# Christmas Closure

**The A Firm is closed over Christmas from 20th December 2018 & Re-opens Monday 14th January 2019.**

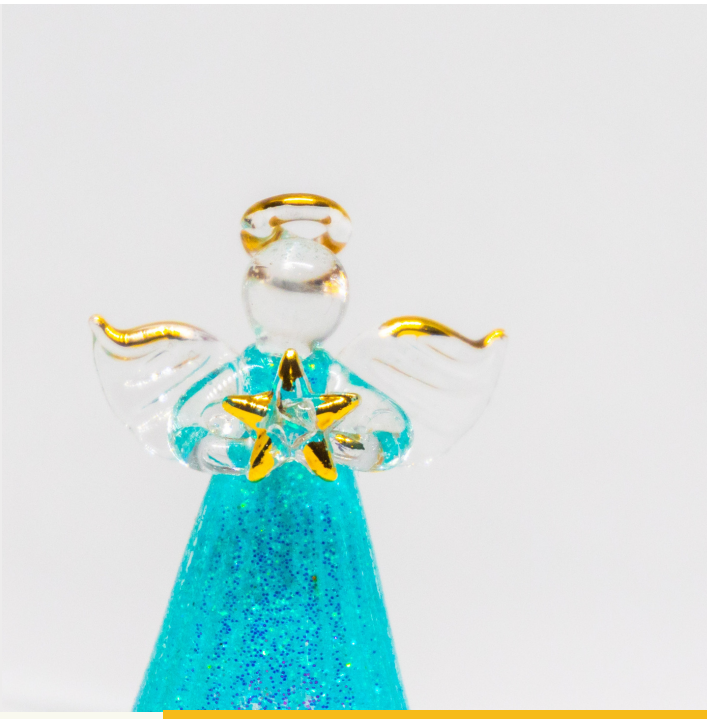
Closed-
20.12.18
Reopen-
14.01.19

Urgent queries to please phone main office **07 5596 4604**, these messages will be checked and urgent queries contacted back.

Wishing you a Merry Christmas & Happy New Year!

# Merry Christmas!

The special holiday newsletter
full of important Tax News



## CHRISTMAS PARTY? THERE'S A TAX FOR THAT

Throwing a work Christmas party this year? Giving out some gifts? There's a tax for that.

It's called fringe benefits tax, and if you aren't careful the taxman could come knocking.

Fringe benefits tax (FBT) is the tax employers pay on benefits they provide to employees, their family or other associates in addition to, or as part of, their salary or wages.

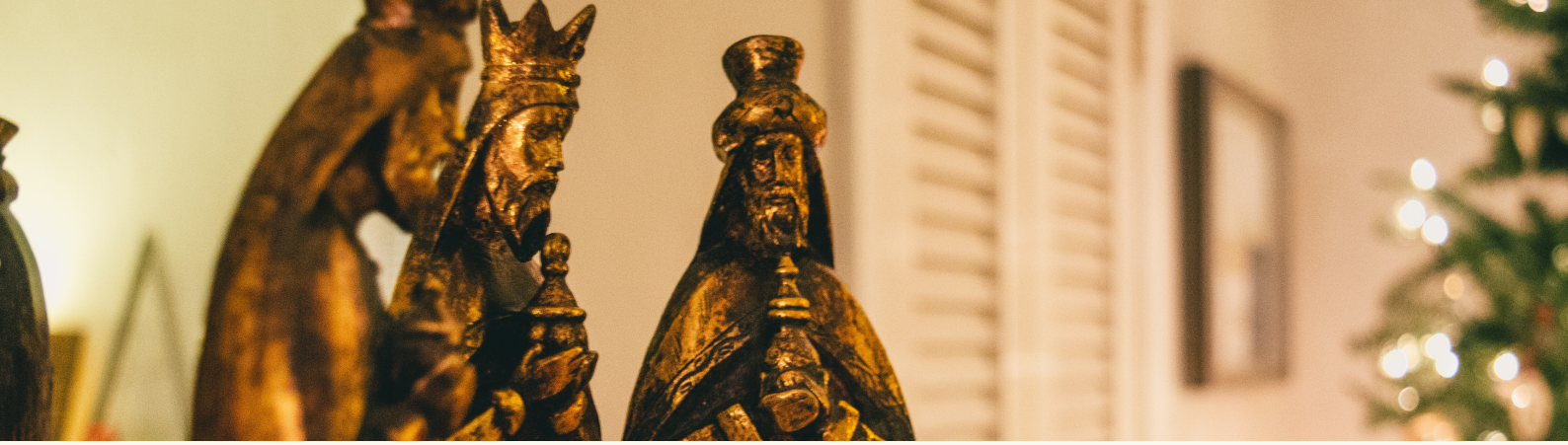
Work cars for employees' private purposes, or paying for an employee's private health insurance come under the FBT regime, but so do Christmas parties.

