Phishing Emails

Information Sheet

Phishing emails are emails sent to you or to your business to gain access to your data or to trick money out of your company (or clients).

These emails are **Frauds, scheming and scams** – attackers commonly target unsuspecting email accounts hoping to make a quick buck, hijack bank details, find passwords, and all kinds of private information.

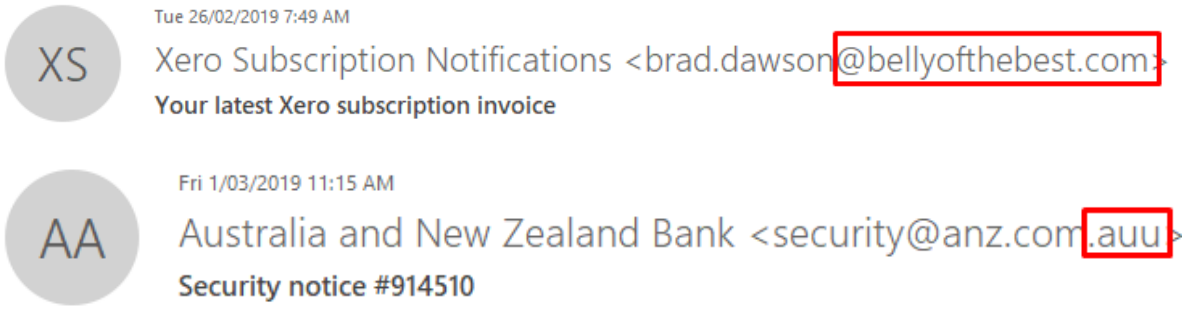
The worst part is: these can come from someone you already know and trust – without their knowledge – something we won't dig into too much in this information sheet.

Having an antivirus or spam filter is not enough. It's like opening your door willingly to a stranger. Clicking on links or downloading anything from emails can still harm your computer, or worse – compromise your information where attackers have access to everything.

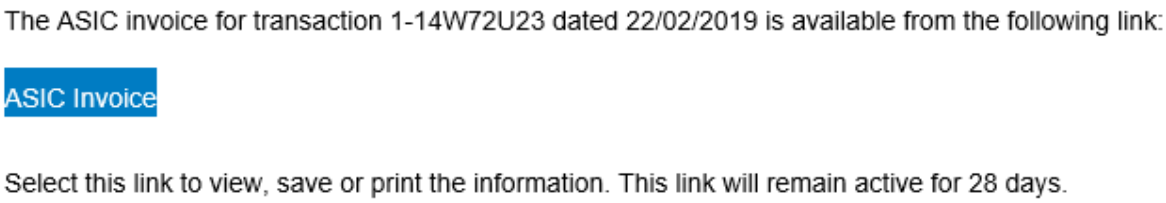
How to spot phishing emails:

In this information sheet we are going to show you 6 different examples of ways a phishing email can present in your inbox;

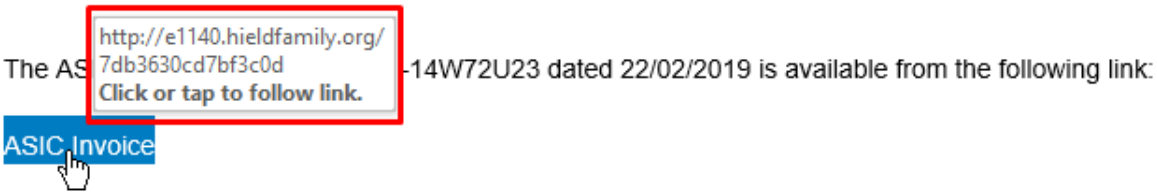
1. **Check the sender's email address – not just the name.**



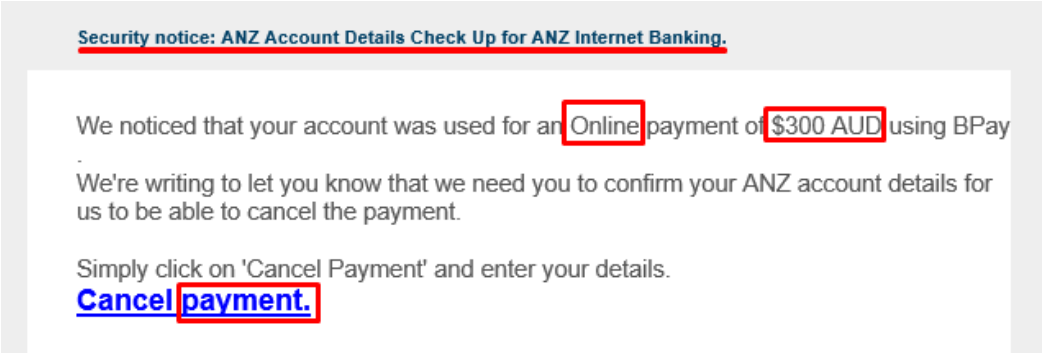
2. **Not expecting an invoice or payment?**
   Call and check with the real company over the phone if they sent you it. **Do not** respond to the email or click any links or attachments until you are sure.



