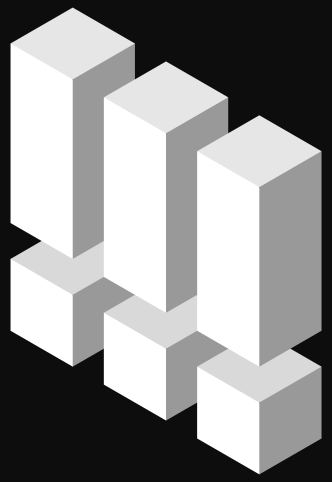
THE TRIPLE THREAT TARGETING YOUR INBOXES THIS EOFY



mailguard

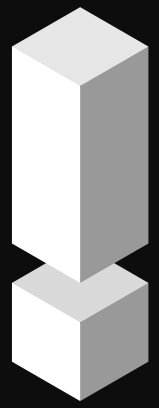
The **End of Financial Year (EOFY)** is a period notorious for finance and tax-related scams affecting business worldwide.

At this time of year, it's not uncommon for employees to receive fraudulent emails with malicious invoices spoofing suppliers in their inboxes, or even phone calls impersonating tax agents asking for confidential data.

But this year, things are expected to be even more treacherous.

As if times aren't already tough enough, this year represents a triumvirate of cybercrime threads, with each one increasing the likelihood of businesses falling victim to a scam.

1. COVID19



The COVID-19 scam explosion

Over the past few months, numerous organisations and agencies – including the intergovernmental Financial Action Task Force, UK Financial Conduct Authority, Dubai Financial Services Authority, and U.S. Financial Crimes Enforcement Network—have stressed the need for all businesses to be vigilant against new and emerging illicit finance scams that have been exploiting the COVID-19 pandemic.

The economic uncertainty triggered by the pandemic has led to the introduction of various new measures to help businesses manage cash-flow and retain employees. While these financial relief measures and economic stimulus packages are welcome responses to the ongoing crisis, they also present huge opportunities for criminals.

And they come at a time when everyone is under extreme stress, distracted and in many instances working remotely, often on less secure personal devices and infrastructure.

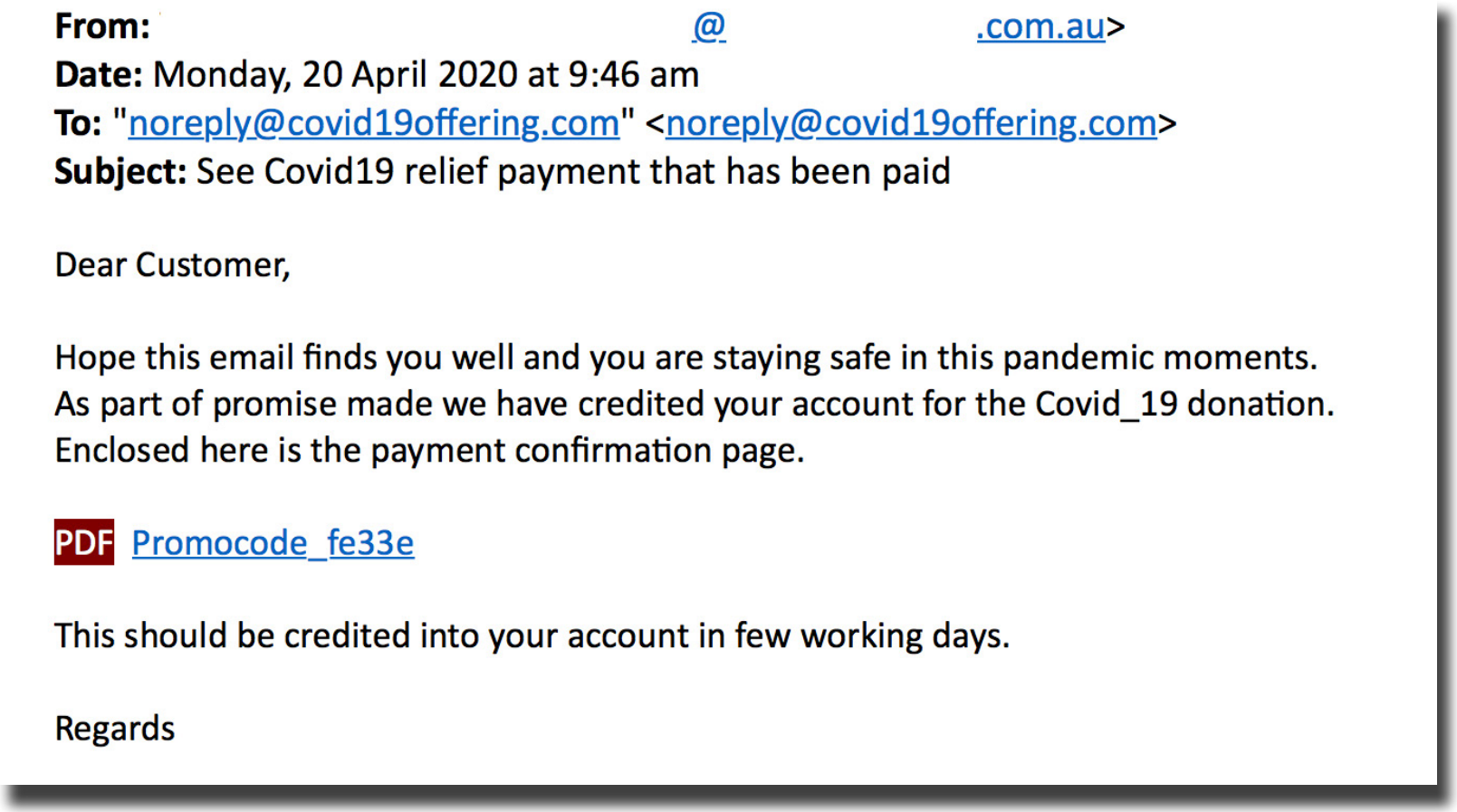
In the United States, it has been reported that scammers are posing as IRS representatives and tricking individuals to steal their COVID-19 stimulus payments. One way they are doing so is by issuing a bogus check, often in an odd amount, then telling victims to call a number or verify information online in order to cash it. Scammers are also telling individuals that they can get their Economic Impact Payment faster if they allow them to work "on their behalf."

