Signals

Security report
June 2020

CommonwealthBank

Welcome

The start of 2020 has been unprecedented in many respects, as Australians have responded to the extraordinary challenges presented by the coronavirus health crisis. It has been a true test of our resilience, collaboration and problem-solving skills, and I have been inspired by the resolve of Australian organisations to adapt, persevere and succeed despite lingering uncertainty.

In this edition's deep-dive, we study the delicate balance between business continuity and cyber risk management that many Australian organisations have grappled with while responding to the challenges of the coronavirus, as they either scaled-up their existing remote working capabilities or introduced them for the first time. As part of the study, we explore how to set your people up for success in the transition.

We also continue our series of 'In-Focus' articles where we explain in easy-to-understand terms how some common cyber technologies work. This issue, we look at multifactor authentication.

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

With my best regards

Keith Howard
CISO

When remote working becomes the rule rather than the exception

Rose Sahyoun
Manager,
Cyber Outreach

Sam Wood
Senior Manager,
Security Awareness

Lessons in balancing cyber security risk management against business continuity in response to coronavirus

The recent coronavirus health crisis has brought to the fore the criticality of well-considered and exercised business continuity plans. Organisations that had underplayed scenarios where their workforce couldn't continue to work from an office or backup site quickly found themselves playing catch-up, as work from home arrangements became the only viable solution for continuing business operations.

Despite a growing trend towards flexible working in recent years, many organisations maintain business models that rely on their people being physically present in the office, or only offer flexible working to a limited number of roles. Even for organisations with well-established flexible working cultures, the rapid shift to remote working arrangements en masse has proved challenging, with company networks groaning under the strain of increased demand for remote access and the pressure to immediately scale to meet this demand.

So what have we learned about remote working, business continuity and the associated security and privacy concerns during this period?

Evergreen security risks under the spotlight

Much of the security and privacy discussion in the coronavirus climate has centred around two main concerns: remote working risks, and coronavirus-related social engineering activity.

These are not new issues – remote working has long been considered more inherently insecure than working from within the four walls of your bricks and mortar premises – but the potential scale of the recent risk exposure has heightened our awareness of these particular issues. In March 2020, the US Department of Homeland Security's Cyber and Infrastructure Security Agency (CISA) was quick to issue an alert to potential remote working threats as more organisations sent their workforces home.[1]

The foremost concern in remote working is the increased risk of data loss or exposure, either accidentally or via targeted activity against your people and networks. This can manifest in a number of different ways:

- Use of less secure Wi-Fi connections, creating an opportunity for an unwelcome third party to eavesdrop on the flow of traffic between your workers and your network
- More corporate technology sitting in homes or being moved about in public, increasing its vulnerability to loss and theft
- Temptation for unsupervised employees to deviate from approved platforms to get the job done
- Repurposing of familiar social engineering scams such as "Tech Support" and business email compromise to take advantage of isolated colleagues
- Malware disguised as fake remote working helper applications such as web conferencing platforms and virtual private networks (VPNs)

As your people head home, so too does your cyber and information security culture. And even if you have your own shop in order, you may come into conflict with organisations that don't, which means you're constantly weighing up your potential cyber risk exposure against business continuity and prioritised business outcomes.

Cybercriminals quick to pivot

Cybercriminals are adaptive and opportunistic, and unsurprisingly, have been quick to take advantage of the coronavirus landscape in their targeting activities.[4] Later in this issue, we take a closer look at coronavirus-themed phishing activity, but a general trend observed has been the targeting of popular services used by remote workers to deliver malware or harvest credentials. Security firm Proofpoint reported in April 2020 that it had observed an uptick in phishing lures abusing popular web conferencing platforms, urging recipients to take immediate action to address security vulnerabilities.[5] There has also been a noticeable spike in the number of hacking attempts, phishing attacks and malware from negligent software downloads, with some malware masquerading as popular collaboration tools.[6] However, cyber-attacks subsequent to the crisis have not necessarily been more sophisticated in nature, but

