# Email Payment Fraud

## A Signals Special Edition

CommonwealthBank

**Brett Winterford**
Senior Manager,
Cyber Outreach and Research

Financial losses caused by fraudulent requests for payment sent by email now count alongside ransomware among the most realised cyber risks to Australian businesses.

In recent years, successive analyses in *Signals* have charted the emergence and evolution of this threat.

In 2015, the typical fraudulent request for payment was a plain-text email sent from a webmail address. The email claimed to be from the CEO or senior director of a firm, and – in broken English – sought an urgent payment be made to a foreign bank account. Most organisations today are familiar with these poorly-crafted scams and - thanks largely to education – fewer are falling for it.

Today, organisations more commonly receive emails purporting to be from suppliers (when an attacker spoofs the supplier's email address) requesting that their bank account details be changed for future payments. This approach demonstrates considerable research about the victims and their business relationships.

We've also seen more cases of 'Business Email Compromise' – in which attackers gain unauthorised access to email accounts of the victim or their supplier, and modify bank details on a legitimate request for payment.

In this one-off edition of *Signals*, we've collated our research into all forms of Email Payment Fraud to provide clients a checklist of the basic countermeasures.

What we've found is that your people and processes, more so than your technology, are key to defending against payment fraud. As the most targeted individuals for profit-motivated criminals, CFOs and payment teams need to play an active role in your organisation's defence.

I hope you find this summary - and our ongoing analysis in *Signals* - a useful resource to help educate your teams.

# Introduction

## What is email payment fraud?

> “Fraudulent request for payments **typically rely on social engineering** – the tricking of a human into making a poor decision”

The speed of transactions today requires accounts teams to be more vigilant than ever when making payments. As payments move toward settlement in real-time, the window for the freezing and recovery of payments misdirected due to deception is diminishing.

In this environment, Email Payment Fraud is a key risk for Australian organisations to mitigate. Over the past few years, many have received emails designed to look like valid requests to make payments to third parties, which include payment instructions or invoices.

In the majority of these scams, the perpetrator imitates one of two parties:

- A supplier of business partner – fraudsters pose as genuine suppliers and submit instructions to alter the supplier’s bank account to one accessible to the perpetrator for payment of future invoices.
- The CEO, director or another senior executive of the organisation – requesting accounts staff make an urgent payment to a supplier or business partner via a nominated bank account accessible to the perpetrator.

Typically the bank accounts provided by the scammer for receipt of these payments are opened in the name of ‘money mules’ – often-unwitting parties to organised crime who agree to move money through their accounts for a fee. Networks of money mules are groomed both domestically and in foreign countries.

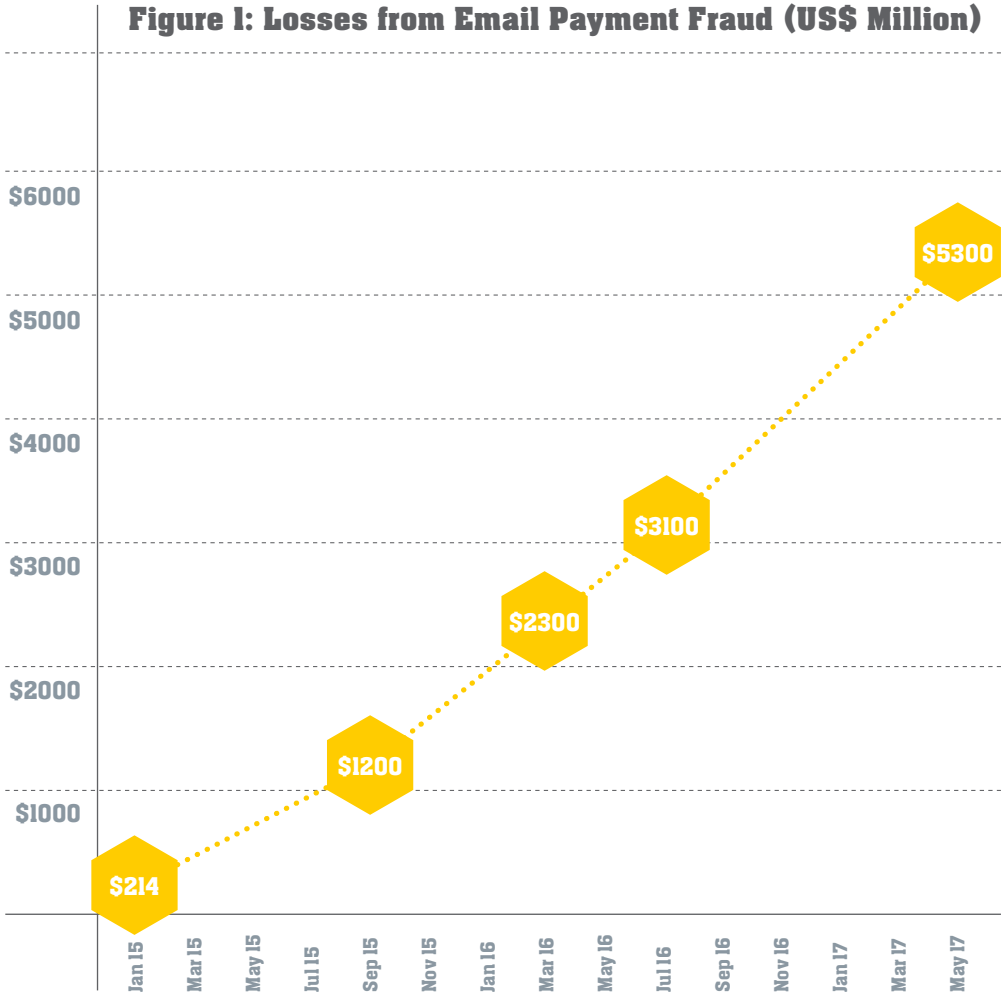
### How did they impersonate my email?

