Signals

Security report
August 2019

CommonwealthBank

Welcome

Australians are expected to clock up a record $532 million of losses to scams this calendar year, according to the ACCC[1], surpassing half a billion dollars for the first time.

The 'Too smart to be scammed?' theme for Scams Awareness Week in August this year questions our propensity to trust – both to trust in others, but also to trust our own ability to pick when something is and isn't genuine.

Unfortunately, it's this tendency to trust and to place our confidence in others that is so often exploited by unscrupulous scammers with devastating consequences for both people and businesses.

Against this backdrop, we thought it fitting to bring out an issue of Signals that focused on the concept of Zero Trust, which starts from the premise of replacing trust with the need to verify.

In this edition we take a look at how organisations of varying sizes can make themselves and their data more secure through applying the principles of Zero Trust – both with respect to architecture and organisational culture.

We then take a closer look at merchant scams – an issue that cannot be ignored by any business processing payments. As usual, we include our regular sampling of the latest phishing and smishing campaigns we've seen over recent months.

As always, we welcome any feedback to cyber-outreach@cba.com.au.

Pete Steel
Acting CISO

Trust No One

"Never Trust. Always Verify."

Melanie Timbrell
Senior Manager,
Cyber Outreach

Bill Mahony
Lead Cyber Engineer

With such a catchy mantra, and adopters ranging from government agencies to security companies to Google[5], it's no wonder organisations of all sizes are increasingly aligning their security posture to this way of thinking.

What is Zero Trust?

Conventional wisdom held that what was inside the organisation's network could be trusted, and therefore what was dangerous was lurking outside the network.

But in a world where we carry our connectivity with us, that premise can no longer be relied upon – which is where Zero Trust comes in.

"Historically from a network perspective, you'd rely heavily on enforcing security at the network perimeter," explains Commonwealth Bank's Head of Security Architecture & Design, Ben Smee.

"But we can no longer afford to be that reliant on single perimeter enforcement points, because it just doesn't match the reality of how people are interconnected. We need to shift the way we do security to something that's much more dynamic."

Where did the notion of "Zero Trust" come from?

First mooted in 2010 by an analyst at research company Forrester,[6] Zero Trust security architecture puts data at the centre of an organisation's security. It relies on organisations knowing what their important data is, where their data is at any point in time, and then mapping the data as it moves not just in and out of the network, but also within the network.

Forrester updated the Zero Trust model in 2018 to become 'The Zero Trust eXtended Ecosystem'.[7] The key shift in the updated model is factoring in a distrust of people, while keeping data at the core of the model. So in order for any person, device or network to access data, verification of any and all of these elements must always occur.

Forrester's Five Steps to Zero Trust Information Security[8]

In its updated model, Forrester outlines five key steps for organisations to follow in re-designing network security.

1) Identify and classify sensitive data and create separate network segments for data with different levels of sensitivity.

2) Map the flows of your sensitive data, including all dependent network and system objects.

3) Architect 'microperimeters' – this means designing secure zones around each of the data classes. Access to zones is limited and strictly enforced with audit and change control tools applied.

4) Continuously monitor your ecosystem analytics – this means logging and inspecting all internal and external traffic for malicious activity and ensuring information flows make sense. Who are the users? What applications are they trying to reach? Is that action appropriate?

5) Apply security automation and orchestration – this means automating processes as much as possible to keep refining and iterating rules and operations.

A different approach to defence

Zero Trust assumes the traditional security perimeter will be breached and that all layers of "defence-in-depth" can be penetrated.

Smee describes the resulting approach as "relying on a suite of controls that cumulatively build confidence."

An example is what's known as adaptive identity and access management. This works by adding context so the authentication service can either grant access or deny it, based on a range of factors that determine the risk of the request.

"Historically we may not have allowed an Administrator to remotely access a critical database. Now with a Zero Trust mindset we can push a lot of trust to identity. That admin will have a trusted laptop with a trusted SOE [standard operating environment] and user agents. They'll use a VPN, will have to present certificates to ensure user agents all pass and then authenticate in order to connect to the database.

"On top of that, Zero Trust might also use additional information we have about the user so if we know they work from 9am to 5pm and they connect at 8pm, we can ask for additional multi factor authentication.

"Then we can say we know they are based in Sydney so if they connect from an IP in Eastern Europe or something, we're going to suspend access," says Smee, who describes the net effect as layering intelligence in order to be dynamic.

For example, in the above scenario if an employee tries to authenticate from an unknown or unusual location, they will either be asked to enter an additional authentication factor, such as a one-time password, or else access would be denied.

