公務機密
資訊安全維護

資安時事案例

惡意廣告｜Malvertising】以線上廣告作為誘餌，散播惡意軟體

抗中國認知戰　政院：別轉傳假訊息

個人資料保護法

什麼是個人資料?

生活中的資安

設定複雜密碼真的安全嗎？密碼管理或許不要再仰賴記憶

數位學習

107年資安動畫金像獎

資安嘻哈擂台

惡意廣告｜Malvertising】

以線上廣告作為誘餌，散播惡意軟體

iThome 文/莊念恩

網釣攻擊事件頻繁，攻擊者以潛藏在廣告背後的方式，使受害者難以察覺。

網路釣魚手法不斷有新變化，電子郵件雖然還是典型的釣魚媒介，但也出現越來越多網釣攻擊的管道。隨著網路的普及化，線上廣告對於商業世界來說，是很重要的宣傳模式，卻也不小心被攻擊者盯上，成了攻擊的媒介，便出現了以廣告作為散播惡意軟體的方法，而且在近年更是有多起事件發生。

這樣的攻擊模式，被稱為惡意廣告（Malvertising），其實是由Malicious advertisement轉變而來的一個通稱。廣義而言，就是一種透過廣告來達成惡意攻擊的手法，而以狹義而言，會因不同的攻擊策略而有不同的定位。但主要的目的，都是希望不被受害者察覺異狀，進而能夠散播惡意軟體。

例如，在2009年，紐約時報的網站曾出現惡意廣告，在讀者瀏覽新聞頁面時，會彈出病毒警告，宣稱讀者的電腦已受感染，誘使受害者下載廣告的安全軟體，然而，紐約時報在當時表示，那些合法廣告，被轉換成病毒警報的惡意廣告，是與自第三方合作的全國性廣告供應商有關。

而同樣與第三方廣告平臺有關的例子，還有Spotify在2011年發生的事件，Spotify免費版的用戶，在無須點擊廣告下，透過偷渡式下載的方式，將惡意軟體安裝在用戶的Windows電腦。而當時有資安人員發現，攻擊者是利用Blackhole Exploit Kit工具來進行攻擊，甚至Spotify在背景播放時，也會進行感染。而Spotify在2016年又傳出一次類似的事件，連MacOS與Linux作業系統的用戶也受害。上述這些事件中，會發現問題多出於第三方廣告平臺，或許這也代表著其審查機制有問題。可惜，在這些事件中未提及真正原因。反而，資安人員有提到因為有電腦漏洞，進而導致惡意軟體更容易被植入受害者電腦。

此外，惡意廣告在近年來，還結合重新導向惡意網站的攻擊事件，也是透過合法平臺滲透至受害者電腦。例如，在2015年，曾發生雅虎的廣告網路（ads.yahoo.com）被入侵，受害者在點擊廣告後，會被重新導向攻擊者利用攻擊套件產生的惡意網站。

而在近期，也出現了類似事件，攻擊者先以合法版本的行動App在Google Play商店中上架後，再置換成惡意版本，在受害者更新版本後，進而感染。由此可知，利用惡意廣告的攻擊不計其數，未來可能還會有更多的新興手法產生

抗中國認知戰　政院：別轉傳假訊息

NOWnews今日新聞 (2021-05-19

國防安全研究院在2020發佈的中共年報中指出，中共對台認知作戰可視「灰色地帶衝突」且會消耗民主資源，國安單位近期應注意共軍戰略支援部隊這支隱蔽性較高的軍種對台進行「沒有硝煙的戰爭」；行政院發言人羅秉成今（19）日接受訪問時表示，中國的認知作戰為得就是分化台灣社會，民眾應避免下載、轉傳假訊息，成為中國認知作戰的工具、成為「假訊息破口」。

國防安全研究院近期發布的中共年報中提到，在2019年新冠肺炎疫情發生後，中共的大外宣手段、對台認知作戰的手段、改變及因應方式；報告指出，認知作戰是藉由資訊與衝突手法，達到改變思維、進而改變行為目的，可從官方與非官方、軍方與民間等協同進擊，不受限平時與戰時，並善用敵方、我方、國際媒體與新媒體等平台。

