Brandjackers' Hit List

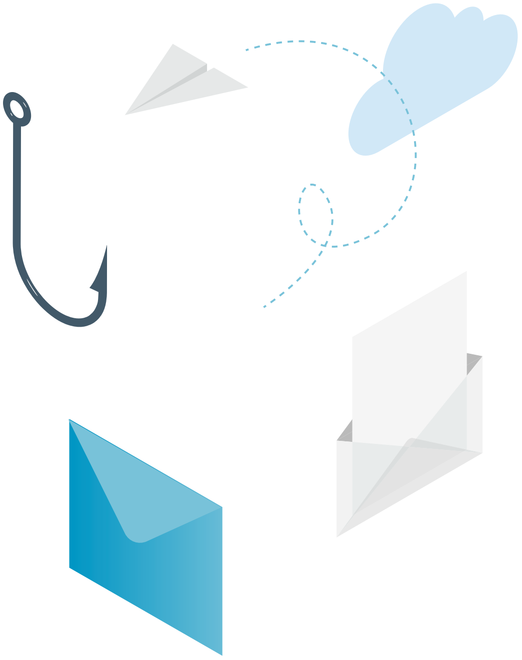
Celebrating 18 years stopping email attacks, we take a look at some of the more popular targets of brand fraud

Brandjackers’ Hit List

Celebrating 18 years stopping email attacks, we take a look at some of the more popular targets of brand fraud

May 2019 marks 18 years since MailGuard first started protecting businesses against email-based cybercrime. Over the years, scammers have come up with increasingly devious tactics to induce their victims into falling for their tricks. One of the most successful tactics is what we like to call ‘brandjacking.’

Brandjacking is when cybercrime groups hijack the trusted relationships that we all have with major brands and companies. Essentially, brandjacking is a kind of forgery. Having realised the powerful influence and impact of brands on the minds of consumers, scammers often exploit the trademarks of well-known companies to deceive their victims and gain their trust.



Playing on the fact that we’re all time-poor, with full inboxes, cybercriminals are hoping we won’t think twice about clicking emails from the brands we know and love. They’re betting that in our rush to clear our unread emails, that we might click on their emails to download nasty ransomware files, or plug our credentials into a phishing page that they’ve created to mimic the real thing.

Often, our trust in brands can be so strong that we don’t even know that our credentials have been compromised. For example, if you get an email from your bank, telco or energy provider asking you to confirm your account details, or perhaps a note to log back into an email portal like Office 365. Many of us will take a few minutes to click through, and then go about our normal day completely unaware that our account has been compromised.

In fact, cybercriminals today have a better strike rate than most marketers.

Taking full advantage of our history and expertise in intercepting ‘brandjacking emails’, we’ve collated a list of brands that are frequently mimicked, along with examples of some of the emails spoofing them.

Tell your team to think before they click. As 2019 brings a new wave of cybercrime, we hope this list proves useful in helping email users to be more vigilant and informed about the nasty emails arriving in their inboxes.

Apple

Email scams spoofing Apple often utilise high-quality graphics and elements that are normally found in legitimate Apple pages. Having convinced recipients that the email is actually from the tech giant, cybercriminals exploit the well-established reputation of the brand to trick the company's legion of fans and loyal Apple users into divulging their confidential data.

Commonwealth Bank

Commonwealth Bank is one of Australia's biggest and best-known banks, and along with that one of the most trusted brands. So, it's irresistible to phishing scammers. MailGuard frequently intercepts phishing email scams in the form of 'new account statements' purporting to be from the bank.

MYOB

Fake MYOB invoice emails are a commonly used scam format. MYOB is a well-known accounting software company, so their brand is a valuable asset for cybercriminals who want to gain the trust of their intended victims.

Microsoft Office 365

Office 365 is among the most frequently brandjacked companies we've encountered over the last 18 years. Email scams spoofing Microsoft are often designed to harvest users' Office 365 login details. As many people – dangerously – use the same log-in and password information across many websites and accounts, victims may inadvertently hand over the keys to their bank accounts and other sensitive account information.

Telstra

Telstra email scams are a regular occurrence in Australian inboxes. Email scams spoofing the company commonly appear in inboxes in the form of fake Telstra bill emails. MailGuard has intercepted many Telstra scams over the years. It is one of Australia's largest telecommunications companies, with almost everyone having an account of some sort, so their trademark is well known and trusted by consumers.

