eftsure

email scams

/How vulnerable are you?

Business Email Compromise (BEC) continues to plague businesses around the world.

The FBI's Internet Crime Complaint Centre says losses from BEC scams topped $12billion globally. In the US alone BEC related losses were US$1.3billion in 2018, almost double the previous year.

Australia had the world's 5th highest number of reported victims behind the US, India, UK and Canada which is staggering given the size of the Australian population relative to the rest of the world.

A report released by the Australian Competition and Consumer Commission (ACCC) in May reveals that losses to "false billing" scams increased by 97% in 2018. And it attributed a large portion of these to BEC.

97%

of losses attributed to "false billing" scams

> **"This is a very sophisticated scam, which is why many businesses only realise they've been caught out once it's too late..."**

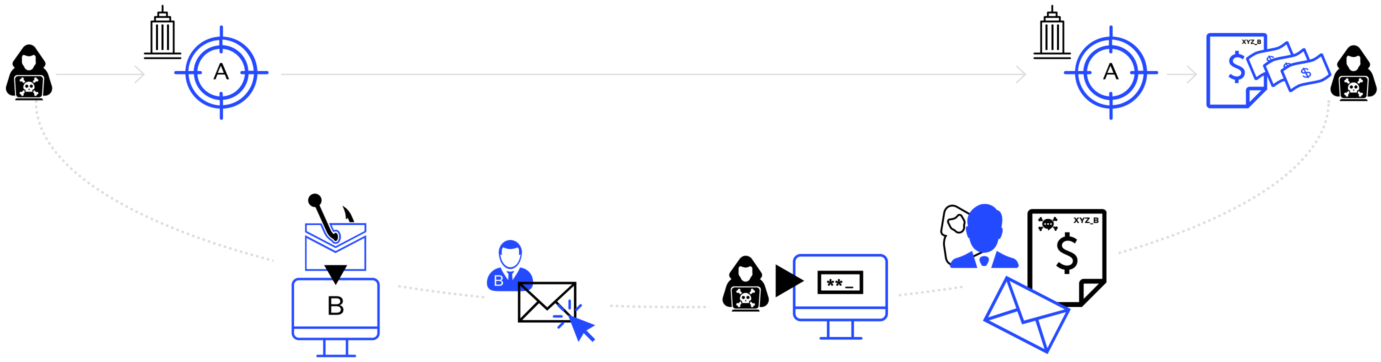
Says ACCC deputy chair Delia Rickard.

The rising figures show that BEC scams, while usually technically simple, are highly effective. Indeed, it takes just one employee – and not necessarily your own – to only be duped once into clicking on a suspicious email link to facilitate an attack.

BEC losses are so significant primarily due to the simplicity and ease of attack combined with the increasingly high difficulty of staff discerning the difference between real and fake emails. Since it is so lucrative, it has led to these attacks being systematically designed and run by organised crime operating businesses with employees trained to perpetrate fraud.

Here's how two dangerous forms of BEC work:

#1 Supplier Email Compromise



Fraudster wants to target a company... (**Target Co A**)

Instead of attacking **Target Co A**, **Fraudster** sends phishing email to a supplier (**Supplier Co B**)

Employee at **Supplier Co B** clicks on email and logs in to a fake site

Fraudster uses details to gain access to **Supplier Co B**'s email account

Fraudster sends finance team at **Target Co A** email informing of change in Bank details and/or an invoice with a new bank account number

