**網路釣魚專題報告**

系級 : 資工系108級

學號 : A1045516

姓名 : 蔡湘俊

指導老師 : 陳建源 老師

1. 魚餌的內容、設計魚餌的動機以及攻擊的方式

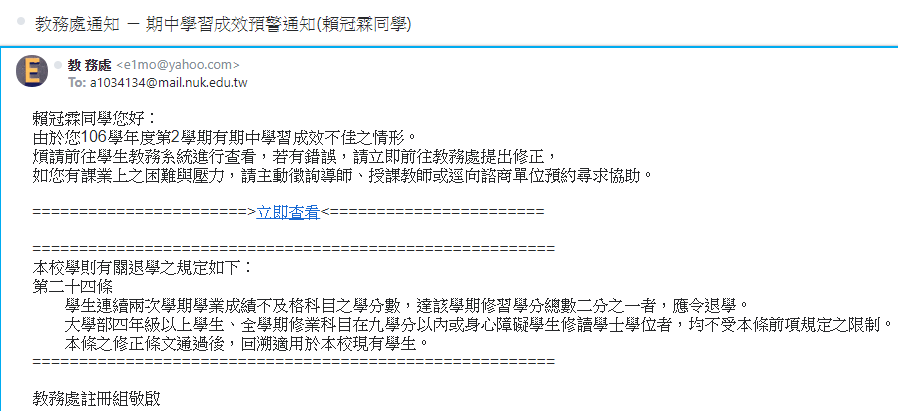
針對本次的網路釣魚專題，我特地針對了每個人所感興趣的或是成功率較高的相關內容下去設計我的魚餌，我一共設計了六種不同的釣魚內容與形式，大致上可以分成三種類型，分別如下 :

* 1. 網頁式的釣魚

我所針對設計的網頁分別是學校的學生教務系統以及Facebook :

* + 1. 學校的學生教務系統

嚴格來說學生教務系統應該只能算是我獲得對方帳密的中間媒介，真正吸引對方來去做輸入動作的途徑是信件的內容，我一直在考慮要寄什麼樣的內容是可以和學校相關並且會讓對方有高度機率會點按進去的，到最後我所想到的就是期中學習成效預警通知，我會選擇他的原因在於我有特別去針對其他學校的信件去做過統計，大部份學校所寄的一些相關活動我看大部分的學生都不會去點開它，更甚至連理會它都不會理會它，有的人更狠就直接把信件給刪除掉，所以我認為寄這種活動相關的資訊鐵定是會失敗的，而像期中學習成效預警通知這樣的信件我還沒有看過有哪位同學是會去不理會他的，而且經過我詢問其他同學點按的動機全都因為怕被當掉，所以才會立即點按信件做確認，因此我才覺得這是一個十分可行的方法，最終才會選擇它作為我釣魚信件的主要內容，那整體信件內容就如下所示 :



而我原本是要用gmail的形式下去做寄信的動作，但是我因為想要模仿學校寄期中學習成效預警通知的信箱，也就是elmo@nuk.edu.tw，但gmail是不允許帳號長度小於6，所以我到後就改申請yahoo信箱，而這樣申請我發覺有一項好處就是用yahoo的信箱下去做寄件的動作也是可行的，原因在於說學校有些信件不是由系統自動發送出來，而是教職人員寄出的話，有許多的教職人員他們都是用yahoo信箱的方式下去寄送郵件，所以就算今天用yahoo信箱去做寄信，其實對方也不太會懷疑。

而我這封釣魚信是針對我其中的一個小天使A1034134賴冠霖-應用數學系-a1034134@mail.nuk.edu.tw，根據我對這位同學一個禮拜的觀察，它的成績算是普通的類型，但是它並沒有被當過任何一個科目，這也意味著這位同學沒有收過任何一次與期中學習成效預警通知相關的信件，那麼我之所以還會針對這位同學設計這封釣魚信件的原因就在於我想要打一個心理戰，正如我前面提到的，大部分學生在收到期中學習成效預警通知的信件的時候是會急著去做確認的動作，而這位同學正好都沒收過任何一次的期中學習成效預警通知的信件，假如建立在這樣的前提下，它突然收到這樣的信件，我在猜他應該是會更加的緊張，並且會更急著去點開這封信件去做確認的動作。

而我設計的攻擊方式就是讓他點下立即查看的連結的時候就會轉跳到我所設計的學生教務系統的釣魚網站，如下圖所示 :



那當目標輸入了帳號密碼之後會產生兩種的情況，一個是當今天目標輸入的帳號密碼是隨便輸或是帳號、密碼有任一欄位是空的和使用者所輸入的帳號、密碼是正確的時候，我就會跳轉到我所模仿的錯誤頁面，如下圖所示 :



當今天是輸入錯的，按下回登錄首頁的連結的時候是會跳轉到我所設計的釣魚網站，而當今天使用者是輸入對的時候則會跳轉到學校的學生教務系統，並且將目標輸入的訊息存入資料庫裡頭，而在這之中我只能判斷他的帳號輸的是對的還是錯的，密碼的部分我就無法去做判斷，也就是當今天目標所輸入的帳號並不是他的學號的時候，我就一律視同錯誤，直到目標是輸入自己的學號我才會跳回到正常的登入頁面，而這樣做也才能盡可能的避免目標亂輸的情形。

1. Facebook

而另一個網頁我是選擇大家最常使用的Facebook，這個Facebook頁面也只能算是我取得目標資料的中間媒介，真正的核心部分還是在於信件的內容，我信件的內容是以要恢復Facebook帳號的名義來去將目標騙到我所設計的假的Facebook，在輸入完帳號、密碼之後，就會立即跳轉到目標的Facebook的內容，並且會將目標的帳號、密碼存到資料庫裡頭，而之所以會直接跳到目標的Facebook的頁面就是利用使用者都會為求方便，然後就會讓瀏覽器去記錄登入的狀態，這樣今天就算其所輸入的Facebook的頁面是假的，也會很自然地轉到目標個人的Facebook頁面，那在這個當下，目標的帳號和密碼也就被我取得到，而目標有可能是還沒有發現的。

而這個假的Facebook的頁面就如下所示 :



這個假的Facebook頁面也是針對我的其中一個小天使A1045515-黃心眉-資訊工程學系-lily040617@gmail.com，我也是經過1個禮拜的觀察之後，我發現目標很常在登入自己的Facebook，那麼這也意味著目標是很注重自己的Facebook，並且其裡頭一定有許多的重要資料，所以我就利用目標對於Facebook的重視，來去寄一封假的Facebook恢復帳號訊息，讓目標誤以為自己的帳號是被別人盜了，然後再將其誘導到假的Facebook頁面去輸入自己的帳號密碼，藉此來去取得目標的帳號密碼，並且直接登入到他自己個人的Facebook頁面，使得目標不易發現自己被釣魚了，所以利用的這種方式也是在打心理戰，來去提高對方跳入陷阱的機率，所以這個就是我攻擊目標的方式，而我寄給目標的信件的內容如下所示 :