Xero

Similar to MYOB, Xero is a popular cloud-based accounting software that is frequently mimicked by cybercriminals. There have been multiple occasions when MailGuard has intercepted large-scale email scams purporting to be from the company – sometimes even twice in one month.

Australian Federal Police (AFP)

Cybercriminals commonly target the AFP when sending brandjacking emails. Playing on the psychology of our relationship with law enforcement, they're manipulating the emotions of users. Who wouldn't be nervous receiving an email from an AFP Officer, and at the very least curious enough to click through to find out more?

ANZ

ANZ Banking Group's trademarks are often exploited in phishing email scams designed to steal confidential data such as account usernames and passwords. Increasingly, MailGuard has seen scam emails purporting to be from the bank ironically using 'security challenge questions' to trick recipients into submitting their data.

Optus

The popular telecommunications company frequently gets embroiled in brandjacking scam emails, with the Optusnet webmail domain, 'optusnet.com.au' often being used as the display address used to send these malicious emails.

Energy Australia

Malicious emails in the form of fraudulent bill notifications from one of Australia's largest energy providers are often sent by cybercriminals. Precisely because EnergyAustralia is such a common household name, it provides an opportunity for criminals to manipulate a large victim pool - especially customers who aren't cyber vigilant and may not spot the differences between malicious emails and genuine ones.

Netflix

Netflix has become a favourite vehicle for email fraudsters. In 2017, MailGuard intercepted a run of Netflix-branded phishing emails that made international media headlines – proof of how powerful well-established brands are when it comes to grabbing attention, and of the impact on a wide range of email users.

National Australia Bank (NAB)

Banks commonly hold a well-established and trusted relationship with customers, mainly because they are the keepers of large amounts of our money. So, when cybercriminals send fraudulent notifications supposedly from NAB informing customers about an unexpected funds transfer, or that their account is locked, email users are naturally concerned.

DHL

Fake parcel email scams are a favourite of cybercriminals, particularly around busy shopping periods like Christmas and the Boxing Day sales. We all love getting something (aside from a bill) in the mail, and with online shopping more popular than ever, it's sometimes hard to keep track of what parcels we're expecting. Exploiting those sentiments, cybercriminals send scam emails impersonating DHL in a bid to trick unsuspecting recipients.

DocuSign

Cybercriminals love targeting DocuSign not only because of the company's good reputation and familiarity, but also because of the nature of their business. Because DocuSign's services require users to click a link to download files, they are a convenient trojan horse for malicious attacks.

Origin Energy

Well-crafted fraudulent e-bill notifications supposedly from Origin Energy often utilise the energy providers branding and logo in order to look more realistic. They tend to spike at traditionally busy times of year, such as Christmas, Easter and end of financial year as people are more likely to be time-poor and less likely to apply their usual scrutiny.

Dropbox

Dropbox's trademark is regularly used by cybercriminals to deliver malicious ransomware downloads, or as camouflage for phishing attacks. Scammers can use Dropbox accounts they hijack to store malicious files or they can sell the login credentials to third parties who may want to access the personal documents people store in their Dropbox accounts to execute identity theft fraud.

Westpac

It's commonly established that banks like Westpac maintain several security measures in their online banking processes. In the malicious emails brandjacking Westpac that MailGuard has intercepted, cybercriminals have deviously included these security measures, such as links to Westpac's legitimate support page. These help to boost the legitimacy of the scam emails.

Australian Taxation Office (ATO)

There have been a number of variations of the ATO scam over the years. Often cunningly designed with the Australian Coat of Arms (trademark of the ATO), malicious emails brandjacking the government agency range from fraudulent tax refunds to phishing emails notifying recipients of new 'tax documents'.

Even if you think you could spot an email scam, are you confident that others in your company would be as vigilant?

It only takes one person in a company to click on a malicious link to allow criminals to seize control.

Don’t take that chance. There’s never been a better time to take on the challenge of breach-proofing your company. The old saying goes ‘prevention is better than a cure’ and that’s certainly the case with cybersecurity.

Defend your company and your inboxes against brandjacking emails.

Talk to a MailGuard expert by calling 1300 304 430, or email sales@mailguard.com.au

www.mailguard.com.au

mailguard

Gold
Microsoft Partner
Microsoft