112 年 11 月政風小品集廉政宣導篇

網購、上餐廳都算為民服務 南投前消保官貪汙起訴

2023-11-08 14:46 聯合報 / 記者江良誠 / 南投即時報導

南投縣前消保官許麗貞利用職務之便，不實核銷每月 5400 元為民服務費，今年 2 月遭南投地檢署搜索調查。檢方調查，許麗貞將為民服務費當成自家小金庫，買漁產禮盒、擴香組，甚至多次和家人到餐廳用餐，都以「為民服務」名義報銷，南投地檢署最近偵結以涉嫌貪汙治罪條例提起公訴。

許麗貞擔任南投縣消保官長達 19 年，今年初廉政署接獲檢舉，她涉嫌利用職務之便，不實核銷業務為民服務費金額數萬元。依貪汙治罪條例移送南投地檢署，檢察官訊後，諭令 10 萬元交保。

未料，許麗貞交保後，又涉嫌勾串證人、偽造證據再度遭檢方拘提，聲請羈押禁見。法官認為，相關證人都已完成筆錄，無串證或湮滅事證事實，才裁定 50 萬元交保。南投縣政府事後將她改調秘書。

檢方調查，許麗貞擔任消保官每月有 5400 元為民服務費，主要用於業務推廣。2020 年 12 月，許麗貞邀縣府員工 4 人，向全國漁會團購漁產禮盒 10 盒，許麗貞訂 4 盒供自己食用或贈送親友，再向團購 4 人收取每份 990 元費用，再拿著發票向新聞行政處申請縣政推行業務費。

另外，許麗貞也數次向 MOMO 和蝦皮購物網站，訂購藤枝擴香組、中式碗禮盒，並以不實發票向縣政府申請縣政推行業務費 5662 元。

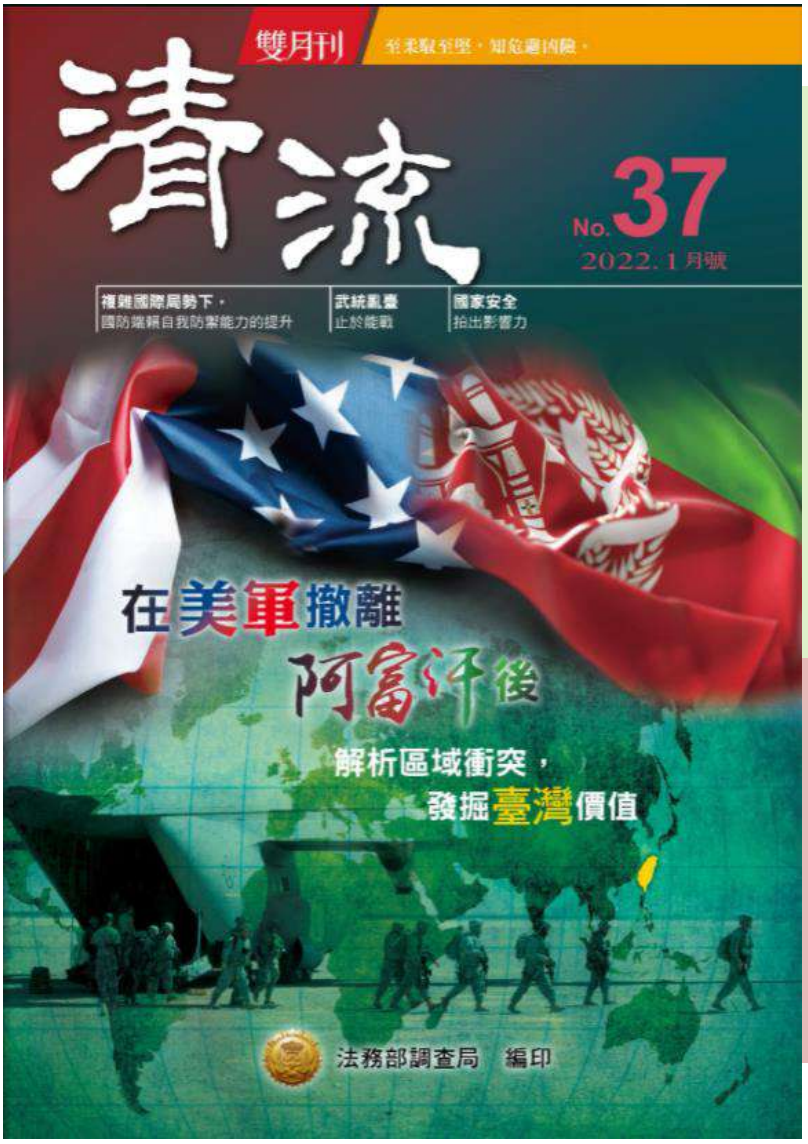
去年 6 月到 10 月，許麗貞 5 度帶著丈夫、女兒到瓦城、陶板屋、布飛娜等餐廳用餐，並將用餐費用以業務推廣費報銷，就連許麗貞出國旅遊不在國內期間，許麗貞也索取縣府員工發票，核銷業務推廣費。