這是直接去模仿Facebook寄這種郵件的形式，來去大大的提高使目標掉入陷阱的機率。

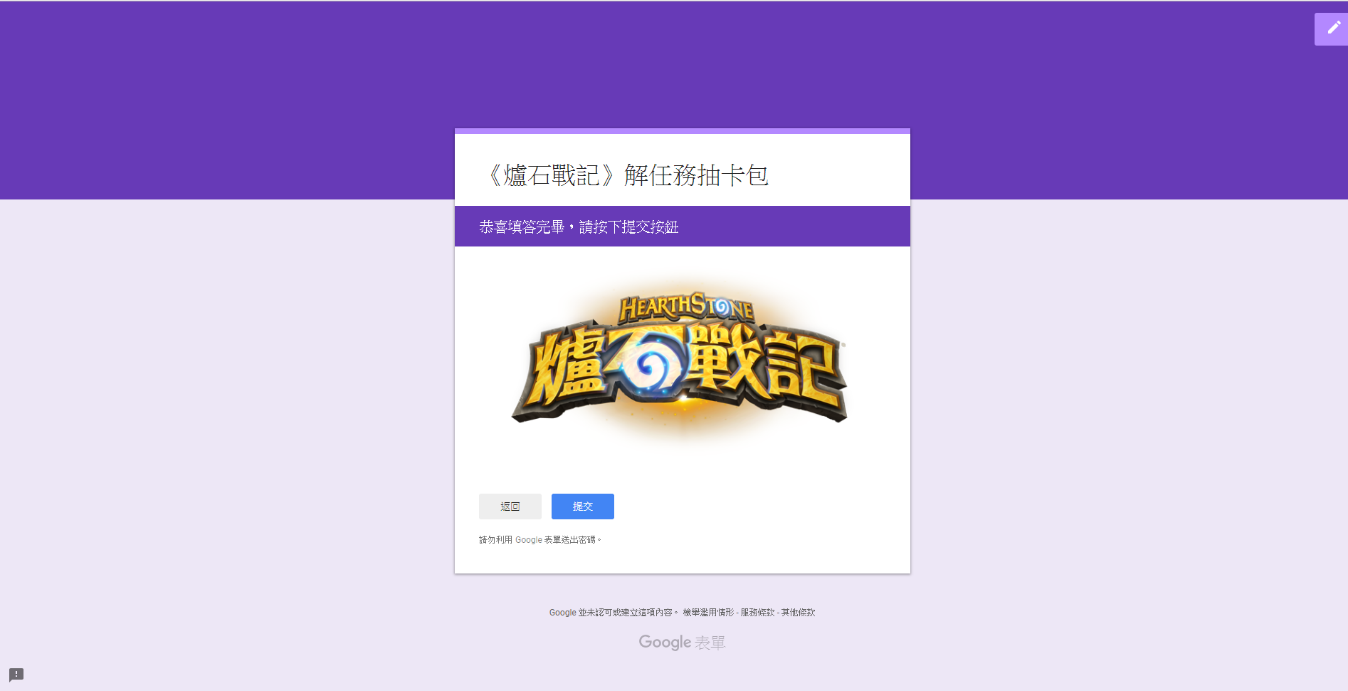
* 1. GOOGLE表單的釣魚

我所針對設計的GOOGLE表單的內容分別是遊戲的爐石戰記、英雄聯盟的抽獎活動以及動漫每月的調查活動 :

* + 1. 爐石戰記的抽獎活動

這個遊戲我本身之前就有玩過，這個遊戲很常在舉辦抽獎的活動，而且它都會要求要參與抽獎的玩家都必須填完相關的GOOGLE表單內容之後，才能獲取抽獎的資格，但因為舉辦抽獎活動的間隔都是大約7、8個月，並且每次的獎品都十分的豐富，故每次都能吸引到大批玩家(包括我自己)前去進行參與的動作，而其表單的設計如下所示 :

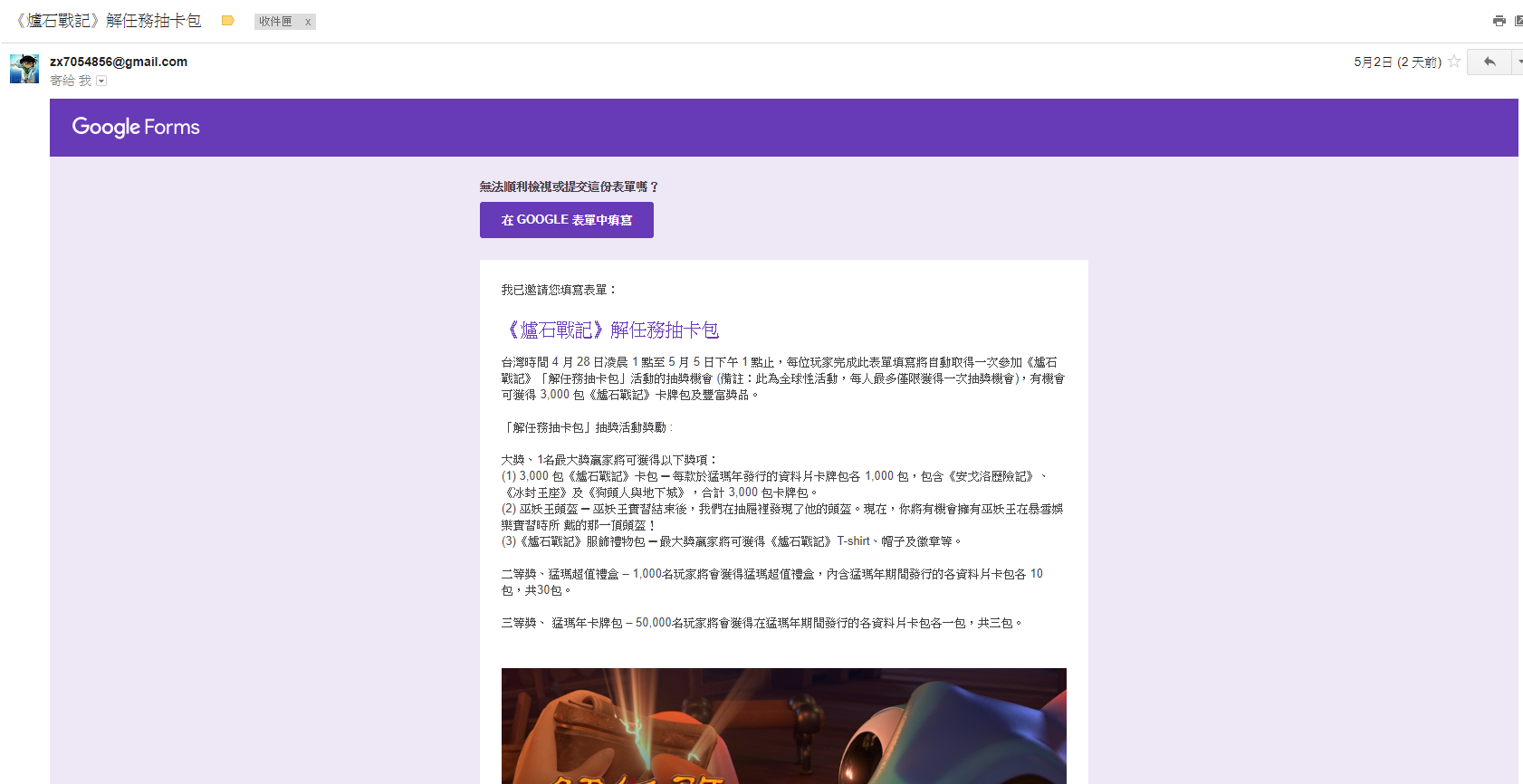






而我會去設計此表單的原因就是我其中的兩個小天使A1045510-王羿捷-資訊工程學系-s1245656@gmail.com、A1045538-王于豪-資訊工程學系green5965745@gmail.com他們兩個都有在玩爐石戰記，並且經兩個禮拜的觀察之後，我發覺他們也都很常參加抽獎活動，而且又加上爐石戰記最近剛好有一個抽獎活動正在進行，所以我覺得這樣的設計很適合拿來去做釣魚，故此我才會去針對他們兩個人來去設計這一個表單。

那麼我的攻擊方式就是透過寄信的方式，而其寄信的方式就是直接利用GOOGLE表單裡頭的寄郵件的功能下去做寄送，而其寄過去的效果就會如下所示 :



