投稿類別：資訊類

篇名：

從 2017 年勒索病毒 WannaCry 事件看資訊安全

作者：

陳奕羶。高雄市立新莊高級中學。二年十二班。

張簡雲翔。高雄市立新莊高級中學。二年十三班。

指導老師：

劉雪珠老師

鄭翔文老師

壹、前言

一、研究動機

西元 2017 年，勒索病毒——WannaCry 席捲全球。現今大多研究都指出：WannaCry 藉由 Windows 的系統漏洞入侵。其實，Windows 開發商——Microsoft，已於當年三月釋出此漏洞的修補檔案，然而多數群眾沒有立即更新系統，才釀成如此嚴重的資訊安全事件。

如今，電腦的使用十分普及。相較於過去，我們可稱這一世代為「數位原住民」，而資訊教育的相關措施理應使各年齡層，特別是國高中生培養出資安素養，但現今資訊安全事件所反應的結果卻與預期背道而馳，這令我們十分好奇，現今的學生是否真的具備素養。

在高雄市市立高雄高級中學 110 級十三班李秉育同學的提議下，我們決定以此 WannaCry 事件做為本論文的主題。並在李秉育同學提供參賽經驗後，本論文以此做為研究目標，調查學生所具備的資訊安全意識是否完整確實。

二、研究目的

(一) 了解 WannaCry 病毒的運作原理及影響
(二) 關於資安對於社會的重要性
(三) 探究台灣高中職生對資訊安全之看法
(四) 提出增進台灣高中職生對資訊安全認知的看法與建議

三、研究方法

(一) 文獻探討
(二) 問卷調查（研究範圍：台灣高中職生）

四、研究流程

圖一：研究流程
（圖一資料來源：研究者繪製）

貳、正文

一、2017 年勒索病毒 WannaCry 事件

WannaCry 為勒索病毒的一種，它的特性是能鎖住受害者電腦的檔案及容易擴散等特性，首先，我們需要先了解 WannaCry 的加密及傳播方式。

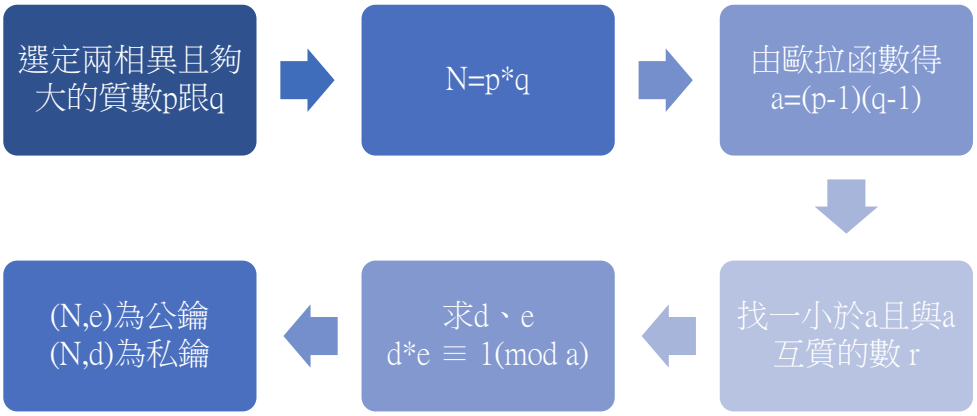
(一) 勒索病毒運作原理

1. 加密方式

下列依序介紹現今較主流的加密方式：

(1) RSA 演算法

這是一種非對稱性之加密方法，需先產生一組公用金鑰及私密金鑰。流程如下：



圖二：RSA 演算法公鑰私鑰產生流程

（圖二資料來源：研究者繪製）

此演算法加密一段文字或檔案前，需先將其轉成數字（使用 ASCII 碼或 Unicode 碼或自行約定等方式），假設轉換出來的數字為 n，加密後所得結果為 w。轉換方式如下：