檢方偵結後，認為許麗貞確認犯行共 13 次、犯罪所得 3 萬 8585 元，依貪汙治罪條例第 5 條利用職務機會詐取財物罪，將許麗貞提起公訴。

新北市政府交通事件裁決處政風室　關心您!!

112 年 11 月政風小品集機密維護篇

法務部調查局《清流》雙月刊---淺談資通安全最弱環節



想要看到月刊更多專欄：
http://mjib-ebook.com/MJIB/no37/index.html

文章往下翻閱

廉能是政府的核心價值，貪腐足以摧毀政府的形象，

公務員應堅持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586

新北市政府交通事件裁決處政風室　關心您!!

你夠在意嗎？考驗人性的社交工程誘惑

◆ 社團法人臺灣 E 化資安分析管理協會、逢甲大學創能學院 ── 林子煒

社交工程形形色色，若不夠留意，駭到你會怕。

社交工程─駭客最有效且省錢之攻擊方式

自從人們可以利用網際網路互通有無，每個人至少都擁有多個網路服務帳號，包括個人或其所屬單位的電子郵件帳號；正因如此，利用資訊科技便利之社交工程犯罪行為層出不窮，且趨勢逐年上升。

社交工程即為人與人之間的攻擊。過去關於此類攻擊定義為「攻擊者藉由社交手法取得系統或網路的資訊」，然而現今攻擊者的目標，已逐漸轉到個人擁有之資訊。此攻擊管道，最常見的為電子郵件、簡訊、即時通訊軟體（如 Messenger、Skype、Line、Instagram、Whats App）等