Google's BeyondCorp

Google's BeyondCorp[9] initiative is often cited as one of the best-known applications of Zero-Trust. Google's primary goal was to shift access controls from the network perimeter to individual devices and users so that employees were able to work securely from almost any location without the need for a traditional Virtual Private Network (VPN).

BeyondCorp operates on three primary principles:

1. Connecting from a particular network does not determine which services you can access
2. Access to services is granted based on what is known about you and your device
3. All access to services must be authenticated, authorised and encrypted.

> Zero Trust assumes **the traditional security perimeter will be breached** and that all layers of "defence-in-depth" can be penetrated

How can small to medium organisations apply Zero Trust?

For Zero Trust to work the way it's intended, fundamentally there is a requirement that organisations know what it is they need to protect.

Once an organisation has identified and classified its important data, then it's about looking at what controls are needed to protect it.

"This is about actually taking an inventory of the IT estate, being able to identify important functions within the estate and put on top of those the right kinds of controls," Smee says.

"For smaller organisations, you don't need to get into sophisticated AI, it's really about getting the foundations right so as you grow, you can scale without too much problem."

Some of the key core components include:

- A robust identity platform so you know who your employees are, what their role is and what are appropriate behaviours for those employees
- Strong identity controls for access such as multi-factor authentication (MFA)
- All employees understanding the need for, and the ability to use, encryption
- Conducting analysis and reviews so you can respond to anything that looks like it could be a threat.

How can larger organisations apply Zero Trust?

Smee describes enterprises as a "different ball game," given these organisations will already have a suite of controls in place.

"The challenge is starting to orchestrate when and how controls are used and making them dynamic – for example, if you currently have a VPN solution, how do you change criteria on the fly in response to other information that comes to light?

"Maybe a zero-day vulnerability is discovered targeting Windows platforms that you know is going to proliferate in a certain way. You might then decide to do a whole bunch of checks on the endpoint before you allow a user to connect.

"This is about understanding key workflows within the organisation and how to start factoring dynamic decisions into that."

For many businesses, the key challenge is getting the basics right: beginning with identifying important data, systems and functions.

On top of that, Smee says, an added challenge for larger organisations is grappling with what roles look like – so if someone does X job, they should never be connecting to Y system as an administrator, for instance.

This really comes down to a principle known as "least privilege", which combines the three elements of the user, their role and their device to constantly learn and adapt.

For some organisations, this looks like monitoring who is executing what commands or accessing which reports and then dialling back permissions to the minimum level required to fulfil their role.

Smee describes this future state of implemented and orchestrated machine learning as coming with its own set of challenges for organisations, for instance where it might be entirely feasible that someone gets locked out of a system but where the central IT Help Desk will not know why it happened or be able to help.

These particular challenges may be some way down the line. For now, many organisations – including some very prominent ones – are seeking effective and practical ways to verify each and every source of network traffic. They look at Zero Trust not just as the next phase in growing the maturity of their security models, but as part of the answer to managing information security in an increasingly connected world.

By the Numbers

34%

of organisations surveyed in EY's 2018-19 Information Security Survey saw careless / unaware employees as their biggest vulnerability[2]

13,698

phishing scam reports in 2019[3]

50%

of organisations impersonated by tracked phishing domains were from the financial services sector[4]

Fostering a Zero Trust organisational culture

Sam Wood
Manager,
Cyber Outreach

Twenty years ago, you could argue it was much easier to pick out who or what didn't belong in our inbox. The first online scams were quite crude and obvious, creating perceptions that only less savvy, inexperienced people got caught by them.

However, thanks to an explosion of mobile broadband access globally, we're now faced with a vast number of shady online operators, seamlessly integrating their activities into general internet noise.

The modern scammer is also an adept emotional manipulator – they know how to prey on our human vulnerabilities, the right amount of pressure to apply and what to say to deflect suspicion. This is why getting scammed has nothing to do with how smart you are, and everything to do with being human, and why adopting a Zero Trust model in human interactions may be our best defence.

Businesses not immune

While scams aimed at individuals have traditionally dominated media reports, businesses are increasingly being targeted. This is because a raid on your company books requires a trivial amount of effort, but can potentially yield a substantial payday for a slick operator.

Stealthy scammers are finding new ways to slip into your normal business processes, as you pay your suppliers, manage your payroll, and serve your customers. They also commonly use social engineering to pursue their goals – pressure and manipulation designed to heighten your emotions and override normal reasoning and judgement.

