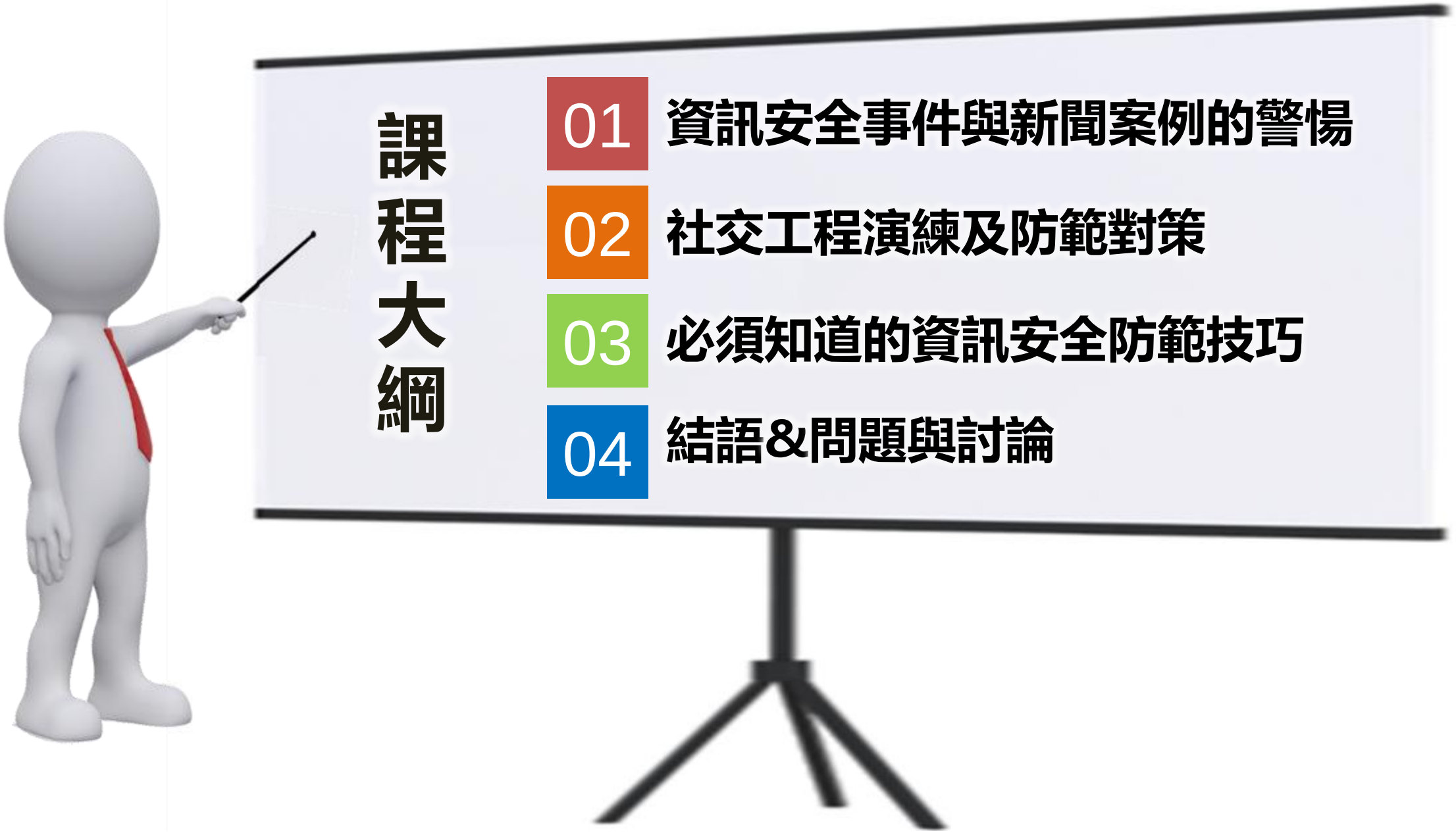
屏東科技大學

社交工程&資訊安全教育訓練

蔡旻芳
中華電信高雄所/教學科
mftsai@cht.com.tw


課程大綱
01
資訊安全事件與新聞案例的警惕
02
社交工程演練及防範對策
03
必須知道的資訊安全防範技巧
04
結語&問題與討論

Part 01

資訊安全事件與新聞案例的警惕

每日都有許多台灣網站受駭

zone-h unrestricted information

Home | News | Events | Archive | Archive ★ | Onhold | Notify | Stats | Register | Login | search...

Mirror saved on: 2020-09-14 01:17:42

Notified by: Black_X12 **Domain:** http://buffalomachineworks.com/root.php **IP address:** 50.31.162.218

System: Linux **Web server:** Apache Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2020-09-14 01:17:42

每日都有許多台灣網站受駭

公開

ZD-2021-00034	公開	光泉牧場股份有限公司	2021/01/14	waffle
光泉 Account takeover				
ZD-2020-00984	公開	垂坤食品有限公司	2020/11/29	pwn
垂坤 Reflected XSS				
ZD-2020-00982	公開	加州椰子國際股份有限公司	2020/11/28	niench20
Caco 帳號接管				
ZD-2021-00029	公開	東森新聞雲股份有限公司	2021/01/13	Alex
東森新聞 XSS 漏洞				
ZD-2020-00980	公開	TACERT台灣學術網路危機處理中心	2020/11/27	pwn
啟英高級中學 校務系統SQL Injection				
ZD-2020-00979	公開	威策電腦	2020/11/27	癡情法王
威策電腦網站，存在XSS漏洞				
ZD-2021-00022	公開	TACERT台灣學術網路危機處理中心	2021/01/08	鄉民
屏東女中				

1 / 531 > +10 >>>

ZeroDay

值得信賴的漏洞通報平台

https://zeroday.hitcon.org/vulnerability/all

ZD-2021-00034 發信 光泉牧場股份有限公司

光泉 Account takeover

僅參考email進行資料修改

```
POST /MBP/SendPassword/ResetPWD HTTP/1.1
Host: www.kc-foods.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 609
Origin: https://www.kc-foods.com
Connection: close
Referer: https://www.kc-foods.com/MBP/SendPassword/ResetPWD
Cookie: _ga=GA1.2.895384644.1610633771; _gid=GA1.2.1673676304.1610633771; __RequestVerificationToken_L01CUA2=
JYxRB4YLf2N4BqGO6IE3glULpAX5uNvVYanyCmj_qYK891v-OgF2DbitJO1JPcHBtMuBobtSKVD7dhvvxxxR9VTO8a8RC00Nej_VaoSdmxE1; ASP.NET_SessionId=
kc2dzurdxeotay44dpvlharf; LoginUserMsg=
[redacted]
gzVI4p
Upgrade-Insecure-Requests: 1

pwd.Email=[redacted]&pwd.PASSWORD=[redacted]Z&pwd.NEWPWD=1234QWer&pwd.NEWPWDCONF=1234QWer&g-recaptcha-response=
03AGdBq26UtKaq6uDVNeZQg3[redacted]jLWTv1iPUXQ4qNo3p0g3_1zzoacqZRt84JtsmUW9hNcWiIPL0NTvMkho7lCGGSORBLI848I_vQeSp5Vv0twt8iK7yRcil27PvvalA-cJU__o-dxui
NmrK8kPtWjS212106jLdLNan[redacted]h4fQhzQAGPu_CwUVWezTGsLtg9sEliS-WFR_dx65o_IleFr2ffWAsOef_smF3S6nZ8vvxSN2I9014LOHgcUB8uX8zgxO9pUuSSFQ7ptFEryLRX6r
```

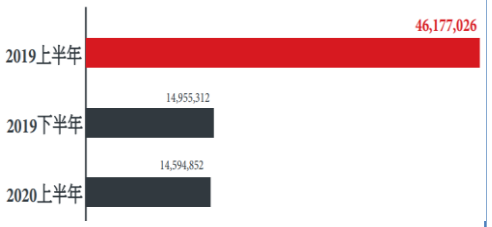
修改密碼與會員資料時，若知道受害者會員註冊email，

修改email參數即可蓋過該會員原有的資料以及密碼

根據趨勢科技安全報告指出 保護因疫情而改變的工作環境

勒索病毒 威脅持續增加

- 勒索病毒依然持續鎖定特定目標(2010)
- 勒索病毒集團威脅公開使用者失竊的資料(2020)

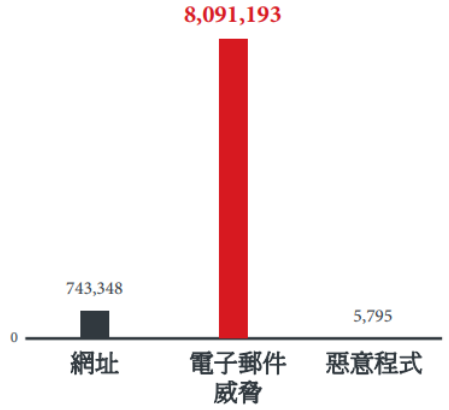


勒索病毒相關元件偵測數量半年期比較 (檔案、電子郵件及網址)

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

網路釣魚網址 威脅變本加厲

- 以新冠肺炎 Covid-19 為主題的攻擊正不斷增加(2020)
- Office 365 的網路釣魚威脅倍增(2019)
- 出現破解雙重認證機制的網路釣魚技巧



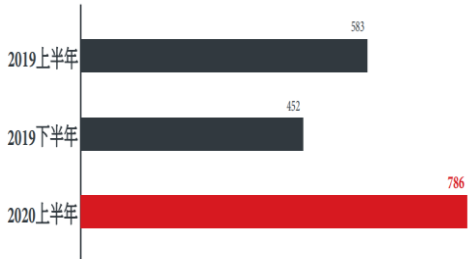
：新冠肺炎 Covid-19 相關威脅的數量與分布 (2020 上半年)。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

資安公告發布 數量增加

Windows 7 已於2020/01/14終止支援

- 漏洞已成為一項迫切但卻難以解決的問題
- 2020 上半年修正的軟體漏洞數量創下歷史新高(RDP 漏洞攻擊/PowerShell 腳本)
- IoT 殭屍網路攻擊數量增加。
- 利用指令列腳本 (Shell Script) 執 行網站遠端指令



ZDI 計畫揭露的漏洞數量半年期比較

資料來源：趨勢科技 Zero Day Initiative™ (ZDI) 漏洞懸賞計畫。

變臉詐騙 威脅持續變形

- 變臉詐騙 (BEC) 數量較 2019 下半年增加 19%，所以應該是有不少歹徒希望趁著 Covid-19這波疫情海撈一筆。

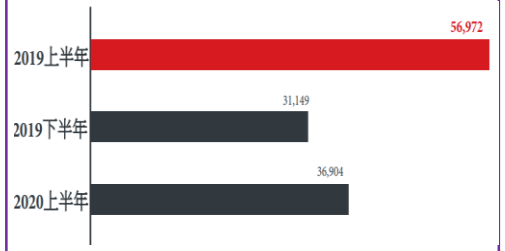


圖 31：變臉詐騙 (BEC) 數量半年期比較顯示 2020 上半年稍微增加。

註：這項資料代表偵測到的變臉詐騙所有攻擊案例，不論攻擊成功與否。

From 2020_midyear_cybersecurity_report_c.pdf

現在正碰到的資安威脅的公司.....