Here's the good news: there are exemptions under FBT that could save your business some money.

The catch: it's not exactly simple to determine what's FBT exempt and what's not. The tax office released a six-page document earlier this week trying to clear the air.

Here are a few tips and tricks to successfully navigate FBT reporting.
Continued page 3...

## News:



**1. Venue matters**

Whether your Christmas party is considered 'entertainment' or 'non-entertainment' is just as important from the ATO's perspective as it is for your employees (haha).

In the tax office's case though, you'll be more likely to be FBT exempt if the premise your party is held at is classified as 'non-entertainment'. BDO tax partner Mark Molesworth explains if the party is at your office it's more likely to be classified as 'non-entertainment', but FBT is complex, so that's only general advice.

**2. A magic number: $300**

When it comes to FBT, $300 is a pretty important number. It's basically the threshold for what classifies as a 'minor benefit' and what doesn't. That's important because minor benefits are often exempt from FBT, but there are some conditions.

A minor benefit has to be infrequent and irregular, meaning you can't throw a Christmas party-scale event every week and still say its minor. Molesworth says a business that holds an end-of-financial-year (EOFY) party and a Christmas party should be okay on this front.

The total amount spent per head also has to be $300 or less, and this is for all similar expenses you're claiming throughout that FBT reporting year for that employee, Molesworth says.

**3. Go for 'non-entertainment' gifts for the best tax outcomes**

Tickets to concerts, movie passes and holidays are classified as entertainment gifts by the ATO and are usually subject to FBT. However, hampers, vouchers, bottles of wine and other similar gifts are classified as 'non-entertainment' and are generally exempt from FBT.

**To summarise, there are a few important questions to ask yourself before you throw your Christmas party.**

How much will it cost? Remember $300 is the magic number.

Where is it, and when will it be held? At the office or outside of work?

Who's invited? Is it employees only? Are partners, clients and suppliers also invited?

Giving gifts? How much are they worth, what type are they and who is receiving?

**Source: https://www.smartcompany.com.au/finance/tax/christmas-party-tax/**

# CHECKLISTS AND TO DO LISTS...

## *Why don't they actually work?*

## SOME STRAIGHT TALKING FROM ANNETTE

I bet we've all had occasions when we walk into the office with great intentions of getting through our checklist that day...without fail. But what normally happens is at the end of the day we find most things still on that checklist.

### *Why, oh why don't checklists work?*

Well they actually do work but there's more to a checklist than just writing the list. To put it simply (and what a great time to remember the golden rules of to do lists) here's the missing links.....

1. **Restrict the number of items on the list to less than 7** – be realistic and allow time for the unknown emergency items that always seem to come out of nowhere. Anything over 7 move to tomorrow (some of those may disappear before you get to them).

2. **Write beside each item the estimated amount of time it will take** to do each task. Then make sure the total of that time only fills in 80% of your available time. This allows for any underestimation of time. If you do get through all the tasks as planned, you could bring back from tomorrow's list one item.

