Signals

Security report

January 2019

CommonwealthBank

Contents

Horizon Scan

Upcoming events of interest

2019
Feb
5

Safer Internet Day, 2019

Celebrated globally, Safer Internet Day is coordinated by the joint Insafe/INHOPE network, with the support of the European Commission. The Office of the eSafety Commissioner is the official Committee for Safer Internet Day in Australia – responsible for driving the initiative nationally. The Office will run a number of activities and events for individuals and organisations.
https://www.esafety.gov.au/saferinternetday

2019
Feb
16-17

Melbourne

BSides Melbourne

BSides Melbourne is a community-driven information security event aimed at creating and enabling a broader and richer conversation on developing ideas. It provides a platform for first-time speakers and students as well as professionals to present their work.
https://www.bsidesmelbourne.com/

2019
Mar
26-29

Singapore

Black Hat Asia

Black Hat Briefings aim to provide attendees with the latest in information security research, development and trends. The briefings are held annually in the US, Europe and Asia include hands-on training taught by industry experts, research presentations and open-source tool demos.
https://www.blackhat.com/asia-19/

Welcome

Happy New Year and welcome to the first edition of Signals for 2019. It's already shaping up to be an interesting year in cyber with developments in policy, legislation and security on the horizon. In this issue, we offer a Deep Dive on the 2019 landscape covering the key security trends to expect, as well as ways organisations can protect themselves from new and evolving threats.

On a personal note, it's also been great to kick off the year with a number of programs aimed at developing and supporting young talent in cyber security. Commonwealth Bank is a proud sponsor of the National Computer Science School (NCSS) and Girls' Programming Network and in January we had the pleasure of welcoming 100 students and teachers from across Australia and New Zealand to our Sydney Innovation Lab for a summer school site visit. Students had the opportunity to connect with security professionals working in our teams and learn about new technology and careers in IT.

On a related note, I'm excited to be launching an important high school program in partnership with the Australian Computing Academy, AustCyber and some of my peers. Over the coming 12 months the program will provide teachers and students four classroom-ready challenges to develop cyber security skills and raise awareness of careers in the space.

I wish you all the best for the new year, and please feel free to reach out to my team with any feedback or suggestions for this publication at cyber-outreach@cba.com.au

Pete Steel
Acting CISO

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Editorial

Melanie Timbrell
Senior Manager,
Cyber Outreach

Charming Kitten serves as timely reminder to get the basics right

As 2018 wound down there was, alas, no holiday on the cyber news front.

After another year of newsworthy breaches hitting big names from Facebook to Marriott, one of the headlines which surfaced in the final weeks of the year and which may have flown under the radar related to the somewhat whimsically named "Return of the Charming Kitten".

In spite of sounding like it belongs in a children's storybook collection, the attack was interesting both as a demonstration of how threat techniques are evolving, but also the importance of getting the basics right.

According to research from a cyber security group called the Computer Emergency Response Team in Farsi (CERTFA)[1], Charming Kitten, which is an Iranian hacking group, targeted the private email accounts of US Treasury officials following the US restoration of sanctions against Iran in November.[2]

The method of compromise was a phishing attack in a pattern seen many times before – hence the warning not to ignore the basics.

The attack sent fake alerts to victims claiming there had been suspicious activity on their accounts, prompting them to login and review the activity, which it seems from the research some of the targeted people did.

In terms of what happened next – a hidden tracking image within the body of the email notified the attackers when the email had been opened and as the victim entered their credentials on a fake login page, the alerted attackers could enter those same credentials in real-time into the genuine login page. If two-factor authentication was enabled, the attackers were able to similarly steal the authentication codes to gain access to the victim's accounts.

At the outset, it's probably worth saying that protecting an account with multi-factor authentication where it's available is a no-brainer as it makes it significantly more difficult for an adversary to steal a complete set of credentials. But it's important to note that weaknesses do exist.

It serves as a timely reminder that in spite of best-laid perimeter defences, phishing continues to be a key threat, and that although cyber criminals continue to innovate, the fundamentals of an effective cyber security program largely remain the same.

We take a look at this, as well as other threats that rely on human error for your business to be aware of in our deep dive *3 cyber threats that count on human error.*

Also in this issue, a look at some of the top trends we think you need to be across as we enter 2019 as well as a discussion of the latest news, observations and regulation.

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

Editorial Panel

Contributors

Katerina Borodina
Intern, Cyber Outreach

Luke Hopewell
Manager, Cyber Outreach

Pete Steel
Acting CISO

Melanie Timbrell
Senior Manager, Cyber Outreach

Briana Wade
Graduate, Cyber Intelligence

Reviewers

Adam Fisch Manager, Cyber Outreach
John Hare Executive Manager, Cyber Outreach
Uri Teitler Head of Cyber Portfolio and Delivery
Samantha Wood Manager, Cyber Outreach

> “Protecting an account with multi-factor authentication where it's available is a no-brainer as **it makes it significantly more difficult for an adversary to steal** a complete set of credentials”

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Trends & Observations

Key trends observed during the quarter

China accused of global hacking campaign

In the final days of 2018, the US Department of Justice charged two Chinese nationals with allegedly belonging to a hacking group known as Advanced Persistent Threat 10 (APT10).[9]

The group is reported to have targeted private companies and government agencies in order to access intellectual property in an effort that spanned the globe and lasted several years.

In the wake of several intelligence agencies rebuking China, Australian Cyber Security Centre (ACSC) head Alastair MacGibbon in an interview with ABC Radio National described it as "an audacious global campaign run by a group that worked on behalf of the Ministry of State Security for the Chinese government."[10]

Foreign Minister Marise Payne and Home Affairs Minister Peter Dutton issued a statement voicing "serious concern" over the hacking allegations,[11] with MacGibbon confirming there were victims in Australia. It follows the revelation earlier in the quarter that Australia-bound internet traffic from North America was re-routed to China for six days in 2017.[12]

Nation state activity previously came under the spotlight in early October when Bloomberg published an article[13] alleging factories in China had inserted small microchips into logic boards used by Amazon, Apple, and other major tech companies. Since its publication, the article has been denied by both the US government and the tech giants involved, but it serves as an illustration of supply chain compromise and what may happen if logic boards aren't properly audited.