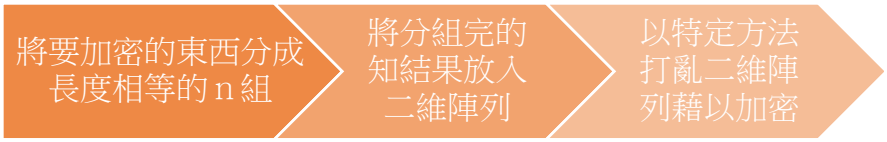
$w \equiv n^{e} (\mathrm{mod}\ N)$

此被加密物件，可以下列方式還原成加密前的數字：

$n \equiv c^{d} (\mathrm{mod}\ N)$

(2) AES 加密法

其為一種利用二維陣列，以特定方式打亂，進而加密檔案的演算法，方法如下：



圖三：AES 加密法加密流程

（圖三資料來源：研究者繪製）

2. 散播方式

下列舉例說明目前主流的散播方式：

(1) 利用電腦系統漏洞

一般電腦系統開發商會自主尋找系統是否存在漏洞，並推出相應的修補安裝檔。但由於有些開發商在更新系統上不會強制用戶安裝補丁，或是部分系統已經不被開發商支援，導致該漏洞雖然已被發現，但許多用戶電腦仍存在漏洞。部分電腦病毒就利用這個情況攻擊電腦用戶。「**2017 年 5 月 12 日的 WannaCry 勒索病毒變種利用了已公開近 60 天的已知漏洞，大肆襲擊全球**」（趨勢科技，2017 年）即其中一例。

(2) 利用社交工程方式

此手法在勒索病毒中最常見，「**通常以欺騙、假冒或口語、交談用字等方式，騙取受害者的資訊**」（李綱，2018 年）傳播方式通常以釣魚郵件、假網址、或下載盜版等方式，迫使電腦用戶的電腦成為傳播媒介，抑或藉機植入惡意程式。如 2020 年台灣因 COVID-19（新冠肺炎）引發口罩缺貨，即有不肖人士以抽獎可抽中口罩做為誘因騙取個資。而 WannaCry 除了社交工程外，另一個特殊的方式是：若網域內的其中一台電腦遭入侵，且沒有及時切斷網路或安裝補丁，也會透過該網域傳播出去。「**一旦企業網路上的某台電腦受駭，災情即可能擴散到企業網路中其他未修補的電腦。**」（陳曉莉，2017 年）

(二) 勒索病毒——WannaCry 事件

1. WannaCry 介紹

這是勒索病毒的一種，此電腦病毒運作及入侵方式與傳統手段有所不同。病毒大多是透過入侵用戶電腦，投放廣告、竊取個人資料、但 WannaCry「**其原先近似木馬程式，皆是暗躲於電腦裡，而勒索病毒顧名思義就是透過加鎖檔案來勒索贖金。**」（李郁苓，2018 年）

2. WannaCry 運作原理

WannaCry 所利用的漏洞，是一個由美國國家安全局利用 Windows 系統中 445/TCP 的資料交流協定漏洞。開發的漏洞利用程式——永恆之藍，「**全球有史以來最嚴重的 WannaCry(想哭)勒索病毒勒索病毒爆發事件，其背後的動力就是 EternalBlue(永恆之藍) 漏洞攻擊手法。**」（趨勢科技，2019 年）

3. WannaCry 之影響

「**資安業者 Avast 發現，WannaCrypt0r 2.0（或稱 WannaCry、WCry）勒索軟體上周五（5/12）同步於全球展開大規模的攻擊行動。**」（陳曉莉，2017 年）WannaCry 在 2017 年 5 月爆發，當日台灣也出現受害者。當時，眾多台灣人未安裝更新檔，且很多企業或公家機關仍使用已不被開發商所支援的老舊電腦系統(如 Windows XP)。再加上當民眾發現自己電腦中毒時，並沒有立即斷網，使得勒索病毒進一步擴散。基於這三個原因，使當時台灣中毒的電腦數量在各國中名列前茅。