3. Then in a different coloured pen, **prioritise those items putting most urgent as 1**.

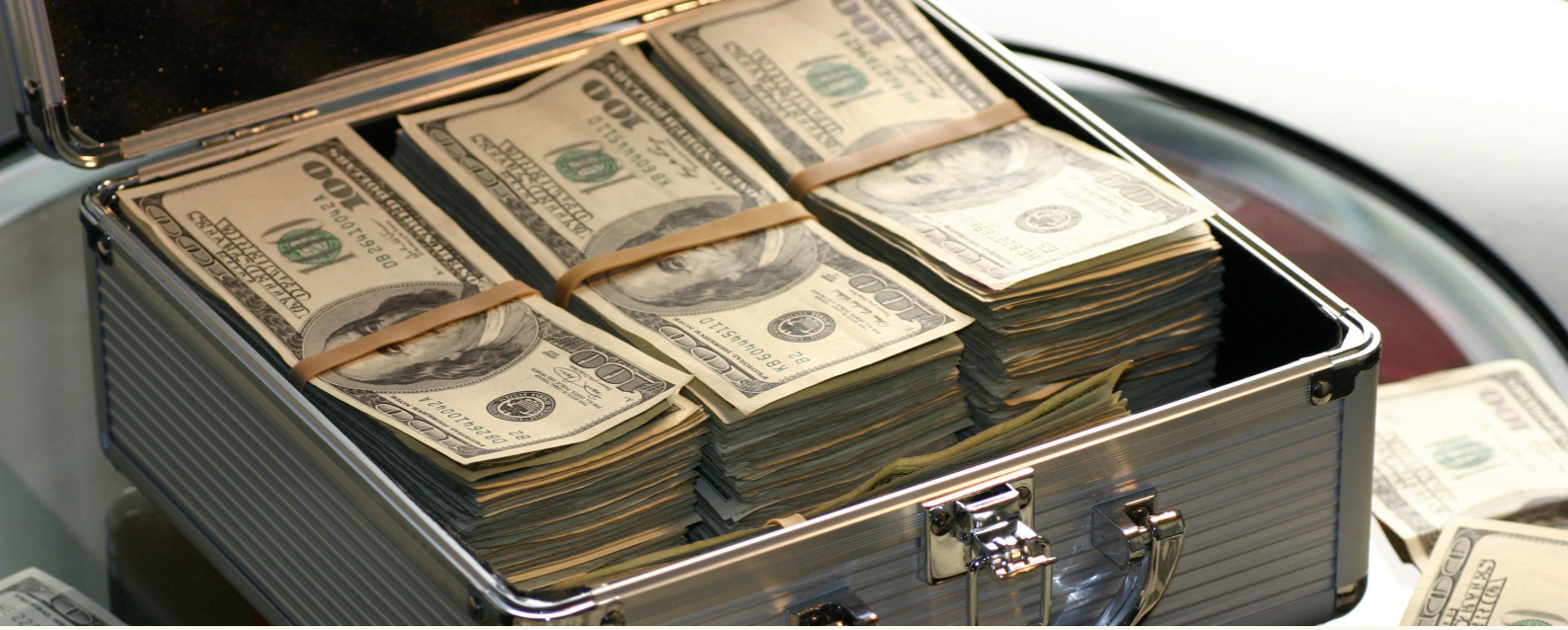
4. Halfway through the day, **review the list** of things left to do and reprioritise if needed.

End of day, doesn't it feel good to have gotten through the list? You bet it does...I've done this for the past 30 odd years and only very occasionally missed doing something.

Use the above for your Christmas and New Year list and see how you go....could make life a lot easier.

Merry Christmas

Annette



# SCAMMERS STEAL OVER $800,000 DURING NOVEMBER

The ATO is warning taxpayers to be on high alert to scammers, with over $800,000 reportedly lost during November. Assistant Commissioner Kath Anderson said over the last month, the ATO has seen an increase in scam phone calls, especially those using software that resembles a legitimate phone number to disguise the caller's true identity.

"The ATO does not project our numbers using caller ID. You can be confident that if there is a number displayed in your caller ID, it isn't the ATO," Ms Anderson said. According to Ms Anderson, the ATO received more than 37,000 reports of scams attempts in November alone, with one elderly person losing more than $236,000 to scammers between June and November this year.

Ms Anderson urged people to be aware of scammers pretending to be the ATO. "Taxpayers should be wary of any phone call, text message, email or letter about a tax refund or debt, especially if you weren't expecting it," she said. Ms Anderson said while the ATO regularly contacts taxpayers by phone, email and SMS, there are some tell-tale signs that it isn't the ATO. The ATO will not:

-use aggressive or rude behaviour, or threaten you with arrest, jail or deportation;

-request payment of a debt via iTunes, pre-paid visa cards, cryptocurrency or direct credit to a bank account with a BSB that isn't either 092-009 or 093-003;

-request a fee in order to release a refund owed to you; or

-send you an email or SMS asking you to click on a link to provide login, personal or financial information, or to download a file or open an attachment.

"If you suspect that you have been contacted by a scammer, you should contact our call centre. It's OK to hang up and phone us on **1800 008 540** to check if the call was legitimate or to report a scam," Ms Anderson said.
Continued page 6...

“Australians play an important role in stopping scammer activity by reporting them to our scam line. Your reports help us to get an accurate picture of what is happening with the current scams, which ultimately helps protect the Australian community.”

The ATO’s dedicated scam reporting line is **1800 008 540**.

To see our latest alerts and for more information visit ato.gov.au/scams.