Typically, fraudulent request for payments rely on social engineering – the tricking of a human into making a poor decision. The scams otherwise rely on one of the following:

- The spoofing (impersonation or forgery) of one party to the transaction (Business Email Spoofing), or
- The hacking of an email account or third-party accounting software used to raise or authorise a transaction (Business Email Compromise).

Over the past 12 months, the latter category has grown at a faster rate. Each of these techniques – and suggested mitigations – will be explored in the pages ahead.

**Figure 1: Losses from Email Payment Fraud (US$ Million)**




*Source: FBI/IC3 https://www.ic3.gov/media/2017/170504.aspx*

# Introduction

## What is email payment fraud?

> “In Australia, we have observed losses from payment fraud growing at a steady rate”

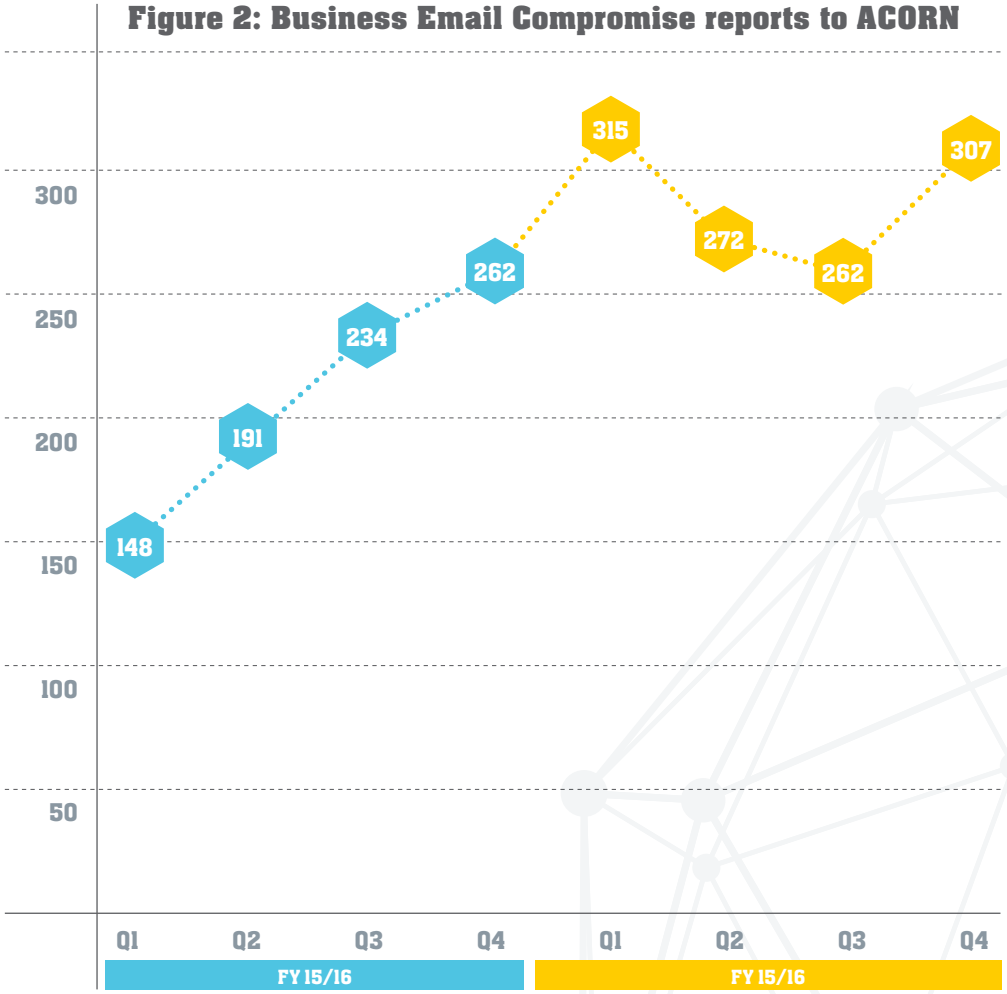
### A global problem

While these scams might sound simple, they have proven exceptionally effective.

According to the FBI, these scams have cost organisations in excess of US$5 billion in losses over two years[i]. Most of the losses have been incurred in developed, Western economies.