CHECKLIST

- Ensure your data is sent over encrypted networks in case it falls into the wrong hands
- Stay up-to-date with news on hardware attacks, and be prepared to possibly replace devices if necessary
- Know your supply chain
- Ensure you practice good cyber hygiene to minimise the chances of becoming an easy target for theft. Visit the https://cyber.gov.au/ website for targeted advice from the ACSC

Industry collaboration leads to malware takedown

The Federal Bureau of Investigation (FBI), Google and 20 tech industry partners worked together to take down two international cyber-crime rings: 3ve and Methbot[17]. The 3ve software infected over 700,000 PCs with advertising malware, causing affected computers to visit counterfeit pages where the creators of 3ve generated fraudulent advertising money.

In a separate instance of malware proliferation, November saw Google discover that 13 apps in the Google App Store contained malware[18]. The apps were removed, but had already been downloaded a total of 560,000 times.

CHECKLIST

- Ensure you have a reliable antivirus enabled and it's kept up to date
- Educate staff about clicking links, downloading apps or visiting unusual websites that could potentially install malware

Data breaches continue to snowball

This quarter saw the failure to detect and report data breaches continue to have large-scale consequences.

The December Marriott breach that could impact up to 500m guests[14] who made a reservation at a Starwood hotel, ranks among the biggest data breaches on record, made worse by the extent of time attackers had access to the system (around four years). While it seems some guests only had basic information, such as name and email address compromised, the bulk of those impacted – currently estimated at more than 300m – had different combinations of highly sensitive information including dates of birth, passport numbers and trip and reservation information stolen.

The company says it is co-operating with law enforcement and regulators, although it still doesn't have definite answers about how attackers initially accessed the Starwood network, which Marriott subsequently acquired in 2016, or why the breach went undetected for such a long period.

In a separate response to a different incident, tech giant Google announced in October it would be shutting down Google+ after discovering a bug in March which allowed third-party app developers to access user data.[15]

Airline Cathay Pacific also came under fire this quarter for belatedly reporting the illegal access and exfiltration of up to 9.4 million passengers' personal data. Information accessed by the hackers included names, nationalities, dates of birth, addresses and passport numbers.[16]

CHECKLIST

- Educate your staff about phishing and best-practice password policies
- Make your board and senior executives aware of the growing regulatory and public focus on data protection, and the potential implications for your business of a breach
- Ensure your organisation is prepared to respond well to a possible data breach and meets its legal obligations by creating a thorough data breach response plan

By the Numbers

30%
increase in business email compromise scams in Australia in 2018[3]

49%
of phishing sites now sport the security padlock[4]

44%
of data breaches attributable to insiders[5]

$400 million
the estimated cost of Australia's cyber security shortage[6]

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Trends & Observations

Pharma & AutoCAD targeted by phishing

Phishers this quarter have focused their attacks on the pharmaceutical industry and AutoCAD software.[19] Drug companies are being targeted by phishing campaigns due to the high value of intellectual property held on new medicines, with phishing emails against drug firms doubling in the last year. Security researchers have also discovered a malware distribution campaign targeting companies that use AutoCAD.[20] The campaign has been active since 2014, with the malware installed through phishing emails containing malicious AutoCAD files. The researchers discovered 40 unique malware modules, which were found to be sending data back to attacker-controlled servers running a Chinese-language installation of server architecture. The attacks have been used to steal designs for bridges, factory buildings, and more.

CHECKLIST

- Autodesk recommends that users limit AutoCAD's ability to execute scripting modules
- Phishing continues to be one of the most common forms of attack – ensure your staff are educated on phishing practices and mitigation

Only as strong as the weakest link

Earlier this quarter, reports were published about Magecart, a group that produced malware which was used to skim credit cards online on sites such as Ticketmaster, British Airways, and Newegg.[21] Magecart also targeted third-party code providers, such as customer service chats, which expanded the group's reach far wider than if they had just attacked specific sites. The Magecart attack has brought attention to how attackers can use third-party services and suppliers to attack businesses.

Recently, the Pentagon created a task force to audit US Government contractors and ensure compliance with cyber security standards.[22]

This news followed the November cyber-attack and extortion attempt on Austal, a Department of Defence contractor that build patrol vessels and frigates for the Australian navy.[23]

CHECKLIST

- Check your supply chain for any potentially vulnerable services your business could be using
- Ensure robust supplier assessments and that contractors are adhering to recommended cyber security standards

Nations enter into cyber security agreements

Singapore has entered into agreements with the US and Canada in an effort to bolster cyber security defence.[24]

Singapore and Canada have signed a Memorandum of Understanding (MoU) which will remain valid for two years, and involves joint efforts on initiatives such as data sharing, developing certification programs, and working together against cyber security threats.

Singapore also announced the signing of a Declaration of Intent with the US, an agreement which covers a series of cyber security workshops.

These follow previous cyber security agreements Singapore has made with Australia, France and India, with the south-east Asian nation emphasising the importance of strong partnerships to combat cyber-crime.

Indonesia and the US also announced an agreement to collaborate on cyber security, with a focus on combating financial crime and developing more education and training programs for the Indonesian National Police.[25]

“Recently, the Pentagon created a task force to audit US Government contractors and ensure compliance with cyber security standards”

By the Numbers

74%
of directors in the UK regard cyber security as a high priority issue[7]

15,670
vulnerabilities published in 2018 by the NIST Vulnerability Database[8]

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Deep Dive:

Cyber trends to watch in 2019

What to expect and what you need to do to keep on top of these changes

Katerina Borodina
Intern, Cyber Outreach

Luke Hopewell
Manager, Cyber Outreach

Artificial Intelligence to up the ante on phishing

Action: Read the Australian Security Directorate’s published advice on ‘Improving Staff Awareness’[26] and its top 10 tips to uplift staff learning.

AI is broadly defined as the ability for machines to mimic human behaviours (such as speech) in order to complete tasks.

An AI system can also follow patterns and make decisions based on a series of variables. AI is already helping businesses increase workplace productivity by automating manual tasks normally done by humans, freeing up time for employees to focus on new projects.

A subset of AI is machine learning, where machines can learn based on their experiences without the explicit programming of humans. In the field of cybersecurity, for example, machine learning systems can analyse existing threat data and work to identify new patterns and threats to a business.

Unfortunately for cyber practitioners, AI and machine learning systems can also be used in the realm of phishing.