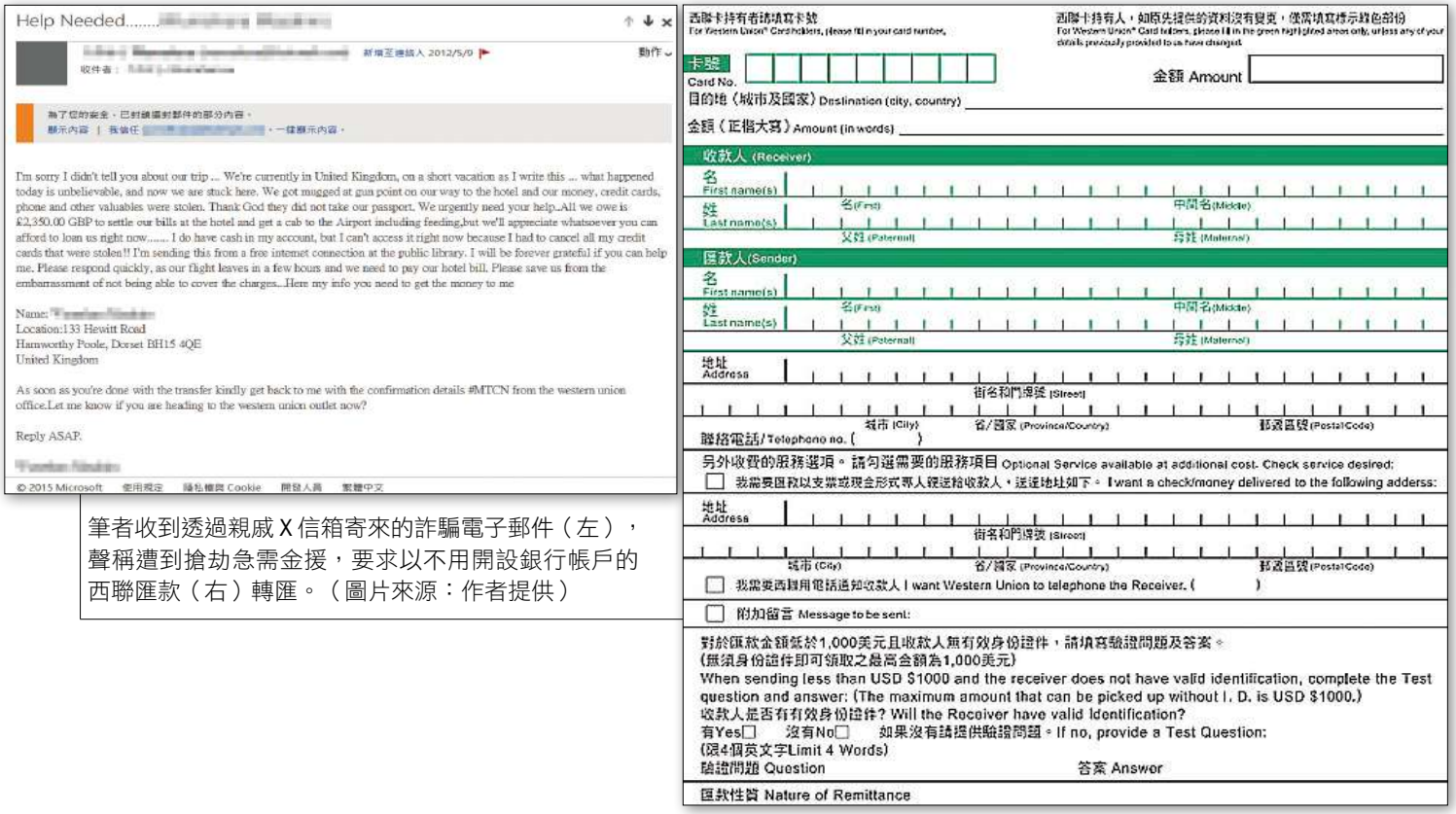
等。為何此種攻擊趨勢會逐年上升？因為對駭客而言，這是最有效、最省成本的攻擊方法。

親身經歷之詐騙案例

以自身經驗為例，某天上午收到親戚X寄來的英文信，信中述說他「正在英國旅遊，但被當地歹徒持槍威脅交出身上所有財產，包括金錢、信用卡、行動電話等。這封信是透過當地的免費網路寄出，現在急需金錢援助，請用西聯匯款（Western Union）匯2,350英鎊（約新臺幣9萬元）給我」。

信中附上姓名與地址，我抱著好奇心利用Google地圖查詢，結果發現那家英國旅館竟然地處在杳無人煙的社區。另個親戚Y也在詢問是否有收到這封信，所以我們研判親戚X的信箱帳戶應該已被盜用，而盜用者寫了這封信，並寄給信箱內所有的聯絡人。

詐騙者指定西聯匯款[1]的原因，係因其匯、收款的雙方都不用開設銀行帳戶，只要填寫雙方英文姓名與出示身分證明即可匯款。作法是在匯款人填妥表格後，系統會產生一組10位數密碼，匯款人只要將


Help Needed.....

I'm sorry I didn't tell you about our trip ... We're currently in United Kingdom, on a short vacation as I write this ... what happened today is unbelievable, and now we are stuck here. We got mugged at gun point on our way to the hotel and our money, credit cards, phone and other valuables were stolen. Thank God they did not take our passport. We urgently need your help..All we owe is £2,350.00 GBP to settle our bills at the hotel and get a cab to the Airport including feeding,but we'll appreciate whatsoever you can afford to loan us right now..... I do have cash in my account, but I can't access it right now because I had to cancel all my credit cards that were stolen!! I'm sending this from a free internet connection at the public library. I will be forever grateful if you can help me. Please respond quickly, as our flight leaves in a few hours and we need to pay our hotel bill. Please save us from the embarrassment of not being able to cover the charges...Here my info you need to get the money to me

Name:
Location:133 Hewitt Road
Hamworthy Poole, Dorset BH15 4QE
United Kingdom

As soon as you're done with the transfer kindly get back to me with the confirmation details #MTCN from the western union office.Let me know if you are heading to the western union outlet now?