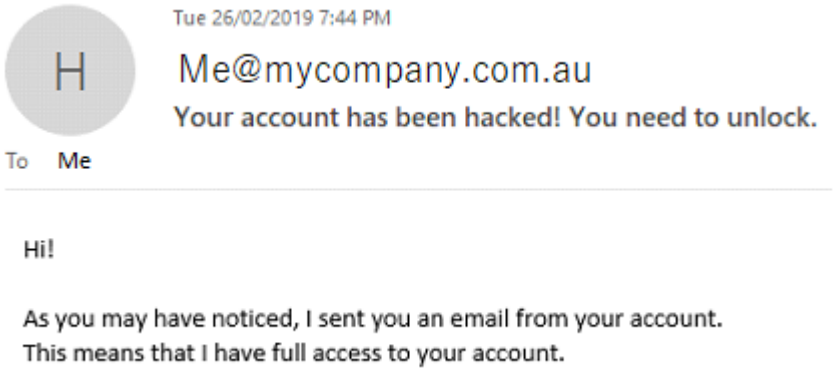
3. **Always** hover over links & attachments first.
   This is a safe way to see where links really want to take you. Many phishing emails can still have actual, real links from companies they trying to impersonate. Be vigilant.



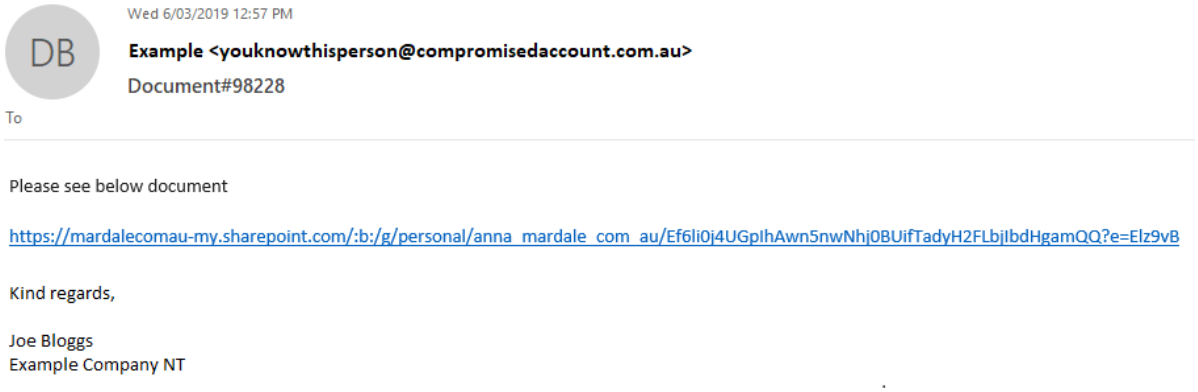
4. **Stay vigilant – look for mistakes.**
   Typos? Spelling errors? Something not look right? Don't touch it. Check with your IT company or ask some co-workers if they can see anything fishy.



5. **Attacks can look like they're from real, known addresses.**
   This is called spoofing. It's not uncommon, and the sender's email account can look to be correct. Attackers can try to make it look like your account has already been hijacked, threatening to release information. Don't fall for it – contact your IT company.



6. **Or come from your friend, family, or co-worker.**
   Someone you know has shared a document to you. It may not have any context, may be super vague, and ask you to click on a link to see a document or file. Don't do it.


DB

Wed 6/03/2019 12:57 PM

Example <youknowthisperson@compromisedaccount.com.au>

Document#98228

To

Please see below document

https://mardalecomau-my.sharepoint.com/:b:/g/personal/anna_mardale_com_au/Ef6li0j4UGpIhAwn5nwNhj0BUifTadyH2FLbjIbdHgamQQ?e=Elz9vB

Kind regards,

Joe Bloggs
Example Company NT

What happens if our business is attacked?

If the worst does happen, time can be a factor.

Contact BlueReef Technology for an immediate assist to help mitigate any problems as the result of a phishing attack.

Phone: 08 8922 0000

Email: help@bluereef.tech