4. WannaCry 事件後之反思

事件發生之後，我們應當反思、檢討為何台灣會成為這次事件中的重災區。經過我們了解事件經過與充分討論後，統整出以下需改善的部分：

(1) 老舊資訊設備過多，沒有定期更新。
(2) 我國資訊教育推廣不利，導致人民部分資訊安全相關概念低落。
(3) 國人未特別重視資訊安全，導致防範意識不足。

依照上述幾點，本文將會以民眾的資訊安全意識情況作討論。為了做正確的相關探究，我們先定義資訊安全並了解它想達成的目標、重要性及推廣方法。

二、何謂資訊安全

(一) 資訊安全定義

「**網路安全只是資訊安全的其中一項，對多數企業而言，雖然建構完善的網路安全能夠保障大部分的資訊安全，但它仍不是全部。**」（iThome，2004 年）部分民眾會將資訊安全與網路安全劃上等號，認為只要網路安全做好，資訊安全即可受到保障。但「**資訊安全的定義就是保護任何與電腦相關事務之安全**」（王振漢，2018 年），換句話說，資訊安全的範圍並不侷限於網路安全，還包含設備安全、資料安全、設備維護、資料備份等方面。只要屬於電腦內部資訊資產或內部資料，皆為資訊安全保護的部分。

(二) 資訊安全之目標

資訊安全欲達成的目標為：

1.確保資訊資產受到保護。
2.建構安全網路環境。
3.保護設備安全且不被電腦病毒侵害。
4.防止電腦遭他人惡意利用。

(三) 資訊安全之重要性

資訊安全防護與疾病防治極為相似，目的皆為如何避免其影響生活。所以資訊安全的重要性跟身體健康一樣重要，應被推廣並落實。

(四) 目前實施推廣資訊安全之舉措

1. 法律規定

「**政府必須藉由國家資通訊安全整體規劃，保持與國際資通訊安全組織訊息同步。**」（王中北，2004 年）政府應對資訊安全有一定的法律規範。2018 年通過之資通安全管理法、資通安全管理法施行細則，及 2019 年通過之資通安全責任等級分級辦法，本國以上述三部法典規範政府機關在資通安全的相關事務，且於資通安全管理法第五條「**主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。**」(「資通安全管理法」，民 107 年）也有相關規定，利用國家力量發展資訊安全相關科技，推動我國資通安全發展，並讓國人得以了解資訊安全。

2. 學校教育

我國資訊教育發展從早期資訊融入教學，到九年一貫課程綱要及普通高級中學課程綱將資訊科獨立出來到自然與生活科技領域內，及近年十二年國民教育課程綱要，將生活科技跟資訊科獨立成科技領域，持續進步與完善課程。資訊教育的演變過程中，從早期加入網路安全為能力指標，至近期在七年級學習內容加入資訊安全做為學習素養指標，近 20 年來資訊教育的沿革，理論上我國在資訊教育跟資訊安全相關教育已發展的十分完善。

三、台灣高中職生對於資訊安全之看法

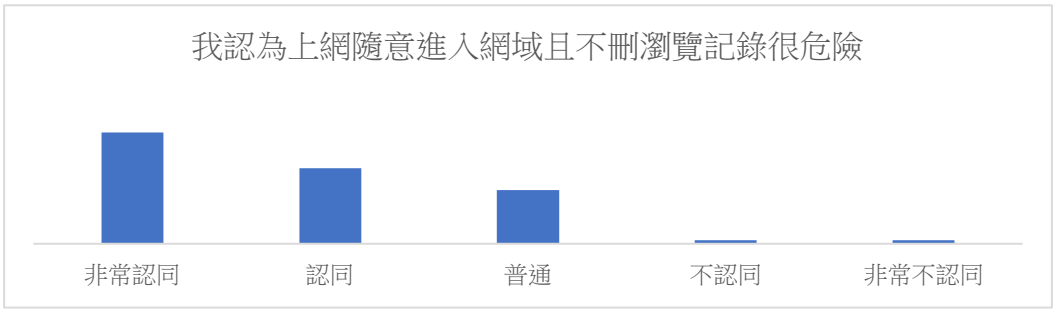
在資訊普及、全球網路化及資訊化的時代，台灣青少年可在高級中等教育階段下培養出完整的資訊素養。但經歷 2017 年 WannaCry 事件及其他資訊安全事件後，我們知道事實未必如此。台灣的政策及教育推廣是否仍有所不足，導致諸多台灣人於此事件中受害？因此我們設計研究問卷，試圖研究台灣高中職生對資訊安全的認知與行為。本問卷總計 61 份，扣除非研究對象所填問卷，共計 60 份。以下分成三個部分——資訊安全看法、資訊安全相關行為、資訊安全推廣途徑依序探討。