Reply ASAP.

西聯卡持有者請填寫卡號 For Western Union® Cardholders, please fill in your card number.

西聯卡持有人，如原先提供的資料沒有變更，僅需填寫標示綠色部份 For Western Union® Card holders, please fill in the green highlighted areas only, unless any of your details previously provided to us have changed.

卡號 Card No.

金額 Amount

目的地（城市及國家）Destination (city, country)

金額（正楷大寫）Amount (in words)

收款人 (Receiver)

名 First name(s)

姓 Last name(s)

名(First) 中間名(Middle) 父姓 (Paternal) 母姓 (Maternal)

匯款人(Sender)

名 First name(s)

姓 Last name(s)

名(First) 中間名(Middle) 父姓 (Paternal) 母姓 (Maternal)

地址 Address

街名和門牌號 (Street)

城市 (City) 省/國家 (Province/Country) 郵遞區號 (Postal Code)

聯絡電話/Telephone no. ( )

另外收費的服務選項。請勾選需要的服務項目 Optional Service available at additional cost. Check service desired:

☐ 我需要匯款以支票或現金形式郵寄給收款人，送達地址如下。I want a check/money delivered to the following adderss:

地址 Address

街名和門牌號 (Street)

城市 (City) 省/國家 (Province/Country) 郵遞區號 (Postal Code)

☐ 我需要西聯用電話通知收款人 I want Western Union to telephone the Receiver. ( )

☐ 附加留言 Message to be sent:

對於匯款金額低於1,000美元且收款人無有效身份證件，請填寫驗證問題及答案。
(無須身份證件即可領取之最高金額為1,000美元)
When sending less than USD $1000 and the receiver does not have valid identification, complete the Test question and answer: (The maximum amount that can be picked up without I. D. is USD $1000.)
收款人是否有有效身份證件? Will the Receiver have valid Identification?
有Yes☐ 沒有No☐ 如果沒有請提供驗證問題。If no, provide a Test Question:
(限4個英文字Limit 4 Words)
驗證問題 Question 答案 Answer

匯款性質 Nature of Remittance

筆者收到透過親戚X信箱寄來的詐騙電子郵件（左），聲稱遭到搶劫急需金援，要求以不用開設銀行帳戶的西聯匯款（右）轉匯。（圖片來源：作者提供）

[1] 成立於1851年，號稱是世界最大的電子匯款公司，在全球超過200個國家與地區設置至少21萬個據點，提供各地收、匯款服務，https://www.westernunion.com/us/en/home.html。

密碼給收款人，收款人就能憑藉英文姓名及密碼進行提款。時至今日，全球已有相當多利用西聯匯款而被詐騙的案例，警方與銀行都無法追蹤及攔截詐騙款。

社交工程郵件之包含要素

以電子郵件來詐騙至少已有十年歷史，然至今仍有民眾上當，因為民眾輕忽或無知，易讓駭客達到欺騙目的。社交工程電子郵件不乏利用聳動的郵件主旨、偽造受害者熟悉的寄件者、以假亂真的郵件內容等等，試圖吸引使用者上鉤。社交工程電子郵件中會有幾個要素，包含超連結、附件、圖片、郵件內容內嵌程式碼。

- **超連結**：有可能會讓受害者連至攻擊者所架設之惡意網站，藉此收集受害者相關資訊。
- **附件**：多含惡意程式，開啟並執行後會潛藏在受害電腦裡，直接將電腦內資料對外傳輸、偷偷側錄用戶使用電腦的任何行為、接續下載惡意程式至受害電腦再執行各項行為等。
- **圖片及郵件內容內嵌程式碼**：能回報給攻擊者表示「登陸成功」，更甚者直接讓受害者電腦自動從中繼站下載小程式（諸如鍵盤側錄工具、螢幕側錄工具等），記錄受害者使用電腦行為，再進行下一步攻擊。

以上要素不一定會同時出現，亦可能交互搭配使用，曾有僅憑單一內容即欺騙成功的案例，造成受害者損失。例如，假冒會議邀請信函，成功欺騙到受害者出門參加會議，加害者利用這段時間闖空門等。