AI in the hands of cybercriminals has the potential to:

Increase the volume and efficiency of phishing campaigns
AI and machine learning programs have the ability to create new phishing content by analysing existing and previously successful material. Working autonomously, a system can therefore efficiently churn out new phishing content at speed, without human interaction.

Increase the sophistication of phishing attempts
Rather than sending a phishing email campaign to a list of potential targets in a bid to steal login credentials or other personal information, an attacker could use AI systems to tailor phishing lures to individual targets. Because of its ability to trawl large amounts of data, researchers have put AI to work on social networks, analysing potential phishing targets, who they talk to (such as customer service accounts) and what they talk about[27]. The AI is then able to use this information to tailor specific phishing messages for the target that they’re more likely to click on. You can read more on this type of attack in our Deep Dive on page nine of this issue.

Enable the proliferation of new threats
AI is already being used in new types of attacks. Experimental malware demonstrated in 2018 allows hackers to systematically scan the entire internet looking for common vulnerabilities present on Internet of Things devices, before infecting them with malicious cryptocurrency miners.[28]

Elsewhere, hackers have used an automated AI program to distribute hoax bomb threats to police departments, schools and other institutions around the world, seeking ransom payments in cryptocurrency.[29]

Scammers are even employing new AI technology to simulate voices as part of an attack that dials random phone numbers to threaten recipients with arrest unless an on-the-spot “fine” can be paid.[30]

The incidence of AI-enhanced attacks is set to increase in 2019 as more hackers take advantage of these new tools. Against that backdrop, the advice contained in the hexagons above is as important as ever.

To help protect yourself against phishing:

1
IF YOU DIDN’T EXPECT IT, YOU SHOULD SUSPECT IT
Spotting context clues is key to identifying phishing emails. For example, did you expect to be contacted by a tourism company offering you a free cruise? Or were you expecting to receive a large sum of cash? If you didn’t expect to receive a particular piece of correspondence, you should immediately start to suspect it. Inspect the message to determine its legitimacy by checking the spelling of a sender’s email and body text, and graphics.

2
BEWARE OF TIME PRESSURES
Don’t be tricked into handing over your data by a campaign applying urgent deadlines. Phishing campaigns often use these time-pressure tactics to implore urgent action from a target in a bid to circumvent one’s better judgment. New campaigns powered by smart AI can even predict when targets are likely to be the most time poor, meaning they’ll be more susceptible to time-pressured threats.

3
IF YOU’RE UNSURE, MAKE SURE
Scammers often pose as banks and other critical services. If you’ve received an email that urges you to click a link to login, make a payment or take other urgent action, pick up the phone and contact the organisation directly. Quote the information you received that you suspect to be fraudulent to verify its validity.

You can learn more about how to spot and avoid phishing compromise on CommBank’s website.[31]

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Deep Dive:

Cyber trends to watch in 2019

> “The best way to protect your organisation against 2019’s evolving malware attacks is to **continue to rigorously pay attention** to getting the basics right”

Increasing scrutiny of third-party suppliers

Action: Ensure you’re always maintaining a good security posture by limiting access to business-critical systems and data; correctly managing user access credentials; encrypting data; updating software and safely storing data.

Security concerns related to third-party hardware and software made headlines throughout 2018. Australian military bases were stripped of cameras made overseas[32], and the Federal Government banned some providers from Australia’s 5G infrastructure build,[33] to name just a few.

It is not just governments which should be carefully weighing up the sensitive data held by third-party suppliers.

In 2018 some widely publicised third-party breaches had significant implications for their customers. Recruitment software company PageUp experienced a breach of its systems that saw thousands of jobseekers and employers impacted, including some of Australia’s largest organisations.[34]

According to research from the Ponemon Institute, 61% of surveyed respondents said they had experienced a third-party data breach (an increase of 5% year-on-year and 12% since 2016).[35] In 2019, we expect the rate of third-party incidents to persist as cybercriminals continue to exploit third-party vendors holding critical business data.

To help protect yourself against these breaches:

1. Limit access to minimum-required for the third-party to perform the contracted services
2. Assign any access credentials to specific users, rather than using generic accounts
3. Validate access at least every six months to disable any users no longer requiring access
4. If possible, enable two-factor authentication
5. Encrypt all data whilst in-transit, never send data in emails without being encrypted
6. Keep desktops and notebooks up to date with software updates, and use a anti-malware engine
7. Consider carefully whether access to email is required on mobile devices (e.g. smartphones and tablets)
8. Consider using a solution such of Office 365 and OneDrive for business email and file storage

The file-less evolution of malware

Action: Check your organisation’s compliance with the Australian Signals Directorate (ASD) Essential Eight checklist[36] to bolster your security against new types of malware.

Each year brings with it new forms of malware, and 2019 will be no different.

Commonwealth Bank’s Cyber Security Centre continues to observe the use of what’s known as ‘file-less malware’. Different to traditional malware that infects a user via an executable (.exe) file downloaded onto the hard disk, file-less malware works by executing code found inside a ‘trusted file’ (such as a .doc or .ppt), making it difficult for anti-virus engines to detect.

When the infected file is opened, a macro of instructions will trigger, that ultimately calls a hacker’s command-and-control infrastructure. Once the hacker has access to the machine, they’re able to perform reconnaissance activities, move around the network, or potentially extract information.

Some attacks may result in additional malware being planted on a target machine to have it complete a specific task or function, such as mining cryptocurrency surreptitiously – a tactic which increases in popularity with a corresponding rise in cryptocurrency values – or to lock it up with ransomware.

While these types of file-less attacks that “live off the land” have been around since 2016, we expect them to multiply in 2019 as the technology makes its way into off-the-shelf hacking kits available for sale on the dark web.

The best way to protect your organisation against 2019’s evolving malware attacks is to continue to rigorously pay attention to getting the basics right.

The ASD Essential Eight Maturity Model[37] presents a series of strategies to protect against and mitigate cyber security incidents in organisations of all shapes and sizes. It suggests employing:

1. Application Whitelisting
2. Patching Applications
3. Restricting Administrative Privileges
4. Patching Operating Systems
5. Disabling Untrusted Macros
6. Using Application Hardening
7. Multi-Factor Authentication
8. Daily Backups

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Deep Dive:

Cyber trends to watch in 2019

> “Competition for the best cyber talent continues in 2019. **A deteriorating external landscape and heightened regulatory environment**[38] will add to the pressure”

No end in sight for talent shortage

Action: Get your organisation involved in developing future talent by sponsoring education initiatives, offering flexible hiring and working arrangements and programs such as internships.

