Mini assignment 2

suspicious features a person should look for in links:

* Bad grammar and misspellings
* Websites with an unusual web address
* Common form pages
* Websites with subtle differences
* More sophisticated attacks sometimes disguise the web address, so the text in the email might say 'http:/ /sydney.edu.au/email' but the link takes you to a different, external site

For emails:

* Names that don't match the email address
* Emails with a strange reply address that doesn't match the From: address
* Alarming tones, threats of account closure and immediate action
* Generic placeholder style language such as "Dear Customer"
* It sounds too good to be true

For social engineering:

They will research their targets (e.g. by seeing their Facebook or LinkedIn profiles) and, based on their research, will then create a highly-customized email that appears relevant to their targets. Spear phishing is often used to target individuals with more access into University systems or with the ability to release funds.

Task 2 :

My own mental model:

I realised im a student, tat’s fond of job opportunities, internship, studying assistance, and gaming.

I subscribed many this kind of websites, and I will constantly receive emails about them.

My reasons for choosing every one of them:

1. The steam promotions email: that email includes very brief information, just about a single game that’s taking discount, and the link to that game in the shop page, which can be used to phishing out my payment methods passwords.
2. Google document email: that email tells me about someone of my friends invite me to edit some file that’s involved in my group projects. It includes a link to the edition page, which can be used to phishing out my google accounts.
3. Indeed job notification: that email includes a list of new jobs that’s for hire in the area I have subscribed, and a link to each one of them. this one can be used to phishing out my personal details.