Online collaboration tools a potential window to corporate operations

The bulk migration to online collaboration tools expedited the adoption of web conferencing platforms, perhaps bypassing the usual requirements for rigorous suitability and security testing in some cases. A number of web conferencing services including 'Zoom' experienced overnight success as social restrictions intensified. The popularisation of the phrase "Zoom-bombing" soon followed, as users reported an increase in the number of uninvited guests joining meetings. Whilst hijacking a Zoom meeting may sound disruptive and intrusive, the real concern lies with those intruders who join with a silent presence - a more insidious threat to corporate security and privacy.[2]

Opportunistic threat actors used "war dialling" methods to discover non-password protected Zoom meetings to facilitate unauthorised access. One particular tool called 'zWarDial' was able to detect an average of 100 meetings per hour with a success rate of around 14 percent.[3]

> Your network and people are **vulnerable to malware threats** regardless of where they are working

rather opportunistic, and as observed by the Australian Cyber Security Centre (ACSC) in their April threat report, extremely responsive to 'breaking' developments, including government announcements.[7]

The ACSC also reported in an early May 2020 advisory that Australian health sector organisations and other essential services were vulnerable to heightened targeting activities by advanced persistent threat actors, urging such organisations to bolster their cyber security controls to prevent potential disruption and unauthorised data loss.[8]

Laying the groundwork for a remote workforce

A Gartner report from March 2020 revealed that 88% of Australian organisations surveyed were instructing or encouraging their workforces to work from home in response to the coronavirus.[9] However, the enactment of business continuity arrangements need not be cause for departure from well-practiced cyber and information security risk management. When developing business continuity plans, or preparing for business-as-usual remote working arrangements, organisations should continue to be guided by the key principles of good privacy practice and consider any legal or regulatory requirements that apply[10].

As you embark on the journey towards facilitating remote working arrangements for your workforce, there are a number of key security and privacy considerations for your enterprise mobility strategy that will guide your decision-making and investment in technology. These include but are not limited to:

- What are the essential applications that your staff need to access to deliver your core business outcomes regardless of where they are working?
- What devices will staff use to access these applications when working remotely (eg will they be provided with corporate laptops, or will they be allowed to connect in a particular way from personal devices)?
- How will you facilitate remote access to your corporate platforms and tools (eg through a Virtual Private Network connection or through cloud-based applications)? How will these connections be secured?
- What is your process for conducting due diligence on any online collaboration tools or remote access tools you're adopting to ensure the security and privacy of your data while staff are working remotely? Do you know how to optimise the security and privacy configurations, and how will you manage any residual risk in these platforms?

Regardless, investment in tools and technology with good functionality and usability will deter employees from deviating towards rogue options, giving your organisation a better chance of keeping its information safe.

Setting your staff up for success

As alluded to previously, remote working can be the ultimate test of your cyber and information security culture. Any habits established in the office – good or bad – will be reinforced at home, so it's essential that you're cultivating a positive baseline cyber security culture.

Whether your remote working arrangements are business continuity or business-as-usual, dedicated employees will seek to comply and do the right thing, but you need set them up for success. Don't assume that your people will intuitively know how to use new tools appropriately – many organisations have reported that coronavirus has been a significant accelerator of technological change, forcing the hand of some resistant technophobes that may have previously been holding out.[11]

Here are some cyber risk management topics you can address through training as you prepare your workforce for remote working:

1 ***Maintaining basic cyber hygiene***

Your network and people are vulnerable to malware threats regardless of where they are working, which is why it's essential to maintain basic cyber hygiene practices such as updating operating systems and applications, enforcing appropriate access controls, and maintaining antivirus programs and network backups. As operating system and application updates typically happen in the background while people are working in the office, you may require your

By the Numbers

1767
malicious coronavirus-themed domains registered globally each day[20]

$700,000
lost by Australians to coronavirus-themed scams[21]

88%
of Australian organisations encouraging employees to work from home as part of coronavirus response[9]

> As your people head home, so too does your cyber and information security culture. **Any habits established in the office – good or bad** – will be reinforced at home

employees to play a more active role in ensuring they are applied when working remotely. Make sure you communicate your expectations around this clearly and often, and automate these updates where possible to promote compliance.

