

Cry for Help

Computer Tips & Tricks

Phishing

Like its synonym (fishing), phishing is about throwing out some bait to try and catch some information.

We see more and more examples these days, where we get a phishing eMail pretending to be from someone that we know & trust. Like our bank, teleco. or freight provider wanting you to confirm your account details, or to click on a link to take you to a fake web site that will load spyware onto your computer and track your key stroke activity.

Remember – any time you click on something – you are giving permission for an action, which may be a lot more than you intended. First thing you might recognise is the fact that you are receiving an eMail from the ANZ Bank about your account details – and you don't have an ANZ bank account. So you need to block that sender and then delete the email.

The second give away, is that banks will never get you to confirm these details in an eMail – so again – block and delete. And thirdly, a hyperlink might take you to a different address than indicated.

Finally, the eMail might just look suspicious. Bad spelling or the grammar might not be quite right, or something else alerts your intuition.

How to check? Firstly, you can ring the originator to confirm the authenticity of the eMail, or you can copy and paste the first sentence of the message into Google to see if others have reported it as a scam. Not a foolproof method, but when they send out thousands of these eMails at a time, it doesn't take long for them to get reported by someone.

Take care!

Jonathan Harris
JNH Software P/L
5259 2304