Competition for the best cyber talent continues in 2019. A deteriorating external landscape and heightened regulatory environment[38] will add to the pressure on organisations to hire more skilled practitioners to handle the increased workload.

While some organisations are collaborating with government and the tertiary sector to encourage more students to pursue careers in cyber, the effect of these initiatives aren't likely to be felt for a number of years.

Australia has been one of the hardest hit by the skills shortage:

- Australia has around 19,500 skilled cyber practitioners working in the sector, representing a growth of 7% in the last two years
- Despite encouraging growth, this still isn't enough to cover the headcount required, with 2300 positions still needed to cover the shortfall
- By 2026, Australia will need an additional 17,600 cyber security workers[39]

The growth in available candidates is encouraging, and since 2017, governments, tertiary institutions and the private sector, including the Commonwealth Bank have worked to build momentum.

The Australian Government established its Cyber Security Cooperative Research Centre in 2018 to develop the nation's cyber security capability, and a number of universities and TAFEs now offer recognised qualifications in cyber security.

Businesses in Australia can also get involved in closing the skills gap, by:

1 Engaging with a range of educational institutions at varying stages of schooling to help generate interest in cyber security

2 Encouraging an interest in cyber security by sponsoring events such as 'capture-the-flag' challenges and on-campus events

3 Offering flexibility in the recruitment process to cater to different start dates and backgrounds for those coming from university

4 Offering flexibility to try different roles in an organisation to support training and development of new recruits

5 Offering continuous learning opportunities and programs

Deep Dive:

3 cyber threats that count on human error

Melanie Timbrell
Senior Manager, Cyber Outreach

2019 had barely begun when an email was circulated to Victorian government employees notifying them of a data breach in which work phone numbers, email addresses and job titles were accessed by an “unauthorised third party”.[40]

The method of attack? An employee’s compromised email account which enabled the download of a partial copy of the Victorian government employee directory.

While employees were reassured that no banking or financial information was affected in the breach, experts have warned the dataset could be used both for commercial gain and potentially by those interested in exerting influence.

The notification email to employees also warned the information accessed could potentially be used to launch more targeted attacks, where employees could be tricked into revealing more valuable information by, for example, criminals impersonating their colleagues.

It serves as a timely reminder of how frequently attackers can rely on people and our foibles to help facilitate their crimes, whether through unwittingly downloading malware, clicking on links, or simply transferring them money when they demand it.

The term social engineering is now used to describe the deception or manipulation of people into divulging information that can be used for fraudulent purposes.

In the information security context, phishing is perhaps one of the best known examples of social engineering.

Trend 1: Business Email Compromise (BEC)

Business Email Compromise is a type of threat which has evolved over the past two to three years. In essence, it’s when a criminal finds a way to takeover a business email address. They then use it to imitate legitimate requests and intercept emails being sent.

It began with attackers sending messages purportedly from the CEO to the CFO of a targeted company asking them to facilitate an urgent payment outside of usual process.

But more recently, there has been a surge in attacks targeted deeper into an organisation. For example, attackers may impersonate senior leaders and target Accounts Payable to facilitate wire transfer fraud. Or engineers in the company may be targeted in cases of intellectual property theft. Human resources may also come in for their share of interest to obtain confidential tax and identity information.

In fact, a recent report from Trend Micro

A quick reminder on phishing and how to spot it

Phish-ing [NOUN]

An email scam used to obtain personal information such as usernames, passwords or bank account details by disguising as a trustworthy source. It often downloads malware (malicious software) onto personal computers or directs users to enter personal information on fake websites.

A suspicious email

Take a look at some common traits of a phishing email

From	Slightlyfamiliarperson@unusual-email-address.com
Subject	Need you to do something very urgently!
Attachment	Weird_attachment_type.exe

Dear John
http://fakelinkdesignedtoruinyourlife.com
Please give me all your passwords, money, drivers licence and bank account details or you won’t get promoted.

Sincerely, The Phish

Stop and think before you click
Don’t be tricked by a sense of urgency and reply or click on attachments. Bogus attachments usually contain malware and can be virtually impossible to spot.

Verify sender addresses
Some sender addresses immediately look unfamiliar or peculiar, others may appear to have a legitimate sender but still seem suspicious. To verify a sender, give them a call or send them a new email after looking up their details through official channels.

Check for fake links and images
Check that links and images in emails are legitimate by hovering your mouse over the link to show its true source. Some hidden links look strange and contain random characters, whilst others try to imitate known organisations and look legitimate.

Always report suspicious emails
If you ever spot a hoax purporting to come from CBA, please help us shut down fake sites quickly by sending the email or screenshot as an attachment to hoax@cba.com.au

Deep Dive:

3 cyber threats that count on human error

Did you know?

More than half of phishing sites now carry the 'padlock' that many people look to for reassurance a site is legitimate?[43]

predicted that over the next year, BEC will target "two levels down the org chart",[41] naming positions such as executive assistants as those likely to find themselves in the line of attack.

Data breaches such as the one experienced by the Victorian government can provide an avenue to these types of highly targeted 'spear-phishing' attacks, which were referenced in the warning email to Victorian state employees.

Several years ago email attackers largely chose one of two tactics for their phishing campaigns, either the mass 'spray-and-pray' that sent hundreds of thousands of malicious emails to unfiltered lists, or small, targeted campaigns with carefully crafted lures.

While there are still base level operators prepared to use the mass phishing techniques, in more recent years the collision of big data, the volume of information stored online and the surge in usage of digital tools and services has enabled the development of social engineering at scale, with devastating efficacy.

The Proofpoint 2018 annual report[42] labels human nature as the key vulnerability, framing cyber security as "not strictly an IT and operations issue".

When it comes to BEC threats, technical controls are often ineffective as there's no malware involved and domains are commonly legitimate given it's a compromise of a legitimate account.

Attacks are generally framed to motivate people to quick action, often employing a sense of urgency, some scare tactics and timing chosen to maximise the chance of success.

According to Proofpoint, 80% of businesses have experienced an email fraud attack.