Ms Anderson was also concerned about the number of taxpayers sharing their personal information with scammers. “Since 1 July, we’ve seen almost 6,000 taxpayers give away their personal or financial information to scammers through things like phishing scams. Your identifying information like tax file numbers, bank account numbers or your date of birth are the keys to your identity, and can be used by scammers to break into your life if they are compromised. If you’ve received an unsolicited email or text, or if you have any doubts about whether any contact is legitimately from the ATO, don’t hesitate to get in touch with us to check."

**Top tips to protect yourself from scammers**

Know your tax affairs – you can log into myGov to check your tax affairs at any time, or you can contact your tax agent or the ATO.

Guard your personal and financial information – be careful when clicking on links, downloading files or opening attachments. Only give your personal information to people you trust, and try not to share it on social media.

If you are unsure about whether a call, text message or email is genuine, don’t reply. Call the ATO on 1800 008 540.

Know legitimate ways to make payments - scammers may use threatening tactics to trick their victims into paying false debts in pre-paid gift cards or by sending money to non-ATO bank accounts. To check that a payment method is legitimate, visit ato.gov.au/howtopay.

Talk to your family and friends about scams - if you or someone you know has fallen victim to a tax related scam, call the ATO as soon as you can.

**Sources:**
**https://www.ato.gov.au/Media-centre/Media-releases/Scammers-steal-over-$800,000-during-November/**
**https://www.ato.gov.au/Media-centre/Media-releases/Scams-alert-as-tax-bill-due-date-draws-near/**

# SCAMS TARGETING ASIC CUSTOMERS

Scammers pretending to be from ASIC have been contacting Registry customers asking them to pay fees and give personal information to renew their business or company name.

These emails often have a link that provides an invoice with fake payment details or infects your computer with malware if you click the link.

**Warning signs the email is not from ASIC**

An email is probably a scam and is not from ASIC if it asks you:

-to make a payment over the phone
-to make a payment to receive a refund
-for your credit card or bank details directly by email or phone

**How do I protect myself from email scams?**

To help protect yourself:

-keep your anti-virus software up to date

-be wary of emails that don't address you by name or misspell your details and have unknown attachments

-don't click any links on a suspicious email

You can also check your registration renewal date; ASIC will only issue a renewal notice 30 days before your renewal date. You can search for your business name on our register and if it's outside our usual timeframe, it might be a scam.

How do I notify ASIC of a potential scam?

If you would like to notify ASIC of a potential scam email, you can forward the entire email to **ReportASICEmailFraud@asic.gov.au.**

Continued on page 8...

## HERE IS AN EXAMPLE OF A SCAM EMAIL FROM 4 DECEMBER 2018.

From: **ASIC Messaging Service** ASIC.Transaction.No-reply@cncpm.com
Subject: ASIC invoice
Date: 4 December 2018 at 12:30 pm
To:

AS

Dear Sir/Madam,

ASIC
Australian Securities & Investments Commission

The ASIC invoice for transaction dated 04/12/2018 is available from the following link:

ASIC invoice

Select this link to view, save or print the information. This link will remain active for 30 days.

If you have any questions, contact us at www.asic.gov.au/question

Regards,

Rosanne Bell
Senior Executive Leader
Registry
Australian Securities and Investments Commission