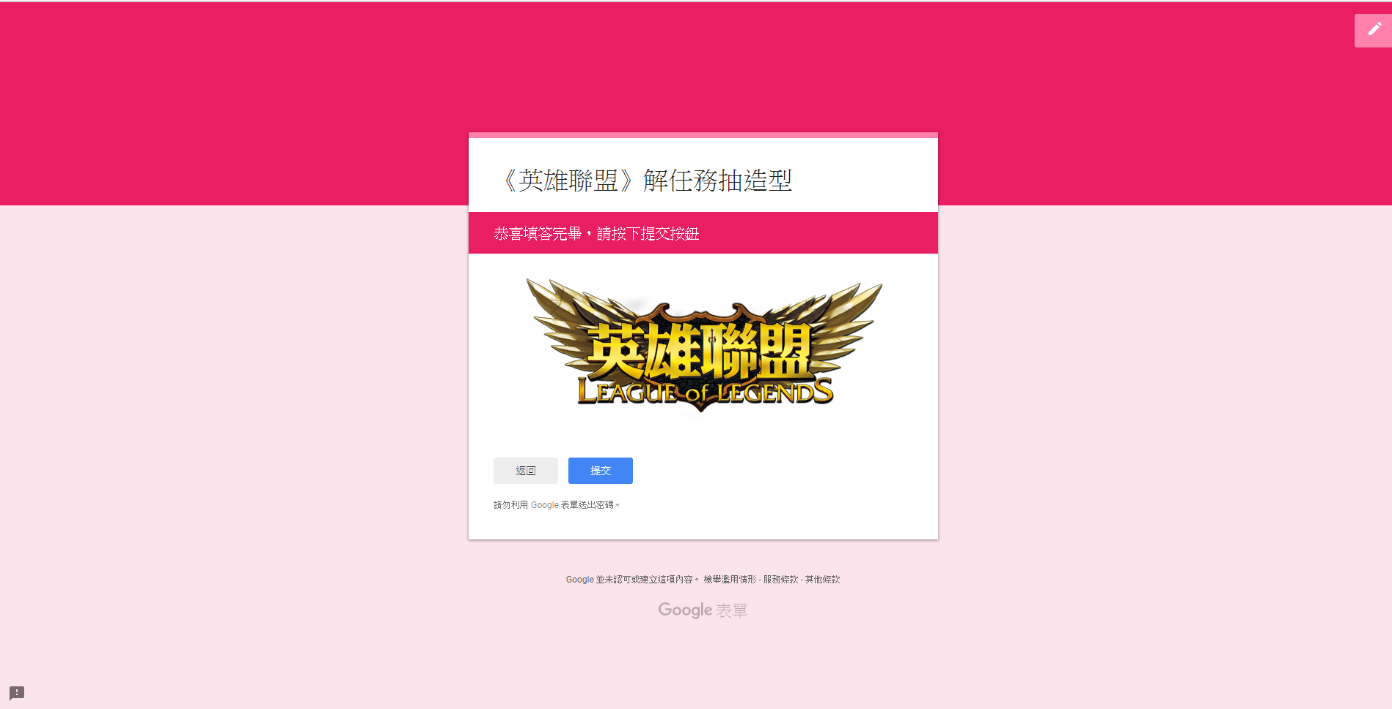
那麼當目標去輸入了表單的內容之後，其目標所輸入的表單內容就會存到我的GOOGLE帳戶內，這樣我就能取得目標的資料。

* + 1. 英雄聯盟抽獎活動

而這個表單的設計理念也是和設計爐石戰記的理念是一樣的，這兩款遊戲都很常辦抽獎的活動，而其中的兩個小天使A1045510-王羿捷-資訊工程學系-s1245656@gmail.com、A1045538-王于豪-資訊工程學系green5965745@gmail.com他們也很常去參加這個抽獎活動，而且在詢問之後也才知道只要是他們所玩的遊戲有辦抽獎活動的時候，他們只要有空的話都一定會去參加，所以可見遊戲的抽獎活動對於他們的吸引力是如此的巨大，而英雄聯盟的抽獎表單設計如下 :

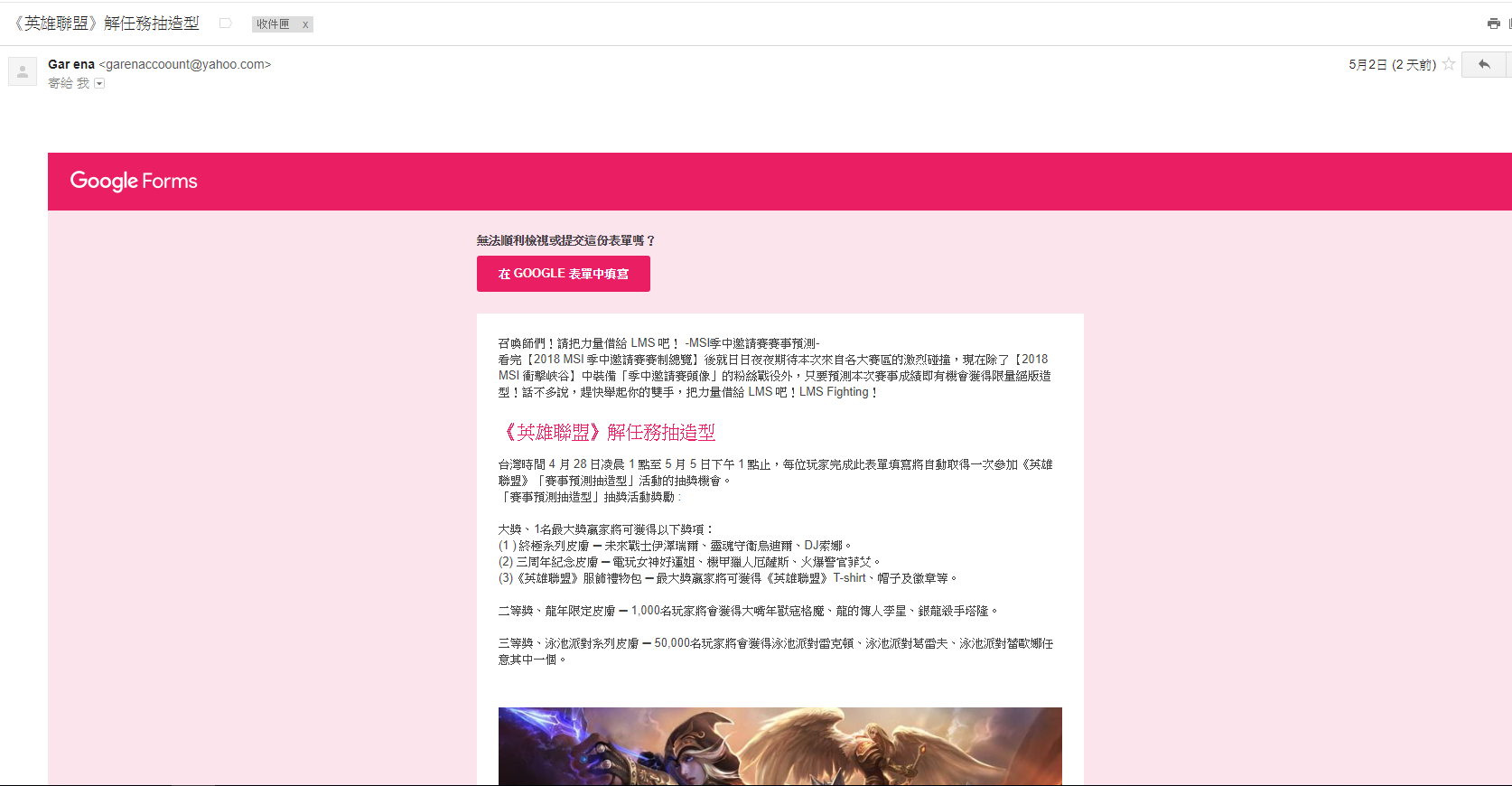








那麼我的攻擊方式就是透過寄信的方式，而寄信的方式也是利用GOOGLE表單內建的寄信系統來去將信件發送給目標，而其形式就會如下所示 :