對此，羅秉成表示，假訊息的危害不用多說，根據學術、政府及民間團體的研究，台灣跟其他國家相比，受境外假訊息攻擊的比例更高；假訊息可達到分裂社會、族群、打擊政府威信、降低人民對政府的信賴，在選舉時更為嚴重，又被稱為「沒有硝煙的戰爭」。

羅秉成說，假訊息跟新冠肺炎一樣，傳播的速度很快、危害很大；面對假訊息，要有自我防護機制，不要下載、轉傳、分享，就能有效防止假訊息的散播。羅秉成舉例近期「化學兵消毒，由於消毒藥劑很毒，要民眾別在戶外飲食」的假訊息，就是典型的認知作戰，一則打擊國軍、二來造成社會恐慌，經檢警調查後已移送6人，呼籲國人不到被當成認知作戰的工具，而政府也會審慎以對、積極查辦，希望國人能共同防衛，不要變成「假訊息破口」。

什麼是個人資料?

小明是一位承辦戶籍資料業務的公務人員，有天一個年輕貌美的妙齡女子前往戶政事務所申辦戶籍遷入，小明驚為天人，但仍壓抑住自己澎派的情緒，請女子填寫個人資料，並為她辦好戶籍變更登記，又利用戶籍資料查詢系統蒐集了許多她的資料。

- 但當晚小明對妙齡女子牽腸掛肚、輾轉難眠，於是起身在FB上po了一段文字「Dear 江小美，妳的出現猶如天使的降臨，讓我的心起了漣漪，妳有一雙水汪汪的大眼，一頭烏黑的長髮。雖然妳最近工作和感情皆不順利，為了轉換心情而搬到我們鄉鎮，但我們男未娶，女未嫁，且妳的生日與我的生日只差了11個月，這不是一個很巧妙的緣分嗎?相信以我不錯的收入，加上妳50萬的年收入，況且妳沒有其他家屬，只要你情我願，我們一定可以組成一個幸福的家庭，將我們優良的基因傳承下去!」

個資法對於個人資料的定義

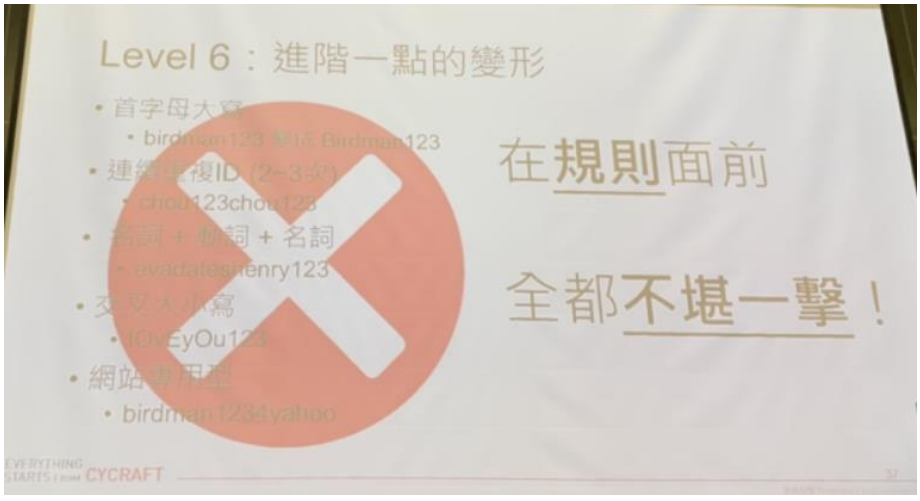
- 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
- 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