*Please consider the environment before printing this document.*

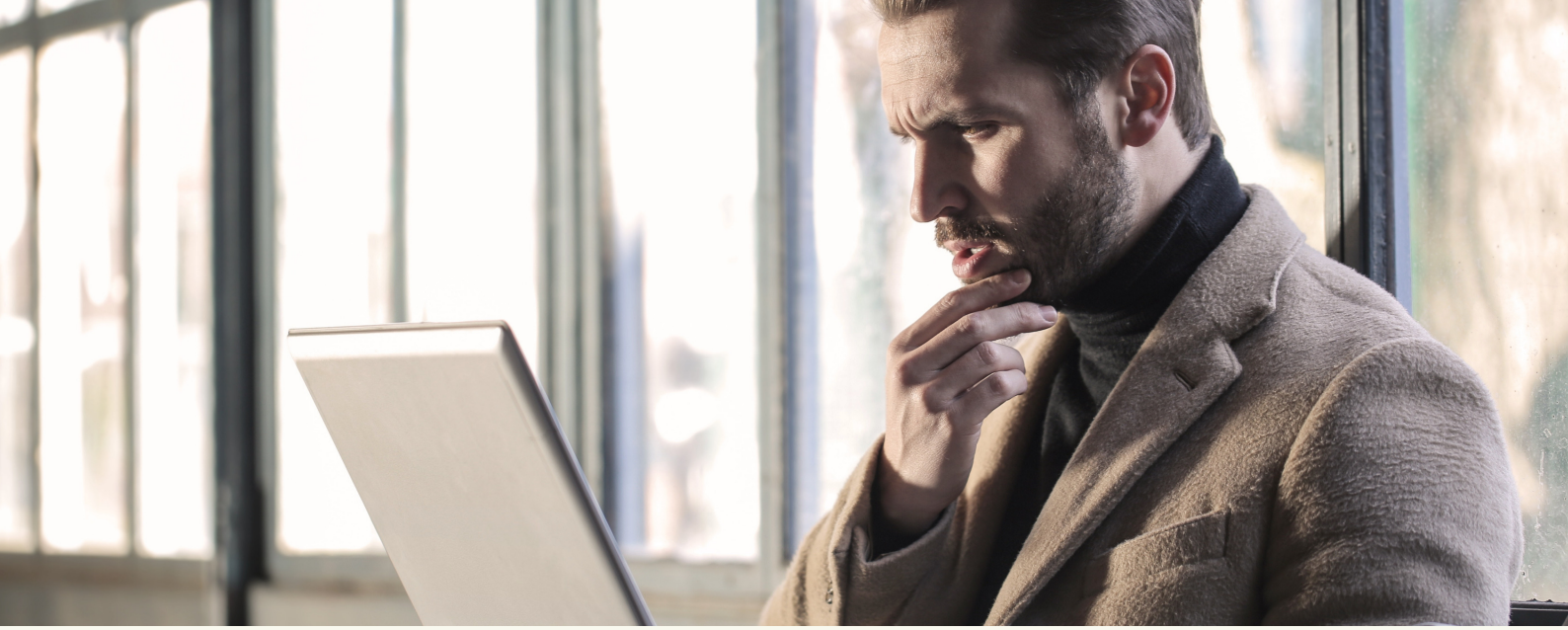
*Information collected by ASIC may contain personal information. Please refer to our Privacy Policy for information about how we handle your personal information, your rights to seek access to and correct your personal information, and how to complain about breaches of your privacy by ASIC.*

*This e-mail and any attachments are intended for the addressee(s) only and may be confidential. They may contain legally privileged, copyright material or personal and /or confidential information. You should not read, copy, use or disclose the content without authorisation. If you have received this email in error, please notify the sender as soon as possible, delete the email and destroy any copies. This notice should not be removed.*

*Unsibscribe*

If the email you received contains the above information, it is not from ASIC.

Source: https://asic.gov.au/online-services/service-availability/scams-targeting-asic-customers/



# SECURITY NOTICE FROM XERO

A genuine Xero email will always come from a xero.com domain or sub-domain address, e.g. @xero.com, @post.xero.com, @send.xero.com, @sendnz.xero.com, @support.xero.com. So if it's not from a xero.com address, be suspicious. But please also be aware that some phishing emails attempt to spoof (impersonate) our sending addresses, so they appear to come from a xero.com address but are actually sent from a different domain.

**Do not click on any links or attachments in suspicious emails.**

We've had reports of people receiving fake Xero Billing Notification emails similar to our post last month.

The email has a subject of 'XERO INVOICE REVIEW' and is being sent from a wide range of individual and business email addresses. The invoice numbers used may vary in an attempt to make the invoice more convincing.

Please be aware that these are not sending addresses nor domains used by Xero, and these emails were not sent by us.

Here is an example of the email:

**From:** Yolonde Van Putten <[redacted]>
**Date:** Thursday, 6 December 2018 at 11:51 am
**To:** [redacted]
**Subject:** XERO INVOICE REVIEW

Dear Recipient,

Here's your Xero subscription Invoice.