In Australia, we have observed losses growing at a steady rate. The Australian Cybercrime Online Reporting Network service received 835 reports of BEC in 2015/16, vs 1156 in 2016/17[ii], a 40% increase. Our own data suggests that victims often choose not to report their losses – which means these numbers may be conservative.

**Figure 2: Business Email Compromise reports to ACORN**




*Source: Australian Cyber Security Centre Threat Report, 2017*

### By the Numbers

**US$5.3 billion**
Global losses since 2015[vi]

**1156**
cases reported to the Australian Government in 2016/17… a **40%** growth in reported scams[vii]

**1 in 4**
losses reported by CBA clients involved compromise of a cloud email account[viii]

# Deep Dive

## Email Spoofing

*Email addresses are trivial to forge*

Just under a third of the Email Payment Fraud cases we studied in 2017 involved the impersonation or "spoofing" of the email address of a senior executive or supplier in an attempt to legitimise a fraudulent request for payment.

A spoofing attack will typically follow the steps outlined in Figure 3:

### Reconnaissance

The most primitive forms of Email Payment Fraud are typically sent from webmail addresses, are worded poorly, and are sent to a large number of potential victims in "spray and pray" spam campaigns.

The 'tells' in these campaigns tend to be obvious. Unfortunately, criminal groups have become more studious, patient and willing to invest money and effort in producing more effective lures in the quest for larger payouts. Most of that effort is spent on reconnaissance.

Reconnaissance activities typically involve trawling social media and other online sources to provide the scammers with important context that allows them to produce campaigns that are more realistic and more difficult to detect. Information useful to an attack might include, for example:

- New supply chain relationships – as advertised in public tender documents or trade press media;
- The names and email addresses of staff with authority to make payments (for targeting emails);
- The dates that a senior director will travel on business, such as when they are advertised as speaking at an event (to make it more difficult for victims to verify whether the request for payment is genuine).

In some cases, law enforcement has encountered cybercrime gangs that hire local 'agents' to produce an in-depth study of business connections in a specific market.

### Delivery

Fraudsters have several means of faking the sender's address.

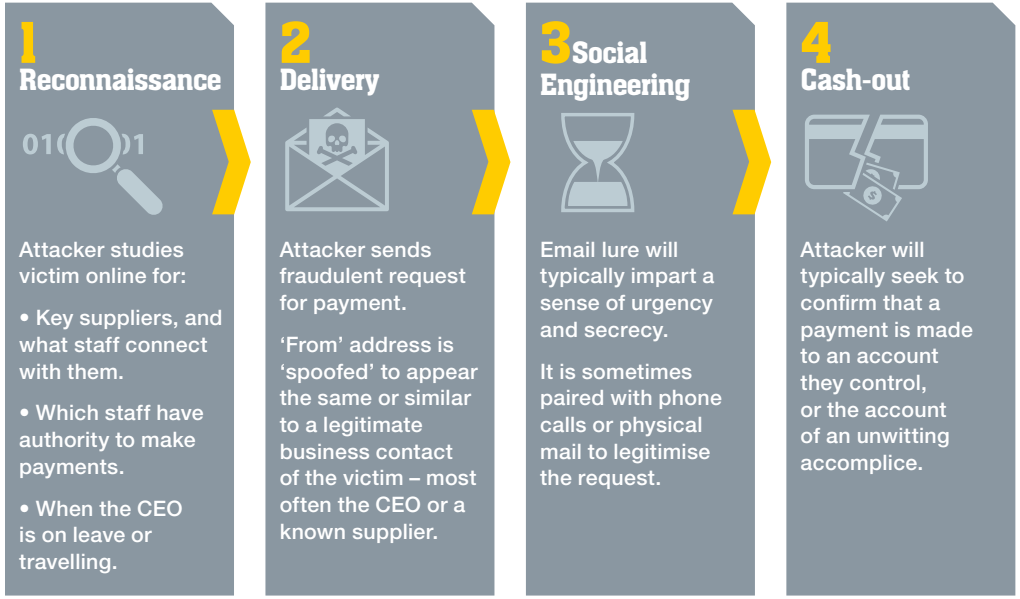
The least sophisticated is to simply register a webmail address in the CEO's name. This can prove effective when the CEO is known to be on leave or travelling for business, making it difficult for the recipient of the email to verify its authenticity unless they work very closely with the CEO.

Other attackers will register domains that are strikingly similar to - or derivative of - the victim or its supplier's legitimate web domain. These attacks – while more effective than registering a webmail address – require the (paid) registration of domains. Registering a domain introduces for the attacker elements of cost (albeit small costs) and a risk of being identified (albeit a trivial one).

The most sophisticated attackers 'spoof' the domain of the target organisation or one of its suppliers. In these cases, the email address in the 'from' field appears to be the genuine address of the entity being impersonated – even though it hasn't been sent from their account. Attackers can readily access very simple tools to spoof email at little to no cost.