2 *Securing devices, connections and business tools*

When embarking on enterprise mobility, most organisations generally prefer to provide staff with company-owned devices because it's easier to manage their security policy compliance. However, if you allow your people to use their personal devices, you may need to provide guidance about how these devices are configured and updated before they can connect to your corporate network.[12]

Once you've determined which devices can access your network and how, it's important to train staff how to do this securely. It's a great opportunity to educate your employees on the dangers of public Wi-Fi networks and teach them how to secure their Wi-Fi networks at home and how VPNs work if they will be using one.

Once you've nominated your preferred collaboration tools, explain their respective security features to your people – this will encourage compliance and suppress any urges to deviate. As an example, if your organisation is using web conferencing platforms to facilitate online meetings, show your employees how to optimise the security settings for their meetings, instead of relying on default settings. This might be by using features such as password-protection, waiting rooms/lobbies, meeting locks and controlled screen sharing by hosts.

You may also recommend limited use of video-calling features on an as-needs basis, and turning off the webcam to prevent possible social engineering efforts.[13]

3 *Social engineering and scams*

Your employees are potentially more susceptible to social engineering away from the office without someone in earshot to give a second opinion on whether a message is legitimate. Social engineering is an act of manipulation designed to exploit our human vulnerability and trick us into doing something we wouldn't normally do, such as clicking on a link, providing sensitive information or processing a payment. Cybercriminals can target your employees via email messages, SMS or even over the phone, for example, tricking an employee to reveal their password by impersonating IT support.

As scammers seek to capitalise on our emotional response to the health crisis, it's important to continue to prioritise the human layer of your defences in your training activities. This includes reviewing and reinforcing processes around separation of duties, particularly for payments, to manage collusion and fraud risks and susceptibility to email payment fraud via business email compromise scams.

4 *Locking down logins*

It's essential to promote secure password behaviours amongst remote workers, with an emphasis on longer passphrases that are unique for each service. You should also consider implementing multifactor authentication (explained in our In Focus article over the page), where available, as an additional layer of security. It's a little extra effort for a significant security benefit. If you're not ready for broad implementation, consider making it compulsory for accounts with a higher risk profile, such as system administrators or finance teams, to start with.[14]

5 *Data handling responsibilities*

Lastly, remote working arrangements shouldn't be an excuse to neglect normal data handling processes and responsibilities. Your corporate IT is more vulnerable to loss and theft when removed from the office, so it's worth providing your staff with some tips on how to minimise these risks, including processes to follow if a device goes missing. You may want to consider installing mobile device management software on corporate devices – these tools will allow you to track the location of a device, remotely block access and erase the data stored on the device, and even retrieve a backup of data stored on the device.[15]

Otherwise, it's important to impress on staff that it's business-as-usual as far as protecting your company and customer data is concerned. Reiterate the importance of locking screens while stepping away from desks, disposing of printed documents securely, considering who is in earshot during sensitive conversations and generally treating your company and customer data with care.

Although your remote working journey may initially feel overwhelming, comprehensive research, careful planning and well-considered communications can smooth out the transition and minimise the impact on your organisation's productivity.

Useful Resources

A number of Government and vendor guides and checklists to assist in this process are available. CommBank's free cyber security eLearning suite, Cool, Calm and Connected is also available to help protect your business. More information, including how to register, is available on the Commbank website.