設定複雜密碼真的安全嗎？

密碼管理或許不要再仰賴記憶

資料來源: iThome 文/莊念恩 | 2021-05-07發表

在很多地方都需要密碼，臺灣使用者常設定好記的密碼，其實都有規則可循，甚至可以從中發現人與人之間的關係，但這都可能成為密碼被破解或重設的依據。



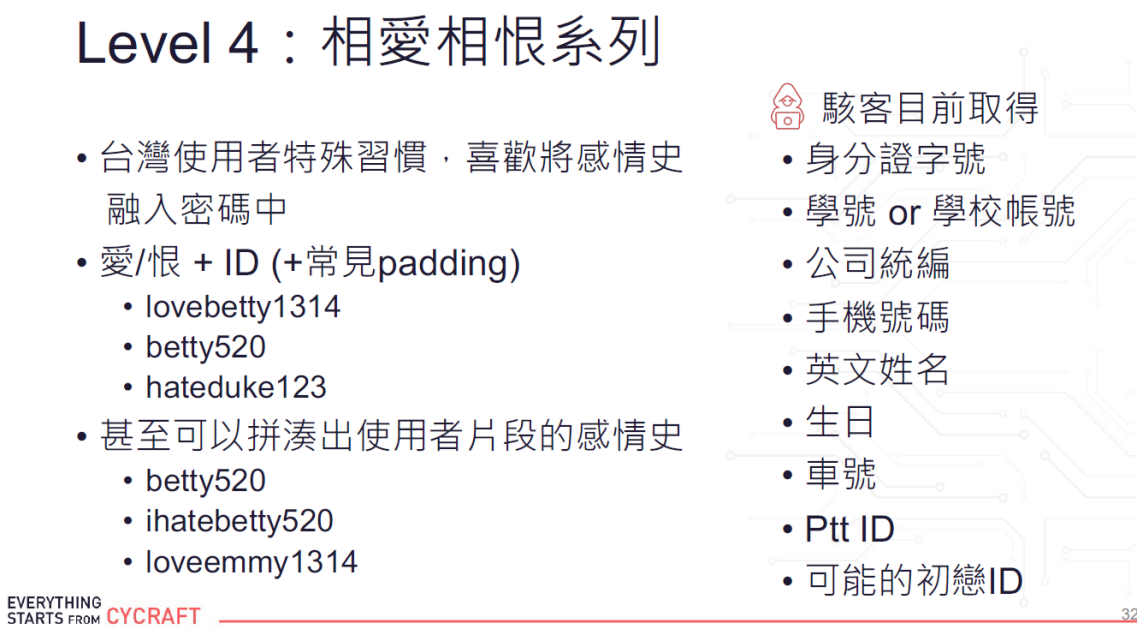
密碼，是很多網站或是安全保護有關的重要通關密語，而密碼設定的規則，卻是一個令人矛盾的地方，因為要好記，使用者可能會在所有地方用相同的密碼，或是使用簡單的變化，但這些都可以被歸納出規則。而這次資安大會的議程中，奧義科技的ML Team軟體架構師楊政霖表示，只要是可以找到規則的密碼，都屬於弱密碼。

何謂弱密碼？就是很容易被有心人士猜測進而破解身分驗證的密碼，如駭客會利用密碼噴灑手法嘗試所有可能組合的弱密碼，以達成目的。而關於弱密碼，楊政霖提到，很多人認為是不是將密碼增加padding（填充字串），或是用常用的詞語組合起來，就可以提昇密碼強度。然而，這還是可以被歸納出規則，因此，楊政霖以6種等級為例來說明，是以一定時間裡，在Hash值中算出最多的密碼組數，將使用者密碼作為分級，首先，第1級的是帶有英文數字的編號，如身分證字號、學號、手機號碼、車號等，其中身份證字號的使用率，常見在50歲以上的臺灣使用者。