(一) 資訊安全看法

以此段在於分析高中職生是否具備資訊安全概念，問卷討論結果如下：

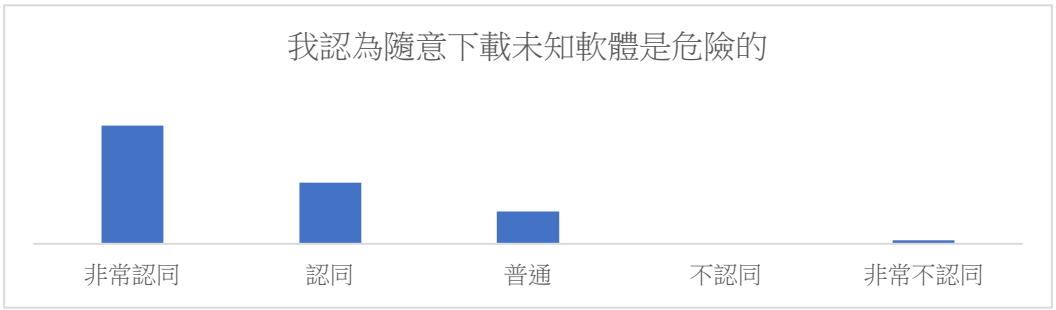
圖四：問卷回答結果-1
（圖四資料來源：研究者繪製）

由圖四可知，60 位學生中有 55 位學生，約 91.67%覺得主動了解資訊安全相關內容及隨時注意相關議題是必要的。



圖五：問卷回答結果-2
（圖五資料來源：研究者繪製）

由圖五可知，60 位受測者中有 52 位，大約 86.67%的受測者，認為隨意瀏覽不知名網站具有一定危險有性；但仍舊有約 25.00%的受測者覺得還好，並未具有危險性。



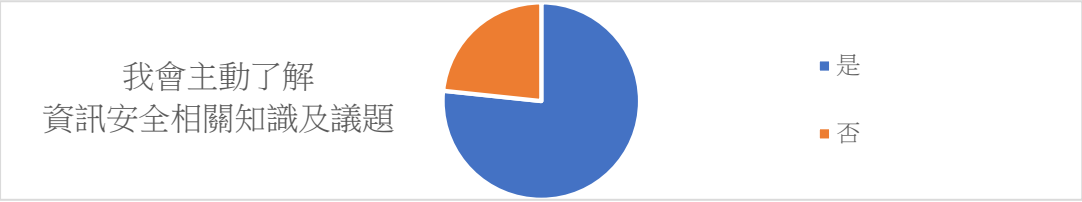
圖六：問卷回答結果-3
（圖六資料來源：研究者繪製）

由圖六可知，有 83.33%的受測者認為來路不明的軟體具有一定的危險性，其中亦有約 16.67%覺得危險性不算非常高。

統整結果，現今高中職生對資訊安全這方面已有一定程度的重視，但是仍有部分學生不太重視來路不明的軟體及網路安全等部分。

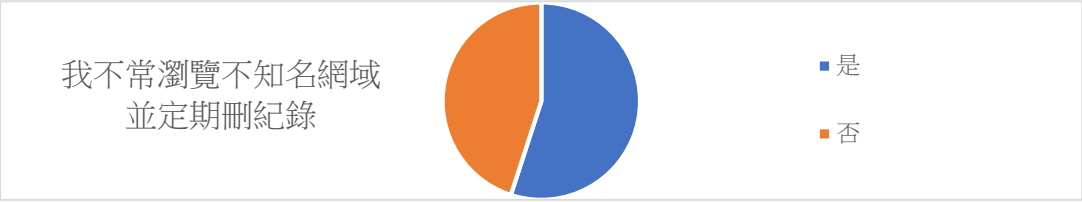
(二) 資訊安全相關行為

雖然上述討論結果得知，目前普遍的高中職都已具有一定程度的資訊安全相關概念，但人們會存有僥倖心理，認為按照正確的觀念行事十分繁瑣，同時相信自己不會是受害者，進而不運用所學相關知識。故此部分為探討受測者在第一部分所述的相關知識是否有如實反應在行動上。以下為討論結果：