Meanwhile in Australia, the federal government has allowed individuals early access to superannuation to minimise financial hardship, but those measures have been seized upon by nefarious actors.

Allegations of identity theft involving 150 Australians forced the government to pause the early release of superannuation, after police froze $120,000 believed to have been ripped off from retirement savings. It was reported that a "sophisticated" attack including an "intrusion into a third party" had allowed the impersonation of workers seeking early access of up to $10,000 superannuation each.

In another case, those seeking welfare payments from the Australian federal government were targeted via a phishing email impersonating Services Australia.

MailGuard, intercepted a similar scam email, that masqueraded as a “COVID-19 relief payment” to deliver malicious links. An image of the scam is featured below.



From: @ .com.au>
Date: Monday, 20 April 2020 at 9:46 am
To: "noreply@covid19offering.com" <noreply@covid19offering.com>
Subject: See Covid19 relief payment that has been paid

Dear Customer,

Hope this email finds you well and you are staying safe in this pandemic moments.
As part of promise made we have credited your account for the Covid_19 donation.
Enclosed here is the payment confirmation page.

PDF Promocode_fe33e

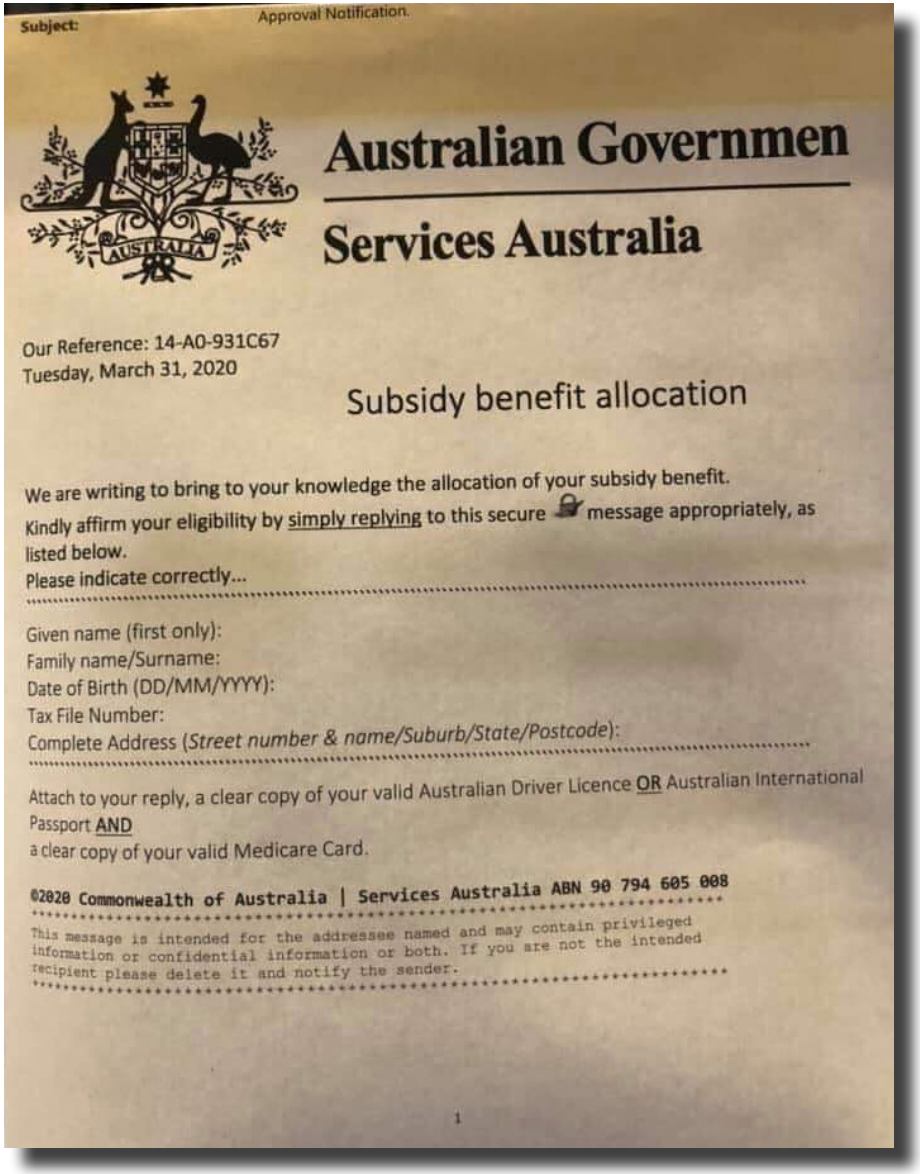
This should be credited into your account in few working days.

Regards

All these scams are dangerous, not only because they attempt to manipulate users already suffering from financial turmoil and difficulties triggered by the COVID-19 pandemic, but because like the measures they exploit, they are constantly evolving.