In Focus:

Locking down your login with multifactor authentication

Nick Roper
Enterprise Services Graduate

Passwords are ubiquitous and offer a convenient solution for denying malicious users access to accounts. However, passwords alone are no longer enough to thwart attackers, and this is largely due to the shortcuts we take to avoid the friction they create in our online experience. These shortcuts unfortunately have the net effect of undermining our online security.

Although long-considered an effective strategy to mitigate most cyber breaches, the value of multifactor authentication has been increasingly underscored in recent years as more every day services enable this feature for the average consumer.

The problem with passwords

The vulnerability of our passwords is best summarised as follows:

a: We're expected to use them for most of the services we access online
b: They create annoying friction as we transact
c: We know we shouldn't pick weak or reused ones, but to ease the friction, we do it anyway

And cybercriminals know that our password game is weak, making their efforts to gain access to our accounts trivial. When a password is short, easily guessed or popular (i.e. 'password' or '12345'), an account is vulnerable to basic password attacks, such as brute force or spray attacks. The former is the practice of entering all possible password combinations for a single username until the correct one is found, while the latter is the practice of trying a common password against many usernames.

However, reused passwords are equally problematic. According to recent research by Lastpass, 69% of Australians surveyed recycle their passwords across multiple online services[16], which may include reuse across personal and work-related accounts. With a treasure-trove of credentials flooding the internet as data breaches continue to hit the headlines, the breach of just one service can leave the door ajar for any others protected by the same password.

> "According to recent research by Lastpass, **69% of Australians surveyed recycle their passwords** across multiple online services"

This is why multifactor authentication, when implemented correctly, can be an effective backstop to prevent someone armed with your password from getting access to your network or accounts.

What is multifactor authentication?

There are three things, or 'factors', you can use to authenticate yourself to a service:

- Something you have (eg a smartcard , key or certificate)
- Something you know (eg a password, PIN, or answer to a secret question)
- Something you are (eg fingerprint or facial recognition)

When a combination of two or more of these factors is used to access a service, it's considered multifactor authentication, or MFA. MFA reduces the risk of unauthorised account access because even if the wrong person has one factor – like a password – they can't complete the authentication process without the second one.

One of the most common everyday examples of MFA is your banking – to withdraw money from an ATM, you need to present something you have (your bankcard) in combination with something you know (your Personal Identification Number). However, there are many other every day examples of MFA that you probably already use without realising!

The most common MFA implementations generally involve the use of a password and one of these:

- Universal 2nd Factor (U2F) security keys
- physical one-time PIN (OTP) tokens
- biometrics, such as your thumbprint of face scan
- smartcards
- mobile apps
- Short Message Service (SMS) messages, emails or voice calls
- software certificates.

It is important to note, that although sometimes used interchangeably, multistep authentication is not the same as MFA, because most multistep implementations use two of the same factors to facilitate authentication, requiring an attacker to pull off only one type of heist to get access.[17]

Where is it available?

Many popular services stretching from social media, to webmail, shopping and popular business tools including Microsoft Office offer MFA, with easy integrations using Microsoft and Google Authenticator apps. A search of the help pages for most popular platforms can help you determine where it's available and how it can be implemented for that service.

Does MFA guarantee that my account won't be hacked?

It's impossible to guarantee perfect security, and MFA does have some potential drawbacks that can be a barrier to implementation.

Physical tokens can be cumbersome, and the introduction of a second-factor into processes can interrupt productivity flows. Advancements in technology also mean that options such as the use of SMS to deliver a second-factor have been deprecated, due to the ability for motivated cybercriminals to port mobile numbers under their control. Additionally, code and number based tokens can be, and regularly are, phished alongside passwords.

However, any potential risks in MFA are outweighed by its advantages, which is why it overwhelmingly offers better protection than a password alone and is considered by the Australian Cyber Security Centre (ACSC) to be one of their Essential 8 Strategies to Mitigate Cyber Security Incidents.[18] Earlier this year, Microsoft revealed that out of 1.2 million compromised accounts that they were monitoring, 99.9% did not have MFA, and from their observations, only 11% of all enterprise accounts were protected through MFA[19]. This indicates that there is a low level of maturity in MFA adoption and many security gains still to be made.

