南投 行政院農業委員會林務局 林區管理處
Nantou Forest District Office

112 年 05 月份廉政宣導

製作人：藍韋倪

【公務員廉政倫理規範】

受贈財物需登記

廉潔倫理莫忘記

請託關說要注意

知會政風保權益

廉政署檢舉專線

0800-286-586

政風室檢舉專線

049-2365134

南投林區管理處政風室 關心您

機關安全維護宣導

逃生的狀況及方法

一般而言，逃生狀況可區分為三種，一是**逃生避難時**，二是**室內待救時**，三則是在**無法期待獲救時**。其方法敘述如下：

一、逃生避難時

1. 不可搭乘電梯，因為火災時往往電源會中斷，會被困於電梯中。
2. 循著避難方向指標，由安全梯進入安全梯逃生。
3. 以毛巾或手帕掩口：利用毛巾或手帕沾濕以後，掩住口鼻，可避免濃煙的侵襲。
4. 濃湮中採低姿勢爬行：火場中產生的濃煙將瀰漫整個空間，由於熱空氣上升的作用，大量的濃煙將飄浮在上層，因此在火場中離地面 30 公分以下的地方應還有空氣存在，尤其愈靠近地面空氣愈新鮮，因此在煙中避難時儘量採取低姿勢爬行，頭部愈貼近地面愈佳。但仍應注意爬行的便利及速度。
5. 濃煙中戴透明塑膠袋逃生：在煙中避難逃生，人體如防護不當，易吸進濃煙導致暈厥或窒息，同時眼睛亦會煙的刺激，產生刺痛感而睜不開。因此如有簡易的裝備能使人們在煙中逃生時，提供足量的新鮮空氣，並隔離煙對眼睛的侵襲最佳。此時即可利用透明塑膠袋。透明塑膠袋一定要夠大（塑膠袋長約１００公分，寬約６０公分），使用大型的塑膠袋可將整個頭罩住，提供足量的空氣供給逃生之用。使用塑膠袋時，一定要充分將其張開後，兩手抓住袋口兩邊，將塑膠袋上下或左右抖動，讓

裏面能充滿新鮮空氣，然後迅速將其罩在頭部到頸項的地方，同時兩手將袋口按在頸項部位抓緊，以防止袋內空氣外漏或濃煙跑進去。同時要注意在抖動塑膠帶裝空氣時，不得用口將氣吹進袋內，因為吹進去之氣體是二氧化碳，效果會適得其反。

6. 沿牆面逃生：在火場中，人常常會表現驚惶失措，尤其在煙中逃生，伸手不見五指，逃生時往往會迷失方向或錯失了逃生門。因此在逃生時，如能沿著牆面，則當走到安全門時，即可進入，而不會發生走過頭的現象。

二、在室內待救時

(一)用避難器具逃生

避難器具包括繩索、軟梯、緩降機、救助袋等。通常這些器具都要事先準備，平時亦要能訓練，熟悉使用，以便突發狀況發生時，能從容不迫的加以利用。

(二)塞住門縫，防止煙流進來

一般而言，房間的門不論是銅門、鐵門、鋼門，都會具有半小時至二小時的防火時效。因此在室內待救時，只要將門關緊，火是不會馬上侵襲進來的。但煙是無孔不入的，煙會從門縫間滲透進來，所以必須設法將門縫塞住。此時可以利用膠布或沾溼毛巾、床單、衣服等，塞住門縫，防止煙進來，此時記住，潮溼能使布料增加氣密性，加強防煙效果，因此經常保持塞住門縫的布料於潮溼狀態是必需的。另外如房間內有大樓中央空調使用的通風口，亦應一併塞住，以防止濃煙侵襲滲透。

(三)設法告知外面的人

在室內待救時，設法告知外面的人知道你待救的位置，讓消防隊能設法救你是非常重要的。如果你待救的房間有陽台或窗戶開口時，即應立即跑向陽台或窗戶之明顯位置，大聲呼救，並揮舞明顯顏色的衣服或手帕，以突顯目標，夜間如有手電筒，則以手電筒為佳。如所在的房間剛好沒有陽台或窗戶，則可利用電話打“119”告知消防隊，你等待救助的位置。