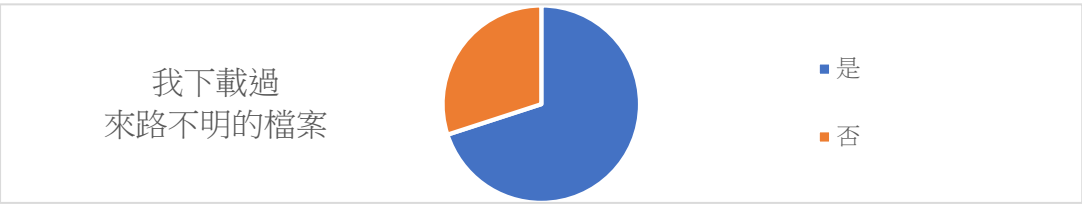
圖七：問卷回答結果-4
（圖七資料來源：研究者繪製）

藉由上圖可以了解，60 位受測者中有 46 位，約佔總受測者 76.67%，會主動了解資訊安全這方面的相關知識。



圖八：問卷回答結果-5
（圖八資料來源：研究者繪製）

圖八顯示出在 60 位受測者中只有 33 位，約佔受測者 55.00%，不常瀏覽不知名網域跟定期刪除紀錄；對比上面資訊安全意識中的「我認為上網隨意進入網域且不刪瀏覽記錄很危險」(圖五)的數據，約 86.67%的受測者認為瀏覽不知名網域跟不刪除紀錄是危險的。由此可以推論出，即使已有相關概念，但亦有部分人們不見得會遵守正確觀念來進行相關行為。

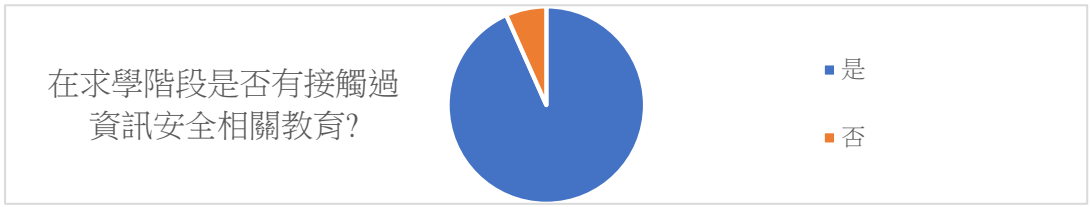


圖九：問卷回答結果-6
（圖九資料來源：研究者繪製）

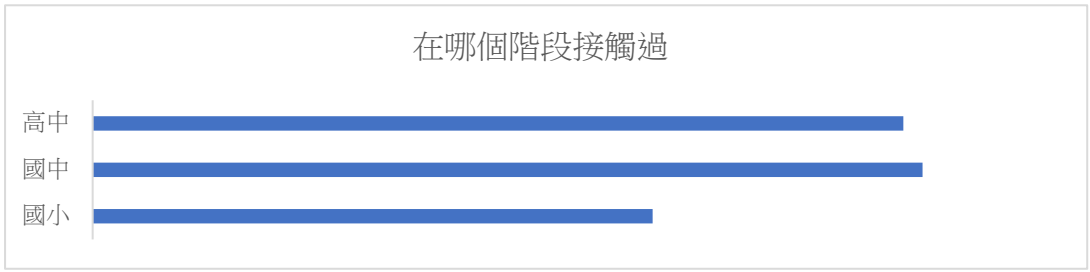
再把上圖跟資訊安全意識中的「我認為隨意下載未知軟體是危險的」(圖六)進行比較，在資訊安全意識中有 83.33%受測者覺得是危險的；本題中，卻僅有 30.00%的受測者沒有下載過來路不明的檔案，證明了縱使來路不明的檔案具有危險性，但大多數人依舊會選擇下載。