One scam that has been particularly prevalent, impacting many businesses globally in the last 4 or 5 years, is Business Email Compromise (BEC). These scams target businesses of all sizes. Using emails that are made to look like they come from someone you know, like your boss, your supplier or your customer, the goal of the scam is to get you to transfer money into an account that the scammer controls. There are two main variations of this scam: in the first, you might receive a fraudulent request for payment that looks like a legitimate expected invoice, or perhaps an email or even a phone call from a supplier saying that their banking details have changed and future payments should be directed a different account.

In the second variation, scammers masquerade as your colleagues, including your boss, requesting that a usually urgent and confidential payment be made to the scammers account. You can read more on this in our May 2019 issue of Signals, or see our webpage dedicated to scams that target businesses at https://www.commbank.com.au/support/security/scams-that-target-businesses.html.

Why that call from "Tech Support" can't be trusted

Scammers are prepared to impersonate people inside your organisation, such as your Tech Support desk. They'll call and explain that there's a problem with your computer. Need to run off to a meeting or lunch? No trouble, they'll say. If you just give them remote access to your computer, they will fix the problem while away so you won't be inconvenienced at all. In a format that's typical of many scams, the scammer creates a problem and then offers a convenient solution so you think they're doing you a big favour.

The dilemma

As humans, our default position is to assume the best of people instead of the worst. We don't approach every human interaction as a potential risk to our safety. However, in a digital landscape crowded with threats, we can't apply those same norms.

While most of us would consider fleecing a charity or a small family-owned business to be a despicable act, a scammer doesn't apply the same moral or ethical filter when selecting victims. Nor would some scammers think twice about duping a family out of their savings as they attempted to buy their dream home, or stealing a pensioner's entire retirement savings and therefore financial independence.

Could it be a Scam?

Some common hallmarks to look for

- Scare tactics, including threats and extortion
- Sense of urgency
- Opportunities that seem too good to be true
- Someone trying to bypass your standard business processes
- Requests that don't seem right based on previous interactions that you've had with a person, supplier, company or customer
- Someone trying to move communications into a different channel

This leaves us with no choice but to adopt a default position of Zero Trust in our digital interactions.

Never trust, always verify

Your best defence against scams is to create a culture consistent with the Zero Trust mantra of "always verify". Actively encouraging your staff to challenge and verify anyone who claims to be an employee, supplier or other trusted party wanting information could ultimately save your business thousands of dollars.

In the case of BEC scams, it's essential you verify the legitimacy of anything that has the hallmarks of a scam via a different channel using officially listed contact details (and

Anatomy of a Scam

First Contact	Hook	First Transfer	Honeymoon Period	More Transfers	Victim becomes suspicious
• Phone • Email • SMS • Social media • In person	• Relationship cultivation • Confidence and rapport building • Side-channelling • Hard sell • Pressure tactics • Emotional manipulation	• Non-alarming commitment • Promise of returns • Promise of reimbursement	• Seemingly good returns • Promises, additional offers • Emotional manipulation and confidence building	• Emergencies • Complications • Ultimatums • Threats • Blackmail • "Not-to-be-missed/all-in" opportunity	• Pressured to transfer goods / funds • Can't get money back • Can't contact scammer • Victim opens up about situation

not contact details that appear in the email). Ideally, speak to a contact you have dealt with before (over a sustained time period) to verify the legitimacy of a request.

Being in tune with how a situation feels is a crucial scam-detection tool. An email or phone call that makes you feel panicked, scared, confused, or compelled to take action immediately, particularly when it has anything to do with where your money going, is worth a second, third or even fourth look.

Be as tenacious as you need to be to verify a request's legitimacy, and be aware that a scammer is going to impatiently try to bluff their way through your suspicions. Due diligence may seem inconvenient when you're trying to move at speed, but your customers, suppliers and other stakeholders will appreciate your actions.

Getting help

- 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 bank and make an official report to police
- If you have been impacted by cybercrime, you should visit the Australian Cyber Security Centre's Report Cyber site (https://www.cyber.gov.au/report)

Protecting yourself

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

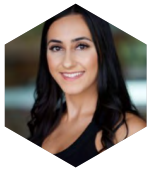
4 Encourage a culture where staff are comfortable to question a payment instruction even if it's from a senior executive

> "An email or phone call that makes you feel **panicked, scared, confused, or compelled to take action immediately**, particularly when it has anything to do with where your money going, is worth a second, third or even fourth look"

In Focus:
Merchant Scams

Ben O'Brien
Digital Fraud
Product Owner

Nisha Nissan
Fraud Risk Manager



With scams front of mind for many Australian businesses this August, merchant scams are a threat any business taking payments should be aware of.

Merchant scams occur when fraudsters pose as other businesses or customers and attempt to have you process fraudulent transactions on their behalf.