Target Co A pays invoice, but money goes to **Fraudster**, not **Supplier Co B**

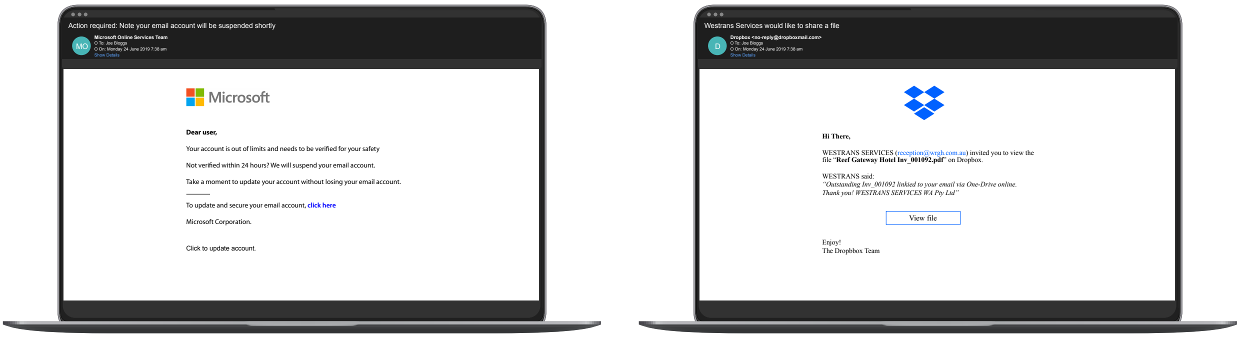
The Fraudsters

More likely sophisticated, skilled and resourced organisations than anarchic 'hackers' – have a target organisation or several target organisations in mind. However, they don't try attack those target companies directly. Instead they set out to deceive them by first infiltrating the email systems of target companies' suppliers and then use that access to imitate the supplier company and send the target company, seemingly authentic but fraudulent communication. There are three steps in this scam.

1 Step one:

Phishing for login credentials.

Criminals send an email to your Suppliers' principals or employees that appears to be from an organisation they are likely to know and trust – for example, it may look as if it's from a bank, utilities company, Microsoft, Netflix, Dropbox or even The Australian Tax Office.



Action required: Note your email account will be suspended shortly

Microsoft Online Services Team
To: Joe Bloggs
On: Monday 24 June 2019 7:38 am
Show Details

Microsoft

Dear user,

Your account is out of limits and needs to be verified for your safety

Not verified within 24 hours? We will suspend your email account.

Take a moment to update your account without losing your email account.

To update and secure your email account, **click here**

Microsoft Corporation.

Click to update account.

Westrans Services would like to share a file

Dropbox <no-reply@dropboxmail.com>
To: Joe Bloggs
On: Monday 24 June 2019 7:38 am
Show Details

Hi There,

WESTRANS SERVICES (reception@wrgh.com.au) invited you to view the file "**Reef Gateway Hotel Inv_001092.pdf**" on Dropbox.

WESTRANS said:
"Outstanding Inv_001092 linkied to your email via One-Drive online.
Thank you! WESTRANS SERVICES WA Pty Ltd"

Enjoy!
The Dropbbox Team

Examples of phishing emails, the first step in a BEC scam.

The email will incorporate these organisations' branding, logos and headers and have an almost identical looking domain address. It will often have a message that evokes sufficient concern and urgency for the recipient to respond and login: e.g "**Your account will be suspended in 24 hours due to non-payment or suspicious activity and you need to login to resolve this.**"

Most people receiving such an email would ignore it. However, a small number may be concerned and respond by clicking on the link which then takes them to a legitimate looking (but fake) site. When the concerned and deceived user enters their login and/or other details on that site, those details are captured and sent to the fraudster.

Out of the hundreds, thousands or hundreds of thousands phishing emails they send out, the fraudsters only need one person to fall for it.

Fraudsters can execute this first phishing stage of the Supplier Email Compromise in a strategic and targeted capacity or a more broadcast approach. If the fraudsters take a **targeted approach**, they will research a target company and determine its related supplier organisations and then selectively phish email login credentials from employees at those specific companies. In a more **broadcast approach** they can simply send out hundreds of thousands of phishing mails and then work back to determine a supplier of a large company.

> “Out of the hundreds, thousands or hundreds of thousands of emails they send out, the fraudsters only need one employee to fall for it”

2 Step two:

Infiltrating and monitoring.

Once the crooks have received the login credentials of an employee at a supplier company they can easily access that suppliers' email system. Once inside the supplier's email system, fraudsters will likely monitor correspondence between the supplier company and employees at the original target organisation. They do this to learn about the users' email style and habits. The more advanced attacks will set up rules and filters that look for keywords such as 'payment', 'invoice', 'account' or 'bank'. When these rules are triggered (for example, when a real invoice is requested), the email is diverted to the hackers instead.