勒索軟體通常包裹著社交工程郵件外衣

近幾年造成全球重大災情的勒索軟體，大部分行為模式即透過社交工程電子郵件，讓受害者點擊後自動下載並執行一個看似無害的小程式，連線至外部中繼站下載勒索軟體主程式，此主程式會開始掃描電腦所存文件[2]後加密，跳出警告訊息，指示受害者利用比特幣付款至指定帳戶以換取解密提示。

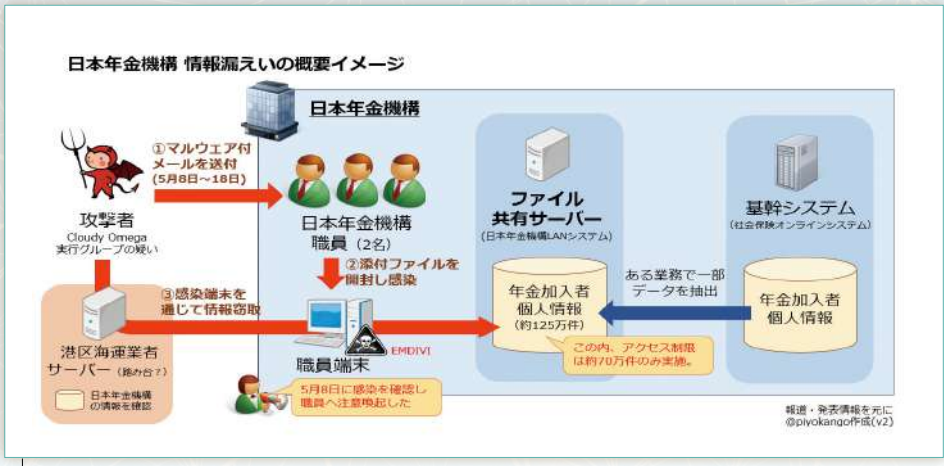
日本年金機構之個資外洩事件

若讀者認為，就算有人「運氣這麼不好」開啟了社交工程電子郵件，造成傷害也不過是個人財產及聲譽。其實損失的嚴重性，絕非想像中的那般簡單。

掌管日本全國國民年金的組織「日本年金機構」（相當於勞動部勞工保險局國

[2] 多為 Office 系列，以及 PDF 或 JPEG 圖檔等企業常見之檔案格式。

大部分勒索軟體的行為模式，即是透過社交工程電子郵件誘惑使用者點擊，而成為受害者。



日本年金機構個資外洩事件示意圖，遭駭主因係員工不慎打開含病毒之社交工程電子郵件所致。（Photo Credit: piyokango, https://piyolog.hatenadiary.jp/entry/20150601/1433166675）

民年金組），於 2015 年 6 月召開記者會，坦誠因員工電腦受駭客攻擊，導致民眾個人資料外洩[3]；整起事件的起因，即為員工不慎打開含病毒之社交工程電子郵件所致。

剛開始是該機構九州分部員工收到社交工程電子郵件，點選超連結後，即被自動下載惡意程式，並開始不正常的電腦連線。

雖然日本國家網路安全中心（National Information Security Center, NISC）[4] 於第一時間發出通報，但因為日本年金機構檢測不出原因，因此僅更新個人電腦的防毒軟體，直到東京本部也有員工收到同樣的社交工程電子郵件並開啟，偵測到儲存年金的資料庫有異常連線行為後，才驚覺事態嚴重。日本年金機構事後雖通知警方，且 NISC 亦緊急派員處理，然已造成所屬 5 個單位內有多達 19 臺的個人電腦遭受感染，最後清查出竟然有高達 125 萬筆的個資外洩，嚴重影響到仰賴年金度日之日本民眾的生活。

社交工程之攻擊方式

由日本年金機構案例可知，只要個人一時疏忽，即使只是小小電子郵件，就有很大機會對企業、群體，甚至國家安全造成危害。

另外，即時通訊軟體也成為社交工程攻擊管道之一。在 COVID-19 疫情高峰時，國內採取口罩預購制，意外出現「口罩釣魚簡訊」，佯稱口罩到貨，引誘使用者點擊簡訊

[3] 《病毒入侵！日本年金機構 125 萬件個資遭外洩》，https://news.ltn.com.tw/news/world/breakingnews/1335620。