An analysis of several hundred attacks published in Signals in late 2016[iii] found that victims are more likely to detect an email as being fraudulent when it has arrived from a different domain than usual, and are also more likely to be sceptical of requests for payment arriving from a webmail account [See Figure 4 on the following page]. Attackers enjoy far greater success when the email is spoofed and appears to be coming from the correct domain in the "from" field.

**Figure 3: Business Email Spoofing**



# Deep Dive

## Email Spoofing

Spoofing is easier for an attacker to employ than you might think. The protocol that email is based on – SMTP (Simple Mail Transfer Protocol) – has no inbuilt safeguards to ensure that an email has been sent by a person authorised to use that address.

Since the early 2000s, Internet standards bodies concerned about the proliferation of spam have developed email integrity and authentication standards to help validate that mail purporting to come from a given domain actually comes from IP addresses associated with that domain.

SPF (Sender Policy Framework) and DMARC (Domain Message, Authentication, Reporting and Compliance) are anti-spoofing standards that are free to implement. To protect your organisation from spoofing-based attacks, it is a very useful exercise to check the Domain Name System settings on your domains to ensure they include SPF and DMARC records:

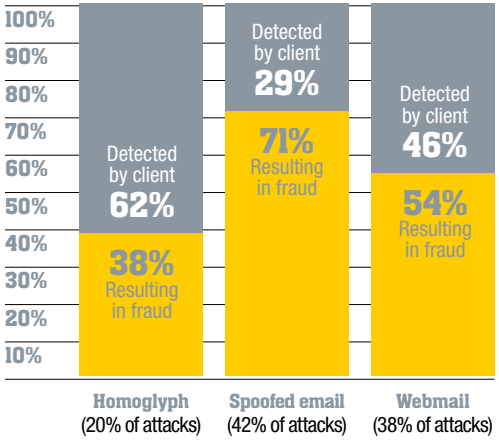
- Generally the owner of a domain populates SPF records with a whitelist of IP addresses associated with the organisation's authorised mail servers. If an attacker attempts to spoof your domain in an email sent to an organisation that also uses SPF records as part of their filtering of incoming email, the suspect email can be blocked or quarantined based on checks against DNS records. (NB: DKIM uses digital certificates to achieve the same result. It is essentially a public key registered as a TXT record in the DNS record of the domain name).

- Assuming the owner of a domain uses SPF or DKIM to attempt to protect their domain, an additional control called DMARC can be called upon to provide additional features. The domain owner publishes a DMARC record which describes how to handle spoofed emails (reject, quarantine, do nothing) upon SPF or DKIM failure. It also provides domain owners with a digest of emails other DMARC-compliant gateways have received and blocked when the SPF or DKIM check failed. This can be useful for knowing when your domain is being abused by attackers.

These controls in combination provide both a level of protection against spoofing and can alert you when fraudsters are attempting to impersonate your domain.

**Figure 4:**
**Efficacy of whaling techniques**

*Source: Signals Q4 2016*




While these measures are trivial to implement, they can be very difficult to fine-tune, and for various technical and business reasons (such as organisations legitimately wanting to use third-parties to send emails on their behalf for marketing purposes), many organisations have been slow to support them. In forums we have run with clients for the last two years, we tend to see between 60% (2016 average) and 85% (2017 average) of clients employing SPF, while only 10% (2016 average) and 12% (2017 average) use DMARC.

Implementation of these measures requires that a system administrator has a very strong understanding of where legitimate mail is sent from using your organisation's domain, as well as what email services are consumed by the organisation. Misconfigurations can lead to legitimate email, such as mailing lists, being blocked. It's thus advisable to implement the controls gradually, possibly one business unit or functional group at a time, testing each for any impact on mail delivery or service interruption that might need to be addressed before moving on to the next.

You should still assume that attackers will continue to find ways to bypass these controls. Your payment processes need to assume that an email from your staff or business partners can – if an attacker is determined enough - be forged in some way.

### Social engineering

Spoofed requests for payment require an attacker to present a convincing forgery while also encouraging their target to make a payment quickly without triggering scepticism or caution.

In 2015 and 2016, many of the 'whaling' scams we analysed contained repeated features suggestive of an operation that sends fraudulent requests for payment at scale[iii]. ('Whaling' emails impersonate the CEO or a senior director of the victim organisation).

The key features of these campaigns are presented in figure 5 overleaf:

# Deep Dive

## Email Spoofing

**Figure 5: Features of whaling emails** *Source: Signals Q4 2016*

### 1 Address Target by First Name

**Present in 96% of attacks**

Most campaigns exhibit evidence that the attacker has researched the names of CEOs and Accounts Payable staff.

### 2 Check target availability

**Present in 48% of attacks**

From mid-2016, campaigns often began by asking whether the Accounts Payable staff were available to complete a payment for the impersonated Executive.

"Are you available this morning?"

"Let me know if you are available."

"Are you in the office?"

### 3 Create a sense of urgency

**Present in 56% of attacks**

Over half of campaigns made specific appeals to the payment being 'urgent' – using terms such as "urgent", "immediately", "ASAP" or "right away".