(四)至易於獲救處待命

在室內待救時，如可安全抵達安全門，進入安全梯間或跑至頂樓頂平台，

均是容易獲救的地點。如不幸地，受困在房間內，則應跑至靠陽台或窗戶旁等待救援。

(五)要避免吸入濃煙

濃煙是火災中致命的殺手，大量的濃煙吸入體內會造成死亡，吸入微量的濃煙則可能導致昏厥，影響逃生。因此務必記住，逃生過程中，儘量避免吸入濃煙。

三、無法期待獲救時

當無法期待獲救時，絕對不要放棄求生的意願，此時當力求鎮靜，利用現場之物品或地形地物，自求多福，設法逃生。

(一)以床單或窗簾做成逃生繩

利用房間內之床單或窗簾捲成繩條狀，首尾互相打結銜接成逃生繩。將繩頭綁在房間內之柱子或固定物上，繩尾拋出陽台或窗外，沿著逃生繩往下攀爬逃生。

(二)沿屋外排水管逃生

如屋外有排水管可供攀爬往下至安全樓層或地面，可利用屋外排水管逃生。

(三)絕不可跳樓

在火災中，常會發生逃生無門，被迫跳樓的狀況，非到萬不得已，絕不可跳樓，因為跳樓非死即重傷，最好能靜靜待在房間內，設法防止火及煙的侵襲，等待消防人員的救援。

公務機密維護宣導

武功極界─無影手 vs. 麥擱騙啦─有影沒

據臺灣警政署統計，自 2017 至 2021 年間，平均 1 年發生 1 萬 3 千例以上。雖近年來的犯罪統計稍有下降趨勢，但受害者仍成千論萬。況且，這些統計數量僅計算已通報的案件，未通報的案件更是不計其數。美國則更甚，IC3 的報告中指出每年平均有 55 萬例，且數量有顯著提升，2017 至 2021 年的通報案數量已暴增 2.8 倍。甚至網路犯罪受害者損失的金額平均每年高達 370 億美金，由此可見，網路犯罪所帶來的威脅不可估量。其中，最常見的手法即為「網路釣魚攻擊」。網路釣魚如同真實世界釣魚，釣客即為隱匿於網路背後的駭客，常見的公務通訊軟體、社群媒體等則是作為駭客的釣場，駭客透過散播魚餌誘使民眾點擊上鉤。

參考 Medium 中 Tyler Chen 所提出的電子郵件範例與社群軟體上的詐騙實例，一旦民眾點擊其中所夾帶的鏈結、下載檔案或是開啟指定程式，便等同於上鉤，駭客成功竊取使用者個人資料、帳號密碼與信用卡號等。

個人案例與防範策略

接著，我們進行個人與企業的受害案例分析，並且說明防範策略。

一、周杰倫無聊猿 NFT 被偷損失上百萬

2022 年 4 月，明星周杰倫在社群網站公布其「無聊猿」非同質化代幣（Nonfungible Token,NTF）被釣魚網站偷走的消息。所謂「無聊猿」是由無聊猿遊艇俱樂部（Bored Ape Yacht Club,BAYC）推出的 1 萬隻各有

無聊猿遊艇俱樂部推出 1 萬隻各有獨特表情的猿猴 NFT 作品。（Photo Credit: Bored Ape Yacht Club, https://boredapeyachtclub.com/#/gallery）

獨特表情的猿猴 NFT 作品，當時每隻價格約在 100 枚以太幣（約 26 萬美金）。

這類事件的起因就是駭客在官方社群網站放上釣魚網址來誘騙被害人。使用者在社群媒體上看見 NFT 的預購訊息，以為可以用較便宜的方式來購買新的 NFT；誘使使用者點擊鏈結後會進入釣魚網站，便可選擇金額開始進行交易手續。然而釣魚網站的交易內容並非預購 NFT 作品，實際上是受害者被鏈結的文章所吸引，毫無警覺內容的真偽，導致駭客成功騙取授權交易。

二、FB Messenger 點擊網址詐騙達高峰

亦有受害者 2020 年在 Messenger 收到名為「我不敢相信是你」的假 YouTube 影片鏈結，想觀看者必須先輸入 Facebook 帳號密碼，一旦使用者於假網站中登入，駭客便成功盜用使用者帳號密碼，隨後再將鏈結散

播給該帳號的好友，讓被害人淪為散播惡意鏈結的工具。根據國外資安廠商 Pixm 發布的最新研究報告，推估全球臉書至少有數百萬位用戶遭誘騙導致個資外洩。

三、個人防範策略

在網路資訊發達的年代，駭客偽裝成一般使用者來散播惡意鏈結進行釣魚已是常態，因此資安意識對於民眾而言已是必修課題之一。防範作為有：

（一）提升潛在威脅警覺性：當收到陌生訊息、開啟未知網址、下載非官方軟體時，人們其實難以辨別其中是否夾帶惡意行為或攻擊，應提高警覺性，避免落入駭客陷阱。

（二）陌生訊息：當使用者瀏覽社群媒體上陌生人所發布的訊息時，應時刻保持懷疑的態度，在進入網址前要先查證訊息的正確性。如 NFT 遭盜取事件中，在社群網站看到 NFT 鏈結時，應先去向官方求證，而不是相信社群網站的訊息。只要使用者對內容產生懷疑並查證，就可以有效避免釣魚事件發生。