(三) 資訊安全推廣途徑

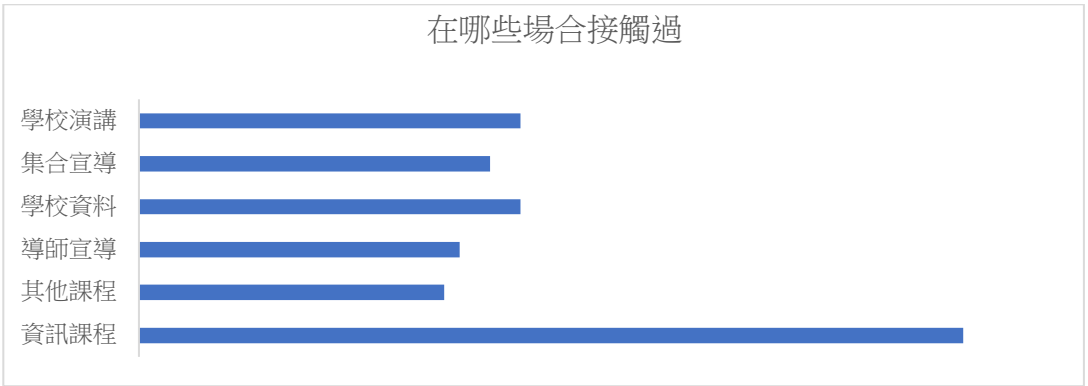
本篇研究限縮於台灣的高中職生，承前言所說，目前高中職生在資訊教育健全的環境下長大，所以設計此部份，探究這些相關知識是否能在教育環境中學到，藉以檢視目前資訊安全教育需加強之處。以下為分析結果：



圖十：問卷回答結果-7
（圖十資料來源：研究者繪製）



圖十一：問卷回答結果-8
（圖十一資料來源：研究者繪製）



圖十二：問卷回答結果-9
（圖十二資料來源：研究者繪製）

上面三張圖中(圖十到圖十二)，有 93.33%的受測者在學校接觸過資訊安全相關教育；而在(圖十二)中，有 96.64%在資訊課程時接觸過。但是仍有少部分受測者回復沒有接受過相關教育，這些學生，可能在資訊安全這方面尚未建立正確觀念。

參、結論

一、研究結果

(一) 資訊安全看法

在這一個部分，91.67%的受測者覺得主動了解資安相關議題是必要的，86.67%覺得隨意進入未知網域跟不刪紀錄是危險的，83.33%的人認為下載不知名檔案是有風險的。從這三個題目中可以看出，高中職生普遍對於資訊安全的看法頗為完善。

(二) 資訊安全相關行為

從這一部份可以看到，76.67%的受測者會主動了解資安相關議題，55.00%的受測者會避免瀏覽未知網域且會刪除記錄，30.00%的受測者沒有下載過未知的檔案。從資訊安全看法跟相關行為這兩大部分來看，其實很多人都是知道，但是不見得會做。由此可見，從了解概念到運用在實際行動上有很大的距離落差。

(三) 資訊安全推廣途徑

根據數據來看，有高達 93.33%的受測者在學校接觸過資安相關教育。且在有接觸過的人中，高達 96.64%是在資訊課程接觸過。由此我們可以知道，目前在資訊安全教育推廣這個面向，學校教育本身相當健全。

二、研究建議

(一) 目前我國資訊教育或資訊安全教育推廣已經相當完善，但在行動方面，眾多受測者所表現出已了解但不願意去行動。未來政府可以在此方面加強宣導，讓學生了解實踐資訊安全觀念的重要性，藉以使資訊安全真正落實。

(二) 本篇研究主要是以高中職生為研究對象，但我們可以看到在網路使用的面向仍稍嫌不足。未來政府可以加強學生在此方面的宣導，令其了解網路使用的重要性，培養正確的使用觀念，降低電腦中毒的風險。