"I need you to attend to this wire transfer immediately"

"Kindly get it done ASAP"

"Handle this right away"

### 4 Validate the payments process

**Present in 41% of attacks**

Attackers will often seek information on how or when payments can be made (especially international payments).

"Are you able to process an international wire transfer today?"

"What details do I need to give to you to make an international wire transfer?"

### 5 Maintain exclusive, direct communication with target

**Present in 100% of attacks**

All attacks solicit a direct reply to prevent target from discussing the matter with other staff. A typical excuse is that the requestor is "in a meeting and can only reply on email".

"Send me confirmation when completed."

"Let me know once its done."

"I will wait for your email."

### 6 Anchor (reference) the payment

**Present in 65% of attacks**

The majority of campaigns ask the target to 'reference' or 'code' the payment to the CEO's or company name, or as a generic "business expense", "admin", "professional services" etc.

"Code to administrative expense"

"I need you to put my name as a reference for this payment."

"... under my personal expenses"

### 7 Promise a follow-up

**Present in 28% of attacks**

Often the attacker will make an excuse for why an invoice is not present, and promise it by a certain time to keep the target from validating with other staff before making the payment.

"I will email invoice soon as I get to my computer

"... once I am done with my meeting"

### 8 Apply pressure

**within 90 minutes**

If the target has responded to more than one email, but has not sent back confirmation of payment, the attacker will typically follow-up with a further email that applies pressure.

"What is the status of the payment I requested?"

"Have you gotten the payment processed? Please advise."

Over time, templated campaigns have grown less effective as finance professionals learn how to spot payment fraud.

As a result, attackers have had to step up their game. Researchers have noted advertisements for copywriters and graphic designers in the same online forums used to trade in malware or recruit researchers and money mules. Today, your organisation should expect to see requests for payment that borrow from key features of your branding and exhibit some level of knowledge of your business processes.

### Cash-out

If you realise you have been tricked into making a payment it is critically important to call your bank as soon as possible (CBA's business clients should call the CommBiz helpdesk on 132 339) and loop in your account manager. It's also important to register the fraudulent request for payment with law enforcement.

Your bank will act immediately to attempt to freeze and/or recall the stolen funds, but has a finite amount of time in which to act before attackers have moved or extracted the funds.

# Deep Dive

## Email Spoofing

**For CommBiz customers:** If you have made a payment in error

**1.** Call CommBiz helpdesk immediately on **132 339**
**2.** Contact your account manager, and
**3.** Contact Law Enforcement.

### Mitigations for Email spoofing

Humans – and technology – are fallible, and each can equally be used to audit the other. Your business processes should assume that email can be forged and that your staff may be tricked into paying an attacker. The best mitigation for payment fraud that makes use of spoofed emails is to adhere to industry standard processes for making and authorising payments:

**1.** Make use of multiple authorisers for payments and enforce strict separation of duties.

**2.** Require large payments or change of beneficiary details to be verified via checks in alternative channels. No payment should be authorised on the basis of a single email.

**3.** Train staff to question and escalate payment requests that look suspicious.

**4.** Whitelist use of your domain for sending email (using Sender Policy Framework contract to SPF/DKIM and DMARC).

### Figure 6: Subject Lines and body text of whaling emails


The top word cloud represents the most common words used in the SUBJECT LINES of whaling emails. They include several notable features. The subject line will often:

- Introduce a sense of urgency ("urgent", "due", "important", "required")
- Inquire as to how the organisation's payments process works ("balances", "funds" "finance")
- Use American terms e.g. "Wire Transfer"

The bottom word cloud represents the most common words used in the BODY TEXT of whaling emails. On first glance, the word cloud reveals that the contents of these scams reflect words you might expect in legitimate requests for payment.

*Source: Signals Q4 2016*

### Figure 7: How to spot email payment frauds

**The request claims to be urgent and/or confidential;**

**You are requested to ignore standard payment authorisation processes;**

**The request includes grammatical and spelling errors;**

**The type of request and the language and formatting are unusual for the supposed sender;**

**The 'reply to' email address is different to the sender's address.**

*Source: Signals Q3 2016*

# Deep Dive

## Business Email Compromise

*How to protect your email account from profit-motivated criminals*

While the number of fraudulent payment requests that employ spoofed emails has not slowed over the last 12 months, there has been a steady rise in the number of Australian businesses that have made payments to attackers after a compromise of their email account or that of an entity they do business with.