So what can you do about this risk?

A key factor of success is how well your employees are trained to spot and recognise threats. Even if you are already using a phishing simulation platform, BEC is something which will typically require supplementary training.

One thing often overlooked with BEC is what led to the compromised email account in the first place. Locking down accounts with new passwords and two factor authentication to force out attackers is an important step in the recovery process.

More generally, training aimed at helping employees understand the risks of opening email attachments or clicking links from unfamiliar sources, and the potential of these to lead to malware or virus infection is also important. If you are a CBA business banking customer, you can talk to your business banker about getting access to our online 'Cool, Calm, Connected' e-learning suite for use in your business.

On the technical side of things, your IT security department should be looking at how to detect malicious macros and other code embedded within attachments.

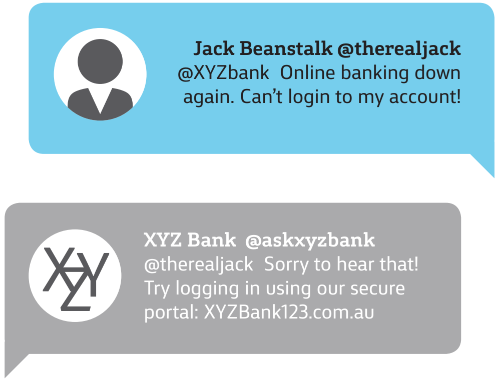
There are a number of filters and solutions available for real-time sandboxing of URLs and attachments, in addition to those built to recognise websites designed to steal credentials.

It's worth considering which of these solutions is right for your business.

Trend 2: 'Angler Phishing'

Angler Phishing is where attackers pose on social media as a customer service representative of a legitimate company, using lookalike social media accounts to insert themselves into conversations between brands and their customers.

With the target of the customer's frustration obvious, the scammers are able to reach out to the victim using a 'lookalike' fake account giving people the option to click on a link for immediate assistance to help resolve their issue. Clicking on the link however, could in turn either see the customer's personal information and login credentials harvested or malware installed on their computer, for instance.



Jack Beanstalk @therealjack
@XYZbank Online banking down again. Can't login to my account!

XYZ Bank @askxyzbank
@therealjack Sorry to hear that! Try logging in using our secure portal: XYZBank123.com.au

Angler phishing is just one of the methods attackers can use to abuse and impersonate business brands via social media and online.

An observation made by Proofpoint is the large number of websites impersonating major brands but sitting on unrelated domains with attackers using "clean" unused or expired domains bought cheap from a secondary market.

"These URLs are valid and have solid reputation scores, making detection by security tools more difficult," according to the report.[44]

In terms of technical solutions to help protect your brand from attacks which aim to trick your employees, partners, vendors and customers, there is 'defensive domain

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Deep Dive:

Building the cyber talent pipeline

> As more businesses adopt more **cloud-based services to facilitate collaboration and improve operational efficiency**, these new ways of working have brought with them new risks

registration', which refers to the practice of buying up internet domains that could be used to imitate your legitimate one.

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a method businesses employ to stop domain imitation in email fraud. It works by checking that the domain in the message 'from' field aligns with other authenticated domain names.

Deploying DMARC can be done in-house if you have a tech team with the capability, otherwise it is possible to partner with an organisation that specialises in DMARC implementation.

Nearly 25% of all suspicious login attempts to cloud services are successful

Approximately 50% of all cloud app users have installed 3rd party add-ons. About 18% of these have access to email and files

Around 60% of cloud service users didn't have a password policy or multi-factor authentication enforced

Data Source: Proofpoint, 2018, 'The Human Factor' report

Trend 3: Factoring in the cloud

As more businesses adopt more cloud-based services to facilitate collaboration and improve operational efficiency, these new ways of working have brought with them new risks.

This includes an increased opportunity for believable phishing campaigns as well as employees taking other action which increases risk to an organisation, such as sharing credentials and information with third parties to make use of cloud services.

For instance, if you use a third party email add-on then you'll legitimately provide your login credentials. Following this a token may authorise the app to synchronise your email on a separate server where security may not be up to scratch.

Alongside this is the use of the cloud to share files which, if not properly governed and monitored can, and frequently does, result in inappropriate access levels both within an organisation and externally.

The Australian Cyber Security Centre has recently published advice for businesses on cloud security.[45] Some of their key callouts include:

- Review and understand your provider's shared responsibility model so you can identify your organisation's responsibilities
- Employ strong authentication mechanisms, including strong passwords and two-factor authentication where available
- Do your own backups

Separate to this, it's important as an employer to have an understanding of which cloud-based apps and add-ons your employees are using and what security measures are in place to protect your data. It's also a good idea to educate employees on best-practice use of cloud-based services, particularly as it relates to treatment of confidential and sensitive information to try and limit careless behavior which could expose your organisation to loss.

Here to stay

At the end of the day, so long as there are limitations and gaps in new technologies, cyber security's most persistent threat will continue to be human error – clicking on a malicious link, falling for a phishing email, using a weak password or being trusting enough to provide information to someone we shouldn't. In this context it's worth every company looking not just at trying to apply technical solutions to a human problem, but considering simple interventions – such as training and emphasising best practices – that can help make attacks less frequent and hopefully less devastating.

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Regulatory and Legal

New laws and legal precedents relevant to security strategy

> Last year, the US Congress passed a law that will **largely ban Huawei and ZTE** use by the US government and contractors

Encryption bill passes Senate

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 was passed through the Senate in December.[46]

The bill will require designated communications providers to provide technical assistance and capabilities to security agencies to help them intercept encrypted messages.

In submissions to the Parliamentary Joint Committee on Intelligence and Security[47], some in the technology industry expressed concerns that the introduction of backdoors into apps would inherently weaken security. Concerns were also raised around the potential to impact Australia's competitiveness by undermining the perceived trustworthiness of Australian-made hardware or software.[48]

The Labor Party hopes to make amendments to the bill when Parliament returns in February.

CHECKLIST

- Get legal advice on whether the law[49] applies to your business and understand any obligations that arise as a consequence
- Keep abreast of any amendments introduced to the law over the coming months

APRA finalises standard aimed at combating threat of cyber attacks

On 7 November 2018 the Australian Prudential Regulatory Authority (APRA) released the final version of Prudential Standard CPS 234, which focuses on information security management. APRA Executive Board Member Geoff Summerhayes described the driver for the new standard as follows: "By introducing CPS 234, APRA aims to ensure all regulated entities develop and maintain information security capabilities that reflect the importance of the data they hold, and the significance of the threats they face."