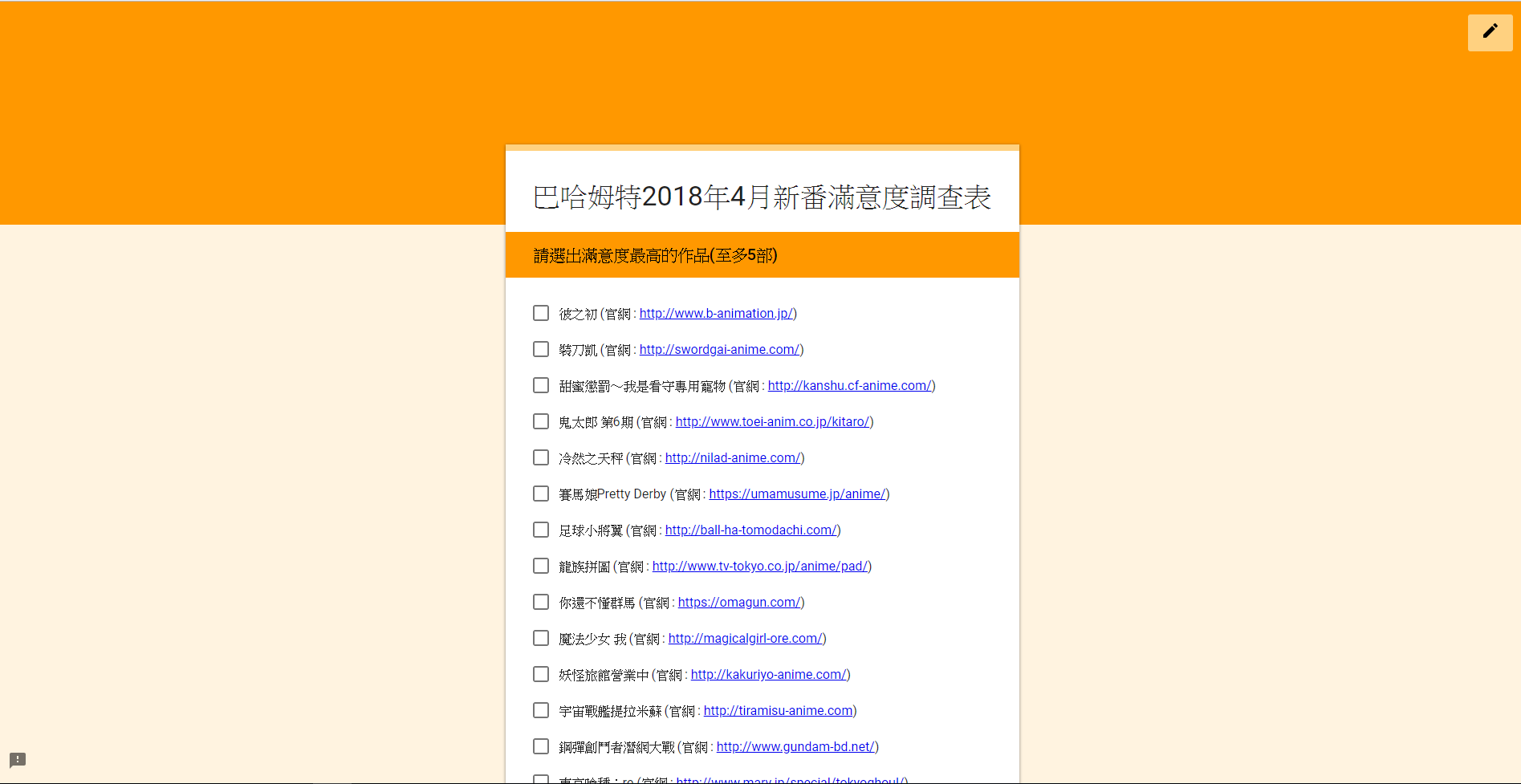
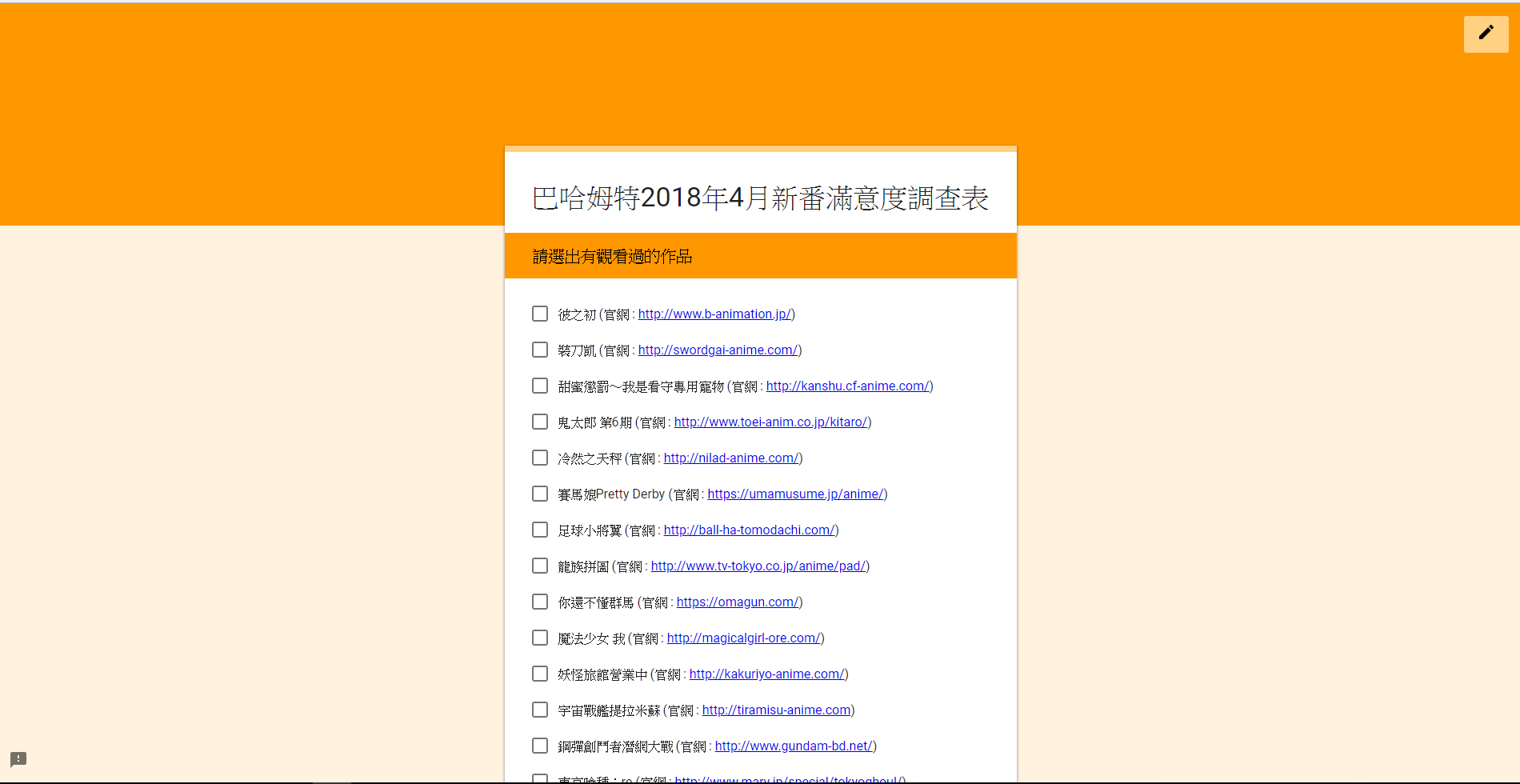