[4] 是日本負責網路危機應變處理之政府單位，為 2015 年 1 月由「內閣官房資訊安全中心」升格而成，代表將網路安全提高到國家安全層次。

內連結，當時亦有不少臺灣民眾受駭[5]。以下再列舉其他社交工程之攻擊種類。

一、**濫發電子訊息**：諸如惡意電子郵件、釣魚簡訊、即時通訊等文字訊息。此類攻擊通常一次廣發給多名使用者，因此亦稱為「垃圾郵件」。

二、**釣魚**：此類攻擊通常會讓使用者「信以為真」，透過話術讓人誤信，進而騙取錢財。近期常見「假交友」、「假投資」即屬此類。

三、**願者上鉤**：經典手法為攻擊者在公司門口隨意丟棄一個隨身碟，該公司不知情員工撿到後，誤以為是公司內有人不小心遺失，為了順利歸還，故而將該隨身碟插進自己的電腦內，殊不知惡意程式就此開始執行。

四、**搭順風車**：尾隨員工進入外人不該進去的區域，進而竊取到公司內部機密資訊。

五、**水坑攻擊**：利用網頁藏惡意程式碼的方式，讓使用者的電腦中毒。只要入侵或偽造目標受害者常瀏覽的網站，植入惡意程式，當受害者瀏覽該網站，即會下載惡意程式。

社交工程攻擊之防範措施

社交工程攻擊防不勝防，面對攻擊，可行的防範措施包含：

一、**使用垃圾郵件過濾器**：現行的郵件伺服器（包括 Gmail）皆有此機制。

二、**定期更新**：隨時更新防毒軟體、防火牆與電腦及手機的作業系統，以防任何安全性漏洞被利用。

三、**仔細確認**：確認訊息與自己是否相關，並查證訊息來源，有必要時打電話向來源確認。

釣魚簡訊經常引誘使用者點擊簡訊內連結，進而竊取民眾個資、詐騙錢財。（圖片來源：內政部 FB 粉絲專頁，https://www.facebook.com/moi.gov.tw/photos/a.105361604800013 1/3275894322438948）

[5] 《台灣詐騙網址暴增 4 倍　駭客冒用口罩預購行騙》，https://www.cna.com.tw/news/ait/202009220313.aspx。

人是最大的零日漏洞，只要使用者資安意識稍有不足，即為攻擊者打開一扇自由進出的大門。

四、**提高警覺**：個人應提防不明電子郵件，並且勿任意點選附檔及超連結。

人是最大的 Zero-Day

社會生活中形形色色的誘惑，即是社交工程對於網路用戶的最佳詮釋，諸如「清不完的木馬，無知與恐懼也；補不完的系統，人腦也」、「人是最大的 Zero-Day[6]」等，雖然只是玩笑話，也道出了防範社交工程的最關鍵要素是「人」。資訊技術發展這麼多年，為何電子郵件社交工程依然是攻擊者的攻擊手段首選，乃因為電子郵件是阻力最小的攻擊路徑，只要使用者資安意識稍有不足，**開啟惡意電子郵件，即為攻擊者打開一扇自由進出的大門，也開闢了一條讓使用者或其所屬組織邁向毀滅的道路**。因此，在日常生活中一定會接觸到電子訊息的我們，勢必要多加瞭解是類攻擊，且必須養成習慣、提防不明電子訊息。相信你只要夠「在意」，必當能防範形形色色且誘惑人性之社交工程攻擊。

社團法人台灣 E 化資安分析管理協會（ESAM）

[6] 在電腦領域中，零日漏洞或零時差漏洞（zero-day vulnerability、0-day vulnerability）通常是指還沒有修補程式的安全漏洞，而零日攻擊或零時差攻擊（zero-day exploit、zero-day attack）則是指利用這種漏洞進行的攻擊。「零時差漏洞」是軟體或硬體的瑕疵，如未能及時修補，駭客就能在不被察覺的情況下透過網路侵犯個人隱私、偷取商業機密與摧毀公共設施等。