In summary, the prudential standard requires APRA-regulated entities to:

- Clearly define information-security related roles and responsibilities
- Maintain an information security capability commensurate with the size and extent of threats to their information assets
- Implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls
- Promptly notify APRA both of material information security incidents and material information security controls weaknesses that will not be remediated in a timely manner

APRA expects regulated entities to comply with CPS 234 from 1 July 2019.

CHECKLIST

- The full text of CPS 234 can be found at: https://www.apra.gov.au/information-security-requirements-all-apra-regulated-entities
- To help APRA-regulated entities fulfil their requirements, APRA will shortly update Prudential Practice Guide CPG 234 Management of Information and Information Technology
- In preparing to meet CPS 234's requirements, regulated entities should bear in mind that the prudential standard requires you to consider not just your internal environment, but also your extended business environment including third parties which manage your information security assets

NZ bans Huawei, joining Australia and the US

The New Zealand government has now banned Huawei from supplying equipment to the country's 5G network[50], after Australia did the same in August. In a statement to the stock exchange, Spark Telecom said New Zealand's Government Security Bureau had made the decision on the basis of national security concerns.

Last year, the US Congress passed a law that will largely ban Huawei and ZTE infrastructure use by the US government and contractors. This ban could potentially be extended to all US companies.[51]

Also in December Japan's government issued instructions to ban Huawei and ZTE from official contracts, with the country's largest telco operators set to follow suit.[52]

In the UK, Head of MI6 Alex Younger has recently said decisions need to be made about Huawei's involvement in Britain's next generation mobile network in view of the actions taken by the US, NZ and Australia.[53]

CHECKLIST

- The security standards of potential suppliers and their ability to meet security obligations should be key factors in procurement decisions for all organisations, not just governments. Ensure you have an active security compliance program that compels suppliers and other partners to protect your data to an expected standard
- Globally, national governments have intensified their focus on cyber security and data protection regulation in recent years, to protect their citizens and national interests. Businesses with a global presence should make themselves aware of these regulations, and the implication of differences across various regions

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Better Practice

The latest advice to consider when setting security policies

Australian Government launches Cyber Security Small Business Program initiative

For: small businesses
The Australian government has partnered with the Council of Registered Ethical Security Testers Australia New Zealand (CREST ANZ) to launch a grants initiative as part of its Cyber Security Small Business Program. Over the next two years, eligible small businesses (with 19 employees or less) can apply for individual grants of up to $2100, covering half the cost of having their cyber security tested by CREST ANZ-approved service providers.

To be eligible you must:

- have an Australian Business Number (ABN)
- be registered for the Goods and Services Tax (GST)
- employ 19 or fewer full-time equivalent employees
- and be an entity incorporated in Australia, a partnership, or a sole trader

You are not eligible to apply if you are:

- a trust (however, an incorporated trustee may apply on behalf of a trust)
- a publicly funded research organisation (PFRO) as defined in appendix A of the grant opportunity guidelines
- a Commonwealth, state, territory or local government body (including government business enterprises)
- a business that employs more than 19 full-time equivalent people

You are not eligible to apply if you have previously received funding under the Cyber Security Small Business Program.

The deadline to apply is 30 June 2020 or earlier if the funding is fully committed.
You can read more and apply using the link below:
https://www.business.gov.au/assistance/cyber-security-small-business-program

Australian Signals Directorate updates Information Security Manual

For: Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), cyber security professionals and information technology managers
The Australian Cyber Security Centre, overseen by the Australian Signals Directorate, has published an updated version of the Australian Government Information Security Manual (ISM). The ISM is designed to help organisations protect information and systems from cyber threats. The guidelines discuss both governance and technical concepts. The complete manual and composite parts are available for download from the below link:
https://www.acsc.gov.au/infosec/ism/index.htm

Security researchers sound warning on some SSDs

For: Cyber security professionals and information technology managers
Researchers have found flaws in the encryption of several popular Crucial and Samsung solid state drives (SSDs), stating the vulnerabilities can be easily exploited to gain access to the data without needing the password.[54] The security researchers warn users shouldn't rely on hardware encryption offered by SSDs alone, and should also use software solutions to secure their data. The findings are not yet finalised, pending peer review although the research was made public after disclosing the bugs to the drive makers.

This report contains general advice for educational purposes only. Please consult your cyber security team and legal counsel for advice specific to your organisation.

Phish Eyes

Recent phishing lures for your security awareness

Report hoax emails to hoax@cba.com.au

> “The usual spate of scams targeting festive shoppers were also out in force, trying to **trick targets into clicking on malware** or enter personal information”

Festive phishing

The December quarter once again saw a rise in festive season-related phishing. In the lead up to year-end, we saw phishing campaigns target some businesses by promising their employees gift cards including from big-name brands such as Amazon, or by using the tactic of prompting them to click on the basis of making a charitable donation.

Gift card and charitable donation scams have both been on the rise in recent years, with consumer watchdog the Australian Competition & Consumer Commission (ACCC) commenting in October they’d observed a rise in charity-related scams and calling the trend of impersonating charities such as the Red Cross, RSPCA or Emergency Relief Services “appalling”.[55]

The usual spate of scams targeting festive shoppers were also out in force, trying to trick targets into clicking on malware or enter personal information such as names, addresses, and credit card details.

Among those seen this year were websites set up for online stores which didn’t exist, fake travel deals and accommodation listings, and fake delivery notices which capitalised on the fact more people expect parcels at this time of year.

There was also the widely publicised ATO phone scam which hit at the end of 2018 and which used threats of arrest over outstanding tax debts to gain cut-through.