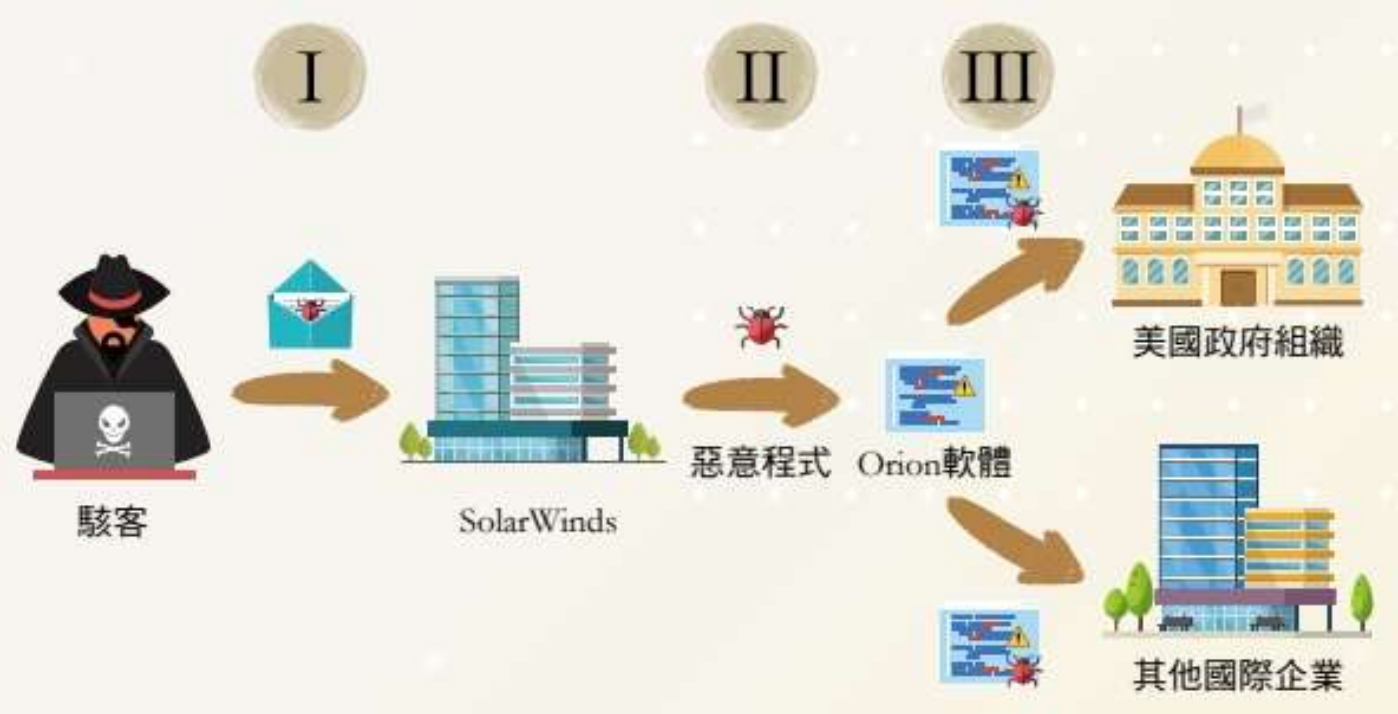
（三）未知網址：收到朋友傳遞的未知網址時，使用者應先確定該消息為本人傳遞，才點擊鏈結。如案例 FB Messenger 點擊網址詐騙中，使用者在收到可疑鏈結後，可透過打電話的方式來確認朋友身分的真偽，避免朋友的個人帳號遭到駭客利用而不自知。

（四）使用威脅檢測軟體：使用檢測軟體可以有效偵測惡意鏈結和惡意程式，大幅降低使用者被釣魚的風險。當使用者遇到必須點擊陌生鏈

結或執行來歷不明檔案的情況時，可以利用 Virustotal 檢測軟體，使用者將鏈結或檔案上傳後，該軟體會自動偵測其是否被資安廠商認證為惡意鏈結或檔案，並產出相應的報告。使用者可自行評估該檔案所伴隨的風險。基於安全考量，倘若有任一廠商對該鏈結報有疑慮，建議使用者不要點擊。