廣達傳遭勒索軟體REvil攻擊，歹徒要脅廣達及蘋果4/27日前購回外洩產品資料...

2021-04-21 12:05 聯合報 / 記者李承穎 / 台北即時報導

+ 資安

駭客勒索廣達一億美元 立委促資安國家隊解決

民眾黨立委高虹安披露駭客勒索我國企業。記者李承穎 / 攝影

高虹安說，駭客要求廣達必須在4月27日之前以加密貨幣XMR(門羅幣)支付5000萬美元，或者在倒計時結束後支付1億美元，這個威脅四月上旬已在業界傳開，如果廣達不開始就贖金進行談判，「所有Apple設備的圖紙以及員工和客戶的所有個人數據將在隨後的銷售中發布」。

而在20日，REvil就在暗網上架設名為「Happy Blog」網站，將Macbook Air M1的詳細設計圖PO出，同時透露還有Apple Watch、Macbook Pro以及ThinkPad Z60m設計圖。

高虹安說，政府既已號稱成立「資安國家隊」，就應該盡快提出包括應對勒索軟體在內的資安解決方案，協助科技產業加強與整合資安防護資源，共同發展最適當的防禦因應措施，以保護我國科技產業與全民的資訊安全不受勒索威脅。

https://udn.com/news/story/6656/5403116

現在正碰到的資安威脅的公司.....

宏碁及日月光相關公司亦是REvil 勒索病毒的受害者.....

宏碁驚爆遭駭 勒索14億元

2021-03-21 01:17 經濟日報 本報綜合報導

宏碁（2353）電腦歐美分公司驚爆遭駭客入侵，勒索5,000萬美元（約新台幣14億）贖金，由於宏碁未付款，駭客已在暗網公布部分財務資料，調查局資安站立案追查，向宏碁取得國外分公司客服伺服器LOG檔，分析比對駭客組織及攻擊手法。

宏碁傳駭客勒索

項目	內容
駭客集團勒索	國外資安網站BleepingComputer報導，宏碁遭REvil病毒團體勒索攻擊，並要求5,000萬美元的贖金，
宏碁回應	將近期異常事件通報多國執法及資訊保護機關，對營運沒重大影響，將強化資安

資料來源：外媒、宏碁　　黃晶琳／製表

https://money.udn.com/money/story/5612/5332416

開出最高的贖金金額。Bleeping Computer隨後也找到可能是勒索訊息的螢幕截圖。該新聞網站推測，宏碁與REvil疑似於3月14日開始進行對話，而從螢幕截圖來看，駭客要脅若是沒有在期限內付錢，贖金就會翻倍到約1億美元。

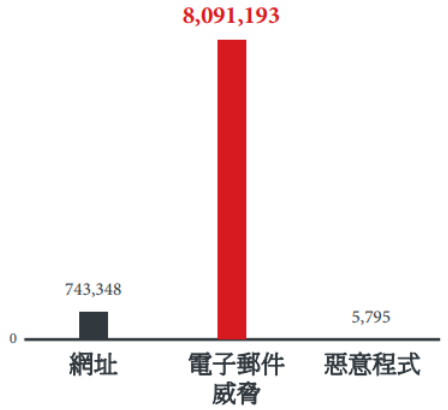
https://ithome.com.tw/news/143355?fbclid=IwAR02hE3fyRFE-mEqL93kROg7t7ofM5dKuP1b0ex5uZbzXyAWjJGTE_CT7M8

根據趨勢科技安全報告指出 駭客仍持續不斷發動攻擊

保護因疫情而改變的工作環境

網路釣魚網址
威脅變本加厲

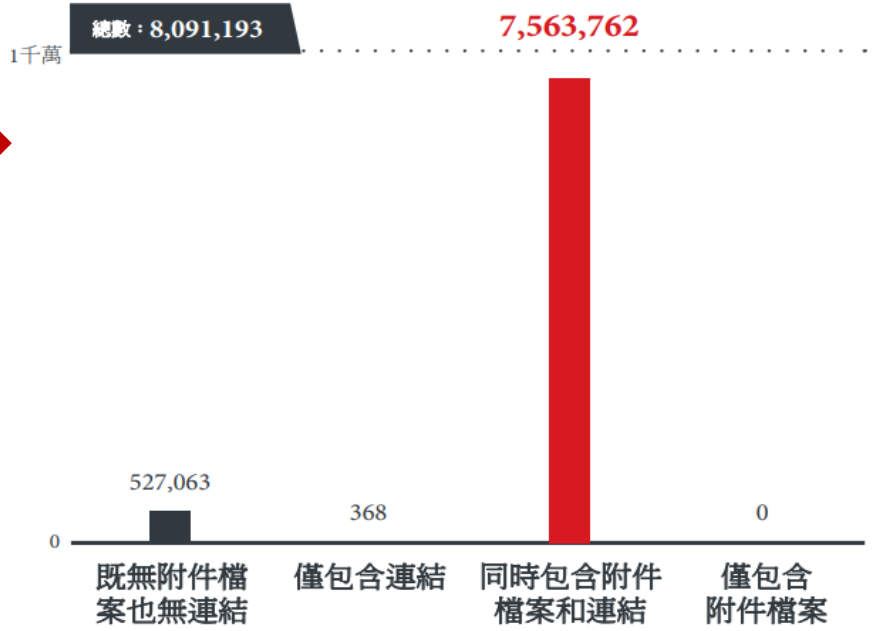
- 以新冠肺炎 Covid-19 為主題的攻擊正不斷增加(2020)
- Office 365 的網路釣魚威脅倍增(2019)
- 出現破解雙重認證機制的網路釣魚技巧



：新冠肺炎 Covid-19 相關威脅的數量與分布 (2020 上半年)。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

我們所偵測到的電子郵件威脅，絕大多數 (93.5%) 都含有一個惡意附件檔案和一個惡意連結。令人訝異的是，完全不含連結也無附件檔案的電子郵件威脅數量，甚至高於僅有其中一種的數量，這顯示歹徒傾向於同時使用惡意連結和惡意附件。



	整體	Covid-19
一月	94,488,577	3,916
二月	100,468,874	9,497
三月	111,026,602	34,197
四月	224,187,318	348,767
五月	252,588,246	168,576
六月	146,542,789	178,395
總數	**929,302,406**	**743,348**

Covid-19 相關惡意網址每月數量，相較於所有惡意網址的整體數量 (2020 上半年)。

註：這項資料代表網站信譽評等服務 (WRS) 偵測到的 Covid-19 相關惡意網址數量。

資料來源：趨勢科技 Smart Protection Network 全球威脅情報網。

From 2020_midyear_cybersecurity_report_c.pdf

你有可能會碰到的資安威脅

最近最熱門的簡訊釣魚新聞(1/2)

國泰世華

全部 地圖 新聞 圖片 影片 更多 設定

約有 11,900,000 項結果 (搜尋時間：0.64 秒)

廣告 · winbank.url.tw/

線上諮詢國泰世華貸款資訊 - 提供【國泰世華】貸款資訊

優質專案 國泰世華貸款資訊 信貸，房貸，車貸，給你豐富的選擇，超低的利率。 速撥貸銀行優惠貸款諮詢網集結各家銀行貸款方案，服務六大承諾是我們的堅持。多元選擇。專業服務。快速核准。申辦簡便。服務: 貸款利率比較, 24H填單預約諮詢。

信用貸款 · 房屋貸款 · 汽車貸款 · 負債整合

廣告 · www.cathay-bk.com.tw/

國泰世華泰幸福 貸款金運用自如 - 【快速申貸看這裡】國泰世華...

線上快速申貸超便利，最快 1 天核貸，還有免費貸款諮詢，國泰世華理財規劃客戶信賴度全國 No.1。線上快速申貸，還有免費預約貸款諮詢，讓您提前做好資金規劃！ 實現夢想無需等待，資金的問題就交給國泰。服務: 泰幸福信用貸款, 職域員工信貸, 一般資金周轉

www.cathaybk.com.tw

國泰世華銀行

國泰世華銀行. 首頁; 數位專區. 數位專區首頁; 數位人生. 學生 上班族 成家立業 家庭主婦 退休族. 數位服務. 網路銀行App 網路銀行 LINE個人化服務 線上申辦櫃檯.

網路銀行

沒有國泰世華網路銀行嗎？立即申辦網銀; 沒有國泰世華銀行帳戶嗎 ...

服務據點

國泰世華提供分行地址、ATM查詢、海外據點查詢，輸入您的位置

思考一下

請問那幾則國泰世華的訊息是有問題的?

2021/2/1 (週一) 上午 04:43

國泰世華銀行 <cathaybk@news.mybank.com.tw>

[外部郵件]【2021年2月份】國民經濟信心問卷調查

收件者 蔡OO

若您有意願參加該活動，請按以上連結參考相關活動辦法，並點選以下前往填寫問卷，並參加抽獎活動連結，本集團將在本問卷調查及抽獎所需之範圍內使用您的姓名、電話、E-mail 等資料。(註：本份問卷調查及抽獎活動所填寫之個人資料將不會使用作為商業行銷用途)。

國民經濟信心向來是影響台灣經濟展望的關鍵因素之一。為了深入瞭解整體經濟、金融市場、及就業和收入對民眾經濟行為的影響，並期冀依此對未來景氣做出研判或預警，本集團每月進行此問卷調查，您寶貴的想法是十分重要的研究依據，敬請您惠予填答。

國泰金控感謝您的支持！

(本次調查問卷回收期間為 2/1-2/7，調查結果

前往填寫

填寫問

*點選上方任一連結，即代表您已詳閱本問卷抽獎活動辦法，

獎所需之範圍內，依相關法規蒐集、處理、國際傳輸及利用本

☆2021 年 1 月份國民經濟信心調查結果已出

【2021 年 1 月份國民經濟信心調查結果】

☆若您不想再收到此類訊息，請點選此處

https://news.mybank.com.tw/cathaybk_a/click.aspx?url=https://www.cathaybk.com.tw/cathaybk/-/media/61a3ea56ade84bd9aa9285b41470afc1.pdf&k=2abwe2v4/rkhxtzxhpp7uczsc0e1lvpelzehvd1fvme=&link_id=165518&c=nzuanib8dw8ff1n5sod+wa==
按一下或點選以追蹤連結。

https://news.mybank.com.tw/cathaybk_a/mailhuntercanceledm.aspx?v=ret8vrwib8g=&k=75hwcimxc599+jshfk2znbhv5bwkbnfj&p=2abwe2v4/rkhxtzxhpp7uczsc0e1lvpelzehvd1fvme=
按一下或點選以追蹤連結。