According to the ATO, more than $800,000 was lost by taxpayers to this scam in November alone.[56]

Abusing social trust

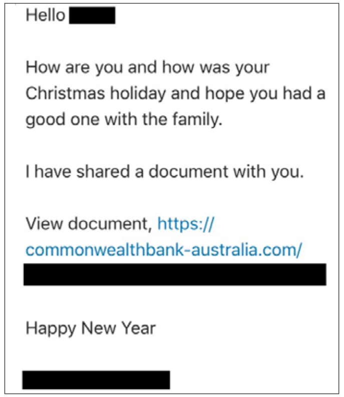
Lately, we’ve seen new examples of phishers leveraging the networking power of social apps. A Facebook phishing message used Messenger to spread a phishing scam in which the recipient’s name and photo would be used to create a supposed ‘viral video’ preview to scare the recipient into clicking. One the recipient opened the link, they would be prompted to log in with their Facebook credentials. Using the stolen credentials, the attackers could then send similar videos to the victim’s contacts.

In other examples of social phishing, attackers have also made Twitter accounts posing as reputable companies and inserting themselves in live conversations between the imitated company and customers. Customers who are following the conversation would be tricked into clicking links supplied by the phisher, believing they were having a conversation with the company. Businesses should be on the lookout for any scam accounts impersonating them, particularly in conversations with customers.

We also recently spotted another social media phishing scam, this time involving LinkedIn.

A person was sent a LinkedIn message from a contact’s compromised account asking them to view a document. The link would then redirect to a fake Onedrive website, where clicking the document would open a fake Microsoft account login page.

This is an example of how attackers are beginning to leverage the power of social media by abusing the trust we have in our contacts. While people are now more aware that email addresses can be spoofed, a message coming directly from a connection on a social media website may prompt less



Hello [redacted]

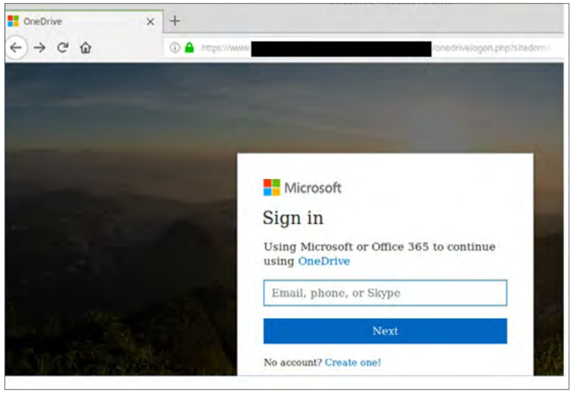
How are you and how was your Christmas holiday and hope you had a good one with the family.

I have shared a document with you.

View document, https://commonwealthbank-australia.com/ [redacted]

Happy New Year

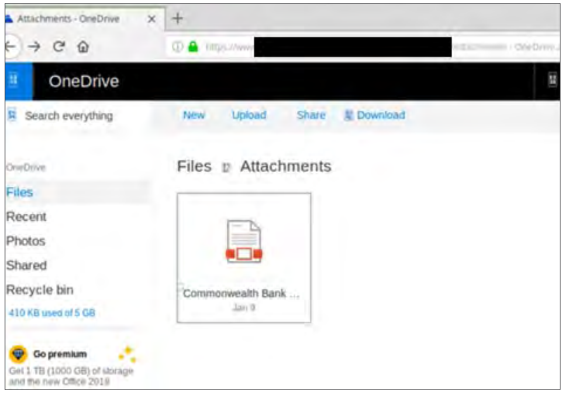
[redacted]



Sign in

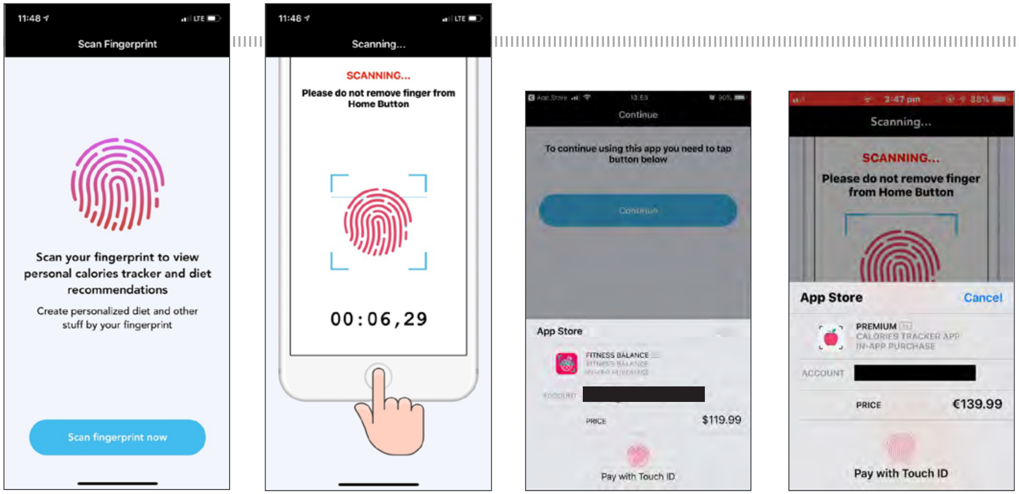
Using Microsoft or Office 365 to continue using OneDrive

No account? Create one!



410 KB used of 5 GB

Get 1 TB (1000 GB) of storage and the new Office 2019



11:48

Scan Fingerprint

Scan your fingerprint to view personal calories tracker and diet recommendations

Create personalized diet and other stuff by your fingerprint

Scan fingerprint now

11:48

Scanning...

SCANNING...

Please do not remove finger from Home Button

00:06,29

13:53

Continue

To continue using this app you need to tap button below

Continue

App Store

FITNESS BALANCE

FITNESS BALANCE

IN-APP PURCHASE

ACCOUNT [redacted]

PRICE $119.99

Pay with Touch ID

3:47 pm

Scanning...

SCANNING...

Please do not remove finger from Home Button

App Store Cancel

PREMIUM

CALORIES TRACKER APP

IN-APP PURCHASE

ACCOUNT [redacted]

PRICE €139.99

Pay with Touch ID

https://www.welivesecurity.com/2018/12/03/scam-ios-apps-promise-fitness-steal-money-instead/

Original image source: Reddit

scrutiny. It's also important to note that the scam site had the green lock – a common misconception is that the lock indicates a website is safe, but it's becoming increasingly trivial for an attacker to obtain the green lock on their own website.

iOS Targeted

According to a press release by mobile security solutions provider Wandera, iOS users experience twice the amount of mobile phishing attacks Android users do.[57]

As well as SMS phishing (smishing), December saw a sophisticated Touch ID scam hit the Apple Store. The scam used a number of apps which posed as health assistants to capitalise on how quick and easy it is to use Touch ID to approve purchases.