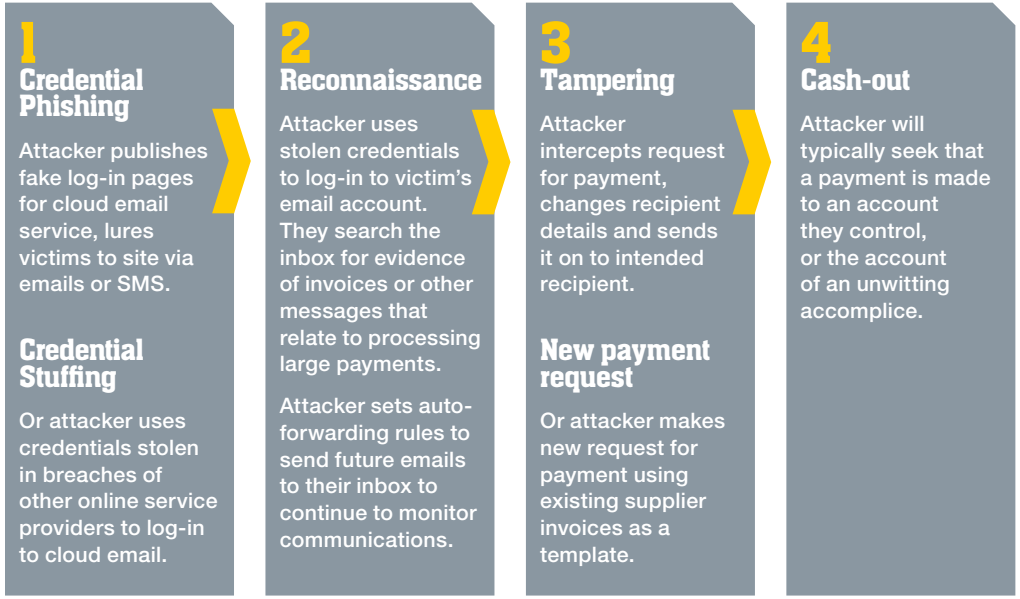
This form of payment fraud is typically coined 'Business Email Compromise' – and is growing more prevalent as organisations shift their corporate email to cloud-based services. Many have made this transition without implementing controls to compensate for exposing inboxes to the public internet. (Without additional configuration, unauthorised access to a cloud-hosted email is only a stolen username and password away). Cybercriminals have seized on this new opportunity, and the range and sophistication of scams that involve unauthorised access to email accounts has risen dramatically.

### Initial compromise

A business email compromise attack would typically play out as outlined in Figure 8:

Today, there are several billion pairs of previously stolen credentials (usernames and passwords) available to attackers on the black market, with fresh streams of credentials offered up for sale at low prices on a routine basis. These credentials are typically stolen in one of two ways: via phishing campaigns or via data breaches of other online services.

**Figure 8: Business Email Compromise**




Perpetrators of credential phishing campaigns create web sites that mimic the branding of legitimate log-in pages and send spam campaigns that try to convince legitimate users of those services to enter their credentials.

Numerous phishing web sites are set up to imitate cloud-hosted email services offered by Google and Microsoft on a daily basis, just as they are for banks and other popular online service providers. They are typically blacklisted or forced offline within hours, but not before a number of users have been tricked into providing the attackers their credentials. Credentials harvested in phishing campaigns are often sold to other criminals whose intent is to commit fraud.

Credentials stolen in past data breaches, on the other hand, are sometimes used by attackers to attempt to access cloud-hosted email accounts in what we call credential stuffing or password re-use attacks. The attacker might attempt to use usernames and passwords stolen in attacks on other online service providers on the basis that

**Top 3 events that lead to fraud losses:** *Source: Signals Q3 2017*

1. 'Spoofing' an email address to request payment
2. Unauthorised access to an email inbox
3. Unauthorised access to accounting software or bank account

**One in four losses**
involved the compromise of a cloud-based email account.

Microsoft has reported a
**300% increase**
in phishing campaigns that imitate its cloud services... and a
**44% increase**
in attempts to break-in to accounts using credential stuffing.[iv]

# Deep Dive

## Business Email Compromise

> “because human memory is generally poor – **we often re-use passwords across multiple online services**”

people often re-use passwords for multiple services. They tend to find a high success rate when using credentials stolen from a social networking service, for example, to log-in to cloud email services like Microsoft Office365 and Google G-Suite, or online accounting software.

In both cases, attackers rely on fundamental human flaws. When a phishing email triggers our sense of alarm or urgency, users will willingly share user credentials before checking the authenticity of a web site. And because human memory is generally poor – we often re-use passwords across multiple online services. Both of these habits can get us in a lot of trouble.

### Malware and business email compromise

As we've discussed, most Business Email Compromise stems from poor credential management on the part of the victim. We have come across several cases, however, in which attackers were able to access a corporate mailbox after infecting a device with malicious software (malware).

While out of the scope of this work, we make the following observations about payment fraud resulting from malware infection:

- The variants of malware used in these attacks are commonly referred to as Remote Access Trojans or RATs. While there are dozens of RATs on the black market, the varieties used for Email Payment Fraud are affordable, stable, cross-platform and often include modules that focus on stealing Outlook credentials.

- While there are several techniques attackers use to infect devices, the most common vectors for these RATs are:
  - *via email file attachments,*
  - *via emails that direct the victim to click on a link to a compromised web site, or*
  - *via offers of fake mobile apps*

The best advice for mitigating malware infection is made available by the Australian Signals Directorate's Essential Eight and Top 35 mitigation strategies.[v]

### Reconnaissance and tampering

Once a fraudster has gained access into an email account, they will search the Inbox and Sent Items folders for invoices, purchase orders or other documents and messages that relate to processing large value payments.

