Signals

Security report
May 2019

CommonwealthBank

Welcome

It's timely to be bringing out an issue of Signals focused on social engineering given this month saw the release of both the Federal Bureau of Investigation's (FBI) 2018 Internet Crime Report and the Australian Competition and Consumer Commission's (ACCC) 2018 'Targeting Scams' report.

Both publications highlighted the rising cost of cyber crime to people, businesses and communities both here in Australia and abroad, with record numbers of reported losses from technology-related scams as criminals increase both their reach and efficiency.

In the foreword to the ACCC report[1], Deputy Chair Delia Rickard referenced the ACCC's collaboration with the private sector, including the Commonwealth Bank. This shared intelligence has helped improve the detection and blocking of scam transactions, aided in the recovery of funds and supported staff training.

In this fight against increasing volumes and sophistication of cyber scams, working together, particularly to raise awareness in the communities in which we operate is of paramount importance.

We hope this issue of Signals will support conversations within your own businesses to help further this end.

May also saw the launch of CommBank Secure, the updated security section of our public website designed to assist both our individual and business customers in understanding and preventing online fraud. I'd encourage you to visit and explore the information available on https://www.commbank.com.au/support/security.html.

This is also the first of our new, shorter versions of Signals to be released throughout the year ahead of a more expanded publication at year-end. As always, we welcome any feedback to cyber-outreach@cba.com.au.

Pete Steel
Acting CISO

Social Engineering

A modern spin on classic confidence tricks

Melanie Timbrell
Senior Manager,
Cyber Outreach

What is social engineering?

Social engineering refers to manipulating someone into performing an action or giving away information. It is a type of cyber crime that relies on "hacking humans", taking advantage of our natural tendencies to trust other people, help our colleagues, be emotionally driven and to comply with requests from people in positions of authority.

How does social engineering play out, and what are the consequences?

Social engineering attempts can come via email, SMS or even over the phone. But regardless of which channel is used, all social engineering is designed to override normal reasoning and judgement. The goal of scammers is to apply pressure in such a way that your emotions are heightened and you act quickly to do something which under normal conditions you'd consider more carefully.

While some social engineering campaigns may lack sophistication and be poorly-targeted [adopt a scatter gun approach], it only takes a small amount of research through social media, company websites or even data breach databases for a social engineer to be able to tweak their activities into a more convincing lure and increase their effectiveness. Some common types of social engineering are:

PHISHING & SPEAR PHISHING

Phishing is an email scam aimed at obtaining personal information, such as usernames, passwords or bank account details by disguising as a trustworthy source. It may also download malicious software onto devices through a compromised attachment or website link, or direct people to a fake webpage where they're asked to provide personal information.

Spear phishing is a phishing email that is tailored for a particular individual, company or industry so it is more likely to be acted upon by the target.

SMISHING & VISHING

Smishing is a phishing campaign that is delivered via text, and vishing refers to a campaign that uses a voice telephone call or message to execute.

In the news...

In April 2019, the Australian Taxation Office (ATO) issued an alert similar to previous notices from September and March 2018 detailing an increase in reports of scammers contacting members of the public claiming to be from the ATO. The technology used made it appear that calls were from a legitimate ATO phone number and were designed to scare people, saying they had outstanding tax debts and threatening arrest if debts were not paid immediately.[5] The ATO advised anyone receiving these calls to immediately hang up and phone the ATO direct on their standard 1800 number to check their legitimacy.

Top tips to help protect your organisation:

1. Slow down -- build a culture of "stop and think before we act"
2. If you or your staff receive a suspicious email, text or voice mail, train people not to click any links, open attachments or respond
3. Keep antivirus up to date and consider using email filters
4. Be aware that publically available information such as that on company or personal social media accounts, or on your company website, can be used by scammers to craft more convincing lures
5. Protect your systems with strong, unique passwords and multi-factor authentication (especially your email accounts) and make sure staff know not to use the same password for business and personal use

BUSINESS EMAIL COMPROMISE (BEC)

These scams target businesses of all sizes. Using emails made to look like they are from someone you know, such as your boss, your supplier or your customer, these scams will request payment be made to an account under the scammer's control.

There are two main examples of these kinds of scams that it's important to be able to recognise.

Supplier email scams occur when a fraudulent request for payment looks like a legitimate expected invoice, or it could be a fake email requesting you update a supplier's payment details for future payments.

Scammers can also masquerade as your colleagues, emailing a request to make an urgent or confidential payment, often in a way that's different from your usual process.

In the news...

In April 2019, the City of Ottawa reported that close to US$100,000 of taxpayers' money had been wired overseas in a BEC scam.