那麼只要目標輸入了表單的內容，那麼目標所輸入的內容就會存到我的GOOGLE帳戶來，如此一來我就能夠獲得目標的個資。

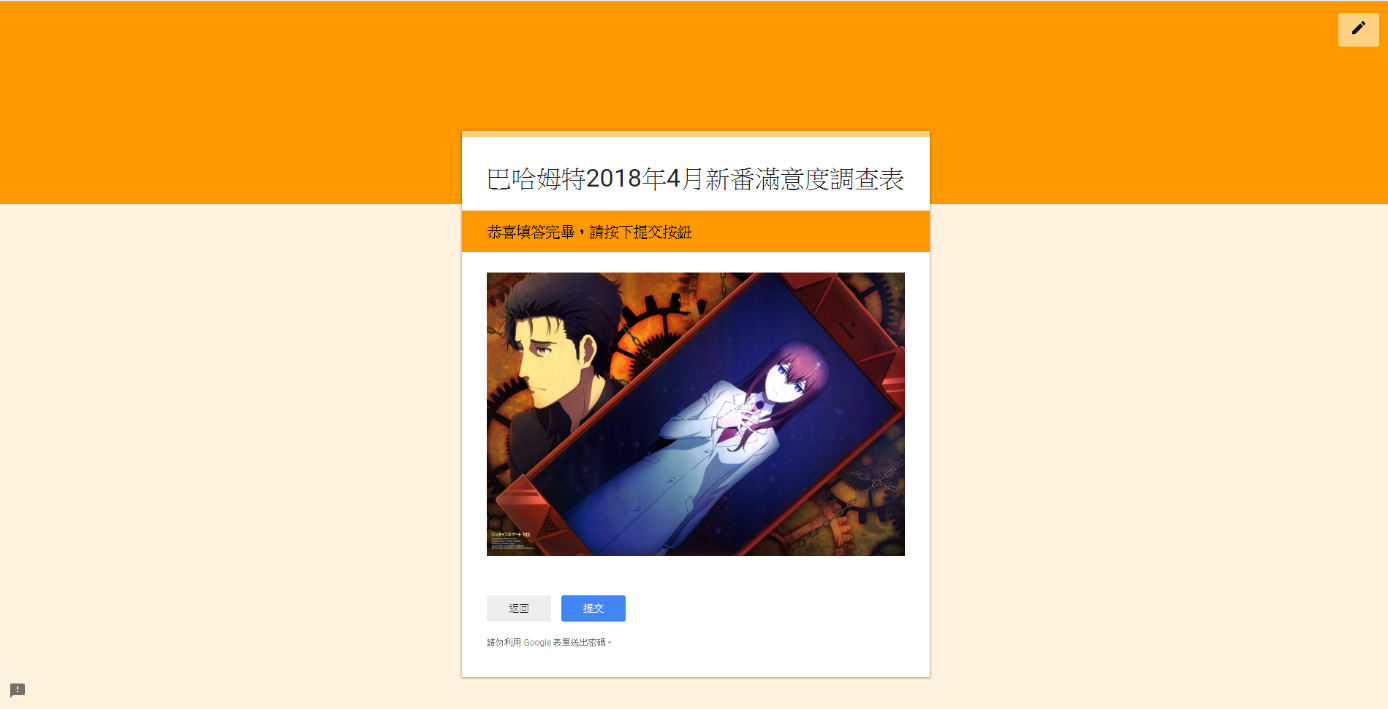
* + 1. 巴哈姆特2018年4月新番滿意度調查表

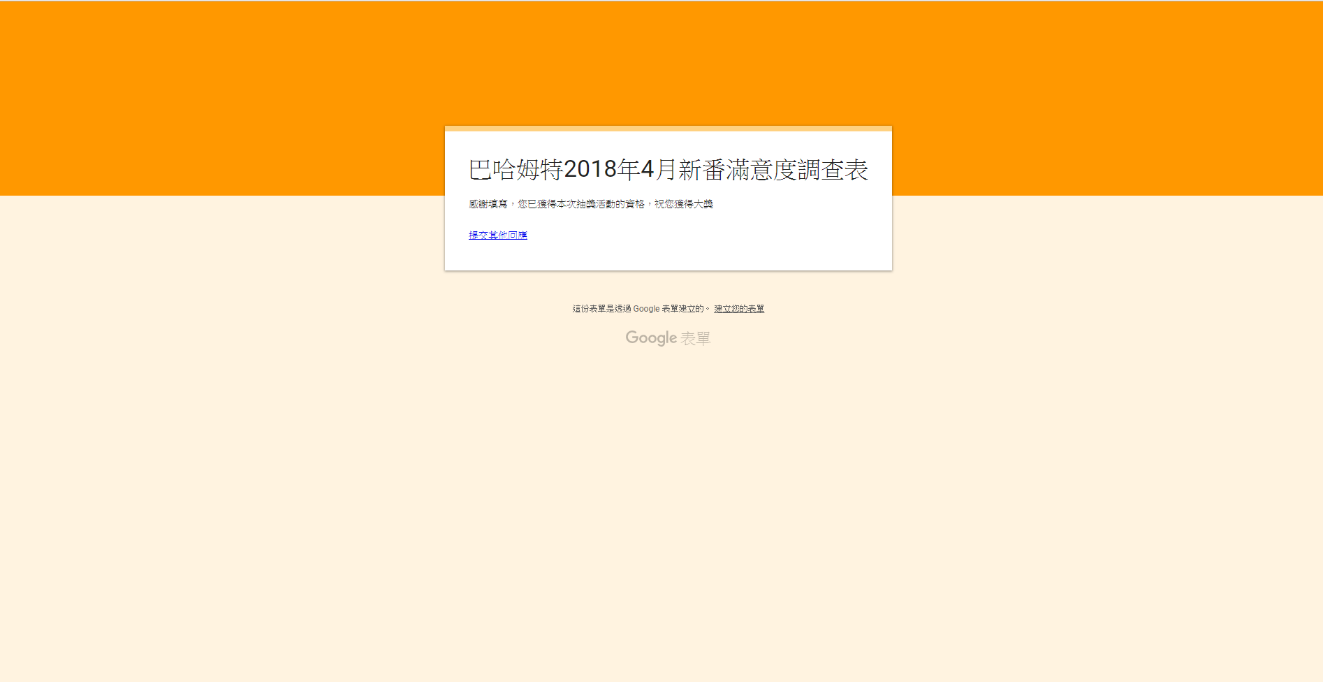
而會去做這個表單的原因就在於我其中的一個小天使A1045521-廖啟翰-資訊工程學系-xkiridox@gmail.com他是一個不折不扣的動漫迷，像這種滿意度調查表填寫了之後還能去參與抽獎的活動，而且其提供的獎項都是足以讓動漫迷為之瘋狂的，所以可以說幾乎只要是動漫迷都會毫不猶豫的來去做參與，而且這件事也是在問了其他動漫迷之後才知道的，所以我才會特地針對他來去設計這樣的表單，而表單的內容如下 :











那麼我的攻擊方式就是透過寄信的方式，而其信件的寄送方式仍然是使用GOOGLE表單內建的寄信系統下去做發送，而其信件的內容如下圖所示 :

