Tip – Phishing Scams

What is a Phishing Scam?

Phishing scams are attempts by scammers to trick you into giving out personal information such as your bank account numbers, passwords and credit card numbers. This is usually done by including a link that will take you to a legitimate looking company's website to fill in your sensitive information. Phishing messages are designed to look genuine, and often copy the format used by the organisation the scammer is pretending to represent, including their branding and logo. They will take you to a fake website that looks like the real deal, but has a slightly different address.

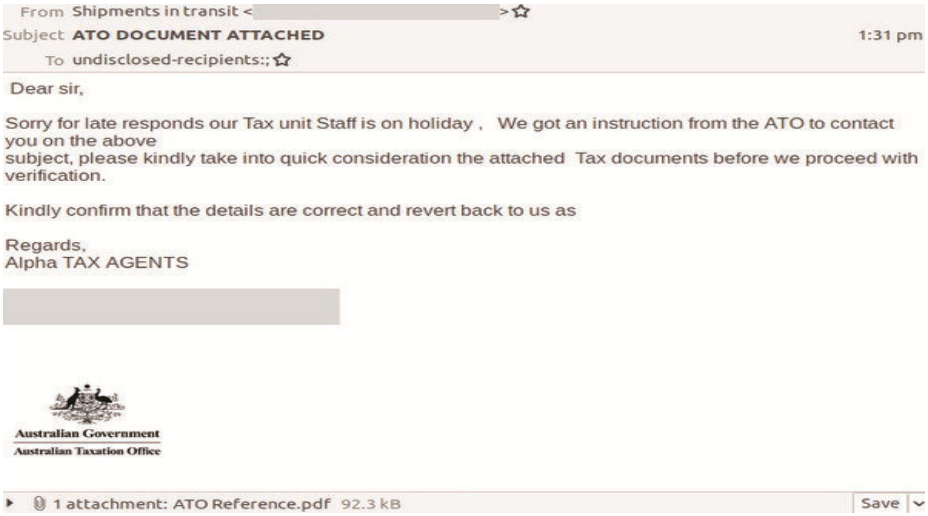
How does this scam work?

A scammer contacts you pretending to be from a legitimate business such a bank, telephone or internet service provider. You may be contacted by email, social media, phone call, or text message. The scammer asks you to provide or confirm your personal details. For example, the scammer may say that the bank or organisation is verifying customer records due to a technical error that wiped out customer data. Or, they may ask you to fill out a customer survey and offer a prize for participating. Alternatively, the scammer may alert you to 'unauthorised or suspicious activity on your account'. You might be told that a large purchase has been made in a foreign country and asked if you authorised the payment. If you reply that you didn't, the scammer will ask you to confirm your credit card or bank details so the 'bank' can investigate. In some cases, the scammer may already have your credit card number and ask you to confirm your identity by quoting the 3 or 4-digit security code printed on the card.

Examples of recent Phishing scam reported in Australia:

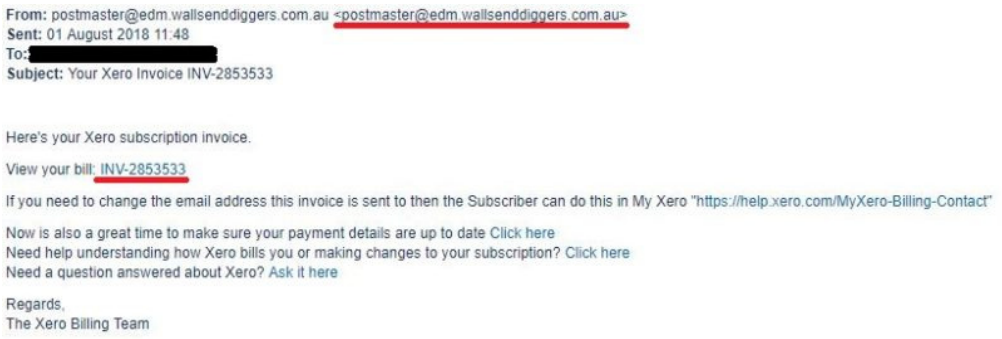
Example 1: Sophisticated ATO email phishing scam

The email scam tells the recipient the ATO is trying to contact them in regards to an undisclosed matter. The victim is then told to download and review a document needed to complete the process. The scam attempts to get victims to login to a fake page using their myGov details – doing this will hand over their username and password to cybercriminals which can be used for identity theft and fraud.



Example 2: Xero invoice email phishing scam

Cybercriminals are sending hoax invoice notifications purporting to be from the company to users. The body of the email is simple, advising recipients that their Xero invoice is ready, and that the amount in the invoice will be debited from their credit card. A link is included to view the bill online. Recipients who click on the link to view their invoice are led to a malicious website asking you to confirm your credit card details.



From: postmaster@edm.wallsenddiggers.com.au <postmaster@edm.wallsenddiggers.com.au>
Sent: 01 August 2018 11:48
To: [redacted]
Subject: Your Xero Invoice INV-2853533

Here's your Xero subscription invoice.