Sometimes this will look like scammers posing as potential business partners, contacting you out-of-the-blue, via phone or email, eager to do business. They may provide you with card numbers to process transactions but then ask you to refund money to a different card or bank account. In many cases, the scammer will be interstate or overseas and their requests will often seem unusual.

You should never process transactions for a third party unrelated to your usual business.

Refund scams

One type of merchant scam is known as a Refund scam. This involves buyers purchasing items and then requesting a refund or claiming they have accidentally overpaid you. The buyer will request that the refund is paid into a bank account or a different card to the one that was used for the initial purchase. Often what happens in this scenario is that the 'buyer' will use stolen card details to initially make the payment and then request a refund be processed to a bank account or card that the scammer owns. In the case that the original transaction was made on a fraudulent card you are likely to receive a chargeback and be required to refund the initial transaction as well as being out of pocket for the money that you have "refunded" to the scammer.

How to protect yourself from refund scams

- If a customer asks for a refund, always refund to the card they used to make the original transaction
- Exercise caution when customers attempt to use multiple card numbers to complete transactions
- Large orders from previously unknown buyers out of the blue should be reviewed to ensure they are legitimate

Case study

A CBA customer who ran a non-profit organisation recently received a donation for an amount of $15,000 paid via credit card. Shortly afterwards they were contacted by the donor who apologised and explained that they had actually only intended to donate $1,500. This was still a considerable donation which the non-profit was happy to receive so they agreed to refund the difference of $13,500 to the donor. The donor requested the amount be refunded to their bank account instead of the credit card. After the non-profit had processed this refund they were advised the original transaction was on a fraudulent card and the business was required to refund the full $15,000 through the chargeback process.

> "They may provide you with card numbers to process transactions but then **ask you to refund money to a different card or bank account.**"

- Be careful of customers asking you to use their card details to pay for a shipping company on their behalf e.g. requesting you to pay a courier to ship their goods interstate
- If you receive an interstate order, consider if there is a genuine reason why a customer would want to have your goods transferred interstate rather than just buy them from a local seller

Online card fraud

As more and more businesses are moving their operations online, there has also been an increase in businesses falling victim to online card fraud. This involves customers placing orders for your goods with stolen card details. Under certain circumstances, for example, if you do not have 3D Secure enabled, you may be required to process a full refund for any fraudulent transactions.

How to protect your business from online card fraud.

1) Always request the card verification code (known as a CVV2 or CVC2) for each transaction

2) Use a security program, such as MasterCard SecureCode or Verified by Visa

3) Monitor your accounts and transactions daily to help identify unusual activity such as inconsistent billing and shipping information

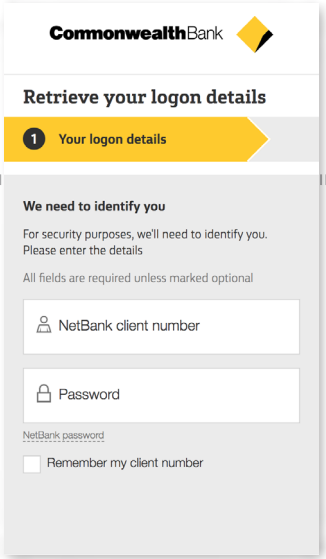
4) Follow good cyber hygiene such as ensuring you're running the latest version of all of your software as well as completing updates as they become available. Run regular anti-virus scans to ensure your customer's card details are protected

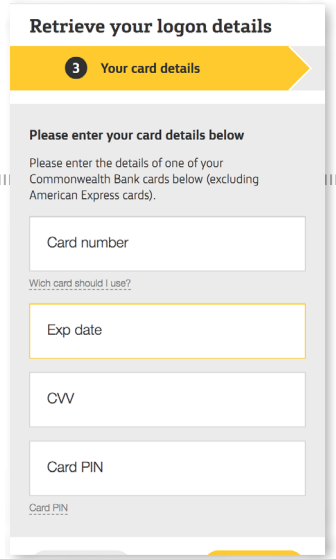
5) Check for unusual email addresses and take extra care with transactions processed using one as fraudsters like to use these to hide their identity

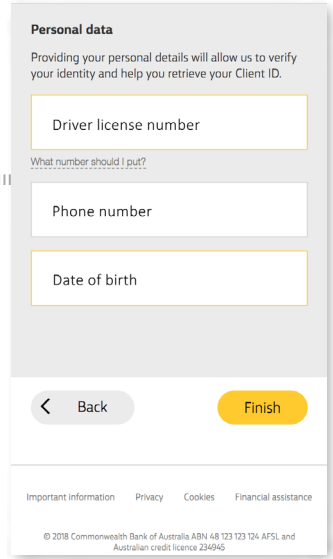
6) Check for fake addresses before you ship by using a Google map search to check the address is real and complete checks to ensure IP location and credit card address match.