企業事件與防範策略

有別於個人案例，駭客對於企業的攻擊更具威脅性，其會針對企業的特色、員工的素質、工作內容進行釣魚郵件的客製化，進而達成各種攻擊目的。這種持續針對特定組織發起的網路攻擊我們稱之為進階持續性滲透攻擊（Advanced Persistent Threat,APT），以下為 APT 案例發生的過程。



一、SolarWinds 網路監控軟體公司遭駭客入侵

SolarWinds 開發的軟體 Orion 主要是幫企業進行網路監控及管理。2020 年 12 月傳出 Orion 遭到駭客入侵的消息，其嚴重性不只影響 SolarWinds 本身，連透過該軟體進行網路管理的企業都深受其害。比較知名的包括

美國國務院、國防部、司法部及 NVIDIA、Microsoft 與 Intel 等國際企業皆傳出災情。只要使用該軟體，駭客就能一舉獲得該組織的網路架構，並且遠端執行惡意程式碼進行攻擊。

這次事件 SolarWinds 企業本身並不是駭客的主要目標，而是與其合作的相關企業。駭客首先透過社交工程手段入侵 SolarWinds 後，並沒有急於進行攻擊，而是持續蒐集資料，第二階段目標就是將惡意程式混入 Orion 軟體中且不被發現，在最終階段經由各企業下載，將帶有惡意程式的軟體散布出去。

根據上述實例可發現，駭客主要是透過釣魚郵件來進行攻擊，因現今企業仍然以電子郵件為主流的通訊方式，其不限時間地點的特性便於員工使用。然而企業中每天需要處理的郵件數量非常多且種類繁雜，一不小心便讓駭客有機可乘，其中最常見的郵件設計內容為商業電郵詐騙（Business Email Compromise,BEC）。

二、BEC 釣魚郵件實例

根據 2022 年臺灣資安公司對 BEC 郵件進行的分析，得出一些常見案例，駭客經常使用像“office”、“president”、“chief”、“director”等高階職務名稱作為電子郵件帳號，透過偽造身分，來向員工索要機密檔案。或是會偽造一個與被冒充人非常相似的地址，包括將某些英文字母和數字互換以達到混淆的目的，像是英文 l（小寫 L）與數字 1（數字一）、英文 o 與數字 0 等，讓受害者難以在第一時間辨認出真偽。因此，使用者收到信件時，應多留意信件的來源地址是否正常，若有異常之處即可

通報或忽略該信件。

三、現今企業的防範措施整體來說，釣魚郵件的設計類型千變萬化，只要謹慎檢查寄件方的電子郵件與檔案就可以有效避免。當你在郵件中看到檔案，可以先確認是否為圖片偽裝、檢查寄件人電子郵件地址是否完全正確等等，千萬不要忽略這些重要步驟。

但企業中每天需要處理的郵件數量極多，單靠員工本身的資安意識來抵擋所有的釣魚郵件有點不切實際，倘若能實現沙盒測試與零信任架構，必定能有效抵抗威脅。因此以下分別介紹沙盒測試及零信任架構這兩種現今企業可用的防範措施。

（一）沙盒測試：BEC 商業詐騙之所以難以抵擋，是因為很難斷定該郵件檔案是好是壞，依目前技術來說，最有效的方式就是進行沙盒測試。通過將環境徹底隔離，模擬檔案執行的情況，並觀察這些程式會做哪些動作？連到哪些網站？安裝哪些程式？做一個詳細完整的分析紀錄並上傳至監控中心。雖然執行過程要一段時間，但只要取得該惡意程式的特徵後，之後檔案只要進行比對就可以確認是否為惡意程式，不必再模擬一次。透過這種方式，可以很好且有效率的分辨出惡意檔案。

（二）零信任架構：於此架構下，不論進行任何操作都需要進行身分驗證，以抵擋駭客入侵後所造成的威脅。基於對各種流量頻繁的驗證，儘管駭客入侵員工的電腦，也難以繞過員工的身分驗證系統進行進一步的攻擊，因此零信任架構是近幾年資安持續推動的方向。例如美

國聯邦政府在頻繁遭受攻擊後，於 2021 年 9 月 7 日公布《聯邦零信任戰略草案》（Federal Zero Trust Strategy），目標是讓企業組織的網路安全架構，都是基於零信任原則而成。

零信任架構示意圖

結語

無論是一般民眾或是政府企業，都會收到來自駭客的釣魚攻擊，手法層出不窮且越加高明。除了依靠系統提供的自動防禦偵測機制外，全民應提升對於釣魚訊息的警覺性以及基本認知，才能計出萬全，去危就安。