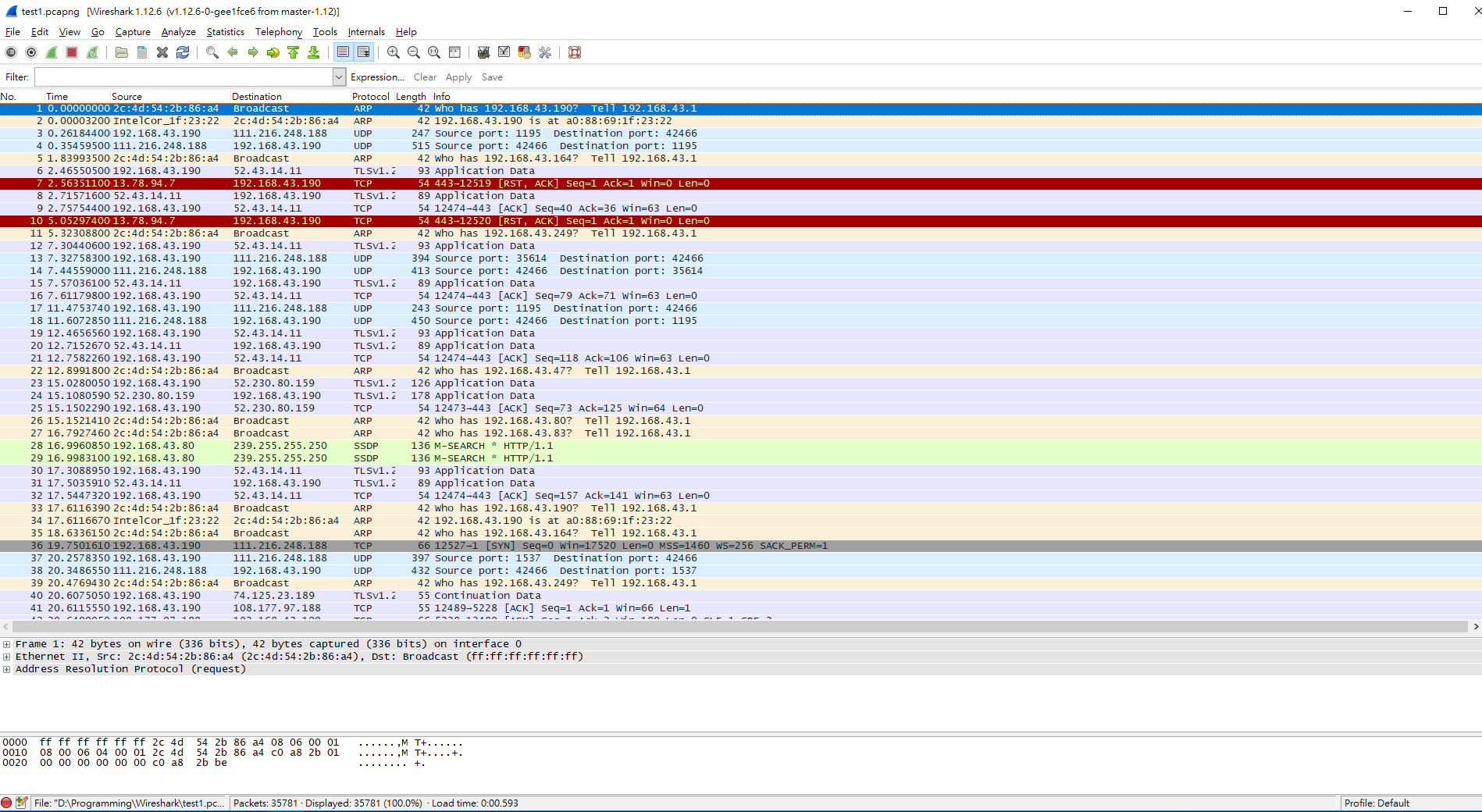


那只要目標輸入了表單的內容之後，其目標所輸入的表單內容會存到我的GOOGLE帳號內，這樣我就能夠獲得目標的個人資訊

而以上其實不論是哪種表單的設計，其最核心的關鍵點還是去針對目標所感興趣的內容下去做設計，並且除了針對每個小天使的喜好不同來去客製化表單以外，我也連同寄件者的信箱都一併做模仿的動作，為的就是要讓整封信件更加的真實，這樣才能使目標上當並且受騙。

* 1. 手機端釣魚以及wireshark的搭配
     1. wireshark的搭配

當初在網路安全公布釣魚作業的時候助教是有來去演示利用wireshark來去監控同網域下的每個使用者所傳送的封包，藉此來去竊取到其他人的帳號密碼，而這也是我最先開始嘗試的釣魚方式，而我的攻擊方式就是我利用自己的手機下去開啟無線熱點，並且將其無線熱點的名字命名成iNUK\_DEV，也就是命名成和學校wi-fi一樣的名字，來去讓其他人連到我所開的基地台，然後再搭配wireshark的監控來去竊取別人的封包，而其wireshark呈現出來的畫面就如下所示 :



而手機畫面下圖所示 :

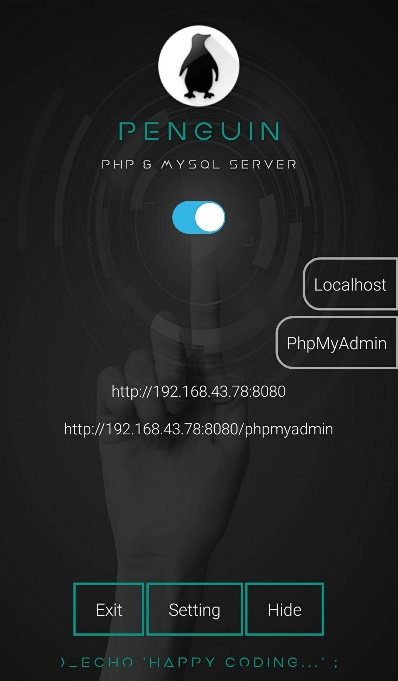
而會想去用這個方法的原因就是因為大部分的高大學生都會去連學校的wi-fi，所以藉由此方式我是有高度的機率可以來去釣到我的小天使的個人資訊。

* + 1. 在手機上架虛擬server

這個設計的核心以及攻擊方式就是要來去模擬學校wi-fi的登入頁面，藉由在手機建立一個虛擬的server，當使用者連上我所開的無線熱點之後，就能夠自動彈出我所設計的假登入頁面，藉此來去獲取目標的帳號以及密碼，又加上高大許多學生都會去連學校的wi-fi，所以我認為這個方法是極度可行的。

所以會想去設計這樣的釣魚就是利用高大學生會來去連學校wi-fi的行為，來去嘗試釣到目標的個人資訊。

其釣魚畫面如下所示 :

而以上的這兩種方法都是用於攻擊所有的小天使，所以可以說這個方法時有極大的可能性可以去獲取小天使的個人資訊。

而以上這幾種方法就是我經過1到2個禮拜針對每一個小天使的嗜好以及感興趣的內容下去做一一設計的動作，目的就是為了大大提高我可以抓到小天使的個人資訊。

1. 攻擊的結果
   1. 工作紀錄表

|  |  |  |
| --- | --- | --- |
| 項目 | 開始時間 | 結束時間 |
| 手機無線基地台 + wireshark 釣魚布置(適用所有的小天使) | 4月16日 | 5月4日 |
| 調查與分析小天使(王羿捷、王于豪) | 4月13 | 4月20日 |
| 調查與分析小天使(黃心眉、廖啟翰、賴冠霖) | 4月13日 | 4月27日 |
| 網頁釣魚(學生教務系統、Facebook)設計以及針對小天使特性下去做調整(賴冠霖=>學生教務系統、黃心眉=> Facebook) | 4月23日 | 4月27日 |
| GOOGLE表單釣魚(爐石戰記抽獎活動、英雄聯盟抽獎活動、動漫調查表抽獎活動)設計以及針對小天使特性下去做調整(王羿捷=>爐石戰記抽獎活動和英雄聯盟抽獎活動、王于豪=>爐石戰記抽獎活動和英雄聯盟抽獎活動、廖啟翰=>動漫調查表抽獎活動) | 4月17日 | 4月27日 |
| 網頁釣魚信件寄送(賴冠霖=>學生教務系統) | 4月26日 | 4月26日 |
| 網頁釣魚信件寄送(黃心眉=> Facebook) | 4月27日 | 4月27日 |
| GOOGLE表單釣魚信件寄送(王羿捷、王于豪=>爐石戰記抽獎活動和英雄聯盟抽獎活動) | 4月23日 | 4月23日 |
| GOOGLE表單釣魚信件寄送(廖啟翰=>動漫調查表抽獎活動) | 4月27日 | 4月27日 |
| 手機虛擬server建置 + 高大wi-fi登入網頁仿造 | 4月20日 | 4月29日 |
| 手機虛擬server攻擊進行(適用所有的小天使) | 4月27日 | 5月4日 |
| 檢查攻擊成效 | 4月16日 | 5月4日 |

* 1. 攻擊成效

以下分別是我每一個攻擊所得到的結果以及成效 :

* + 1. 網頁式釣魚(賴冠霖=>學生教務系統、黃心眉=>Facebook)
       1. 賴冠霖=>學生教務系統 ---------------------> 失敗