3 Step three:

Interception and imitation.

Now aware that the supplier is about to issue an invoice to the target company, the criminals will use easily available software to doctor that invoice so that it still looks like it's from the real supplier and send it to the target company. They may add their own bank details, hoping you will pay into that account, or they may say: "**Our bank account details have changed. Please use make payment into our new account (which is their account).**" They also change the phone number on the invoice to a number that will reach them instead of the real supplier in case the target company calls to check. To pre-empt the call, the fraudsters sometimes even call the target company ahead of sending the compromised email to advise the target that they are calling them to let them know they have changed their details. They typically say that because there is so much fraud in this area, they are calling to allay their concerns.

In order to create a greater sense of authenticity, the fraudsters will often use the same language and style of your supplier's previous email communication, even imitating idiosyncrasies such as slang or colloquialisms. The seemingly real but compromised email will often contain the email trail of all your previous correspondence. If you remain suspicious and mail the supplier back to double check whether their bank details have indeed changed, your supplier probably won't get that email. This is because the fraudsters have inserted filters into your supplier's email system so the queries you send are diverted back to the hackers and they will again reply to you, again imitating your supplier.

It's important to note that the compromised supplier email's come from the supplier's legitimate email address. They are, in fact, authentic emails however they contain fraudulent details.

Recently, the owner of homewares business Sage & Clare fell foul to this step of a BEC scam, **losing $10,000** when she placed an order with a long-term supplier in China. For about three to four months she was actually exchanging emails with the scammers and not the suppliers themselves. Just before she had to make the final payment for the order, she was told the supplier had changed its bank account due to auditing issues. She later found out that the order and the $10,000 she paid had gone to the crooks.

#2

Executive Email Compromise

In this scam, sometimes called CEO or Executive Fraud , fraudsters follow a similar overall approach to Supplier Email Compromise but here the goal is not to impersonate a supplier. Rather, the fraudsters aim to impersonate someone of status and authority in your own organisation with the goal of instructing a more junior employee to make fraudulent payment

Step one:
Phishing for login credentials.

Using the same monitoring and phishing email tactics used in Supplier Email compromise, the fraudsters gain access to your organisations email system. While they may use other forms of hacking, given companies' pervasive use of both email and connected applications, phishing is relatively simple and only relies on a single person to be deceived to lead to broader access that enables the scam.

Step two:
Infiltrating and Monitoring.

Once they have login credentials to your organisations' email system, they can monitor emails between staff members involved in the payments lifecycle. While in Supplier Email Compromise they are aiming to observe and learn the timing and language of communication between suppliers and customers, here fraudsters are observing your own internal payment authorisation habits and protocols.

Step three:
Imitating and Instructing.

Once they've identified the chain-of-command and the correct protocols, the fraudsters will imitate a senior executive, perhaps the CFO or CEO, and at a relevant time, instruct a targeted junior staff member (likely in the Finance Department) to make a payment into a bank account belonging to the fraudster. As with Supplier Email Compromise, the email comes from the senior executive's legitimate email address and does not contain any malicious attachments or obvious signs of fraud.

Fraudsters will often create a sense of urgency around the payment – for example, making their demands near the end of the working day or week. And, abusing the authority of the senior executive they are imitating, may even threaten serious consequences if payment isn't made.

Many attacks are timed when the executive being imitated is traveling (ideally internationally) and the email is sent just prior to the executives' flight departure. The fraudsters determine the travel schedule from the compromised email account and calendars. The goal is to time the sending of the email such that if the employee being asked to make a transfer wishes to call to confirm, the executive will be unavailable as he/ she will be on a flight.

In a case report by the Australian Cyber Security Centre (ACSC), cybercriminals posed as the CEO and Chief Operating Officer (COO) of a large business and then sent a spoofed email, purporting to be from the CEO (who was travelling at the time), requesting a large payment be made by the financial controller.
A second email, purporting to be from the COO, was then sent to the financial controller. **This email contained a false email trail approving the CEO's request for payment**.

Not realising the request was a scam, the business made two payments to the cybercriminal's overseas bank accounts,, one for over US$200,000 and one for almost US$300,000.