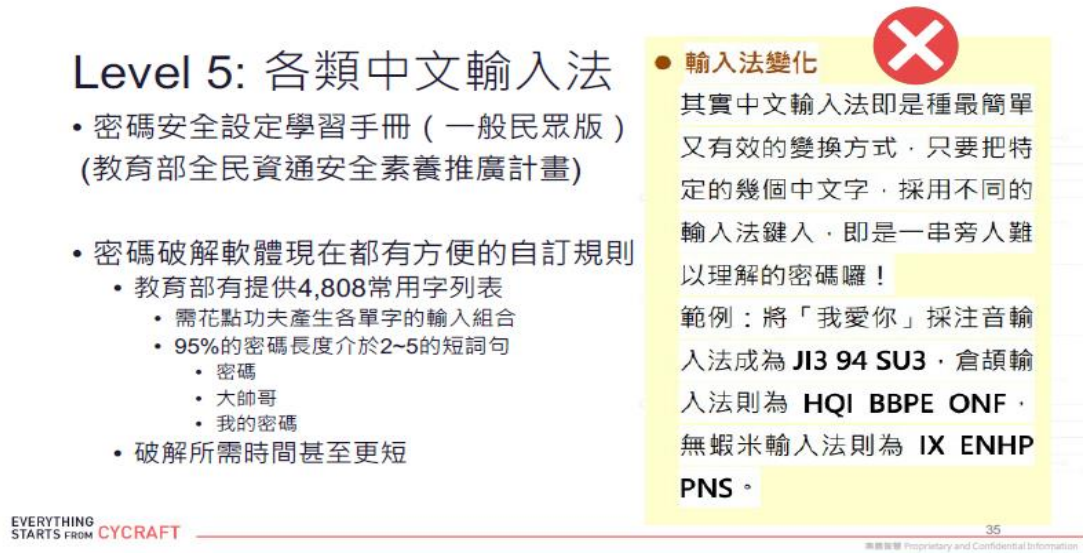
第2級是以常用的英文名字或ID加上數字、大小寫或變換順序，因為臺灣人的英文名字重複率非常高，駭客也容易在網路上得到英文姓名的清單。ID部分則是駭客透過持續嘗試累積ID名單。而數字方面，有生日、連續數字或是手機號碼做為變化的組合元素

接著是第3級，以PTT的ID加上數字做變形，但駭客其實很容易取得PTT的ID，如果繼續嘗試一樣可以破解。

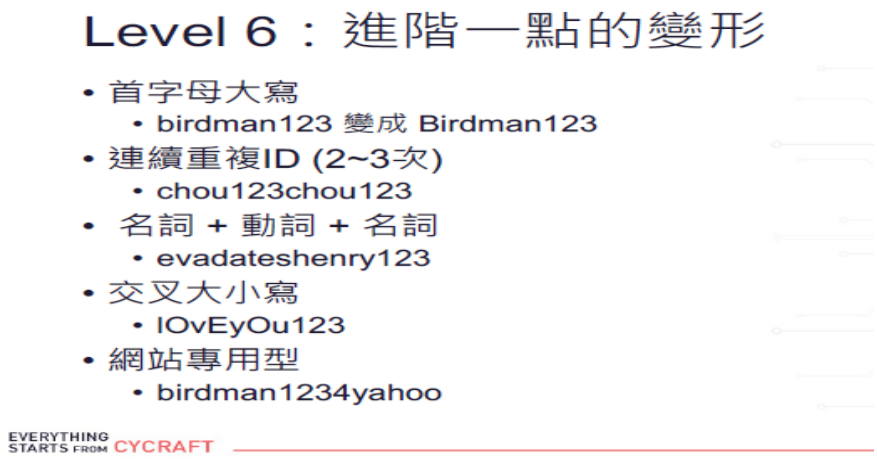
而第4級，則是屬於臺灣使用者的一種特殊習慣，大家喜歡將感情史融入密碼中，譬如自己與誰的愛恨情仇，楊政霖表示，這是在研究中臺灣使用者很常見的規則，而這樣的規則，其實是讓人有重設密碼的機會，因為只要有人知道了片段關係，甚至就可以回答出安全提示所設的題目，如您的初戀情人的名字。



接著，第5級是各類中文輸入法，根據教育部的全民資通安全素養推廣計畫，建議可以用中文輸入法作為密碼，但這其實在駭客取得用字列表，搭配可能的組合，反而是更快會被破解。



再來的第6級則是進階的變形，楊政霖統計出有70%的使用者會將首個英文字母設為大寫，或有些是將舊密碼或ID重複達到系統的規定，而在這過程中，他也觀察出一些有趣的組合，像是狀聲詞加上一個名字或ID，或是用中文輸入法將私人恩怨設定為密碼。



最後，楊政霖表示，如果要夠亂又夠強的好密碼，就會不好記，因此他建議可以使用密碼管理（password manager），以提升密碼的複雜度。而他也提到密碼的保護方法，可以利用雙因素驗證（Two-factor authentication，2FA）服務。