View your bill: INV-2853533

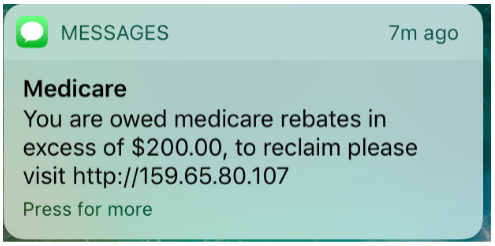
If you need to change the email address this invoice is sent to then the Subscriber can do this in My Xero "https://help.xero.com/MyXero-Billing-Contact"

Now is also a great time to make sure your payment details are up to date Click here
Need help understanding how Xero bills you or making changes to your subscription? Click here
Need a question answered about Xero? Ask it here

Regards,
The Xero Billing Team

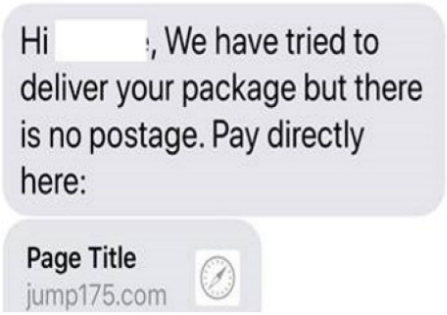
Example 3: Medicare & Aus Post SMS scam

Scammers are sending active phishing emails and SMS pretending to be form Medicare or AusPost, telling people they are owed a rebate or they need to pay to have your parcel delivered. It will prompt you to enter your full name, a memorable work, a card number and a card expiry number.



MESSAGES 7m ago

Medicare
You are owed medicare rebates in excess of $200.00, to reclaim please visit http://159.65.80.107
Press for more



Hi [redacted], We have tried to deliver your package but there is no postage. Pay directly here:

Page Title
jump175.com

Example 4: Fake 'Account is hacked' phishing email

Recently we are noticing a lot of 'Your account has been hacked email' targeting our Kindergartens. The scammer is pretending to send email from the Kindergarten's own email address and asking them to pay $1000 in bitcoin to release their account. The scammer is masquerading his malicious email address and using kindergarten's own email address as the sender address and tricking kindergartens in believing that their email account is actually been hacked.

From: [redacted]@kindergarten.vic.gov.au
Sent: Friday, May 03, 2019 7:42 PM
To: [redacted]@kindergarten.vic.gov.au
Subject: [redacted]

This account is hacked! It will be good idea to change the pswd immediately!
You might not know me me and you are definitely interested why you're getting this letter, proper?
I'm ahacker who exploitedyour emailand digital devicesa few months ago.
Never make an attempt to talk to me or find me, it is hopeless, considering that I forwarded you this message using YOUR hacked account.
I created malware software on the adult vids (porno) website and guess that you spent time on this site to have a good time (you know what I mean).
During the time you have been watching vids, your browser began to act as a RDP (Remote Control) with a keylogger that gave me the ability to access your display and web camera.
Then, my software programobtainedall data.
You have wrote passwords on the sites you visited, I caught all of them.
Surely, you could possibly modify each of them, or have already modified them.
But it does not matter, my malware renews needed data every time.
What actually I have done?
I compiled a reserve copy of every your device. Of all the files and personal contacts.
I created a dual-screen movie. The 1st section reveals the video that you were observing (you've got a very good preferences, wow...), the second screen displays the video from your web camera.
What exactly must you do?
Good, in my view, 1000 USD is basically a reasonable price for our small secret. You will do the deposit by bitcoins (in case you don't recognize this, go searching "how to purchase bitcoin" in any search engine).
My bitcoin wallet address:

1KTkfCtqKQbcZi6EbHuEBGq4QgaiYNEgks

(It is cAsE sensitive, so copy and paste it).
Warning:
You will have only 48 hours in order to make the payment. (I have an exclusive pixel in this message, and at this moment I understand that you have read through this email).
To trackthe reading of a messageand the activityin it, I utilizea Facebook pixel. Thanks to them.
(Everything thatis appliedfor the authorities might actually helpus.)

How to protect yourself from Phishing Scams?

- Be alert to the fact that scams exist. When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam.
- Do not open suspicious texts, pop-up windows or click on links or attachments in emails – delete them: If unsure, verify the identity of the contact through an independent source such as a phone book or online search.
- Don't respond to phone calls about your computer asking for remote access – hang up.
- Beware of any requests for your details or money. Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust.
- Be careful when shopping online. Beware of offers that seem too good to be true, and always use an online shopping service that you know and trust.
- Review your privacy and security settings on social media websites like Facebook and Twitter.

- Never open an attachment (especially a .zip file or .exe file) unless you are expecting it. Files from unknown senders often contain malware or virus.

- Keep in mind companies like Xero, they commonly use a PDF attachment to send invoices rather than a link to an external website.

- Never trust any email or SMS asking you for your personal information like passwords, bank details etc.

Have you been scammed?

If you think you have provided your account details to a scammer, contact your bank or financial institution immediately. If you are unsure contact our KITP helpdesk before clicking on any links on a suspicious email.

We encourage you to report KITP of any suspicious email you might have received or if you think you have been scammed you can contact ACCC – Australian Competition & Consumer Commission and use their Report a scam page to any scams.

Conclusion

Every year, scammers get more advanced and introduce new phishing strategies to bypass defences that were designed for last year's threats. Remind yourself to second guess requests for information, money or passwords.