資料來源：清流月刊

消費者保護宣導

正確看待食品添加物，享受安全安心的飲食生活

食品添加物之安全性常受到大眾關注，其實食品添加物已有數百年使用歷史，謹慎添加可以提升食品的品質與安全，最重要的是合法合理的使用。

食品添加物最初多為天然存在的物質，例如：莓類含有苯甲酸、乳酪發酵過程產生丙酸、醋發酵產生醋酸等，這些酸除賦予食品特殊風味外，同時因酸鹼度下降，也抑制微生物生長，而延長食品的保存時間。核苷酸磷酸鹽(例如：5’-次黃嘌呤核苷磷酸二鈉及 5’-鳥嘌呤核苷磷酸二鈉)則是存在於香菇、魚類等食品中，與存在於昆布中的麩胺酸一樣，可以加強食品鮮味的呈現。

食品添加物的使用目的也很多元，例如：香腸添加亞硝酸鹽除可維持鮮紅肉色外，更重要的是可以防止肉毒桿菌中毒；沙拉油添加維生素 E 可以防止油脂氧化；餅乾、鬆餅添加膨脹劑產生鬆軟口感；醬汁中添加粘稠劑增加附著性及口感；甜味劑可讓不適合吃甜食的人，也可以選擇具甜味的食品，除維持食品的感官特性外，更重要的是保障食品的安全。

世界各國對於食品添加物均定有使用標準加以管理，規定使用範圍、限量及規格，我國也定有「食品添加物使用範圍及限量暨規格標準」，這些標

準的訂定均參考動物安全性試驗資料、國際間相關法規標準與准用情形、各種食品添加物品項之理化特性、加工用途及其使用之必要性、使用食品之種類、範圍、加工製程及添加量等具體文獻資料，並考量國人飲食習慣及健康風險等情況，審慎評估後據以訂定。業者應確認產品使用食品添加物的合理性，依照標準添加合法食品添加物，則尚不致對消費者健康造成危害。

食品添加物謹慎添加可以提升食品的品質與安全，最重要的是合法合理的使用。業者得視其產品配方之需求，依「食品添加物使用範圍及限量暨規格標準」之相關規範使用食品添加物，且應備有產品配方、加工製程及相關品保資料等予以佐證，並應依食品安全衛生管理法之規定標示。

資料來源：食品藥物管理署

廉政案例宣導

公務員常見刑責態樣-不違背職務收賄罪

一、案例概述

「高西錢」係 A 環境公司（下稱 A 公司）之負責人，其以 A 公司之名義標得 B 機關之設備操作維護案。「高西錢」為求迅速完成資料核備、估驗計價及撥款流程，基於行賄之犯意，於機關旁邊超市約見 B 機關技工，即承辦上揭採購案履約業務執行事宜之「乖乖弟」，請求加速請款流程，並交付賄款 3 萬元，於交談過程中得知「乖乖弟」確有依約加速完成陳核程序，「高西錢」為表達謝意，隨即再加碼交付 1 萬元之賄款。

二、 法條依據

1. 貪污治罪條例 第 5 條第 1 項第 3 款 對於職務上之行為收受賄賂罪。
2. 貪污治罪條例 第 11 條第 2 項 對於公務員不違背職務之行為交付賄賂罪。

三、案例研析

1. 所稱職務上之行為，係指公務員在其職務範圍內所「應為」或「得為」之行為。而所謂「不違背職務收賄罪」，是指公務員收受賄賂或其他不正利益，而做「合法」的行為。
2. 無論違背或不違背職務收賄罪，皆需具有「對價關係」，須所收受之賄賂或不正利益與行為人的職務具有相當「關聯性」，方能夠成本罪。至於關聯性成立與否，則由法院就具體個案認定之。此外，行賄人本身也需具備「行賄之故意」，才可成立本罪。
3. 本案經法院審酌，被告「高西錢」基於行賄之犯意，交付財物予依法從事公務之人，期加速行政流程，犯罪事實甚明，惟考量渠對犯行坦承不諱，爰依貪污治罪條例 第 11 條第 2 項、第 4 項規定，應執行有期徒刑 1 年 2 月，褫奪公權 1 年，緩刑 2 年。公務員「乖乖弟」雖未違背職務，卻貪圖不法財物，破壞官箴，惟考量渠犯後坦承犯行，並繳回全部犯罪所得，確有悔意，依犯貪污治罪條例之不違背職務收受賄賂罪處有期徒刑 2 年，緩刑 3 年，向公庫支付 30 萬元，褫奪公權 3 年，扣案之犯罪所得 4 萬元沒收，後經最高法院三審判決定讞。