最近最熱門的簡訊釣魚新聞(2/2)

假國泰世華銀行釣魚簡訊 三天全國21人財損300萬元

2021-01-30 17:37 聯合報 / 記者廖炳棋/即時報導

刑事局指出，近日警方接獲多名民眾報案，聲稱收到「偽冒國泰世華網銀」的釣魚簡訊，內容：「『國泰世華』您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用」，這樣的訊息誘使被害人到假網銀登入頁面中輸入真實網銀的帳戶及密碼，詐騙集團就據此惡意連結、盜用被害人銀行帳戶，將款項轉帳至人頭帳戶，造成被害人財物損失。

刑事警察局統計，1月27日到1月29日止，全國警察機關受理「涉及國泰世華的釣魚簡訊（惡意連結）」檢舉案有83件，其中出現被害人帳戶遭盜用的報案有21件、財損金額超過新台幣300萬元，案件數還在持續增加。

https://udn.com/news/story/7320/5218306

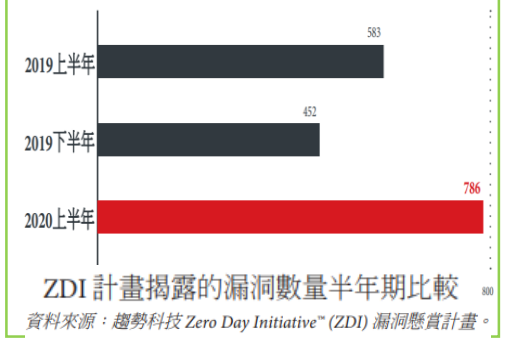
根據趨勢科技安全報告指出

保護因疫情而改變的工作環境

歹徒趁著這波疫情興風作浪，發動一波又一波以 Covid-19 為主題的攻擊，在各大平台撒下大量誘餌，包括：電子郵件、社群網路、惡意網站，以及冒牌的行動應用程式 。
其中最受網路犯罪集團青睞的就是視訊會議軟體，因為人們在被迫隔離的期間需要一種有效的溝通方式，駭客對視訊會議軟體的攻擊，從故意擾亂會議進行 (例如Zoom 轟炸) 到利用軟體安裝檔來夾帶惡意程式，進而發動網路攻擊等等。

資安公告發布數量增加

- 漏洞已成為一項迫切但卻難以解決的問題
- 2020 上半年修正的軟體漏洞數量創下歷史新高(RDP 漏洞攻擊/PowerShell 腳本)
- IoT 殭屍網路攻擊數量增加。
- 利用指令列腳本 (Shell Script) 執 行網站遠端指令



- 2019 年 Zoom 軟體在 Mac 電腦上被發現有資安漏洞，導致 Zoom 軟體可以在不須經過使用者同意下，**自動開啟鏡頭**
- Zoom 的安全威脅 – 使用者圖方便，**不喜歡設定密碼**
- 創辦人背景有強烈**中國色彩**，雖在美國上市但**主要開發團隊皆在中國境內**

https://bit.ly/2CvJGEk https://www.ithome.com.tw/news/137058

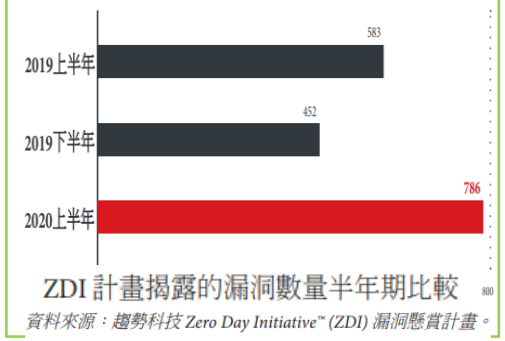
根據趨勢科技安全報告指出

保護因疫情而改變的工作環境

歹徒趁著這波疫情興風作浪，發動一波又一波以 Covid-19 為主題的攻擊，在各大平台撒下大量誘餌，包括：電子郵件、社群網路、惡意網站，以及冒牌的行動應用程式 。
其中最受網路犯罪集團青睞的就是視訊會議軟體，因為人們在被迫隔離的期間需要一種有效的溝通方式，駭客對視訊會議軟體的攻擊，從故意擾亂會議進行 (例如Zoom 轟炸) 到利用軟體安裝檔來夾帶惡意程式，進而發動網路攻擊等等。

資安公告發布數量增加

- 漏洞已成為一項迫切但卻難以解決的問題
- 2020 上半年修正的軟體漏洞數量創下歷史新高(RDP 漏洞攻擊/PowerShell 腳本)
- IoT 殭屍網路攻擊數量增加。
- 利用指令列腳本 (Shell Script) 執 行網站遠端指令



最早公布遭DDoS攻擊的是遠振資訊，在最近連續三天都有發布相關公告。他們先是在20日，於自家網站證實遭受攻擊，而根據他們在21日揭露的資訊顯示，這次事件的發生，最早是從19日傍晚23時開始，隔日情況變得更嚴重，**一日內就遭遇3波攻擊**，早上、下午與晚上都有，**每次都持續1到2小時**。

Insecam 線上即時WEBCAM網站

http://www.insecam.org/

Insecam **Most popular** Manufacturers Countries Places Cities Timezones New online cameras FAQ Contacts

ENHANCED BY Google

IP cameras: Kaohsiung

« 1 2 **3** 4 5 6 »

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

Watch Hi3516 camera in Taiwan, Province Of ,Kaohsiung

漏洞警訊公告

行政院國家資通安全會報技術服務中心
National Center for Cyber Security Technology

「Insecam」網站暴露多款無身份驗證機制或使用預設密碼之網路攝錄影機畫面，允許任意使用者觀看即時影像畫面，進而造成機敏資訊洩漏

透過搜尋引擎找IOT漏洞-破解印表機

https://www.shodan.io/

Part 02

社交工程演練及防範對策

資安威脅

勒索軟體/DDOS攻擊

駭客入侵、資料外洩

漏洞攻擊、操控IoT裝置

APT進階持續威脅

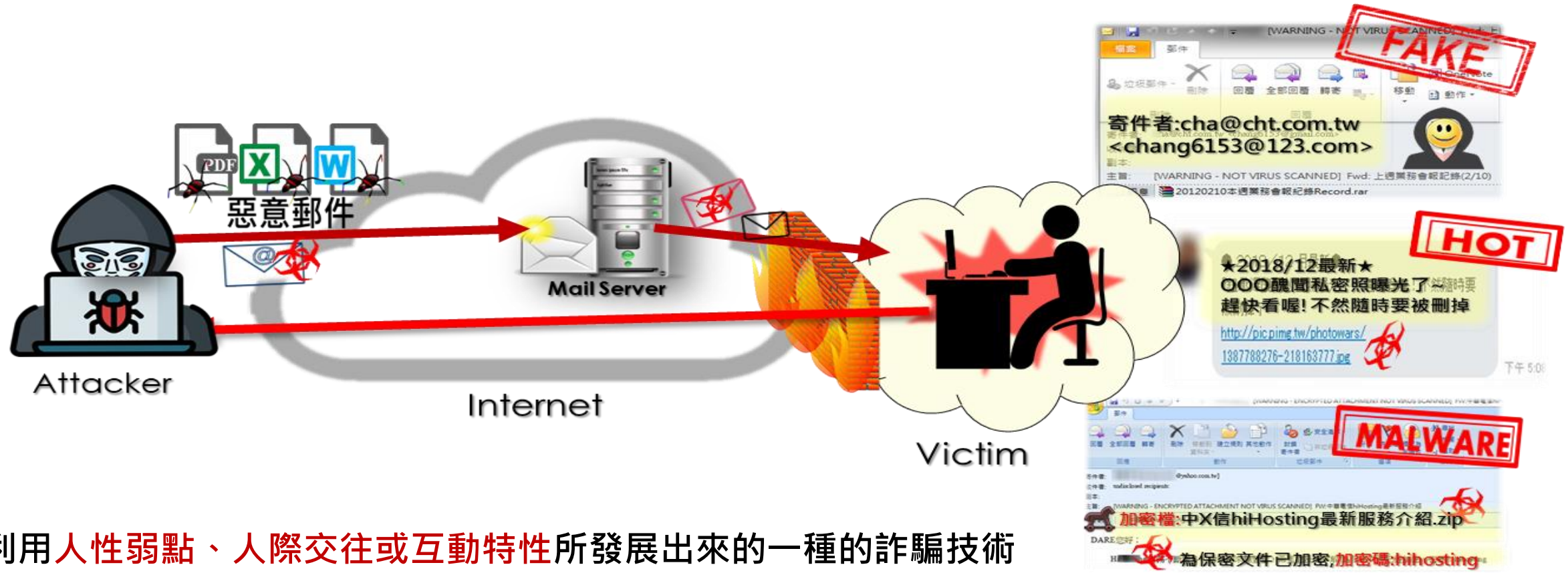
資訊安全防範對策

社交工程

郵件安全設定

釣魚網站/

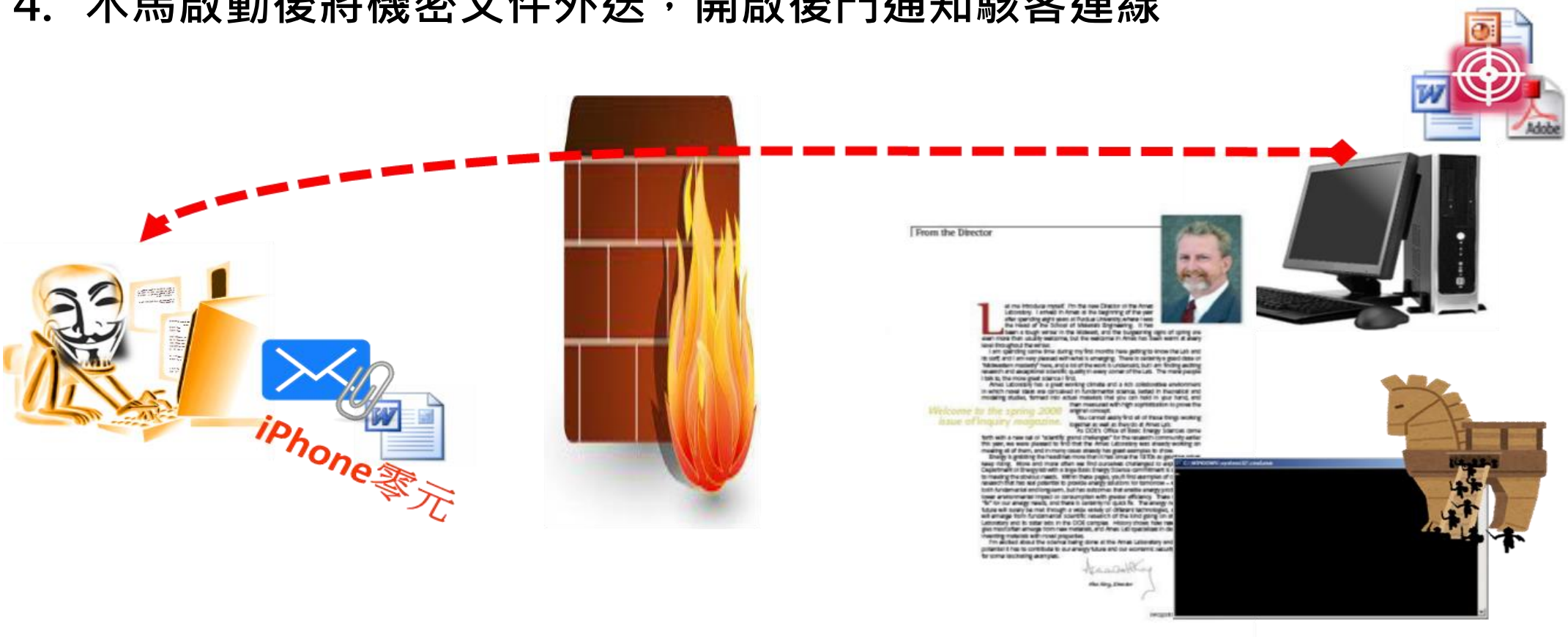
社交工程威脅與攻擊



- 利用人性弱點、人際交往或互動特性所發展出來的一種的詐騙技術
- 透過電話、電子郵件等方式偽裝身份誘騙您上勾受騙...
- 以郵件的攻擊最為常見，目的是為了避開嚴密的資通安全防護技術

