Social Engineering: Hacking the Human

Miroslav Doncevic, Managing Director, Digital Medical Systems Pty Ltd

The constant news of cyber security attacks resulting in major data breaches is just part of the Digital Age, with some hacks reaching national prominence – for example, the Optus [1] and Medibank ransomware attacks in late 2022 [2], which impacted and caused great distress to millions of Australians whose personal information was hacked. This inevitably leads to the strengthening of privacy and corporate legislation and regulations by governments, with higher penalties imposed on organisations and directors for "large or repeated privacy breaches", with the stated goal, *"to incentivise businesses to take strong privacy and cybersecurity measures to protect the personal data they hold*". [3]

The *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* [4]*,* which came into law on 13 December 2022*,* has four key objectives:

"1. to significantly increase penalties for serious or repeated privacy breaches;

2. to give the Office of the Australian Information Commissioner (OAIC) enhanced powers to request information and conduct compliance assessments of the notifiable data breach regime;

3. to give the OAIC new enforcement powers, allowing the OAIC to require entities to conduct external reviews of their internal procedures and to publish notices about specific privacy breaches to affected individuals; and

4. to introduce new information sharing powers for the OAIC and the Australian Communications and Media Authority (ACMA)." [5]

The *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* has increased maximum penalties for an individual to, *"not more than $2,500,000"*, and for a body corporate, *"not more than the greater of: $50 million; three times the value of any benefit obtained through the misuse of the information; or, if the value of the benefit obtained cannot be determined, 30 per cent of a company's domestic turnover in the relevant period*. [6]

Ouch! Given all of this loud and clear messaging, directors and practice managers must urgently take action to improve cyber security, especially in the context of healthcare providers *again* being the highest reporting sector for data breaches, according to the latest Notifiable Data breach Report from OAIC. [7]

Information systems are broadly comprised of three interconnected components: *People, Processes, Technology*.

Improving the cyber security of *Processes* and *Technology* is well understood, for example; developing and implementing cyber security standards based policies, procedures, standards, and guidelines for the *Processes* component; implementing controls such as Multi-Factor Authentication (MFA) for enhanced access control and authentication, deploying the latest Extended Detection and Response (XDR) anti malware software systems with Artificial Intelligence (AI) and Machine Learning (ML) technologies, and installing Next Generation Firewalls (NGFW) for perimeter defence, etc. for the *Technology* component.

The *People* component is the weakest link and that is well known by hackers as well, so that is where *Social Engineering* comes in to play.

Cyber security veteran and author, Ian Mann, defines *Social Engineering* (SE) as:

> *"To manipulate people, by deception, into giving out information, or performing an action".* [8]

In another, more descriptive definition from the OAIC, *Social Engineering* is:

> *"An attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations"*. [9]

Social Engineering cyber attacks can be described in four categories or variations, all based on the broad basic theme of deception:

Phishing

Phishing, a play on 'fishing', being the metaphor of using a baited hook or lure that tricks the fish into biting, and getting hooked, in this case, cyber attackers deceiving the unwitting human with fraudulent email messages into giving confidential information, such as IT systems login credentials, passwords/passphrases, credit card details, enticing the human to open an attachment, (which contains malicious content), or to visit a fake website that will ask the user to provide login information, i.e., online banking logins, or the downloads malicious content into the user's computer/device upon being opened.

Most of us have seen the various fake emails pretending to be from a large organisation we trust to make the phish more believable, i.e., Telstra, AGL, Australia Post, Australian Federal Police, ATO, etc., all of which are getting much more realistic and consequently, becoming harder to detect as fakes.

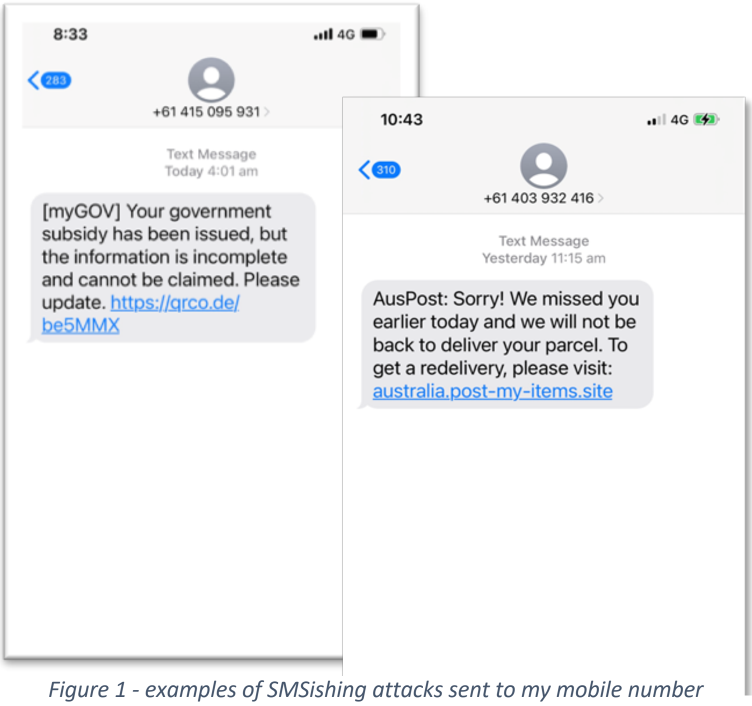
In the most recent OAIC Notifiable Data Breaches Report [10], phishing is the second highest method for malicious actors gaining access to accounts after ransomware.

Variants:

Phishing attacks against businesses, government and other organisations are also known as Business Email Compromise (BEC).

Spearphishing attacks are phishing attacks that specifically target an individual, or a specific group in an organisation.