肆、引注資料

iThome（2004 年）。資訊安全是什麼？。2020 年 2 月 22 日，取自 https://www.ithome.com.tw/node/29124

王中北（2004 年）。**主管資訊安全風險源知覺、數位化程度對中小企業資訊安全治理成熟度影響之研究**。實踐大學企業管理研究所：碩士論文

王振漢(2018 年)。**國軍雲端資料中心資訊安全評估指標之研究**。國防大學資訊管理學系：碩士論文

李郁苓（2018 年）。**影響個人對於勒索病毒威脅防範與行動採取因素之研究：保護動機理論觀點**。銘傳大學企業管理學系：碩士論文

李綱（2018 年）。**社交工程攻擊防制之研究-以釣魚郵件為例**。國防大學網路安全碩士班：碩士論文

陳曉莉(2017 年)。WannaCry 2.0 勒索蠕蟲狠襲全球，上百個國家受駭，台灣也是重災區。2020 年 2 月 18 日，取自 https://www.ithome.com.tw/news/114144

陳曉莉（2017 年）。即使漏洞修補了兩年, WannaCry 仍是 使用 EternalBlue 漏洞攻擊手法中最多的。2020 年 2 月 18 日，取自 https://blog.trendmicro.com.tw/?p=62316

資通安全管理法（民 107 年 06 月 06 日）

趨勢科技（2017 年）。《資安漫畫》系統漏洞是什麼? 為何要更新修補程式? 2020 年 2 月 8 日，取自 https://blog.trendmicro.com.tw/?p=50091

（附錄）問卷內容

台灣高中(職)生對於資訊安全的看法及行為

這是一份匿名問卷，所有回答皆不具名。本問卷主要目的在於調查台灣人對於資訊安全的看法，及自己有無做到保護個人資安的行為。本問卷所有問題皆無對錯，亦無優劣，故請您完全依照自己的經驗回答，感謝各位。

本分問卷名詞定義：
資訊安全係指一切可保護個人資料或資訊設備資料的所有行為, 其範圍包含資訊(網路)安全、資訊安全相關行為(如:電腦病毒防範、電腦系統漏洞修補等)以及得知資安的途徑。
高中(職)生係指目前正在就讀普通型高級中等學校、技術型高級中等學校或綜合型高級中等學校的在校學生。

敬祝　心想事成

張簡雲翔、陳奕羶、李秉育 敬上
（有＊的為必填題）

個人資料

性別＊

□男
□女

請問您目前就讀下列哪一種學校＊

□普通型高級中等學校
□技術型高級中等學校
□綜合型高級中等學校
□我目前非高中(職)生

對資訊安全的看法

我覺得主動了解資訊安全相關知識及議題有必要＊

□ □ □ □ □
1 2 3 4 5

我認為隨意下載未知軟體是不對的＊

□ □ □ □ □
1 2 3 4 5

我覺得個人裝置有設密碼的必要性＊

□ □ □ □ □
1 2 3 4 5

如果電腦中毒我認為自己有責任＊

□ □ □ □ □
1 2 3 4 5

資訊安全相關行為

我會主動了解資訊安全相關知識及議題＊

□是
□否

我不常瀏覽不知名網域並定期刪紀錄＊

□是
□否

我的個人裝置有安裝防毒軟體＊

□有
□沒有

我下載過來路不明的檔案＊

□有
□沒有

我會關注電腦系統是否存在漏洞＊

□是
□否

我會自己安裝系統的更新＊
□是
□否

我會自己安裝應用軟體的更新＊

□是
□否

我的資訊及通訊設備有設密碼＊

□是
□否

得知資安的途徑

在求學階段是否接觸過資訊安全相關教育?＊

□是
□否

承上題,在哪個階段接觸過(可複選)

□國小
□國中
□高中

承上兩題,在哪些場合接觸(可複選)

□資訊課程
□其他課程
□導師宣導
□學校資料(如學校雜誌或某處室發的宣導單)
□集合宣導
□學校演講
□_____（其他）

是否於其他地方接觸過資訊安全相關訊息(可複選)＊

□無
□親朋好友
□路邊店家
□社群軟體
□各類網頁平台
□_____（其他）

感謝您的回覆，我們這邊已經收到您的回覆，如果可以的話可以再幫我們分享出去給你身邊的高中(職)生，謝謝。

敬祝　心想事成

張簡雲翔、陳奕羶、李秉育 敬上