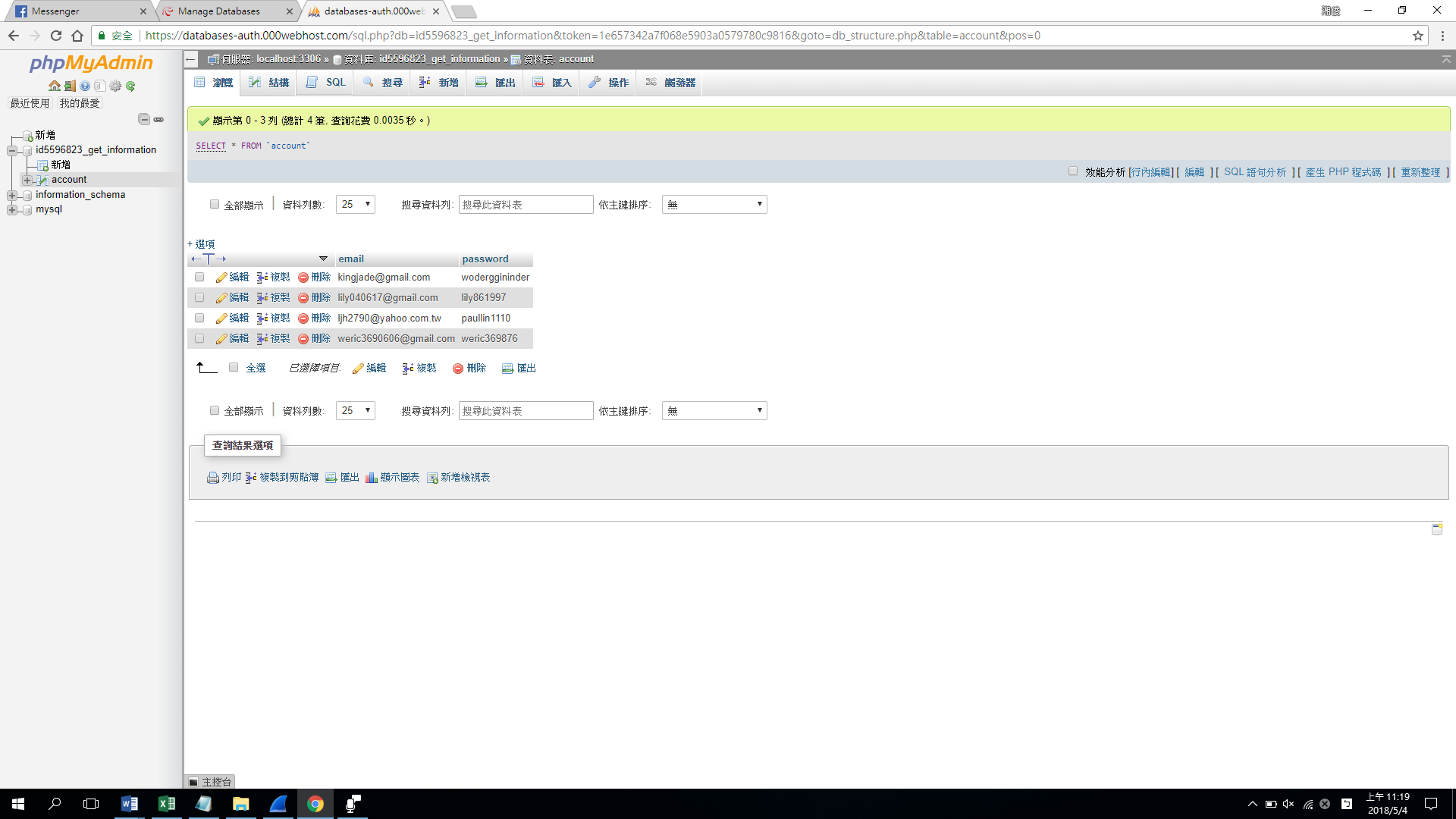
我覺得會失敗的原因有三個，第一個就是因為我是在攻擊的這三週寄的信件，所以大家的警戒心都異常的高，又加上大部分大家都是寄學校相關的信件到自己的小天使那，所以導致大家本身都不太會去看學校的信箱了，結果因為這個釣魚攻擊就更加的不會去看了，也不會去相信。

而第二個原因就是我所製作的假的學生教務系統的網域名我是無法去給他做修改，更甚至覆蓋掉這個網域名，造成假如目標去細看網址的話一定會馬上發現這個網頁是假的而不是真的，除非目標真的沒有去看網址的習慣，否則我覺得很快就會被識破，更不用說要他輸入他自己的帳號以及密碼。

而第三個原因就是有很高的機率目標早已就看過期中預警通知的信件是長怎樣的樣子，所以目標在一看到信件的時候就可以很明顯地知道這封信不是學校寄的，那麼它自然就不會受騙了。

(2) 黃心眉=>Facebook ---------------------> 成功

其實在要去實施Facebook的釣魚之前我是先針對別人的小天使下去做測試，來去看看成效如何，而我原本是沒有抱持多大的信心，畢竟學生教務系統這個釣魚方法已經先失敗了，所以我這個Facebook的方法也只是抱著嘗試的心態，結果讓我十分意外的是竟然真的有人上鉤，其實我是蠻意外的，雖然我無法確定他輸入的是否是正確的還是假的，但能有所收穫讓我是十分的訝異的，而那些我拿來做測試的小天使分別有俞建玨、林冠宏、王彥翔這三個人，而他們被釣到的帳號密碼分別如下所示 :



所以建立在這樣的基礎下，我就立馬把這封信件也寄到我的小天使-黃心眉那，而讓我既驚喜又意外的是我的小天使她也上鉤了，也就是綠色方框的那組帳密就是我的小天使被我我釣到的帳號以及密碼。

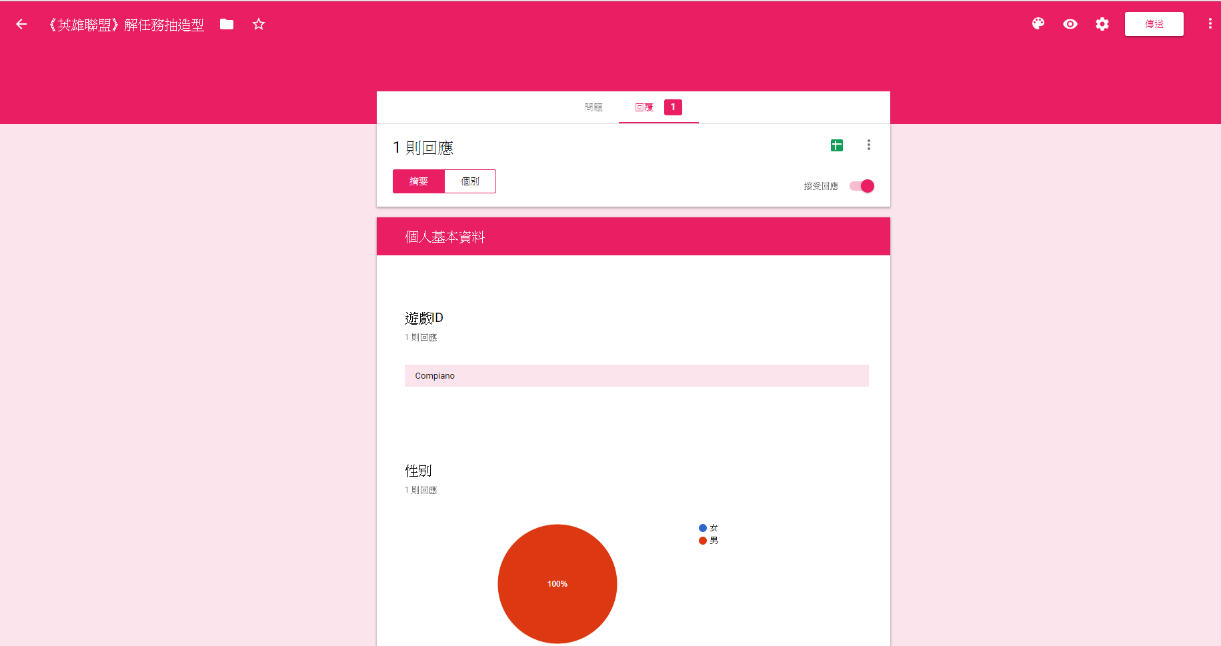
所以由此可以知道一點的是Facebook對於大家的重要性是極度的重要，大家的FB裡頭都有許多自己珍貴的資料，沒有人會希望自己的FB資料被別人竊取光光，所以我在猜想大家一定是處於心急的狀態下才會去做輸入的動作，否則假如今天這個東西對她真的是極度不重要的話，那麼她也不會傻傻地讓我釣到，可見用FB來去做釣魚真的十分的有效。