社交工程攻擊手法

1. 蒐集訊息
2. 駭客利用Word/PDF等漏洞，將木馬夾在附件檔案中
3. 到處發信嘗試進行滲透
4. 木馬啟動後將機密文件外送，開啟後門通知駭客連線



透過Word漏洞攻擊-社交工程攻擊手法

1. 蒐集訊息
2. 駭客利用Word/PDF等漏洞，將木馬夾在附件檔案中
3. 到處發信嘗試進行滲透
4. 木馬啟動後將機密文件外送，開啟後門通知駭客連線

案例分享:台灣健保局發現有人冒用健保局網址，連結木馬程式。

偵查第九大隊

網路釣魚的目的希望達到受害者數量最大化

發稿時間 2013/5/27 上午 08:23:03

標題 偵破駭客偽冒健保局名義寄發惡意電子郵件盜

冒充健保局，駭客木馬盜取萬筆中小企業個資

數位時代網站 | 撰文者：劉翰謙整理 發表日期：2013-05-27

早前台籍駭客大歡時，由台灣駭客取得的騙人成績，對許多台灣民眾而言，可說多少出了點怨氣。不過，日前刑事警察局破獲，嘉義縣一名男子以健保局名義，夾帶惡意程式寄發電子郵件，竊取許多中小企業的個資，顯然又再次喚醒，眾人為何會聞「駭」色變。

據了解，今年4月底時，健保局便發現有不明人士以北區業務組名義，發送內含名為「二代健保補充保險費扣繳辦法說明」連結的電子郵件，點擊下載執行後，使用者的電腦便會遭到其中的木馬程式入侵，允許遠端的駭客監控電腦，進而竊取資料，而被「駭」者的聯絡人資訊，又成為下一次的目標，如此周而復始，於是累積了萬筆的個資外洩。

寄件者: 北區健保局業務組 [nhioffice.gov@gmail.com]

收件者:

副本:

主旨:

先生/小姐

受駭公司名稱

受害公司電話

補正資料已依照貴單位提出

相關修正檔已於下方載點

請查照

載點："員工修正補充要點下載修正"

或至 健保局全球資訊網 使用工商憑證

我們學到什麼?開啟郵件請先留意....

來路不明的電子郵件，不開啟

公務無關的超連結及附檔，不點選

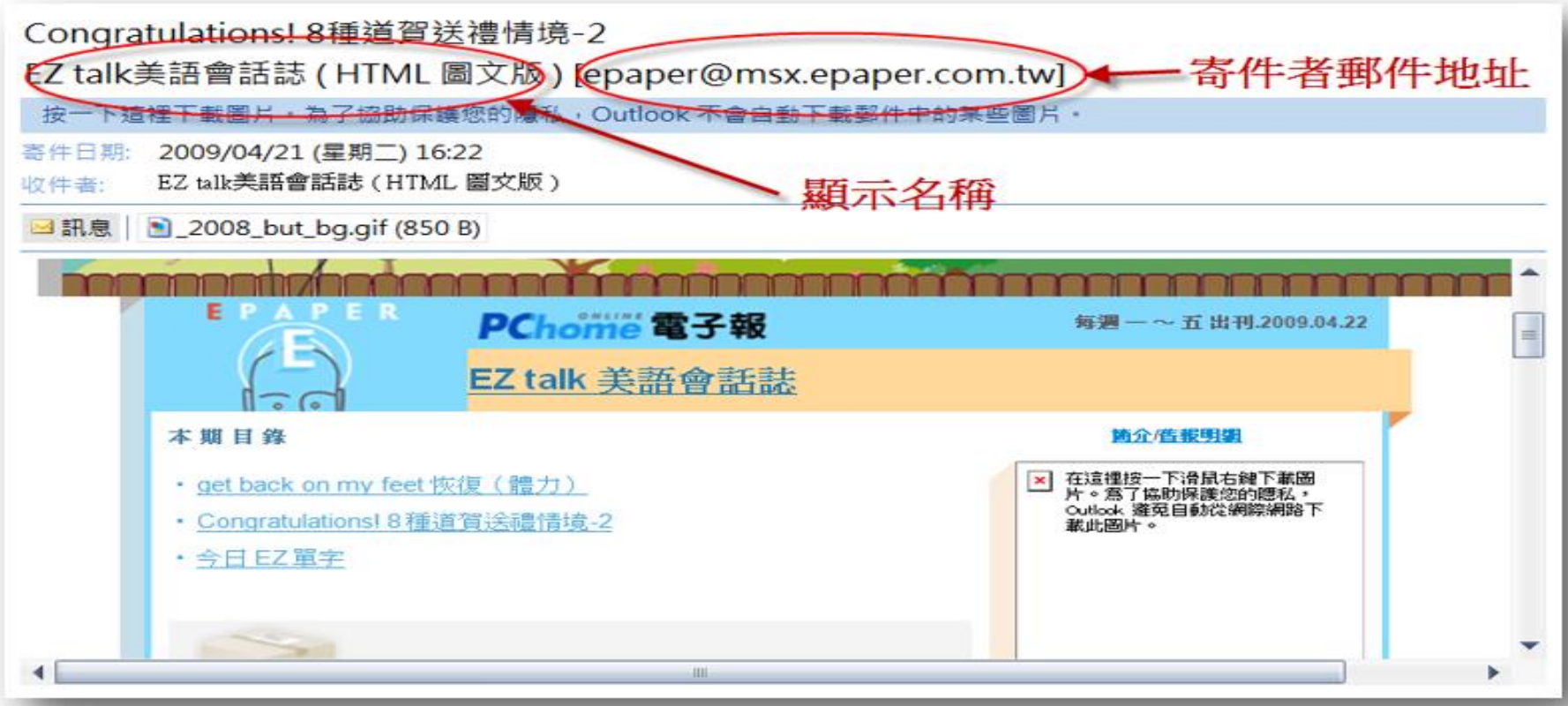
「二代健保補充保險費扣繳辦法說明.doc」

執行檔偽裝的 Word 文件檔

from https://blog.trendmicro.com.tw/?p=5299#more-5299

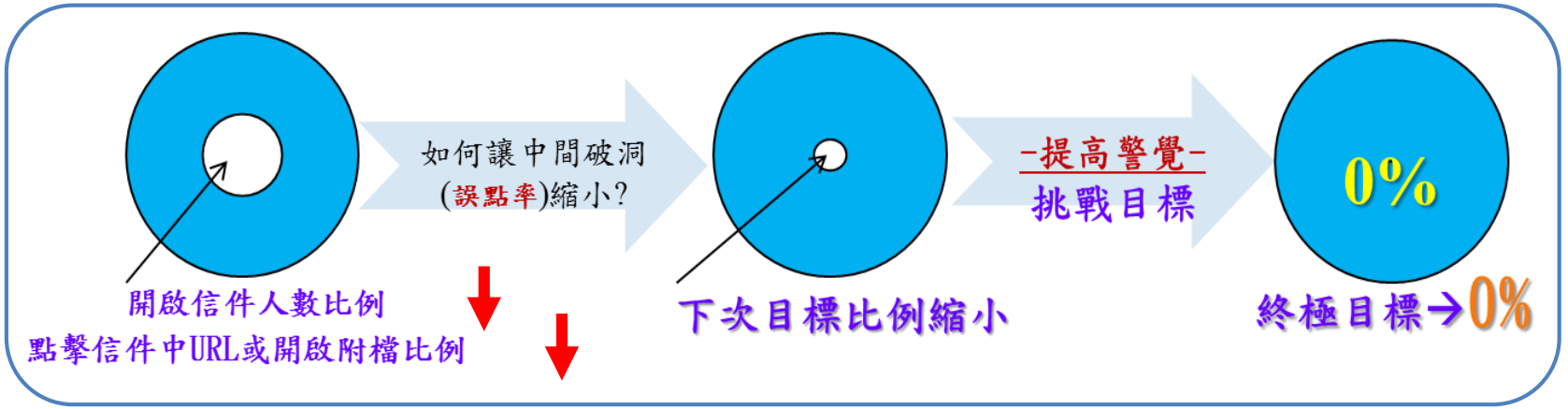
利用郵件特性-社交工程攻擊手法

比對顯示名稱與電子郵件帳號?



這些欄位都是可以改的!