The attacker aims to play 'man in the middle' between any two parties establishing the details of a transaction over email. Ideally they are looking for large value payments between two companies, but have been known to tamper with payment details for other large transactions between individuals and small businesses, such as property settlements.

Attackers will seek to intercept and tamper with existing invoices to replace the bank account details listed for payment, or email customers from a compromised account advising of new account details for future payments. If the account they hack into belongs to a person with purchasing authority, they might simply demand a subordinate make a payment on their behalf.

In many attacks we've analysed, fraudsters have demonstrated patience in order to increase the possibility of netting a large payment that goes undetected for long enough to successfully extract the victim's cash from money mules. They refer to these scams as the "long con", and will monitor an inbox for some time while waiting for a large payout opportunity. Often the attackers set up mail forwarding rules to automatically send messages to the webmail accounts they log into more regularly.

### Cash-out

If you realise that your inbox has been compromised, check your bank statements immediately to ensure payments were made

### Who is attacking us?

Research by SecureWorks and Trend Micro note that Business Email Compromise – in which attackers hack an email system as a precursor to tampering with payments – is a mature industry in West African countries like Nigeria, where employment prospects are otherwise slim. These criminal networks consist largely of graduates from simple social engineering scams. These actors have grown more patient, and are prepared to invest in malware (such as remote access trojans) or in buying access to stolen user credentials from phishing campaigns. While perpetrators are by no means limited to West Africa – indicators from many of the attacks we've seen (even those that originate in Asia) are very similar to practices West African cybercriminal groups are renowned for.

### What payments are at risk?

*Any payment arranged over email:*

- Invoices between suppliers, especially among tradesman, engineering and construction firms, manufacturing and distribution.
- Payments to staff (payroll).
- Beneficiaries of property sales (trust accounts) or payment of rent.
- Beneficiaries from the sale of expensive items (vehicles etc.)
- Beneficiaries from settlement of a will.
- Beneficiaries from tax refunds.

*Source: Signals Q3 2017*

# Deep Dive

## Business Email Compromise

> “Multi-factor authentication **limits attackers from accessing a service** using only a stolen username and password”

### More information

- Microsoft’s security best practice for O365
- Google’s security best practices for G-Suite
- Microsoft’s guide to detection of an attack
- Microsoft’s guide to triage of a compromised O365 account
- Google’s guide to detection and triage of a compromise G-Suite account

### Strategies for protecting your cloud email

*Source: Signals Q3 2017*

#### 1: Theft of Credentials

| METHOD OF ATTACK | ESSENTIAL DEFENCE | ADVANCED DEFENCE |
|---|---|---|
| Attackers acquire user credentials stolen in phishing campaigns. | **1.** Multi-factor authentication limits attackers from accessing a service using only a stolen username and password.<br>**2.** Password Wallets/Managers help users create unique and complex passwords for every service they use.<br>**3.** Enforce password policies that lock a user out for a period of time after a number of failed attempts. | Consider deploying physical security tokens for multi-factor authentication on high-risk workstations. |
| ‘Credential stuffing’ – attacker tries usernames and passwords stolen in other data breaches to log in to your email account. | | |
| Attackers infect a user’s device with malware to steal credentials. | **1.** Set web browsers to automatically update and keep operating systems patched.<br>**2.** Ensure users operate as the least privileged user (not admin/root).<br>**3.** Filter web traffic (via internet security software/antivirus.)<br>**4.** Implement security awareness programs. | Talk to your relationship manager about whether NetLock is appropriate for your business. |

#### 2: Unauthorised access to email account

| METHOD OF ATTACK | ESSENTIAL DEFENCE | ADVANCED DEFENCE |
|---|---|---|
| Attacker is able to log-in using stolen credentials on an account that is not protected by multi-factor authentication. | Use the ‘Conditional Access’ rules offered by Microsoft Office365 and Google G-Suite.<br>While their approaches vary, these rules allow an administrator to set conditions of access according to whether the user is inside or outside the enterprise network, whether they are on managed or unmanaged devices or according to a set of whitelisted IPs addresses, for example.<br>For any combination of these scenarios, rules can be set to accept, deny or force a multi-factor challenge for access to the inbox. | Microsoft offers additional rules-based and machine learning algorithms to detect and block anomalous log-in behaviour as a premium (paid) service.<br>Google uses a range of machine learning-based detection into its standard G-Suite offering. |
| Attacker is able to log-in using stolen credentials of an administrator’s account that is not protected by multi-factor authentication. | | Limit the number of accounts that require ‘global’ or ‘super user’ administrative access.<br>Microsoft offers a premium (paid) privileged access management solution. |