Social engineering rather than technological wizardry

While BEC (whether Supplier Email Compromise or Executive Fraud) is a pervasive and rapidly growing cybercrime, it relies more on social engineering and manipulation than cyber dark arts.

Fundamentally, BEC exploits the identity problem of a digitally connected world: **our inability to determine exactly who is on the other side of the computer**. Furthermore a key point to note is that whilst a business owner or CFO can control exactly how they process payments themselves (although they still can be fooled), they have less control over their own employees' behaviour and usually no control over their supplier's processes. No matter how stringent the security around the business itself is, the vulnerability lies in the numerous email accounts of employees of all their suppliers ; a domain completely beyond a business's control.

The point of payment problem and difficult recovery

Losses resulting from BEC and electronic payments are extremely difficult to prevent and recover.

Australian banks do not verify that BSB and account numbers match account names at the point-of- payment. So, if the payment has been made into the wrong account, the banks do not detect or signal it. BEC attacks exploit this fact – they change bank account details but leave the Payee name the same. The person making or authorising the payment therefore checks the name and amount against an invoice and these are correct. What they often don't realise is the bank completely ignores the name and relies solely on the BSB and account number. This means even if the account name is correct, it is irrelevant and makes no difference if the account number is wrong.

In addition, banks are not liable to recover the money should an erroneous or fraudulent payment be made. That's because you, the user, **authorised** the payment and why, in many countries this type of fraud is called Authorised Push Payment Fraud (APPF).

And, thanks to the launch of the New Payments Platform, Australians can now send money in "real time" – a change cybercriminals no doubt welcome because they can quickly take the money and run if their scam succeeds.

Plus, the fraudsters may be operating in foreign countries which may not be willing to cooperate with Australia. **The Australian Federal Police has no authority to carry out inquiries in a foreign country without approval through official government channels**.

What can you do about it?

1 Gain awareness and promote a security conscious culture:

Attend cyber events, subscribe to some of the many security newsletters available online and distribute this information to your employees, colleagues, customers and suppliers.

Different government departments, such as the Australian Cyber Security Centre, provide information and tips on how to mitigate cybersecurity risks.

Certain cyber security firms – such as Kaspersky – can develop and run simulations and games which are both fun and educational for everyone in the organisation.

Crucially, encourage and then make it safe for staff to question any payment instructions that don't 'look right', even if they are from very senior executives or trusted suppliers.

2 Review your company practices:

In particular, look at your password and other security controls. Strengthen your company's passwords by making them longer and more complex. Certainly do not share passwords across multiple sites or permit weak passwords.

A two-step authentication of a user's identity should be implemented on all apps – including in particular email systems. It's a simple and powerful measure.

Identity management tools are also effective.

3 Enforce protocols in finance teams:

These include the separation of duties and independent verification for changes to bank details. Never trust or rely on emails for bank account changes. And any all new supplier additions or changes should be checked via a call back to the supplier, again using an independently sourced phone number.

Restrict and isolate access to ERP modules and applications. Only give certain people the access that they need.

Finally, set-up exception reporting in your ERP wherever possible.

4 Create and enforce policies:

Recognise that employee email accounts are gateways to highly sensitive information and attacks. So your policies might, for example, restrict what information can be kept in email inboxes and for how long it can be kept before securely archiving it.

Set up email alerts for exceptional incidents. This can be set up on most modern email systems might alert you if someone from another country, say logs into your system or if your account is sending out large numbers of emails in a short period.

Promptly remove access to your system once freelancers, consultants and staff have left the company.

5 Use tools to secure and verify details throughout the payment lifecycle:

Verify all suppliers at all key points throughout the payment lifecycle – that is, at the stages of supplier onboarding, supplier changes and maintenance, payments-file upload and at the point of final payment.

There are, however, few systems or tools that cover the entire payments lifecycle. Secure supplier onboarding processes may lack automation and automated ERP supplier onboarding may lack security features.