*In July 2018, the city treasurer received an email which she thought was from the city manager asking her to transfer US$97,797.20 to the bank account of a US firm. The email reportedly told the treasurer that the matter to which it related was confidential, so it wasn't to be discussed with anyone else in the office and any questions were to be directed to the manager via email. In this instance the email address of the real city manager had been **"spoofed"**. This is where an attacker can use software to manipulate the 'from' address so it appears as though it's from someone within your own organisation.*

A few days after transferring the initial amount, the treasurer received another request appearing to come from the city manager requesting an additional amount be transferred to the same account. This email however, happened to arrive during a meeting at which the city manager was present. This led the treasurer to ask him about the request, which of course he knew nothing about. As expected, the incident has taken a personal and professional toll on the treasurer, although in positive news, the city has taken steps to help make it harder for staff to be taken in by these kinds of scams.

These measures include the requirement for different staff members to create and approve payments and mandatory security awareness training for employees.

Top tips to help protect your organisation:

1. Before you make a first-time payment for any amount you are not prepared to lose, call the person or organisation you are paying on a trusted number
2. Ensure all of your accounts, especially your email accounts, have strong, unique passwords and are setup with second-factor authentication (e.g. SMS) where available
3. Setup a payments approval process for your business, preferably requiring multiple approvers, with no exceptions
4. Encourage a culture where staff are comfortable to question a payment instruction even if it's from a senior executive

BAITING

This is another type of social engineering attack that tries to pique a person's interest and therefore convince them to take action, often involving accessing a USB drive.

An example could be where an employee may be enticed to plug a USB drive labelled with something compelling (e.g. "2019 Bonuses") into a USB port. Attackers can install malware onto the USB drive which is executed on the machine into which it is inserted. The malware may enable the attackers to remotely survey and control the infected device and potentially spread throughout a network.

A research paper presented at the 2016 USA Black Hat cyber conference by Elie Bursztein[7] looked at whether dropping USB keys really works. In the research, 297 USB keys were dropped on the University of Illinois campus carrying various labels such as "Confidential" and "Final Exam". The keys contained plain html files which would "ping" on opening. The study found 45% of the dropped USB keys "phoned home". Interestingly, the study also included a voluntary survey to try and draw out people's motivation for picking up and accessing the drive. Of the 21% who completed the survey 68% said they were trying to return the key to the owner, demonstrating how criminals cynically exploit people's desire to 'do the right thing', as well as their natural curiosity.

It also emphasises the importance of getting staff to think twice before plugging anything into a USB port.

In the news...

In March 2019, a USB thumb drive was confiscated from a foreign national who was arrested at Donald Trump's Mar-a-Lago resort in Florida.

In April, a US Secret Service agent testified in the detention hearing for the woman that the USB drive was then inserted into a laptop at which point it began installing malicious files.[8]

While it's unclear whether the USB was inserted into a specific offline computer purely for analysis or if the ensuing concern of the Information Security community[9] was justified, the very presence of the malware-infected USBs in Mar-a-Lago goes to show how real this threat is.

Top tips to help protect your organisation:

1. Make staff aware of these types of scams, and give them an appreciation for the fact that hackers will see their devices as access points. This is why it's important to keep operating systems and applications up to date and use security features that allow remote tracking, locking and wiping of devices

What to do if something goes wrong

Time is of the essence if something goes awry, so it's important to make sure your staff know what process to follow in the event something has gone wrong and feel comfortable to speak up and report quickly.

An incident management plan will help your business respond fast and efficiently. It's also a good idea to keep a paper copy of the updated plan in case you are ever locked out of your system.

In terms of general advice, however:

- Contact your bank if you have given financial details to a scammer or anyone you are not sure should have them
- If you have made a payment to a scammer, contact your financial institution and make an official report to police
- If you have been impacted by cybercrime, you should also report it to the Australian Cybercrime Online Reporting Network (ACORN)
- Report other scams to Scamwatch.

By the Numbers

$60m

the cost to Australian businesses of business email compromise (BEC) scams in 2018.[2]

US$2.7 billion

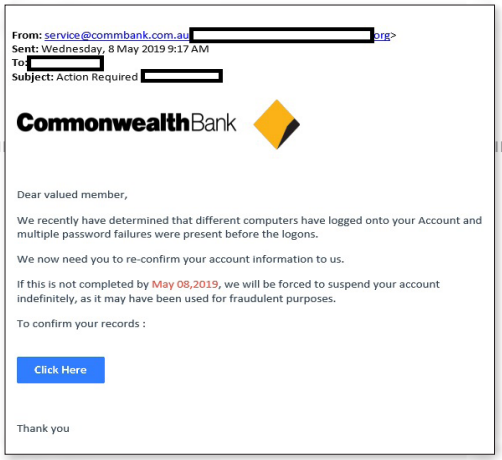
in financial losses in 2018 from "internet-enabled theft, fraud, and exploitation", according to the FBI's Internet Crime Complaint Centre (IC3).