Criminals are, in fact, closely watching government announcements and are changing their scams within hours to reflect the latest information being issued – information that may not yet be familiar to businesses and/or professionals, such as that related to financial support, making it harder to discern whether that information is legitimate or not.

Featured right:
Phishing email impersonating Services Australia.
(Credit: 7news.com.au)



Subject: Approval Notification.

Australian Governmen

Services Australia

Our Reference: 14-A0-931C67
Tuesday, March 31, 2020

Subsidy benefit allocation

We are writing to bring to your knowledge the allocation of your subsidy benefit.
Kindly affirm your eligibility by simply replying to this secure message appropriately, as listed below.
Please indicate correctly...

Given name (first only):
Family name/Surname:
Date of Birth (DD/MM/YYYY):
Tax File Number:
Complete Address (*Street number & name/Suburb/State/Postcode*):

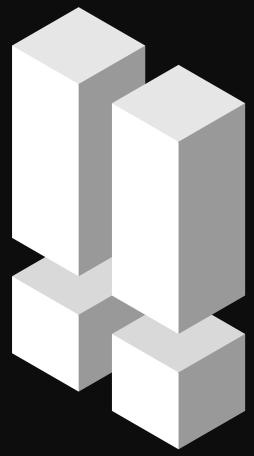
Attach to your reply, a clear copy of your valid Australian Driver Licence OR Australian International Passport AND
a clear copy of your valid Medicare Card.

©2020 Commonwealth of Australia | Services Australia ABN 90 794 605 008

This message is intended for the addressee named and may contain privileged information or confidential information or both. If you are not the intended recipient please delete it and notify the sender.

1

2. EOFY



The “administrative nightmare” facing businesses at EOFY

The EOFY period is characterised by stress and panic, with accounting and finance professionals working under stringent deadlines to complete financial reports, tax returns and to make sure all the necessary paperwork is sorted in accordance with respective taxation bodies.

