國立中壢高級商業職業學校

105年度資安宣導研習課程

報告人：中壢高商技士　　張之旗

105年11月15日

大綱

一、線上資訊安全學習課程

二、資訊安全基本概念

三、近期資訊安全攻擊與防範個案

大綱

一、線上資訊安全學習課程

二、資訊安全基本概念

三、近期資訊安全攻擊與防範個案

1-1線上資訊安全學習課程

- 依據「政府機關(構)資通安全責任等級分級作業規定」，各學院、專科學校及高級中等以下學校之資安責任等級為C級，每年一般使用者與主管至少須接受3小時資安宣導課程並通過課程評量。
- 煩請同仁於105年12月15日前，於「e等公務園」、「台北e大」或「文官e學苑」等數位學習網修滿3小時資安相關數位學習課程並取得認證時數。

1-1線上資訊安全學習課程

- 「e等公務園」網址：
  - https://elearning.hrd.gov.tw/index.php
- 「台北e大」網址：
  - https://elearning.taipei/mpage/
- 「文官e學苑」網址：
  - https://ecollege.nacs.gov.tw/Nacs/index

1-1線上資訊安全學習課程

- 「e等公務園」資安課程建議清單：
  - 資安案例分享_e-mail社交工程及防護(行政院資通安全辦公室提供)-認證時數1小時
  - 資安管理-個人篇(行政院資通安全辦公室提供)-認證時數1小時
  - 資訊安全(國家發展委員會提供)-認證時數2小時
  - 資訊安全概論(行政院資通安全辦公室提供)-認證時數1小時
  - 檔案資訊安全(國家發展委員會檔案管理局提供)-認證時數1小時
  - 資安風險管理概觀(窄頻)(行政院資通安全辦公室提供)-認證時數1小時
  - 資安風險評鑑實務(行政院資通安全辦公室提供)-認證時數1小時
  - 資訊安全管理系統政策制定與資訊安全組織建立(行政院資通安全辦公室提供)-認證時數1小時
  - 資訊安全稽核介紹與實務(窄頻)(行政院資通安全辦公室提供)-認證時數1小時
  - 資安管理-主管篇(行政院資通安全辦公室提供)-認證時數1小時
  - 資安管理制度(ISMS)標準—ISO/IEC 27001：2013介紹-認證時數1小時

1-1線上資訊安全學習課程

- 「台北e大」資安課程建議清單：
  - 資訊安全-認證時數3小時
  - 資訊安全-網路資安事件分析-認證時數5小時
  - 資訊安全-行動裝置安全防護-認證時數5小時
  - 日常工作中如何落實資訊安全(中華郵政股份有限公司提供)-認證時數1小時
  - 我的電腦不怕駭-資通安全實務(高雄市政府公務人力發展中心提供)-認證時數2小時

1-1線上資訊安全學習課程

- 「文官e學苑」資安課程建議清單：
  - 個人隱私資安防護-認證時數2小時
  - 資訊安全-認證時數3小時

大綱

一、線上資訊安全學習課程(3小時)

二、資訊安全基本概念

三、近期資訊安全攻擊與防範個案

二、資訊安全基本概念

2-1 什麼是資訊安全

2-2 常見的資訊安全事件

二、資訊安全基本概念

2-1 什麼是資訊安全

2-2 常見的資訊安全事件

2-1 什麼是資訊安全

- 資訊安全
  - 意為保護資訊及資訊系統免受未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀。
  - 有關資訊保護之研究的總合稱為資訊安全。

二、資訊安全基本概念

2-1 什麼是資訊安全

2-2 常見的資訊安全事件

2-2常見的資安事件

- 使用者資訊安全認知不足造成資料外洩
- 不安全的密碼保護及設定
- 誤上釣魚網站

2-2常見的資安事件

- 使用者資訊安全認知不足造成資料外洩
- 不安全的密碼保護及設定
- 誤上釣魚網站

2-2常見的資安事件

一般都會注意…

- 建立安全的周邊環境…

2-2常見的資安事件

據統計有80%的資料遺失,是因為內部人員有意或無意之下所造成的結果

2-2常見的資安事件

- 使用者資訊安全認知不足造成資料外洩
- 不安全的密碼保護及設定
- 誤上釣魚網站

2-2常見的資安事件

- 資料來源：YAHOO！奇摩 新聞

123456 最不安全的密碼寶座

自由時報 – 2014年1月22日 上午6:11

你的電腦密碼還在使用「123456」嗎？市場研究公司SplashData分析2013年數百萬個被盜的密碼，結果顯示，「123456」登上最不安全的密碼寶座。

過去長居不安全密碼首位的是「password」，今年「123456」首度擠下「password」，成為第一名。其他不安全密碼依序是，「password」、「12345678」、「qwerty」、「abc123」、「123456789」、「111111」、「1234567」、「iloveyou」、「adobe123」。