For more guidance on MFA architecture and implementation, review the ACSC's *Implementing Mutli-Factor Authentication guide*.

> “Any potential risks in MFA are outweighed by its advantages, which is why **it overwhelmingly offers better protection** than a password alone”

Phish Eyes

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

Rumi Solanki
Enterprise Services Graduate

Current events are common fodder for cybercriminals seeking to craft convincing phishing lures, and we've observed plenty of coronavirus-themed phishing activity to-date in 2020, as scammers exploit our natural anxiety and curiosity in the global health crisis. In a recent report, Palo Alto Networks reported that well over a million coronavirus-themed domains have been registered this year, and it estimated that, on average, 1767 malicious coronavirus-themed domains are registered globally each day.[20]

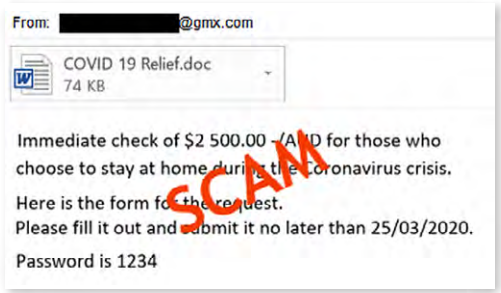
The Australian Competition and Consumer Commission's (ACCC) Scamwatch service has also reported that Australians have so far lost over $700,000 to coronavirus-related scams with further losses likely to be incurred.[21]

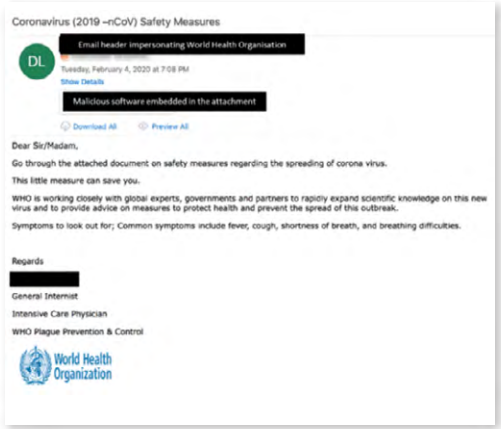
Abusing our trust in official institutions

In Australia, cybercriminals have been quick to use government relief payment themes as phishing lures, leaving members of the community whose jobs have been impacted by shutdowns particularly susceptible. In one example, scammers impersonated the Australian Government, distributing phishing emails that included a malicious attachment disguised as a fake form to claim relief payments. When opened, the attachment installed malicious software, intended to steal sensitive personal information from victims such as usernames, passwords and banking details.

In a more crude variant of this scam, cybercriminals crafted similarly-themed emails without any Australian Government branding, claiming that an immediate payment of $2,500 was available on completing and submitting the attached form. However, the attachment included was designed to install malicious software on a device when opened.

In an example of a coronavirus-themed lure with global appeal, scammers impersonated the World Health Organisation (WHO) under the pretext of sharing measures to limit the spread of the virus. In the body of the email, they included information on coronavirus symptoms to make it seem legitimate, but the attached document contained malicious





software designed to facilitate further access to the victim's device for nefarious purposes.

Diversifying their activities across multiple channels

Scammers were also quick to pivot the focus of their smshing (phishing via SMS) activities in response to the coronavirus landscape. Common lures have included guidelines, restrictions and tips to protect against coronavirus, often made to look like they have been sent by official Australian Government senders. However, these messages directed recipients to bogus domains hosting malware. Although defenders move as fast as possible to nix these domains to protect our community, cybercriminals establish new ones just as quickly to continue their activities unabated.