Phish Eyes

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







The past month saw CommBank launch an SMS and phishing alerts public webpage at www.commbank.com.au/support/security/sms-phishing-scams.html. This is where we will post an up-to-date feed of the latest phishing emails and SMS messages targeting our customers. It provides an easy reference point for people to confirm that what they've received isn't legitimate.

Fake security and lockout alerts attempt to harvest credentials

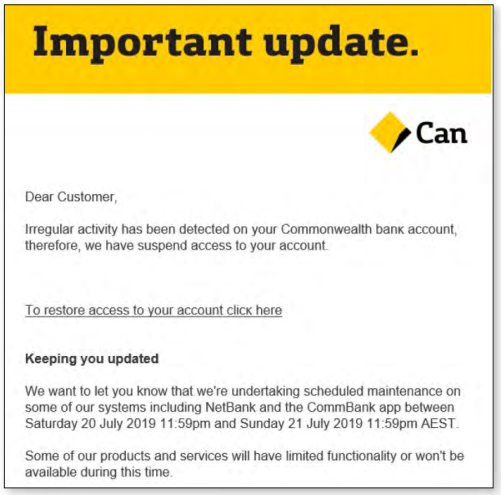
The recent months have seen a number of malicious communications sent to customers, disguised as security alerts related to their CommBank accounts. Varying in sophistication, the emails generally either claim account access has been disabled or restricted, or say that due to a new security process, customers need to verify account details in an effort to harvest customer login credentials.

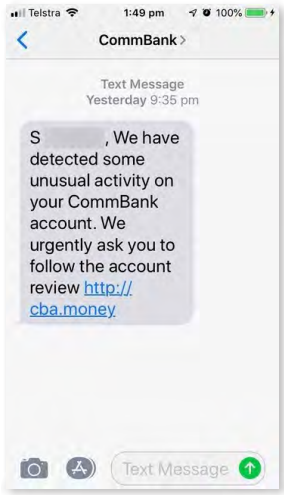
Some of the recent spate of fake emails and SMS messages mimicked security notifications claiming that NetBank access had been temporarily suspended to help protect the security of a customer's account and containing a link to restore access.

One of the emails in this vein reported by a number of customers, modified legitimate outage communications from the Bank, inserting a preface with the malicious link.

In June, an enumeration attack on another financial institution saw attackers query a large number of Australian mobile numbers via an online banking portal to reveal the matching PayID short names. This enabled the fraudsters to develop SMS messages with phishing links that were made more credible because they incorporated the PayID short names.

The phishing sites that the links in the SMSs led to were designed to harvest not just NetBank login credentials but also other personally identifiable information, which could then be used for a range of nefarious purposes.





Small businesses warned on email procurement scam

Small to medium businesses supplying IT and electrical goods are being warned about an email procurement scam which relies on social engineering that has already resulted in financial loss for a number of organisations.[10]

The scam unfolds as follows:

1) An email arrives from a spoofed email domain, possibly also with a stolen signature block, so it appears to come from an executive of a university or other large Australian organisation

2) The email initiates an exchange, in which the scammer asks for a quote and then may proceed to place an order for IT equipment with the requirement of credit being extended for a number of days as part of payment terms

3) The target organisation is then directed to send the goods to an Australian freight forwarding company, at which point it is sent on using a different delivery name overseas

4) You guessed it: the payment never happens and the goods are never seen again.

> **Apply the Zero Trust mentality** and undertake due diligence on new customers

It's always a good idea to apply the Zero Trust mentality and undertake due diligence on new customers and orders by calling on a number that is trusted or looked up from an official website rather than the one provided in the unexpected contact to verify a request is real.

Endnotes

1 https://www.accc.gov.au/media-release/record-losses-expected-as-scammers-target-australians
2 https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf
3 https://www.scamwatch.gov.au/about-scamwatch/scam-statistics
4 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-attack-economy-report-2019.pdf
5 https://go.forrester.com/blogs/next-generation-access-and-zero-trust/
6 https://go.forrester.com/blogs/tag/zero-trust/
7 https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210
8 https://go.forrester.com/wp-content/uploads/2019/07/Forrester-5-Steps-To-ZeroTrust-Security.pdf
9 https://cloud.google.com/beyondcorp/
10 https://insidesmallbusiness.com.au/featured/smes-warned-over-email-scam

CommonwealthBank