112 年 11 月政風小品集安全維護篇

案例解析～「「恐怖情人-9 號電梯復仇記」

一、緣起

某日某市政府電梯內，傳來淒厲中摻雜著痛苦萬分的哀嚎聲，一名女子血流滿面倉皇奔出電梯，至辦公處所向同事求救，沿著走廊至電梯留下觸目驚心的斑斑血痕，受傷的女子是該機關內的員工，原本已經下班的她，因為被前前男友跟蹤心生恐懼，因此又折回辦公室，但仍無法阻止悲劇發生，不無令人遺憾。

二、案情因果

在市政府擔任短期女工讀生，因拒與前男友復合，前男友竟於某日下午於該名女工讀生上班之公務機關電梯及樓梯間附近埋伏，直至女工讀生下班至地下 1 樓停車場騎著機車回家，前男友一路尾隨，並語多恐嚇且面露猙獰神情，試圖尋求復合，女工讀生當下非常慌張且害怕，於是又折回辦公場所停車場，也主觀的認為前男友應不敢於公務機關對她不利，惟前男友仍不死心，又跟著女工讀生搭乘地下 1 樓電梯，兩人於電梯門關上後疑因談判破裂，前男友突然從牛仔褲右後方口袋掏出美工刀，朝女工讀生臉部攻擊，女工讀生奮力掙脫，卻躲不過一刀接一刀的攻擊，臉、頸上被狠劃 5 刀，留下深可見骨的傷口，前男友行兇後隨即快步跑出電梯逃逸。臉龐血流如注的女工讀生在電梯抵達 2 樓時趕緊衝出去直奔辦公室，同事被她全身是血的模樣嚇了一大跳，除協助女工讀生送醫急救外，立即向市政府警衛隊求援，市府警衛人員緊急通知消防局及轄區分局偵查隊到場處理。此案凸顯政府機關

內部維安問題，有確實檢討之必要。

三、問題分析

從本事件發生的原因分析，員工遭受危害或機關設施(備)易遭破壞之因素：

(一) 執行公務時發生之危害

1. 對於政府施政不滿引發之群眾陳情、請願、抗議事件。
2. 民眾不滿政府行政處分所引發危安事件。
3. 員工執行公務時發生意外事件。

(二) 機關行政廳舍規劃管理問題

1. 適當執行門禁管理

門禁管理是機關內部辦公廳舍安全維護之第一道關卡，但實際執行卻是十分不容易，主要原因是地方政府為一開放式服務機關，民眾、廠商若有洽辦公務之需求，得直接登門入室前往各科室辦理，確實造成各機關門禁安全管理上之困難。

2. 未能落實監視系統電子城牆

本案於案發後 5 小時內逮捕嫌犯，最主要係因監視器錄製之犯罪現場情況，但如在案件發生之前，能由監視器發現異常，機先阻止，則應可將傷害降至最低。

(三) 員工個人身心因素致危害機關安全

感覺統合失調、精神心理異常、工作挫折、情緒失控、感情 糾紛、家庭失和、在外負債結仇...等，皆可能造成員工自身或機關安全危害的因子，導致發生機關安全維護事件。

(四) 未加強執行安全教育

應讓員工孰悉求救管道及設施，並能確實掌握求救時點，是保護人身安全

之第一道防線，也是最直接、最有效之方法。本案李女有多次機會可求救，但都因加害者是熟識之人，未能及時警覺，而一再錯失求救時間，以致最後仍釀成悲劇。

四、研擬改善

每天平均有 5~6 千人進出之市政中心傳出兇殺案，該市市長及各級主管相當震驚，除要求警方加強治安，並責成府內相關單位加強門禁安全管理，保障員工上班安全外，另由秘書長召集全府各機關高層召開安全會議，檢討門禁管理及相關安全維護問題。