電子郵件社交工程演練測試



- ❑「電子郵件警覺性測試」實施目的：
  - 提升同仁警覺性及辨識惡意電子郵件的能力，以降低公司眾多個人電腦設備及主機受駭風險。
- ❑辦理時間：每年二次，上下半年各辦理一次
  - 演練完成均會進行社交工程宣導，
  - 內容包含惡意電子郵件的識別要領、電子郵件的安全須知等
  - 提高單位人員收信時之警覺心

電子郵件社交工程防範(1/2)

透過電子郵件進行社交工程攻擊之常見手法

施放誘餌，引誘中計

01

針對寄件者/收件者

使用**假冒身分**方式(例如以公務機關、金融機構、電信業者、熟人、同事、往來廠商等身份假造)

02

針對郵件主旨/內容

以**熱門議題、大眾關切主題**為郵件標題及內容

騙誘安裝，入侵攻擊

01

透過附加檔案騙誘安裝

夾帶附件(含惡意程式)，**誘使**使用者點選後**植入木馬程式**

02

透過超連結騙誘連結

夾帶超連結，**騙誘**收件人**連結至釣魚網站**

電子郵件社交工程防範(2/2)

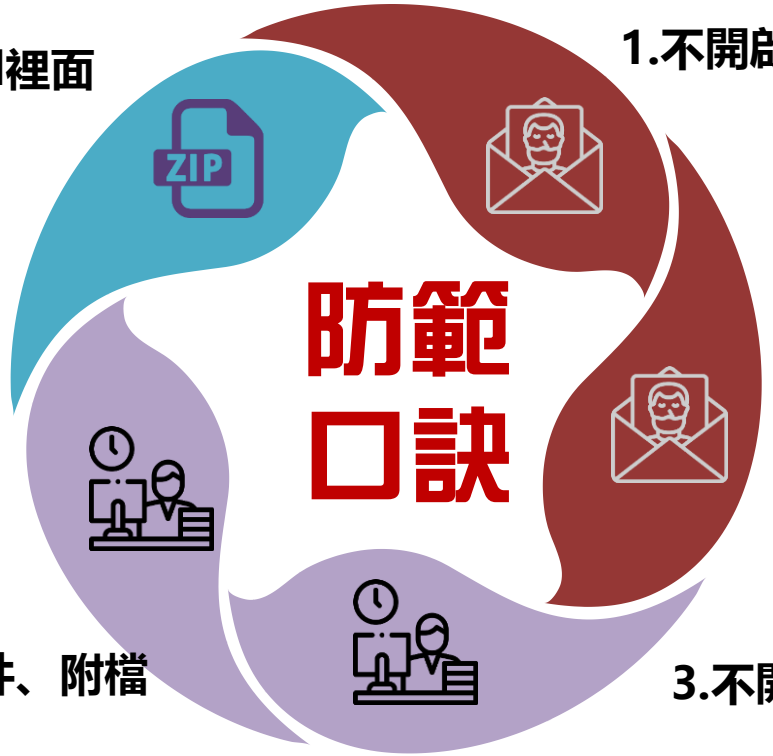
1.不開啟寄件者為陌生名字之信件

2.不開啟寄件者為公司同仁，
但非公司網域之信件
(mail.chimei.com.tw)

3.不開啟以非公務信箱寄送公務之信件

4.不開啟密碼直接放在E-Mail裡面
的加密壓縮附件

5.不開啟與公務無關之主旨信件、附檔
不點選非公務網址之連結



辨識惡意郵件要領

主旨欄位有標示[外部郵件]，

表示此信是從公司外部寄來的信，

需要提高警覺:如與公務無關則勿開啟；

即使與公務有關，如有疑慮，

仍需以電話向寄件者確認是否寄發此信件，

以避免被惡意郵件攻擊(如勒索軟體)。

屏東科技大學
電子郵件社交工程演練信件範本(1/3)

項次	信件標題
1	吃隔夜菜恐食物中毒、敗血症
2	請立即執行安裝最新版本的微軟 Microsoft Windows Update
3	超神發明「刮刮樂貼紙」藥罐！　刮開自動打勾、提醒吃藥免動腦
4	連簽 15 道行政命令　拜登上任先廢川普政策
5	28 個 Chrome、Edge 工具含惡意程式碼，收集用戶數據賺錢

日期	點擊人數
2021-03-25　寄發第一封	3
2021-03-26　寄發第二封	5
2021-03-27　寄發第三封	1
2021-03-28　寄發第四封	0
2021-03-29	4
2021-03-30	5
2021-03-31　寄發第五封	3

屏東科技大學
電子郵件社交工程演練(2/3)

受測人員共101人
每人演練郵件共5封
全部共寄出505封信

開啟信件類型統計

信件類型	開啟信件圖片人數	點擊 URL 或開啟附件人數	任一行為點選人數
保健類_吃隔夜菜恐食物中毒、敗血症	2	7	7
擬真類_請立即執行安裝最新版本的微軟 Microsoft Windows Update	6	2	7
時事類_連簽 15 道行政命令　拜登上任先廢川普政策	3	2	5
保健類_超神發明「刮刮樂貼紙」藥罐！　刮開自動打勾、提醒吃藥免動腦	2	1	3
科技類_28 個 Chrome、Edge 工具含惡意程式碼	2	0	2

屏東科技大學
電子郵件社交工程演練(3/3)

受測人員共101人
每人演練郵件共5封
全部共寄出505封信

測試結果

演練梯次/點擊比例	總開啟信件人數比例	點擊信件中之URL或開啟附件人數比例
109年第一次	7.98%	7.45%
109年第二次	7.54%	3.02%
110年第二次	7.92%	8.91%

信件圖片開啟率

本次受測總人數計101 人，曾經開啟信件圖片者，計有 8人，誘騙成功率為 7.92%。

URL點擊率

本次受測總人數計 101 人，曾經點擊信件URL者，計有 9人，誘騙成功率為 8.91%。

Word附件開啟率

本次受測總人數計 101 人，曾經開啟信件附件者，計有2人，誘騙成功率為 1.98%。

超連結或Word附件點擊率

本次受測總人數計 101 人，曾經點擊信件URL或開啟信件Word附件者，計有9人，誘騙成功率為 8.91%。

Part 03

必須知道的資訊安全防範技巧

Line訊息要學會看盾牌顏色!