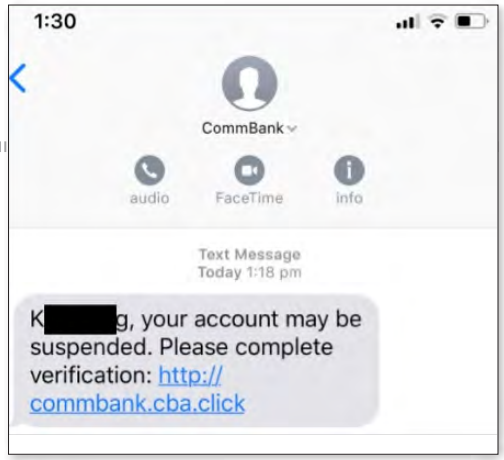
The most financially costly complaints involved business email compromise, romance or confidence fraud, and investment scams, which can include Ponzi and pyramid schemes. In 2018, the IC3 received **20,373 BEC/e-mail Account Compromise (EAC) complaints** with adjusted losses of over **$1.2 billion**.[3]

2/3 of all Australian companies surveyed for the 2019 Telstra Security Report reported a cyber security breach in 2018.[4]

Phish Eyes

Suspicious about a CBA-themed email?
Help us and our customers by reporting it to hoax@cba.com.au





Payroll scams show variation on the BEC theme

Earlier in this issue, we spoke about business email compromise (BEC).

One BEC variation that has recently become more prevalent is "payroll scam".

In these kinds of scams, cyber criminals target individuals within the HR, payroll or finance function of an organisation with the ultimate aim of getting employee salaries transferred to their accounts instead.

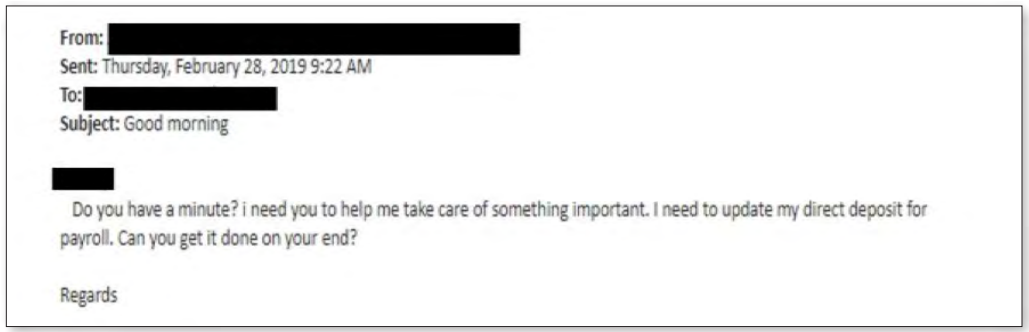
Often the victim will receive an email that has been doctored so it looks as though it comes from an executive or employee of their own company. The email will say they have recently changed banks and ask to modify the details of the direct deposit account for their salary.

In some cases which have been reported[10], the initial contact from scammers will simply ask for the process to change payment details or request clarification on the deadline for changes to be in effect for the next pay cycle. In this case, the first contact will be all about obtaining information to craft a more targeted second touchpoint.

So – if the first person contacted in HR or payroll tells the scammer that to change over bank details you need to login to the XYZ system and then select the ABC option, in order not to raise any red flags the scammer may simply thank them and then move on to someone else in payroll.

They could then send this second person a very legitimate sounding email about the fact they've been trying to login to the XYZ system but when they do so the ABC option isn't displaying properly and if they don't get it changed today they're going to miss the cut off for their next pay so can they please just help out and swap the payment details over. This may make the second person more susceptible to "helping out" a frustrated and anxious employee.

Another variation on this may be what looks like an email from the CEO or executive sent to their assistant and asking them to make the change, which is another potential way cyber criminals can socially engineer their way around systems that require login credentials.



If successful the scam often won't get picked up until the employee notices they haven't been paid.

Recent months have also seen the usual suspects in terms of phishing emails and SMS messages trying to harvest login credentials with a number of customers recently reporting the above email.

Another phishing attempt reported by customers in recent weeks and which has been understandably worrying for those who receive them have been SMS messages which ask customers to click on a link to verify their account, but which contain within the body of the SMS their full name.

Most likely the phone numbers used by scammers for the distribution of this smishing campaign came with names associated. These may have been obtained from an external data breach or other phishing campaigns where personal information was requested from victims. This, combined with the fact the scammers have replaced the sender label with CommBank, could help to further legitimise the messages with prospective victims.

Endnotes

1 https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018

2 https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018

3 https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

4 https://exchange.telstra.com.au/breach-expectation-new-mindset-cyber-security-success/

5 https://www.ato.gov.au/General/Online-services/Identity-security/Scam-alerts/#April2019

6 https://www.cbc.ca/news/canada/ottawa/city-treasurer-sent-100k-to-fraudster-1.5088744

7 https://www.blackhat.com/docs/us-16/materials/us-16-Bursztein-Does-Dropping-USB-Drives-In-Parking-Lots-And-Other-Places-Really-Work.pdf

8 https://edition.cnn.com/2019/04/08/politics/mar-a-lago-yujing-zhang/index.html

9 https://mashable.com/article/malware-usb-mar-a-lago-plugged-in/

10 https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bec-payroll-scam-your-salary-is-mine/