those which have expired. One such tool recommended by the UK NCSC is Specops Password Auditor the link to their site is: https://specopssoft.com/product/specops-password-auditor/

If you just want to see if your password is on the list you can access the NCSC top 100,000 password list here: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt. If you see a password that you use in this list you should change it immediately.

This year's top 10 passwords to avoid are:

123456	123456789	qwerty	password	111111
12345678	abc123	1234567	password1	12345

Microsoft urges users to stop using phone-based MFA

Microsoft has started to urge users to stop using telephone-based multi-factor authentication (MFA) solutions (e.g. one-time codes sent via SMS and voice calls). They recommend that users adopt newer alternative authentication methods like hardware key, mobile app, mobile app push, biometrics, risk-based auth, or even password less authentication**.** Both SMS and voice calls are transmitted in "cleartext" which means that they are easily intercepted. Making SMS and call-based MFA "the least secure of the MFA methods available today". There are a number of authentication software products some can be found here: https://lnkd.in/ehqEiHZ

Why you shouldn't double tap on a picture

Social media is full of messages like "Double tap the picture too see what happens, you won't believe it!". Do you know why? Well this is what happens when you double click on the image … it gives the article a like. It is a clever way for someone to spread clickbait junk marketing or scams. I'll be remembering this next time I see a message to double click and will avoid the temptation.

At Christmas watch out for suspicious links

With Christmas just around the corner it is again time to be super vigilant about emails again. It is all too easy to click that link because you're in a rush or it comes from someone you trust. But if you receive something you aren't expecting then follow my motto "if in doubt report it and delete the message" because it's better to be safe than sorry. After all a genuine the organisation will contact you again to see why you haven't responded. You can find guidance on how to report suspicions emails here: https://www.ncsc.gov.uk/information/report-suspicious-emails

What Got Hacked at The Tianfu Cup Competition

The Tianfu Cup 2020 is an international cybersecurity hacking competition. This year saw successful hacking attempts made on multiple Adobe, Apple, Google, Microsoft, Mozilla, and Samsung software products. Patches for all the demonstrated bugs demonstrated are expected to be released in the coming days so **make sure you keep your eyes open for the updates and install them.** Software found to be vulnerable include Apple iPhone 11 Pro running iOS 14 and Safari browser and Samsung Galaxy S20 running Android 10 as well as:

Adobe PDF Reader	ASUS RT-AX86U router	CentOS 8
Docker Community Edition	Google Chrome	Microsoft Windows 10 v2004
Mozilla Firefox	TP-Link TL-WDR7660 router	VMware ESXi hypervisor

You can read more here: https://thehackernews.com/2020/11/windows-10-ios-chrome-firefox-and.html

Blogs of The Week

NCSC - Secure Remote Access for Critical Infrastructure

The NCSC produces some very helpful guidance on remote access architecture design. This week it expanded the offering with a blog on remote access to Critical National Infrastructure. Showing how the NCSC's guidance can be used, the key principles and documentation required and the cloud security principles to follow. There are some very useful diagrams in the piece too. You can read the blog here: https://www.ncsc.gov.uk/blog-post/cni-system-design-secure-remote-access

Andy Graham – MHFA999- My 5 Favourite Mental Health Apps

This is an old blog by Andy but super helpful at this difficult time. Andy is a mental health first aid instructor and this blog features the apps that he uses to help maintain his own mental wellbeing. The bonus is they are all free. Technology is regularly seen as a cause of stress and anxiety but as Andy says it can also be very useful in helping us to maintain our wellbeing. His Top 5 Apps are: My Chakra Meditation 2, Qi Gong Meditation Relaxation, Stay Alive, Breathe, Think, Do With Sesame Street, Anxiety Release. You can read his blog which explains what each app can help with here: https://mentalhealth.fitness.blog/2018/08/01/my-5-favourite-mental-health-apps/