Whaling, is again, a specifically targeted attack on a senior official or manager (or 'big fish')



+61 415 095 931

Text Message
Today 4:01 am

[myGOV] Your government subsidy has been issued, but the information is incomplete and cannot be claimed. Please update. https://qrco.de/be5MMX

+61 403 932 416

Text Message
Yesterday 11:15 am

AusPost: Sorry! We missed you earlier today and we will not be back to deliver your parcel. To get a redelivery, please visit: australia.post-my-items.site

Figure 1 - examples of SMSishing attacks sent to my mobile number

SMiShing

Smishing, (*SMS*-ishing), where the attacker uses text message to entice the recipient into clicking a link and thus sending the attacker confidential information on the smart phone or downloading malicious programs to the smartphone, as shown in this typical examples sent to my mobile phone number.

Vishing

Another variant, *Voice* phishing is the use of telephony to deceive or manipulate the victim as in the other forms of Social Engineering. If you have received a scam call where the caller claims to be from some important organisation and you must go to a website to pay an account or fine, that is a vishing attack.

Impersonation

It sound incredible, but people are still tricked by an attacker, impersonating someone else, usually an authority figure such as a manager that the victim has heard of but doesn't know, a law enforcement officer, etc. We used to call the attacker a 'con artist'.

The common Social Engineering tricks that hackers will use one of the following techniques to play the human weak link according to the ACSC Small Business Cyber Security Guide :

> "• **Authority:** Is the message claiming to be from someone official or someone senior in the business?
>
> • **Urgency:** Are you told there is a problem, or that you have a limited time to respond or pay?
>
> • **Emotion:** Does the message make you feel panicked, hopeful, or curious?
>
> • **Scarcity:** Is the message offering something in short supply, or promising a good deal?
>
> • **Current events:** Is the message about a current news story or big event?" [11]

Before we may be tempted to think that Social Engineering attacks are about small scams however, let's go back to the Medibank hack from October 2022. How did the hackers get into Medibank systems and exfiltrate the data of up to 4 million Australians?

Nick Bonyhady, writing for the Sydney Morning Herald, says that:

> *"Logs obtained by cybersecurity researchers and seen by The Sydney Morning Herald and The Age indicate someone with access to internal Medibank systems had their company login credentials stolen from their web browser. The credentials were stolen some time around August 7."* [12]

What?

> *"…someone with access to internal Medibank systems had their company login credentials stolen from their web browser"?*

Looks like a good old Social Engineering attack that enticed that someone to go to a fake website via malicious link…

AFP Commissioner Reece Kershaw, naming Russia as the source of the Medibank cyber attack, called it, *"a crime that has the potential to impact on millions of Australians and damage a significant Australian business", and an "unacceptable attack on Australia…"* [13].

Hmmm, the environment has changed. Humans *are* the weakest link in cyber security, and yet also our greatest asset, our *'eyes and ears'* on the ground so to speak. Directors and practice managers must implement a continuous Social Engineering training program for all staff. Social Engineering attacks are very serious threats to your healthcare systems cyber security, with the latest 2023 Ransomware Insights Report from cyber security vendor Barracuda finding that **"69% of ransomware attacks began with an email".** [14]

The risks cannot be higher. More to come… Be cyber safe.

Miroslav Doncevic is the Managing Director of Digital Medical Systems, a Managed IT service provider specializing in primary healthcare IT and cyber security. Miroslav has a Graduate Certificate in Cyber Security, and is a NIST Cyber Security Framework Practitioner. He is currently studying a Master of Cyber Security. Miroslav can be contacted on 1300 865 977, or mobile 0412 032 915, or via email miroslav@dms-it.com.au

References:

[1] *Optus* says *it has been hit by a cyber attack that has compromised customer information, retrieved from https://www.abc.net.au/news/2022-09-22/optus-hit-with-cyber-attack-impacting-customers-/101466036*

[2] *Health insurer Medibank Private hit by cyber attack*, retrieved from https://www.abc.net.au/news/2022-10-13/health-insurer-medibank-hit-by-cyber-attack/101531392

[3] *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. Second reading*, retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22chamber/hansardr/26227/0016%22

[4] Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, retrieved from https://www.legislation.gov.au/Details/C2022B00116

[5] *Increase in privacy penalties given go-ahead - Privacy Amendment Bill passes both Houses, retrieved* from *https://www.gtlaw.com.au/knowledge/increase-privacy-penalties-given-go-ahead-privacy-amendment-bill-passes-both-houses*

[6] ibid, retrieved from https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22chamber/hansardr/26227/0016%22

[7] *Notifiable Data Breaches Report January-June 2022*, retrieved from https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2022

[8] *Hacking the* Human*. Social Engineering Techniques and Security Countermeasures*, p11, Ian Mann, Routledge, Taylor & Francis Group, 2008

[9] OAIC, (2022) Notifiable Data Breaches Report: January-June 2022, retrieved from https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2022

[10] ibid, retrieved from https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2022

[11] Cyber.gov.au, (2022) *Small Business Cyber Security Guide*, retrieved from https://www.cyber.gov.au/sites/default/files/2021-11/ACSC_Small_Business_Cyber_Security_Guide_V6.pdf

[12] Nick Bonyhady, (2022) *How Medibank joined Optus in hack hell*., retrieved from https://www.smh.com.au/technology/how-medibank-joined-optus-in-hack-hell-20221021-p5brt3.html

[13] AFP Labels Medibank Cyber Breach 'an Unacceptable Attack on Australia', and Names the Country Behind It, retrieved from https://www.gizmodo.com.au/2023/01/medibank-cyber-incident/

[14] 2023 Ransomware Insights Report, retrieved from https://www.barracudamsp.com/resources/reports/2023-ransomware-insights-report