4 Mind Games Cybercriminals Play In Email Scams

mailguard

4 Mind Games Cybercriminals Play In Email Scams

It's not just luddites who fall for scam emails. Even cyber-savvy employees can get sucked in. Many find themselves scratching their heads and wondering "how did I fall for that?" But while it's easy to see the mistake in hindsight, recognising the scam before it gets you is the real challenge.

Once, cybersecurity was as easy as implementing a cutting-edge security system that could detect weaknesses quickly. However, today, cybercriminals play sophisticated mind games. They exploit human emotions and errors. Cybercrime is more than just hacking into technology. It involves getting inside users' minds too.

In this guide, we show you the most common tricks that scammers use to create email scams. Share it with your teams to raise their awareness about how to defend themselves. You might just beat these cybercriminals at their own mind games.

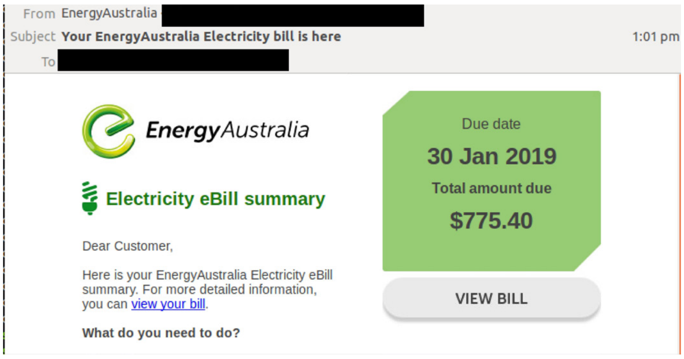
1

Exploiting brand trust

Big brands have a powerful influence on consumers. Brands are designed to generate customer trust and loyalty. Scammers take advantage of this by masquerading as well-known companies. In this way, they trick victims and gain their trust.

The average person is also time poor and has a full inbox. Cybercriminals hope 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, we might click on their email links. We might download nasty ransomware files, or plug our credentials into a phishing page that they've created to mimic the real thing.

Here's an example. You could get an email from your bank, telco or energy provider. That email may ask you to confirm your account details or log into an email portal like Office 365. Many of us will take a few minutes to click through. We then go about our normal day, completely unaware that our account has been compromised.



From EnergyAustralia [redacted]
Subject **Your EnergyAustralia Electricity bill is here** 1:01 pm
To [redacted]

EnergyAustralia

Electricity eBill summary

Dear Customer,

Here is your EnergyAustralia Electricity eBill summary. For more detailed information, you can view your bill.

What do you need to do?

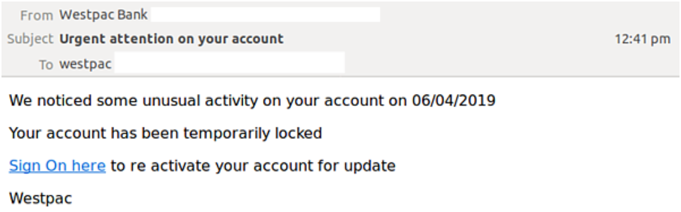
Due date
30 Jan 2019
Total amount due
$775.40

2

Using curiosity to kill the cat

Everyday, our team at MailGuard intercept "phishing emails", or emails that are designed to steal your data. These emails evoke emotions like fear, and create a sense of curiosity and urgency to trick us. Because it's human nature to be curious, we click on unfamiliar links in emails that seem intriguing. We can't resist taking a peep at those business opportunities that land in our inbox. This leads us to submit our confidential data through dodgy emails. Similarly, extortion threats use the power of fear to gain our information.

How do scam emails evoke emotion? They use urgent subject lines like 'Action Required,' or include time-sensitive instructions. For example, you could get a notification from your bank saying that suspicious activity was detected in your online banking. The email tells you that your account will be deleted if you don't confirm your identity within 24 hours. This makes people take action immediately, without thinking too much about the email's credibility.