This year, many companies are also finding themselves learning about new schemes and processes, for financial benefits and schemes that have been introduced to curb the economic challenges unleashed by the COVID-19 pandemic.

For many finance professionals, this has created a major stream of new work, with new rules, conditions and eligibility requirements.

It hasn’t been easy.

In Australia, for example, it has been reported that applications for the $130 billion JobKeeper program are creating “an administrative nightmare for businesses”, increasing stress levels and uncertainty. Finance, legal and accounting departments are among those facing intense pressure, having to navigate the complexities arising from the new measures in the middle of an already busy period.

That is perhaps why the Australian Taxation Office (ATO) has been called on to provide swift and extensive guidance on the government’s economic stimulus measures to help curb misinformation and to assist businesses. It’s also little surprise that the ATO and the Fair Work Ombudsman are reporting a rise in queries and complaints about issues arising from the pandemic, including those arising from the economic measures introduced.

Unfortunately, what makes things worse is the lack of easy answers that can help overcome the complexities of understanding and implementing these new measures – especially with scammers eagerly exploiting the confusion for their own financial gain.

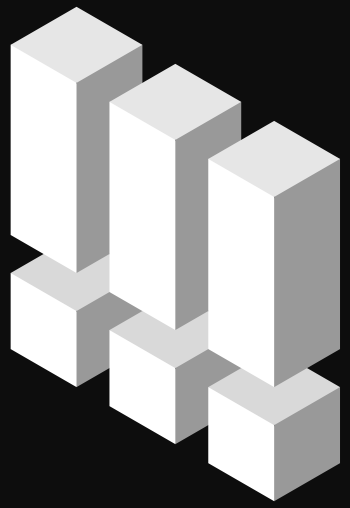
With remote working becoming the norm for many businesses, finance teams can no longer seek quick answers and guidance from colleagues by leaning across the table when, for example, someone on the phone, supposedly from a government agency, unexpectedly demands their company's banking details to wire a new relief payment (like what happened in the recent JobKeeper phone scam). Many government agencies and taxation bodies typically recommend calling their hotlines in these instances, but with the reported rise in queries and complaints, phone lines may end up being jammed, with long waiting times.

In addition, financial strains and resource limitations may accentuate frustrations. Reduced business hours, for example, may pose limitations for accounting teams when attempting to meet stringent deadlines for a new tax rebate, and the increasing termination of personnel in many businesses may make it harder to communicate and clarify relevant details.

All this increases the likelihood of scammers being able to successfully manipulate stressed, distracted minds and exploit them into doing their bidding – such as clicking on an innocent-looking phishing link, downloading a ransomware-ridden file, or revealing confidential business data over the phone.

Time-bound finance and accounting professionals, who are dealing with a large volume of financial data during EOFY, while navigating new & complex legal and business measures including payroll and taxation submissions, are particularly vulnerable to scams – and schemers are well aware of this.

3. TARGETED CYBER ATTACKS



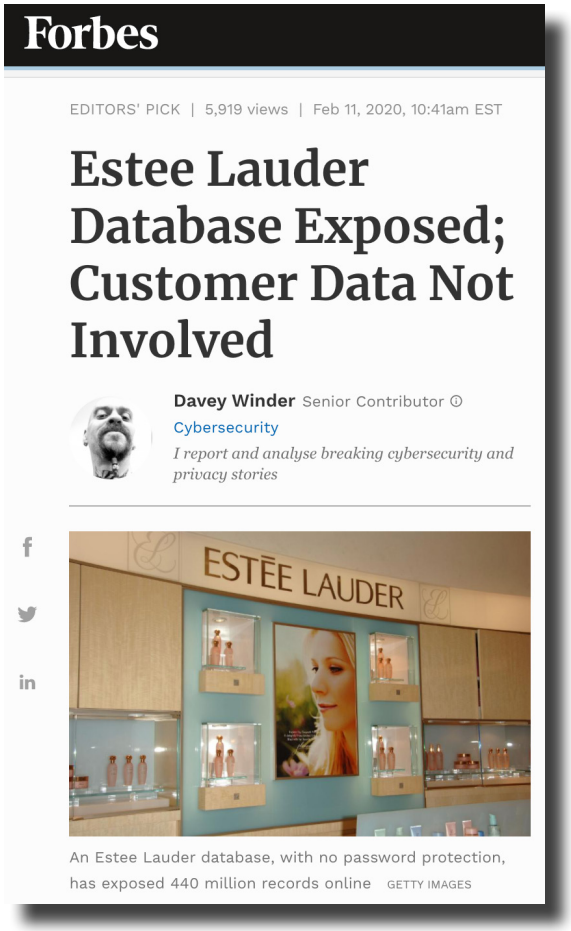
Targeted cyber-attacks continue to disrupt corporate giants