該市府政風單位並立即提出相關改善方針，函發各主管機關參考，並至各機關執行安全維護業務督檢，彙整各機關安全管理缺失，提出相關策進作為，落實執行安全維護工作如下：

（一）嚴格要求員工依規定配戴識別證，並不定期進行抽查。

（二）劃定訪客接待區域，並指定專人負責接待及管控事宜，避免訪客任意遊走辦公場所，衍生機關安全及公務機密維護問題。

（三）機關內部劃分責任區，由指定負責單位加強巡視，午休及下班後，應重覆確認無洽公民眾逗留。

（四）公務員因執行公務與民眾有所衝突或傳涉有情感、金錢糾紛之訪客，應責成所屬單位嚴加注意防範，俾免危害事件發生。

（五）檢討監視系統有無設置盲點，並定期檢視維修，確保最佳功能。定期召開機關安全維護會報，俾利檢討機關各項安全設施。

（六）協調事務單位適時辦理各項突發性危安狀況演練，使員工能充分處置，以降低危害。

（七）各機關發生重大危安事件時，務必及時通報，俾利提供協助處理。

（八）執行下班後及例假日電梯出入管制，以員工識別證進行驗證通行。

（九）檢視機關緊急求救設備(如緊急求救鈴)是否齊備，效能完善與否。

五、結語

全國各縣市政府部門屬於民眾洽公極為頻繁之處所，在便民與安全之間，門禁管理極具重要性，但如何管理確具難度，端賴各機關依據各別經驗，適時調整管理模式。機關安全維護工作是具有層次變化的工作，而人員之生理 、心理等情狀對安全的影響很大，也是難以控制與預測的部分。有時可能因為人為個別因素，而導致安全事件發生的機率與程度的變化，有時也可能因為人員的及時控制，而使安全事件不會發生或不再擴大。因此，精準控掌機關狀況是安全維護工作上之關鍵。

資料來源: 法務部廉政署

廉能是政府的核心價值，貪腐足以摧毀政府的形象，

公務員應堅持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586

新北市政府交通事件裁決處政風室　關心您!!

112 年 11 月政風小品集消費者保護篇

萬里蟹產季 稽查餐廳避消費糾紛

2023-10-27/記者柯毓庭 / 新北報導

新北市法制局考量保障消費者權益，加上近期新北市萬里蟹進入產季豐收期，近日前往轄區新北市石門區富基漁港、萬里區龜吼漁港稽查，初步調查結果並未有偷斤減兩或一種菜有兩種價格的情況。

今年 8 月，北海岸知名海產勝地龜吼漁港爆出代客料理業者消費爭議，有民眾向媒體投訴，業者有 2 種版本菜單，一種提供給本地消費者，另一種提供給外國遊客，其中給外國遊客的菜單金額較貴，疑似坑殺國外消費者。

當時業者稱是「菜單來不及更換」，並非惡意坑殺。消保官近日會同經濟部標準檢驗局、新北市農業局漁業管理處前往稽查，發現該餐廳已統一菜單價格。

消保官另外針對其他業者代客料理菜單與海鮮攤商磅秤一併稽查，經校對檢查，發現富基漁港 36 間攤商共 25 台磅秤，以及龜吼漁港 40 間攤商共 45 台磅秤均符合規定；現場餐廳業者代客料理部分，也未發現 2 種菜單。

除了 2 種菜單外，先前也曾傳出民眾與代客料理業者因服務費、料理費等額外費用產生消費糾紛。當時消費者到店後表示自己是「熟客」想搏感情算便宜一點，結帳時因店家收取料理費不滿，店家則解釋稱因消費者自稱「熟客」，才會沒有先說明將收取料理費。

消保官向業者逐一宣傳交易價格揭露宣導，提醒消費者務必在消費前先確認菜單標示價格與額外收費部分，以避免產生消費糾紛，若在漁港因消費產生疑慮，也可向漁市駐點管理人員反應。

新北市政府交通事件裁決處政風室　關心您!!

112 年 11 月政風小品集反詐騙篇

📣⚠️請 Android 用戶慎防 RCS 或多媒體釣魚詐騙簡訊📲❗

「Google RCS」即時通訊功能近期遭詐騙集團不當利用，假借國內知名業者名義，大肆發送常見的「積分即將到期」及「罰款尚未繳納」詐騙訊息，藉此誘騙民眾點擊釣魚連結，民眾一旦點擊可能遭植入惡意程式竊取認證碼或依連結網站指示輸入「個人資料、金融帳戶帳號或信用卡號」等資料，詐騙集團即可取得民眾重要的個人資料及金融資訊。

如果收到「+號開頭之境外簡訊」，且有上述關鍵字及夾帶可疑網址等內容切勿理會，亦請 Android 手機用戶可關閉 RCS 即時通訊功能，以避免收到詐騙訊息!!

參考資料來源：內政部警政署 165 全民防詐騙網