From Westpac Bank
Subject **Urgent attention on your account** 12:41 pm
To westpac

We noticed some unusual activity on your account on 06/04/2019

Your account has been temporarily locked

Sign On here to re activate your account for update

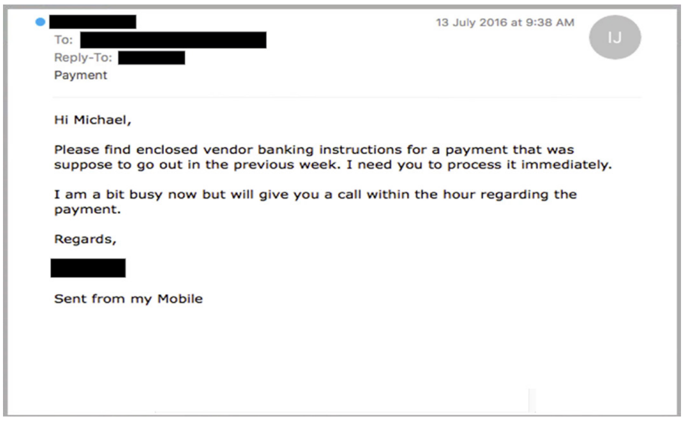
Westpac

3

Leveraging professional relationships

Cybercriminals use social engineering to scam their victims. A social engineer uses publicy available information to accurately pose as a C-suite executive via a personalised email that demands urgent action like making a financial transfer or revealing confidential information. Email fraud like this is also sometimes called whaling, Business Email Compromise (BEC) or CEO Fraud.

A whaling attack takes advantage of the relationship between the target and the CEO or other senior executives. By mimicking a high-ranking executive, whaling uses the power that the executive has over their subordinates to drive immediate, unquestioning action. These attacks are very much a hack against a human, rather than against
a computer.



[redacted]

13 July 2016 at 9:38 AM

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

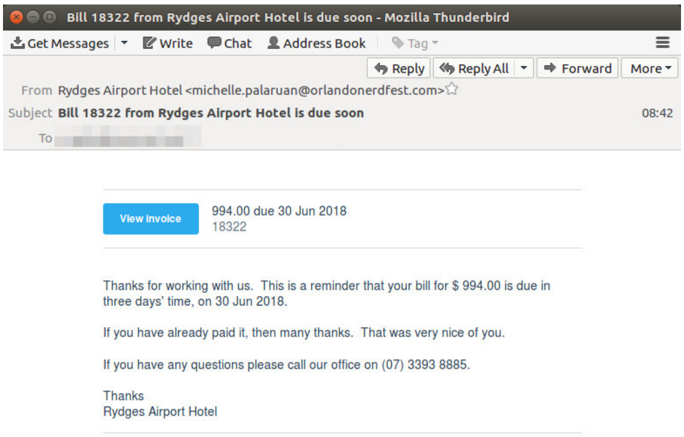
4

Working in silly season

It’s pretty simple psychology, actually. If you’re going to try and trick someone, it’s best to do it when they’re busy or distracted. And there are specific seasons of the year when people are busiest.

The End-Of-Financial-Year (EOFY) period is one example. At this time, companies are reconciling their numbers and filing tax returns. They’re in a panic to get financials finalised and paperwork filed with the Australian Tax Office. As a result, employees receive a lot of invoices, bills, payroll and finance-related documents. They’re also so busy that they let their guard down.

Black Friday and Cyber Monday also make people vulnerable to cybercrime. These one-day sales pressure customers to complete their purchases as soon as possible, in case they lose the deal to someone quicker. Tempted by those time-sensitive deals, shoppers readily click on scam email links without taking their usual precautions. This time-critical tactic is a classic phishing technique which discourages people from checking for validity.



Bill 18322 from Rydges Airport Hotel is due soon - Mozilla Thunderbird

From Rydges Airport Hotel <michelle.palaruan@orlandonerdfest.com>

Subject **Bill 18322 from Rydges Airport Hotel is due soon** 08:42

To [redacted]

994.00 due 30 Jun 2018
18322

Thanks for working with us. This is a reminder that your bill for $ 994.00 is due in three days' time, on 30 Jun 2018.

If you have already paid it, then many thanks. That was very nice of you.

If you have any questions please call our office on (07) 3393 8885.

Thanks
Rydges Airport Hotel

Cybercriminals often pose as fake retailers to trick consumers. But they also pose as other businesses involved in the supply chain, like parcel delivery, tracking notifications and banking services. We receive hundreds of messages from these services every day, so it's important to be able to differentiate the legitimate from the illegitimate.

Learning to spot scam email techniques is a great way to help defend against cyber-attacks. But it doesn't give you full protection. Talk to MailGuard about how you can secure your business.

Email info@mailguard.com.au or call at 1300 304 430.

www.mailguard.com.au

mailguard

Gold
Microsoft Partner
Microsoft