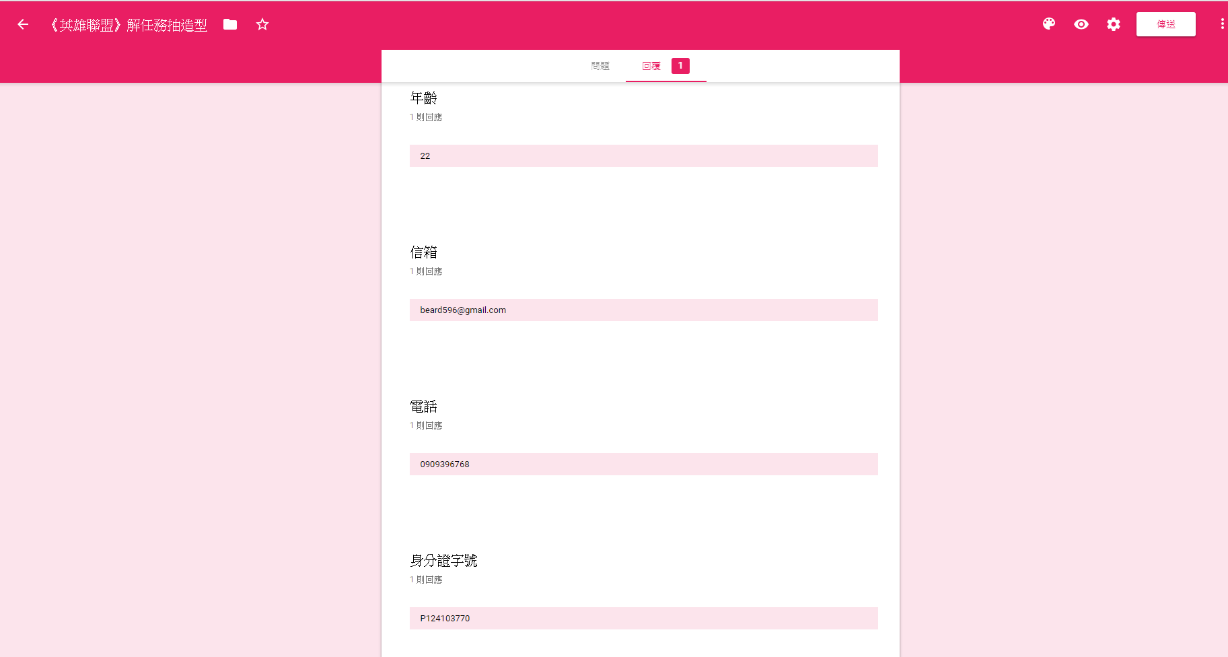
* + 1. GOOGLE表單釣魚(王羿捷=>爐石戰記抽獎活動和英雄聯盟抽獎活動、王于豪=>爐石戰記抽獎活動和英雄聯盟抽獎活動、廖啟翰=>動漫調查表抽獎活動)
       1. 王羿捷=>爐石戰記抽獎活動和英雄聯盟抽獎活動 ---> 失敗

這個會失敗的主因有兩個，第一個是我是在這三週的攻擊時間寄出這封信的，所以大家都處於高度的警戒，所以連點開都不去點開，而第二個原因就是我可能疏忽了目標已經沒有再玩這兩款遊戲了，所以如果對方收到的話一定會感覺怪怪的，因此也不會去做任何填寫的動作，所以才會導致最後的失敗。

(2) 王于豪=>爐石戰記抽獎活動和英雄聯盟抽獎活動 --> 成功

在我寄的這兩份表單，只有從英雄聯盟抽獎活動這個表單釣到他的個人資料，而爐石戰記抽獎活動之所以會釣不到的緣故就是他沒有再去玩這一款遊戲了。所以才導致他的英雄聯盟的資料是沒有釣到的，而我釣到的資料分別如下所示 :





而我認為這個可以成功的緣故就像我前面提到的設計動機一樣，目標是只要看到與遊戲相關的抽獎就會很積極的去做參與，所以我覺得能釣中目標與這個原因是極度相關的。

* + 1. 手機釣魚(所有的小天使)
       1. 仿造學校wi-fi名稱 + wireshark監控 -----------> 失敗

這個方法之所以會失敗的原因就是我誤以為將電腦連上手機所開出來的wi-fi，透過別人連上我手機的wi-fi之後，我已從電腦的wireshark監控到連上我的wi-fi的人的封包，結果正確的做法應該是要從電腦上開AP才對，這樣我才能監控到連上我這個AP的使用者的封包，所以才會導致我最後的失敗，因為我原本想說如果這項東西能夠成功的話，那就會變得很容易，因為我在試的期間，我的SSID的名字是改成跟高大一樣的名字，所以就像老師上課講的，誰的訊號強，對方就會自動連到這個較強的訊號，而我那時試的時候確實有需多人就連上我所開的無線基地台，但無奈於這樣的緣故，導致最後是以失敗作為收尾。

(2) 手機自建虛擬server + 模仿高大wi-fi的登入頁面-> 失敗

我覺得會失敗的原因有兩個，第一個就是要能夠連上我這個仿造的高大wi-fi的登入頁面，必須輸入我server的IP才連結的到，而這樣做就十分的奇怪，並且別人也不會傻傻地去輸，而且又加上連IP都遮不掉的話，那麼就更不可能成功，而第二個就是我無法讓我仿造的高大wi-fi的登入頁面在別人連接到我所開的wi-fi的時候，自動彈出這個仿造的畫面，就跟高大的一樣，所以因為這兩個主要的緣故，才會導致這樣的方法最終走向了失敗。

1. 心得報告

在做完了這一次網路安全的釣魚專題的時候，我發覺我所身處的網路世界真的是十分的可怕，這期間我一直持續的分析與觀察網路釣魚的手法，可以說是一個比一個還要來的犀利，有的可能和善一點的就只是寄釣魚信件，可是有些極端一點的就直接把要攻擊的目標的電腦系統直接做入侵的動作，讓目標想要防也都防不了，可以說真的是十分的可怕，在我以前的時候，我在上網的時候根本就沒有去多想危不危險的問題，我當時的概念就十分的單純，反正只要是能用的並且對我是有意義的網站就是好網站，可是到現在認真的思考過後才發現我以前一直處於十分危險的狀態，隨時都有可能被人家把我自己的個資都給盜取光光。

而在我以前的時候還真的是發生過這樣的問題，導致我的FB帳號被中國大陸的駭客給盜取走，那時我不論怎樣去改就是始終會被駭客給破解，導致我整個FB的帳號完完全全的報銷掉，連救都救不回來，可以說那時候我真的是完完全全的嚇到了，這也導致我之後在上網的時候就變得很小心翼翼，就是為了避免同樣的事情又再度的發生。

而這次自己在嘗試做釣魚的時候可以說是遇到了許多的難關以及問題，在上課的時候聽老師講感覺好像都蠻容易達成的，可是等到真的要去做的時候我才發覺到根本就沒有那麼的容易，而且其實這次做的許多東西都充滿著破綻，只要目標警戒心稍微高一點的話，那可以說根本就無法掉到別人的資料，所以我這次還能釣成功兩個人只能說是算我運氣好而已，而且剛好目標的警戒心也沒那麼的高，要不然說實在的我雖然做了一大堆的方法，也針對了每一個人做分析以及特定的釣魚設計，但做出來的東西真的是連檯面都登不上，而且根本完完全全就是一個失敗品，所以我認為我在網路安全這一個領域上還有許多是我要去學習的，絕對不是像我所想像的那麼的簡單，因為在這個領域的背後還暗藏著許多我所不知道的祕密，所以也是多虧老師出了這項釣魚的專題，才能夠讓我更加的清楚自己對於網安的知識還是過於的粗淺，而且需要好好的去做加強的動作。