The eftsure solution:

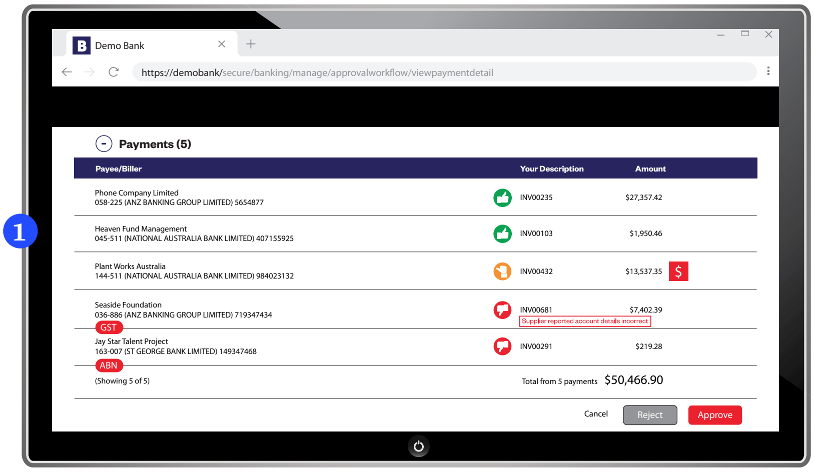
eftsure's unique Know your Payee solution does what other systems cannot: it provides real-time supplier verification and alerts throughout the payment lifecycle: at the point of supplier onboarding, through supplier changes, prior to uploading a payments file and finally at the Point of Payment; in your banking environment.

In doing this, eftsure is unique in its ability to mitigate the risk of loss due to Business Email Compromise be it Executive Fraud or Supplier Email Compromise.

eftsure operates throughout the payment lifecycle:

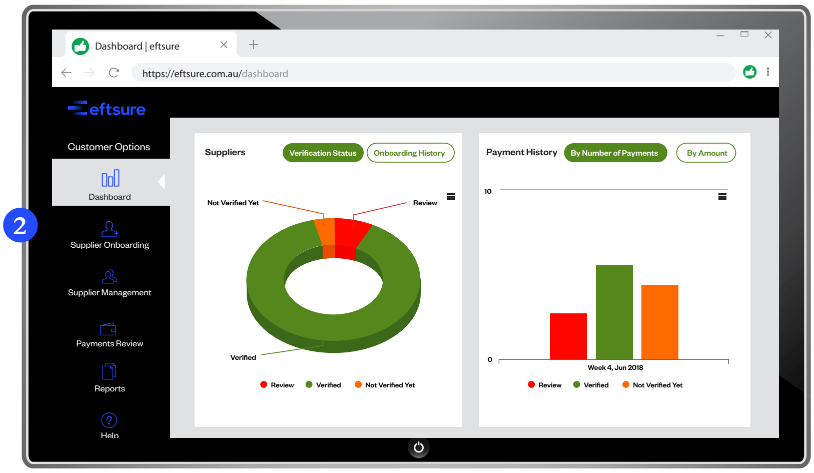
1. At Point of Payment eftsure provides simple, powerful traffic light alerts indicating supplier verification (or lack thereof) and tax compliance.

2. When onboarding suppliers, eftsure's online portal provides a secure and streamlined way to add new suppliers, update existing supplier details and a live dashboard view of their status.


1
B Demo Bank
https://demobank/secure/banking/manage/approvalworkflow/viewpaymentdetail

Payments (5)

Payee/Biller		Your Description	Amount	
Phone Company Limited 058-225 (ANZ BANKING GROUP LIMITED) 5654877	👍	INV00235	$27,357.42	
Heaven Fund Management 045-511 (NATIONAL AUSTRALIA BANK LIMITED) 407155925	👍	INV00103	$1,950.46	
Plant Works Australia 144-511 (NATIONAL AUSTRALIA BANK LIMITED) 984023132	✋	INV00432	$13,537.35	$
Seaside Foundation 036-886 (ANZ BANKING GROUP LIMITED) 719347434 GST	👎	INV00681 Supplier reported account details incorrect	$7,402.39	
Jay Star Talent Project 163-007 (ST GEORGE BANK LIMITED) 149347468 ABN	👎	INV00291	$219.28	
(Showing 5 of 5)		Total from 5 payments	$50,466.90	



eftsure

To find out more contact:

info@eftsure.com.au

Visit: **www.eftsure.com.au**