As we grapple with the current pandemic, and the enormous health and economic stresses that it brings to bear, cybercriminals are quietly launching sophisticated attacks that are, unfortunately, resulting in enterprise-wide disruptions. It is crucial that companies remain alert to the potential for sophisticated, targeted attacks.

There have been multiple reports this year of corporate giants from all industries falling victim to cyber-attacks. In February this year, Estée Lauder was embroiled in a data breach in which 440 million records were compromised. The following month, a total of 5.2 million Marriott Hotel guests were impacted when a hacker gained access to the accounts of two hotel employees.

The US Small Business Administration said in April that approximately 8,000 individuals who had applied for emergency business loans due to the COVID-19 disruptions had their information stolen in another data breach. Furthermore, in May, Swiss low-cost airline EasyJet revealed that the personal information of 9 million customers was accessed in a "highly sophisticated" cyber-attack on the airline.

Featured right:
Estee Lauder
Database Exposed
(Credit: Forbes.com)


Forbes

EDITORS' PICK | 5,919 views | Feb 11, 2020, 10:41am EST

Estee Lauder Database Exposed; Customer Data Not Involved

Davey Winder Senior Contributor
Cybersecurity
I report and analyse breaking cybersecurity and privacy stories

An Estee Lauder database, with no password protection, has exposed 440 million records online GETTY IMAGES

The former head of the Australian Cyber Security Centre, Alastair MacGibbon, also pointed out that l ocal government agencies and big Australian companies have recently fallen victim to cyber-attacks "with unprecedented visibility."

There have been several reports of cyber incidents on Australian organisations including logistics company Toll Group, mining firm BlueScope Steel, in government with Service NSW, and financial services company MyBudget, and even an attempted infiltration of the WA Premier's office. Mr MacGibbon warned that these targeted attacks are "just the tip of the iceberg"; many organisations fail to report cyber breaches, or worse, do not even know about them."

"The recent attacks are revealing in several ways. We are more used to seeing prominent US organisations being the victims of big cyber incidents, for example, Google or Equifax.

Although Australian organisations have always had cyber vulnerabilities, the increase in large attacks since mid-2019 shows we are increasingly visible and attractive to cyber attackers. The data is patchy, but we have observed an increase in attacks and a rise in the penetration of networks and targeting of confidential information," he writes.

Featured right: Recent cyber-attacks just the tip of the iceberg (Credit: afr.com)


FINANCIAL REVIEW

Exclusively for AFR subscribers.

Advertisement

Technology Cyber security

Opinion

Recent cyber attacks just the tip of the iceberg for Australia

Toll Group, BlueScope and Service NSW have all fallen victim to cyber criminals in recent days. The government and industry need to sharpen their response.

Alastair MacGibbon
Contributor

May 18, 2020 – 1.00pm

In a year already marred by natural and biological crises, cyber security failures remain a critical threat.

Staying safe from threats this EOFY

Global, disruptive events like the COVID-19 pandemic will always be the epicentre of fraudulent schemes, and when these new scams collide with an environment that's already made fragile by stressed and distracted professionals, it is a recipe for disaster.

While the convergence of these three threads of cyber risk isn't surprising, it points to the crucial need for businesses to ensure their teams are extra vigilant this EOFY.

The onus is on all of us to consistently review our defences, our systems and processes. In the context of email security, we know that nine out of 10 businesses are being impacted by phishing, even when most have an email security solution in place. We can't assume that's as good as it gets.

Don't accept that risk. If you're not already with MailGuard, explore other solutions to layer your email defences and to protect your brand, your people and your data.

Cybercrime is moving at warp speed. If you don't act, your business may be the next headline.

For support protecting your business from cybercrime, please reach out to our team.

expert@mailguard.com.au

mailguard.com.au