看到問題點了嗎？

辦別facebook真假粉絲團~

看到問題點了嗎？

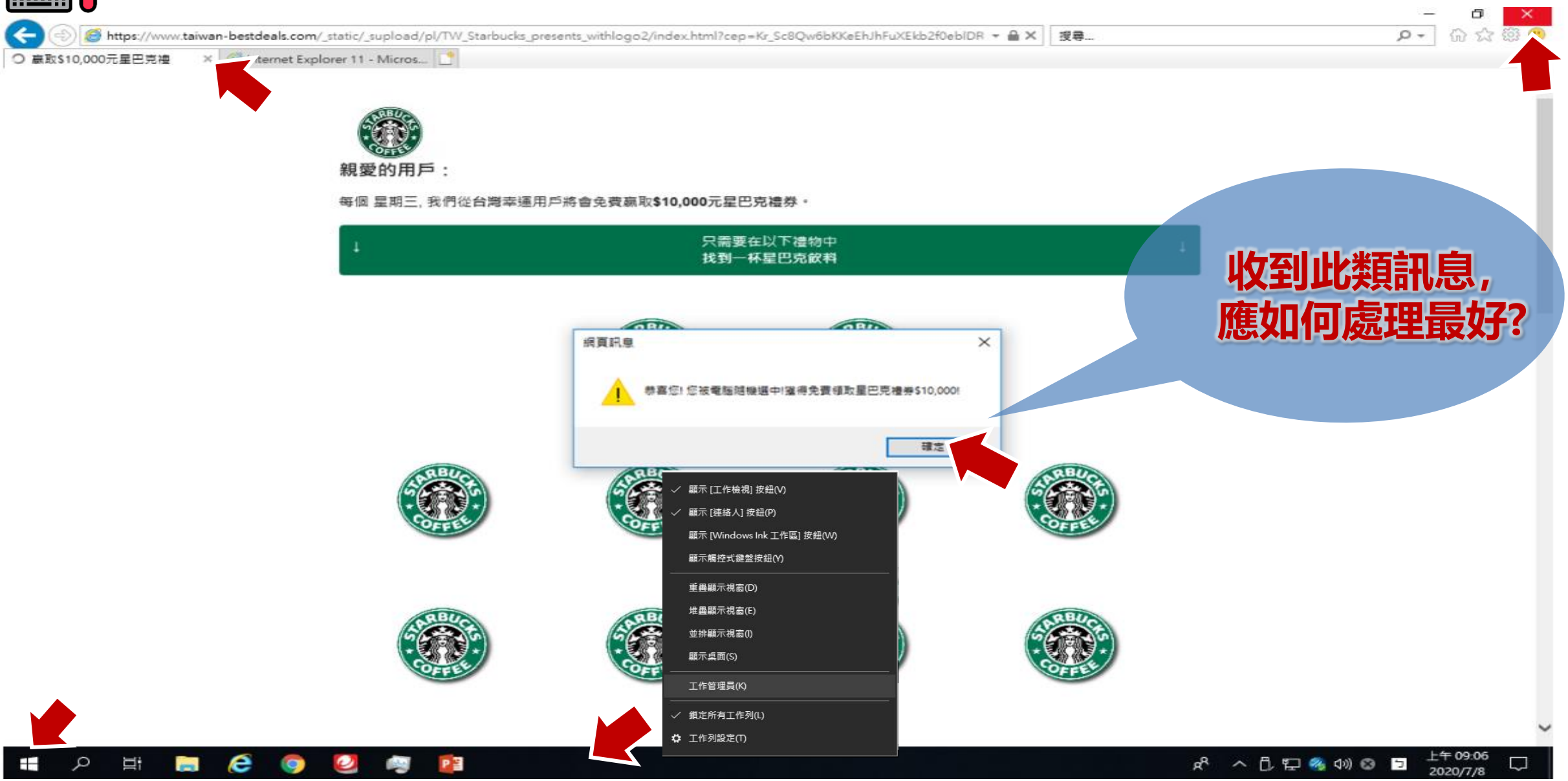
TREND MICRO 趨勢科技

星巴克咖啡同好會

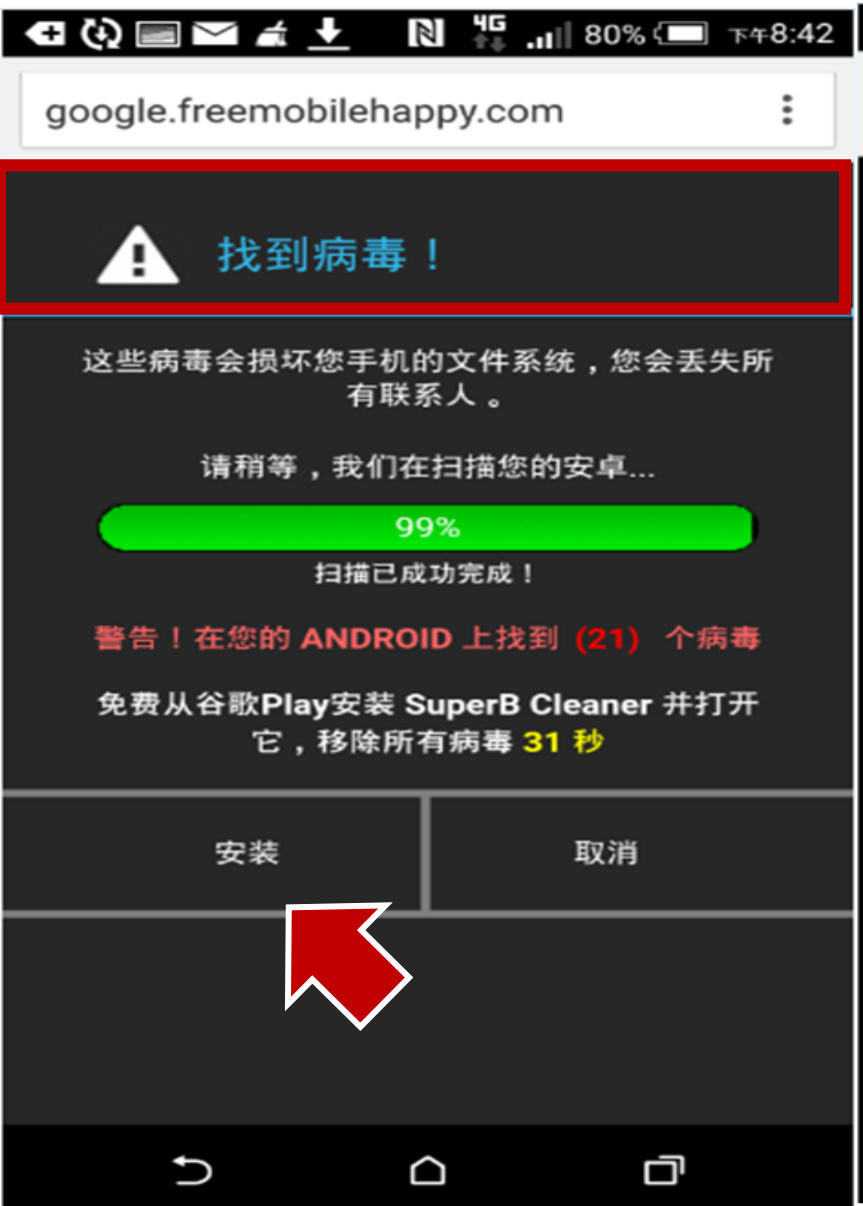
星巴克咖啡同好會 (Starbucks Coffee)

Trend Micro
@TrendMicro

瀏覽網頁出現釣魚訊息時，該怎麼辦?



(惡意)手機惡意程式 看到問題點了嗎？



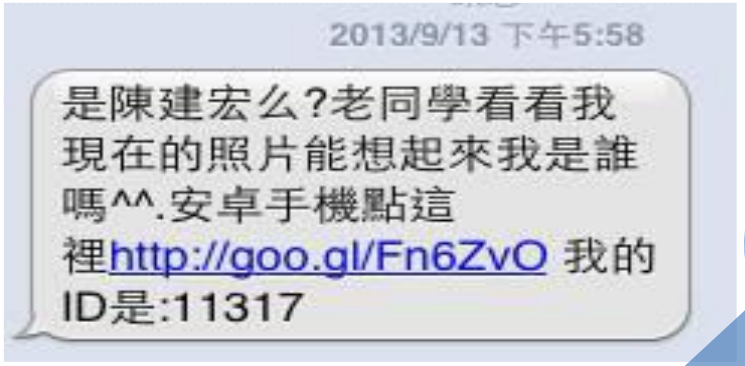
手機詐騙簡訊攻擊


中華電信 3G 上午10:10 88%
訊息 (105)
0961-238-299
編輯
通話
加入聯絡資訊
訊息
2013/9/13 下午5:58
是陳建宏么?老同學看看我現在的照片能想起來我是誰嗎^^.安卓手機點這裡http://goo.gl/Fn6ZvO 我的ID是:11317
訊息
傳送


photo.appphoto.net
您的好友ID:(11318)向您分享了她的照片
照片如無法顯示.智慧手機請點擊這裡下載圖片程式.
下載完畢后左上角出現箭頭圖標.啟動程式后輸入您朋友的ID（11318）.即可獲得她分享給您的照片
google.com
下完后按住通知欄下滑打開
14:06
Wi-Fi
GPS
正在進行
作為媒體裝置連接
通知
清除
photo-31.apk
下載完成
點擊安裝


※※為方便下載.本程式未上傳至GOOGLE PLAY市場.※※
※※未設置允許安裝非MARKET應用程式的手機※※
※※請按下圖所示修改手機設置※※
步驟1.點擊下載完畢后左上角的通知欄裡會出現PHOTO.APK的下載圖標.點擊安裝后彈出窗口點擊設定
步驟2.允許安裝非MARKET應用程式.彈出窗口點擊確定
步驟3.重新下載您的好友發送給您的程式.下載完畢后在左上角的通知欄裡會出現PHOTO.APK
安裝后即可查看您的好友分享給您的照片
照片分享
安全性
SIM 卡鎖定
設定 SIM 卡鎖定