The apps would invite users to use Touch ID to get a calorie tracker, or take a heart rate measurement for example, although once a person scanned their fingerprint the apps would very briefly show an in-app purchase popup charging up to $120 while dimming the screen to make it very difficult to see the prompt.

According to a Wired article on the scam, the charging of "exorbitant, unscrupulous fees within apps violates Apple's App Store guidelines; the apps in question, innocuously named 'Heart Rate Monitor', 'Fitness Balance app' and 'Calories Tracker app' have all been pulled.

"It's unclear if they came from separate developers, or one person operating multiple developer accounts," Wired said.[58]

Endnotes

[1] https://blog.certfa.com/posts/the-return-of-the-charming-kitten/

[2] https://www.abc.net.au/news/2018-11-06/iranians-fear-more-economic-pain-as-us-sanctions-kick-in/10468492

[3] https://www.itnews.com.au/news/business-losses-to-email-spoofing-scams-skrocket-acc-516061

[4] https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

[5] https://www.pwc.co.uk/audit-assurance/assets/pdf/insider-threat-for-google.pdf

[6] https://www.computerworld.com.au/article/650122/400-million-cost-australia-cyber-security-skills-shortage/

[7] https://www.forbes.com/sites/adigaskell/2018/11/28/the-growing-importance-of-cyber-security-skills/#52d55f1d139d

[8] https://nvd.nist.gov/vuln/search/statistics

[9] https://sc.cnbcfm.com/applications/cnbc.com/resources/editorialfiles/2018/12/20/China%20case.pdf

[10] https://www.abc.net.au/radionational/programs/breakfast/australian-businesses-hit-by-audacious-global-hacking-campaign/10645274

[11] https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx

[12] https://www.smh.com.au/technology/how-china-diverts-then-spies-on-australia-s-internet-traffic-20181120-p50h80.html

[13] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[14] https://thewest.com.au/business/500-million-guests-victims-of-marriott-hotels-data-hack-ng-b881038492z

[15] https://www.cnn.com/videos/business/2018/10/08/google-plus-security-bug.cnn-business

[16] https://www.thestar.com.my/tech/tech-news/2018/11/13/cathay-pacific-cyberattack-far-worse-than-thought-after-airline-admits-facing-intense-hack-for-more/

[17] https://thehackernews.com/2018/11/3ve-ad-fraud-google.html

[18] http://fortune.com/2018/11/26/google-play-malware-apps/

[19] https://www.zdnet.com/article/phishing-warning-if-you-work-in-this-one-industry-youre-more-likely-to-be-a-target/

[20] https://www.zdnet.com/article/new-industrial-espionage-campaign-leverages-auto-cad-based-malware/

[21] https://techcrunch.com/2018/11/13/magecart-hackers-persistent-credit-card-skimmer-groups/

[22] https://www.nextgov.com/cybersecurity/2018/12/pentagon-considers-cybersecurity-certification-its-contractors/153330/

[23] https://www.abc.net.au/news/2018-11-02/austal-ship-cyber-attack-and-extortion-attempt-national-security/10458982

[24] https://latesthackingnews.com/2018/11/20/singapore-enters-into-cyber-security-agreements-with-us-canada/

[25] https://www.straitstimes.com/asia/se-asia/indonesia-and-us-sign-pact-to-cooperate-on-cyber-security-on-sidelines-of-interpol

[26] https://cyber.gov.au/business/guides/improving-staff-awareness/

[27] https://observer.com/2017/01/spear-phishing-twitter-machine-learning/

[28] https://www.upguard.com/blog/resilience-in-the-age-of-automated-hacking

[29] https://www.theregister.co.uk/2018/12/14/nationwide_bitcoin_bomb_threat_a_bust

[30] https://www.sbs.com.au/yourlanguage/hindi/en/article/2018/11/21/have-you-received-phone-call-threatening-arrest-you-its-scam

[31] https://www.commbank.com.au/security-privacy/report-hoaxes.html

[32] https://www.abc.net.au/7.30/banned-chinese-cameras-are-being-used-by-the/10239036

[33] https://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438

[34] https://www.businessinsider.com.au/pageup-data-breach-recruitment-australia-companies-2018-6

[35] https://www.opus.com/ponemon/#ponemon_form

[36] https://acsc.gov.au/publications/protect/essential-eight-explained.htm

[37] https://acsc.gov.au/publications/protect/essential-eight-maturity-model.htm

[38] https://www.cso.com.au/article/645445/australia-only-has-7-percent-cybersecurity-expertise-it-needs/

[39] https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2018

[40] https://www.abc.net.au/news/2019-01-01/victorian-government-employee-directory-data-breach/10676932

[41] https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf

[42] http://get.proofpoint.com/pdf/pfpt-us-wp-human-factor-report.pdf

[43] https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

[44] http://get.proofpoint.com/pdf/pfpt-us-wp-human-factor-report.pdf

[45] https://cyber.gov.au/business/guides/cloud-computing-security/

[46] https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018

[47] https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018

[48] https://www.abc.net.au/news/science/2018-12-07/encryption-bill-australian-technology-industry-fuming-mad/10589962

[49] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

[50] https://www.smh.com.au/business/companies/new-zealand-joins-australia-in-banning-huawei-20181128-p50iz5.html

[51] https://www.smh.com.au/world/north-america/white-house-considers-emergency-order-to-ban-huawei-and-zte-entirely-20181227-p50ohd.html

[52] https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html?utm_term=.e512feed9514

[53] https://www.thetimes.co.uk/edition/news/mi6-boss-alex-younger-tells-britain-beware-march-of-chinese-technology-giants-like-huawei-022pw9kqw

[54] https://techcrunch.com/2018/11/05/crucial-samsung-solid-state-drives-busted-encryption/

[55] https://www.scamwatch.gov.au/news/warning-about-fake-charity-scams

[56] https://www.smh.com.au/business/small-business/it-s-not-us-ato-s-fresh-warning-as-scam-losses-hit-830-000-20181203-p50jsj.html

[57] https://www.wandera.com/about-wandera/wandera-in-the-media/press-archive/iphone-users-suffer-twice-many-mobile-phishing-attacks-android-users/

[58] https://www.wired.com/story/iphone-touch-id-scam-apps/