In more sinister variations of these messages, cybercriminals have spoofed (mimicked) legitimate Australian Government contact details in such a way that a bogus message appears in-line with legitimate messages from the Australian Government.

A number of Australian Government services, including the ACSC's Stay Smart Online service and ACCC's Scamwatch service continue to monitor and share information publically about the latest coronavirus-themed scams.

Business-as-usual for brand abuse

Although we observed a short period where scammers appeared to be favouring coronavirus-themed lures, they were quick to return to their traditional phishing messages via SMS and email abusing the CommBank brand. In 2020, we've seen a continuing trend

of lures related to banking with CommBank, whether it be a notification of suspicious activity, an account that needs to be verified, or that account access has been suspended. All share similar hallmarks:

- Purporting to come from CommBank, even spoofing legitimate CommBank sender addresses
- Urging the recipient to take action, such as verifying their account details immediately
- Links to domains that closely resemble legitimate CommBank domains, that when clicked on, typically direct the recipient to a fake form that harvests their personal information.

Last year we launched an alerts page on the CommBank website that allows members of our community to quickly compare messages received claiming to be from CommBank against known hoaxes. Visit https://www.commbank.com.au/support/security/sms-phishing-scams.html for more information.

Superannuation scams under the spotlight

Scammers have sought to capitalise on changes to superannuation access in response to the coronavirus and the resultant economic conditions impacting many Australians. Australian Government agencies such as the Australian Federal Police and ACCC have reported scammers repurposing common social engineering techniques such as cold-calling victims, offering to help them get early access to super, but instead phishing their personal information to facilitate identity theft and draw down on super funds.[22]

These scams highlight the challenge of disrupting the activity a few steps upstream from where money changes hands – helping victims to recognise social engineering attempts and protect their information is the first step, but robust verification processes before releasing payments play a crucial role in potentially disrupting a scam and limiting financial losses.

CommonwealthBank

This issue's publication team:

Sam Wood
Senior Manager Security Awareness

Rose Sahyoun
Manager Cyber Outreach

Rumi Solanki
Enterprise Services Graduate

Nick Roper
Enterprise Services Graduate

Endnotes

1 https://www.us-cert.gov/ncas/alerts/aa20-073a
2 https://www.forbes.com/sites/advisor/2020/04/07/the-ultimate-small-business-work-from-home-guide/#3c-f1ae753b88
3 https://krebsonsecurity.com/tag/zwardial/
4 https://www.itnews.com.au/news/hacking-against-corporations-surges-as-workers-take-computers-home-546904
5 https://www.proofpoint.com/us/threat-insight/post/remote-video-conferencing-themes-credential-theft-and-malware-threats
6 https://www.zdnet.com/article/hackers-target-remote-workers-with-fake-zoom-downloader/
7 https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020
8 https://www.cyber.gov.au/threats/advisory-2020-009-advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services
9 https://www.cmo.com.au/article/672072/report-most-australian-employees-work-from-home/
10 https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
11 https://www.zdnet.com/article/how-coronavirus-may-accelerate-the-future-of-work/
12 https://www.cyber.gov.au/advice/covid-19-protecting-your-small-business
13 https://www.cyber.gov.au/publications/web-conferencing-security
14 https://www.ncsc.gov.uk/collection/small-business-guide/using-passwords-protect-your-data
15 https://www.ncsc.gov.uk/collection/small-business-guide/keeping-your-smartphones-and-tablets-safe
16 https://blog.lastpass.com/2020/05/new-report-how-are-australians-treating-passwords.html/
17 https://www.lifehacker.com.au/2016/10/the-difference-between-two-factor-and-two-step-authentication/
18 https://www.cyber.gov.au/publications/essential-eight-explained
19 https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/.
20 https://unit42.paloaltonetworks.com/covid-19-cloud-threat-landscape/
21 https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams
22 https://www.smartcompany.com.au/coronavirus/jobkeeper-scams-ato-business-owners/