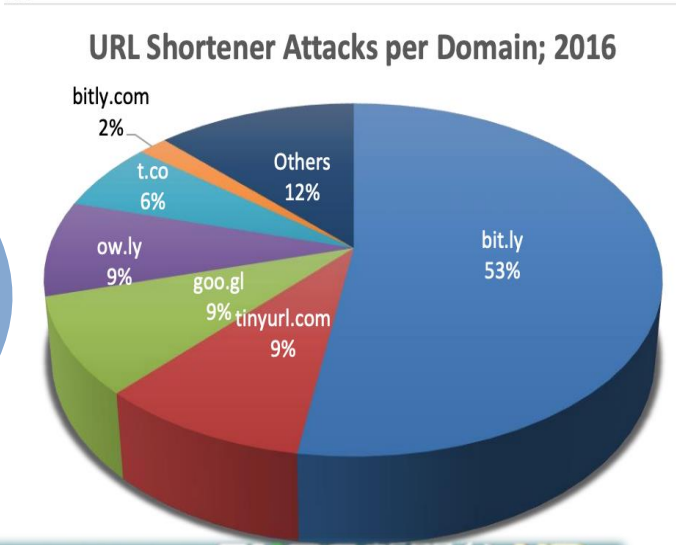
短網域成為釣魚網站最大的代罪羔羊



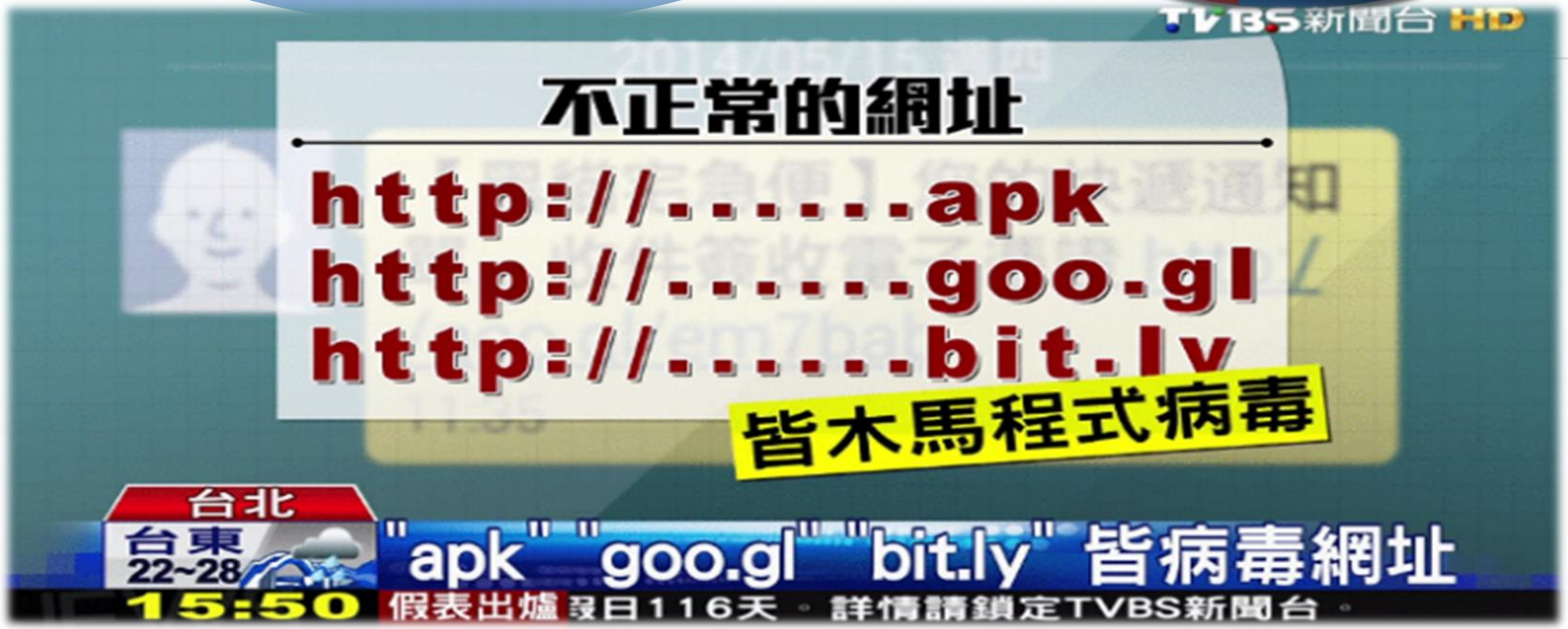
手機亂按http://goo.gl簡訊網址　破財還幫散佈近500封

詐騙網站被抓到，把詐騙網址用短網址來轉址，就可以輕鬆逃過黑名單。所以才會有新聞說，看到goo.gl、bit.ly都是詐騙，雖然誤導民眾，但短網址難辭其咎。

Google短網址停止服務

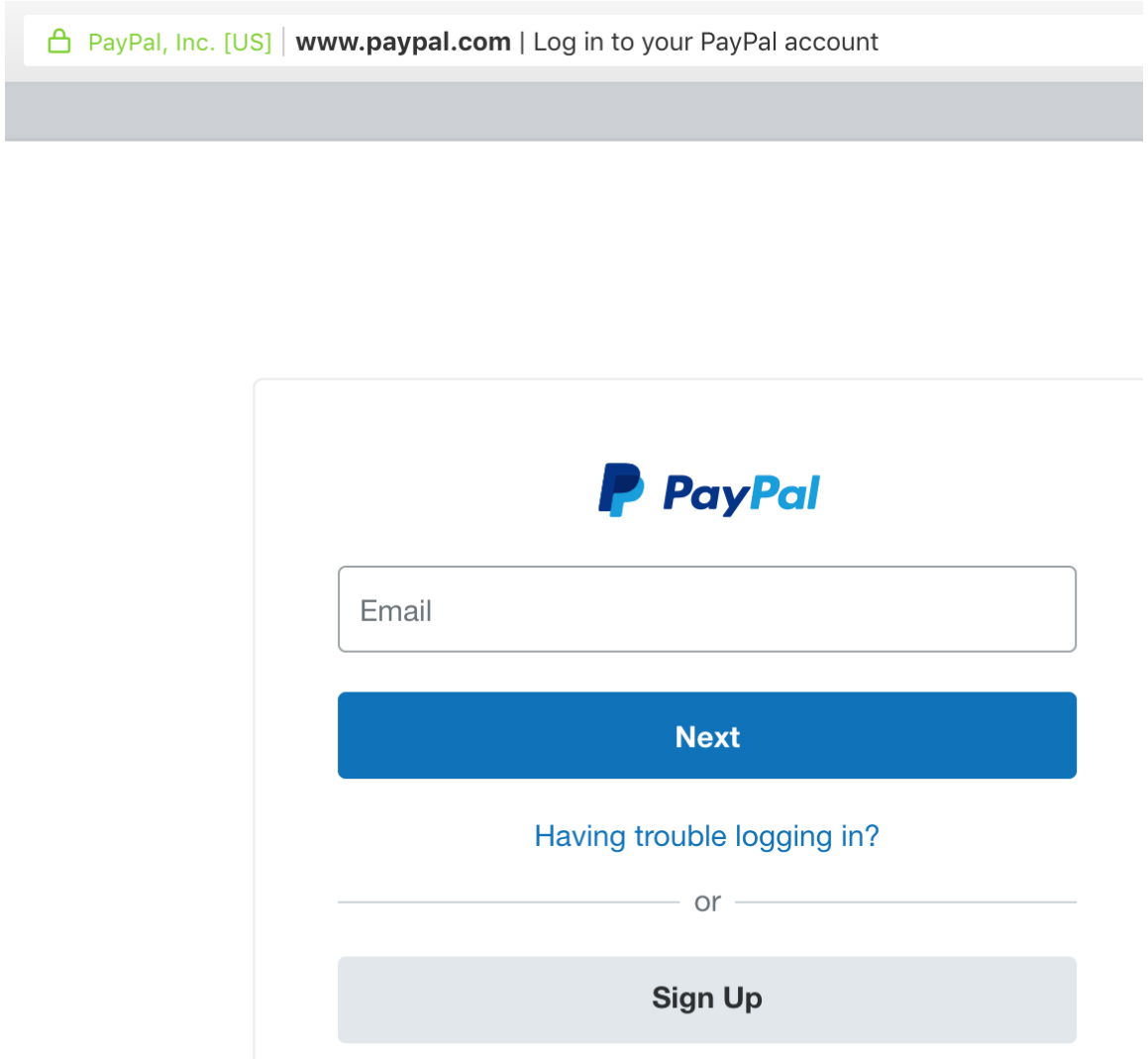


▲慘！一旦手機被成功植入惡意程式後，就會利用消費者手機至app市集購買遊戲點數。（圖／東森新聞）

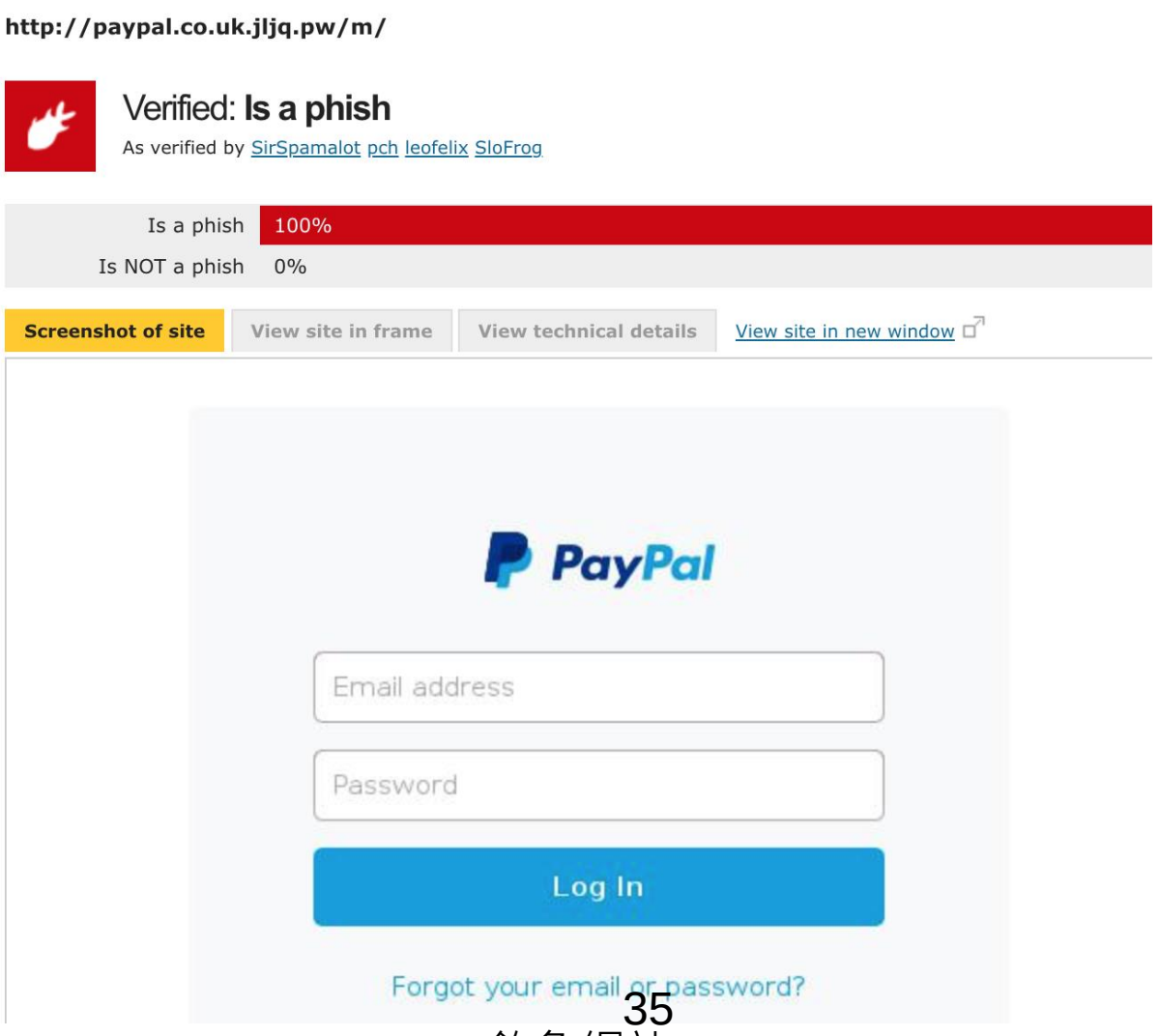


釣魚網站 (1/2) – 與真實網站相似

- 模仿官方網站的登入頁面，誘導使用者輸入帳號密碼



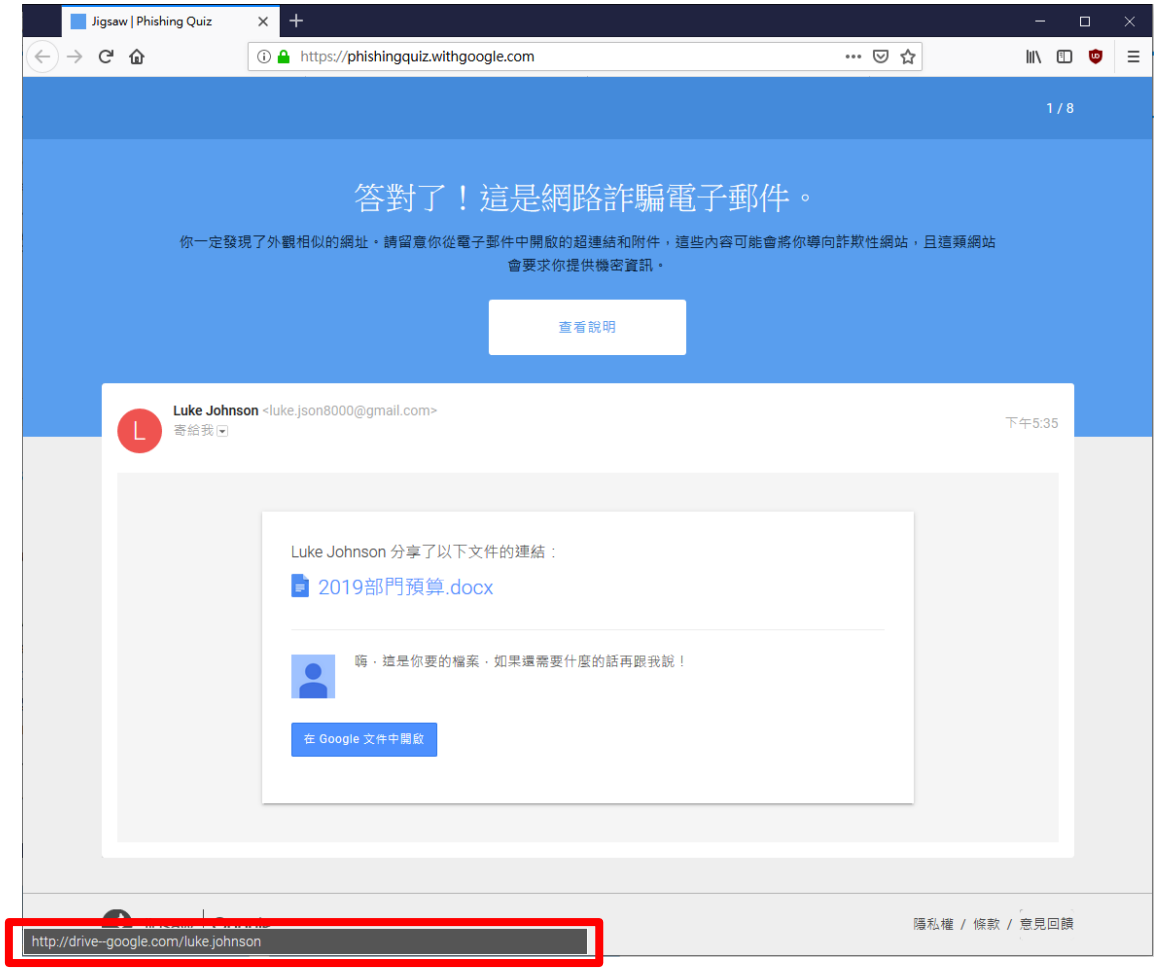
正確的網站