#### 3: Reconnaissance of the inbox

| METHOD OF ATTACK | ESSENTIAL DEFENCE | ADVANCED DEFENCE |
|---|---|---|
| Attacker sets mail forwarding rules to send mail to their own account. | Consider conditional formatting mechanisms that distinguish (through colours or alerts) when email is being sent to or received from internal versus external domains.<br>If users report any strange behaviour in their inbox, check if any mail forwarding rules have been applied. While these can usually be seen in the user interface of Office 365, administrators should also check under the hood using PowerShell commands. | Microsoft offers additional rules-based and machine learning algorithms to detect and block anomalous mail forwarding behaviour as a premium (paid) service. |

#### 4: Fraudulent request for payment

| METHOD OF ATTACK | ESSENTIAL DEFENCE | ADVANCED DEFENCE |
|---|---|---|
| Whaling attack (attacker impersonates staff with purchasing authority and requests a payment) | Ensure your payments authorisation process “assumes compromise”:<br>**1.** Make use of multiple authorisers for payments and enforce strict separation of duties for payments.<br>**2.** Require large payments or change of beneficiary details to be verified via additional checks in multiple channels. No payment should be authorised on the basis of emails from a single account.<br>**3.** Education your treasury and accounts teams in how to recognise Email Payment Fraud. | |
| Attacker impersonates a supplier (or other party to a transaction) and requests a change of beneficiary details or submits a new invoice. | | |

#### 5: Fraudulent payment is made

- Contact the CommBiz helpdesk and your relationship manager immediately.
- Report the matter to the Police.
- Use the following guides to triage of compromised accounts provided by Google and Microsoft.

# Deep Dive

## Business Email Compromise

**For CommBiz customers:** If you have made a payment in error

**1.** Call CommBiz helpdesk immediately on **132 339**
**2.** Contact your account manager, and
**3.** Contact Law Enforcement.

to the right beneficiaries. If you discover that invoices have been tampered with, it is critically important to call your bank as soon as possible (for CBA's business customers - the CommBiz helpdesk is on 132 339) and loop in your account manager. It's also important to register the payment with law enforcement.

Your bank will act immediately to attempt to freeze and/or recall the stolen funds, but has a finite amount of time in which to act before attackers have managed to move or extract the funds.

### Mitigations for Business Email Compromise

First, ensure that an attacker requires more than just your username and password to access your email account. Most web services offer consumers two-step verification as an optional measure to protect access to the service. This challenges users to authenticate (prove their identity) in more than one channel before they can access a system. Typically it takes the form of a one-time code sent to the user's enrolled mobile device at the time of log-in.


Remote access to critical services – such as business email, accounting software, your payroll processing bureau, or any privileged access, require the next level of protection: multifactor authentication.

Multifactor authentication requires the user to combine something they know (a username and secret password on a web interface, for example) via one channel, and confirm with something they have (such as a physical token) or something they are (a biometric identifier) in another.
Most business-grade cloud email services also offer Access Control Lists that restrict access to an account under certain conditions, such as within a trusted IP range.

It's also important to think about how you would prevent fraud even if your email inbox were to be compromised. This requires the organisation to set up payment processes that don't rely exclusively on email as a channel for raising and authorising payments.

### Assume attackers will attempt to access your email accounts

**Enable multi-factor authentication on email and accounting software.**

**Use access control lists (conditional access rules) for cloud-based email.**

This restricts access to a given account to specific IP addresses, for example.

**Enforce password policies that:**

**a)** Require long and complex passwords and ban obvious or frequently used ones.

**b)** Temporarily lock-out users after several failed log-in attempts.

**Teach staff how to identify phishing campaigns.**

## Endnotes


**i:** https://www.ic3.gov/media/2017/170504.aspx

**ii:** https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

**iii:** https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/commbank-signals-q4-2016.pdf

**iv:** https://blogs.microsoft.com/microsoftsecure/2017/08/17/microsoft-security-intelligence-report-volume-22-is-now-available/

**v:** https://www.asd.gov.au/infosec/mitigationstrategies.htm

**vi:** https://www.ic3.gov/media/2017/170504.aspx

**vii:** https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

**viii:** https://www.commbank.com.au/content/dam/commbank/assets/business/can/business-insights/signals/signals-q3-2017.pdf


CommonwealthBank

# The 60-Minute Security Challenge

*Six things you can do in an hour for better security:*

Our busy professional lives leave little time for personal admin. All of us are probably guilty of putting off a security update or refreshing our passwords to a rainy day. So the team behind *Signals* set ourselves a challenge: what advice would we give to somebody that only had one hour to press 'reset' on security? Here's what we came up with:

- Check if your passwords have been stolen in (known) data breaches. Type in the email address you use to sign up for online services at https://haveibeenpwned.com
- Set up two-step verification for access to your online accounts, where available. This will require you to enter a short code sent to your mobile device after you've typed in your username and passphrase.
- Scrap passwords. Replace them with passphrases. Passphrases beat passwords for length and complexity, and computers trump humans for remembering them. So maybe try out a Password Manager?
- Switch on automatic updates for your web browser(s). Your browser is your first line of defence against many online threats.
- Back up your data – keep backups both online and offline. You can never be too careful.
- (Still awake?) Time to update your operating system. This, we admit, might take some time. So go get some fresh air - you've done great.