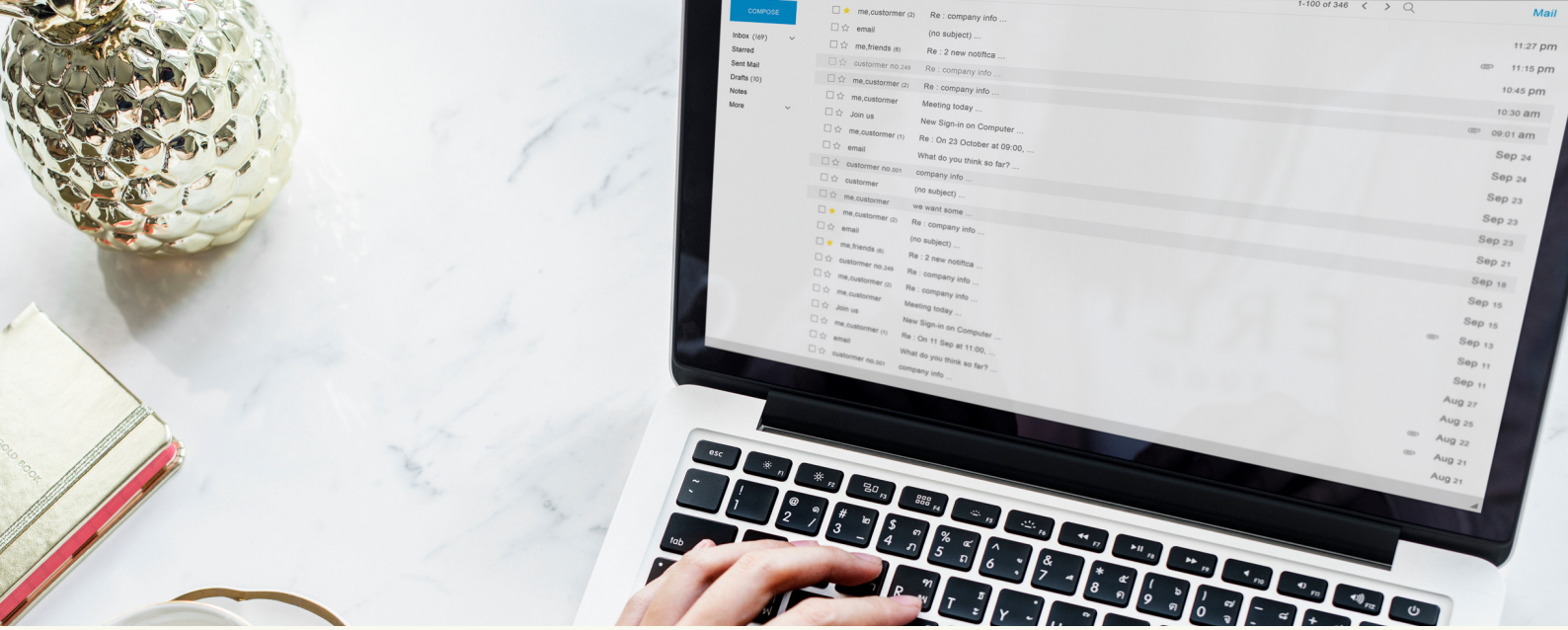
Kindly click on to view INV-43321

The amount will be debited on your credit card on or after Dec 2018.

You can change your pricing plan, billing details and payment method in Xero, you can also cancel or transfer your subscription to someone else by following the highlighted link.

Regards
Yolonde Van Putten
The Xero Billing Team.

Continued page 10...



If you have received this email, you should report it as phishing and delete it. Do not click on any links present in the email. The links in this phishing email will redirect you to a malicious website.

If you're an existing Xero user, we recommend enabling Two-Step Authentication (2SA) as another layer of protection for your account. You can find out more about 2SA here.

If you suspect you've received a phishing or malicious email, and it says it's from Xero or uses Xero's logo, do not click on anything in the email – please report it by forwarding the email to **phishing@xero.com**.

A phishing email is a favoured way for cyber criminals to get access to your sensitive information, such as your usernames and passwords, credit card details, bank account numbers, etc. This kind of email may look as if it has come from a trustworthy source, but will attempt to trick you into:

-clicking on a link that will infect your computer with malicious software
-following a link to a fake (but convincing looking) website that will steal your login details
-opening an attachment that will infect your computer.

Once you are hooked, the cyber criminal may be able to steal or extort money from you, or gather sensitive personal or business information that they can use for other attacks. However, you can protect yourself and your business by being aware of these scams, and by knowing what to look for that may help you identify a malicious email.

**Try to avoid a phishing attack by following these rules**

If you receive a suspicious email make sure you:

-DO NOT CLICK on any link or attachment contained in the email.
-DO NOT REPLY to the email.
-Report the email by forwarding it to phishing@xero.com if it is Xero-branded.
-Delete the email.

Update your anti-malware (anti-virus, anti-spyware) and run a full scan on your computer.

**Sources:**
**https://www.xero.com/nz/about/security/**
**https://www.xero.com/blog/security-noticeboard/**