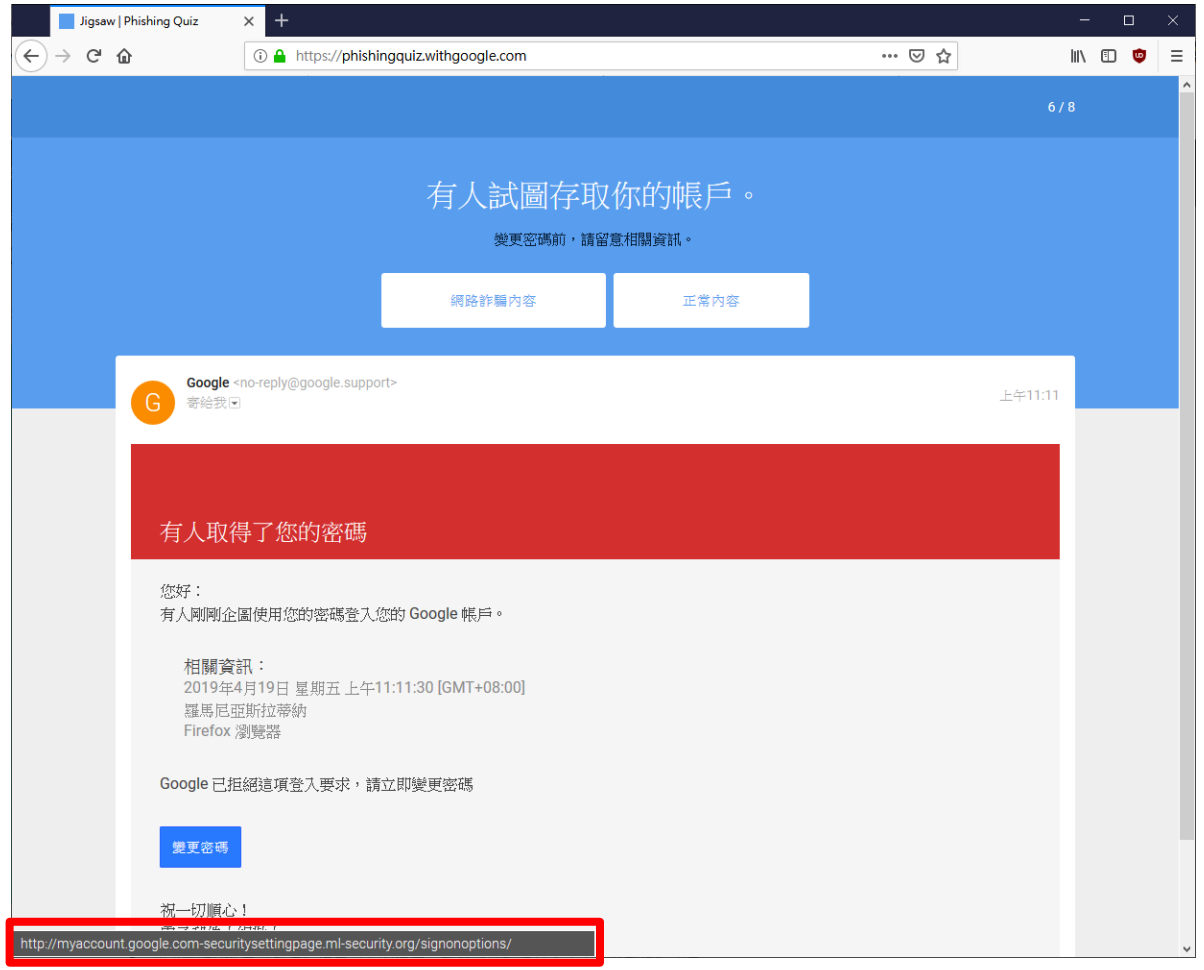


釣魚網站

35

Google釣魚網站小測驗

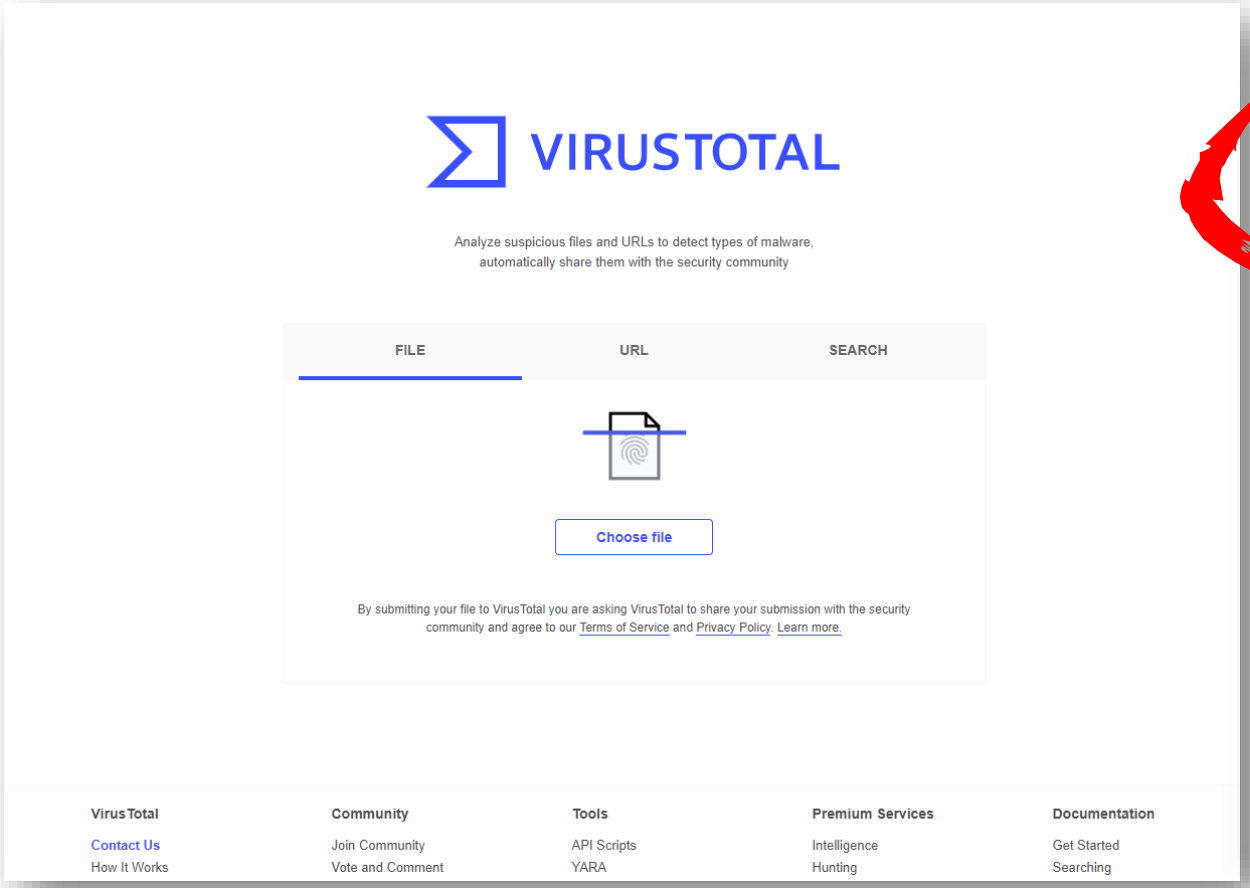


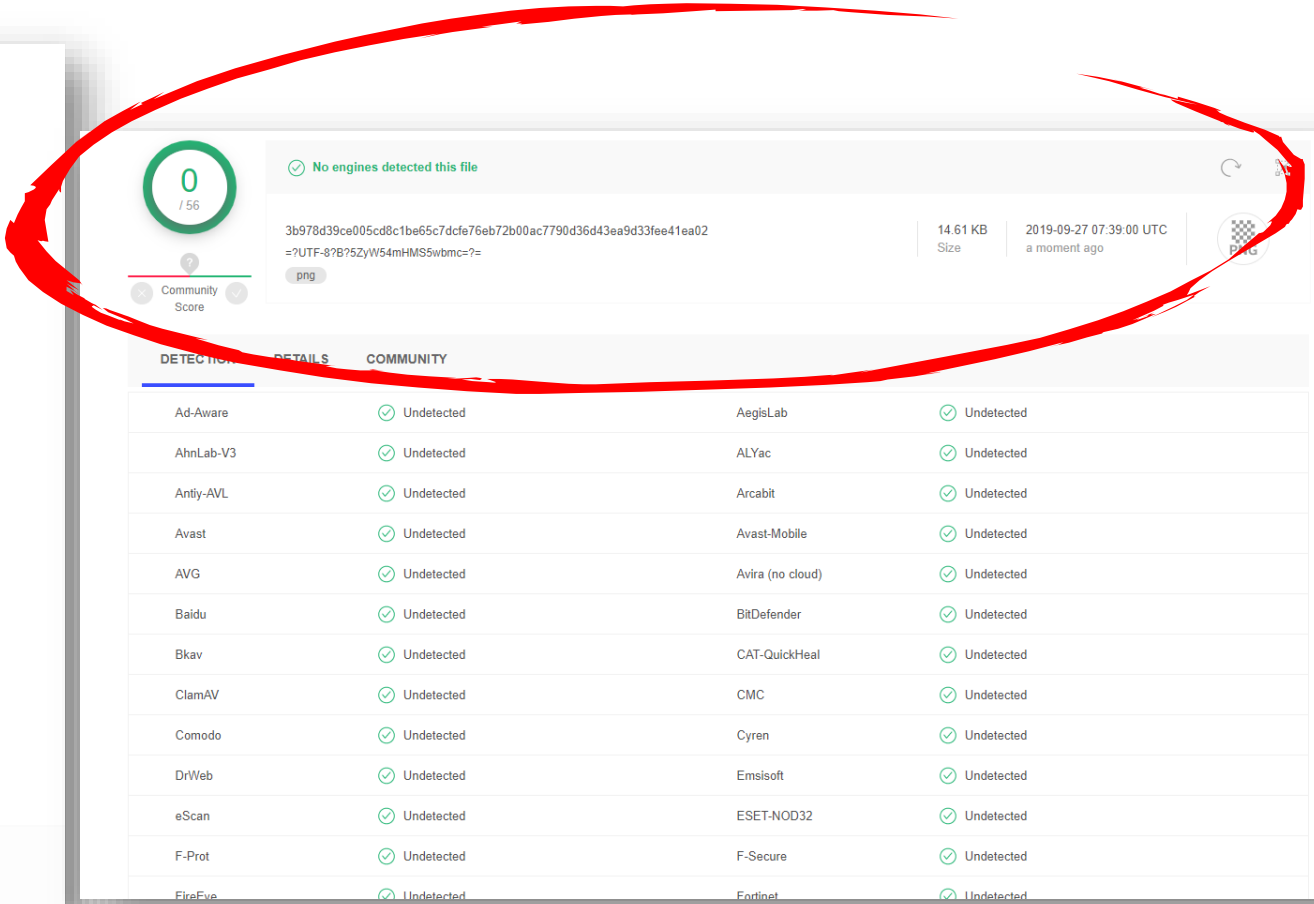


Ref: https://phishingquiz.withgoogle.com/

如何檢測惡意程式

- 利用網路上資源來進行惡意程式檢測
  - Virustotal https://www.virustotal.com/gui/home/upload





Part 04

結語&問題與討論

針對資安-機關 因應原則

只有在平時就做好準備，

才能快速因應突如其來的資安威脅

正確的資安觀念

- 提高警覺
- 加強危機意識

01

- 預防
- 詐騙手法攻擊

02

謹慎的防範動作

- 不隨意開啟
- 下載郵件或軟體

03

- 定期系統更新
- 定期資料備份

04


Q & A
感 謝 聆 聽 !