SplashData建議個人或企業應使用8位或更多位的密碼，並混合各種類型字元。

2-2常見的資安事件

- 密碼設定訣竅如下
  - 至少 6 個字元的密碼
  - 使用數字、字母、符號（＃％＄@...）混合穿插的密碼字串
  - 不使用過於複雜而無法記憶的密碼
  - 避免使用簡單且字典查得到的單字或學校名稱縮寫
  - 若要使得密碼簡單易記，使用者可以選擇喜愛的名字但務必穿插數字或符號以增加密碼破解的難度。例如將happyjohn 修改為h@ppyj0hn 。

2-2常見的資安事件

– 密碼保護訣竅如下

- 將密碼存放於高安全性的地方。
- 定期更新密碼，減少密碼外流的機率。
- 若懷疑有人可能知道你的密碼時，即刻更改。
- 不隨手寫下密碼 。

2-2常見的資安事件

- 使用者資訊安全認知不足造成資料外洩
- 不安全的密碼保護及設定
- 誤上釣魚網站

2-2常見的資安事件

– 詐騙網址

hxxp://yahooo.s3.topnic.cn/data/bak/

2-2常見的資安事件

- 正確的Yahoo登入頁面應是 https://login.yahoo.com/..

2-2常見的資安事件

- 誤上釣魚網站
  - 正常網站https://ebank.bot.com.tw
  - 釣魚網站http://ebnk.bot.conn.tw

  - 正常網站http://tw.bid.yahoo.com
  - 釣魚網站http://tw.bids-yahoo.com

大綱

一、線上資訊安全學習課程(3小時)

二、資訊安全基本概念

三、近期資訊安全攻擊與防範個案

3.近期資安攻擊與防範個案

- (1)「看著這些照片，好懷念以前的日子！」按訊息連結 被詐5千(資料來源：自由時報)
- (2)LINE帳號被盜 一招火速搶回(資料來源：自由時報)
- (3)宅急便病毒化身35種簡訊，一人中鏢好友恐全難逃(資料來源： NOWnews今日新聞)
- (4)電子郵件夾帶病毒(資料來源：衛生福利部中央健康保險署)
- (5)勒索病毒(資料來源：趨勢科技)

3.近期資安攻擊與防範個案

- (1)「看著這些照片，好懷念以前的日子！」按訊息連結 被詐5千(資料來源：自由時報)
- (2)LINE帳號被盜 一招火速搶回(資料來源：自由時報)
- (3)宅急便病毒化身35種簡訊，一人中鏢好友恐全難逃(資料來源： NOWnews今日新聞)
- (4)電子郵件夾帶病毒(資料來源：衛生福利部中央健康保險署)
- (5)勒索病毒(資料來源：趨勢科技)

3.近期資訊安全攻擊與防範個案

(資料來源：自由時報)

- 攻擊方式
  - 在智慧型手機的Line或臉書接獲訊息，直接點選連結網址。
  - 以為老朋友...怎麼都不認識。
  - 木馬程式來襲 啟動小額付款。
  - 1小時後即收到電信公司小額付款通知簡訊，有人因而損失5000元...

3.近期資訊安全攻擊與防範個案

(資料來源：自由時報)

- 防範方式
  - 小額付款預設開啟 最好取消
  - 警方指出，經由IP追查，這類詐騙集團的主機都設在中國，讓警方難以直搗其總部，提醒民眾，要避免被騙，就是不要點選來歷不明的訊息連結網址，也不要下載可疑的APP軟體，最好打電話要求電信公司取消小額付款功能。

3.近期資安攻擊與防範個案

- (1)「看著這些照片，好懷念以前的日子！」按訊息連結 被詐5千(資料來源：自由時報)
- (2)LINE帳號被盜 一招火速搶回(資料來源：自由時報)
- (3)宅急便病毒化身35種簡訊，一人中鏢好友恐全難逃(資料來源： NOWnews今日新聞)
- (4)電子郵件夾帶病毒(資料來源：衛生福利部中央健康保險署)
- (5)勒索病毒(資料來源：趨勢科技)

3.近期資訊安全攻擊與防範個案

(資料來源：自由時報)

- 「你的LINE帳號被詐騙集團盜用了！」最近很多人接到朋友通知，往往不知所措。
- 刑事局提醒，其實只要第一時間取消「允許自其他裝置登入」，並變更密碼，搶回帳號的機率非常高。
- 選取LINE「其他」→「設定」→「我的帳號」後，把「允許自其他裝置登入」的打勾取消。

3.近期資訊安全攻擊與防範個案

(資料來源：自由時報)

- 填寫問題反應表（https://line.naver.jp/cs/），更重要的是趕緊一一通知周遭朋友，不要被剛剛的訊息騙了！
- 警方提醒，為避免手機不小心遺失，被人撿到後登入LINE使用，也可以在「其他」→「設定」→「隱私設定」中選取「密碼鎖定」，輸入密碼鎖可簡單保障安全。
- 當然，手機或電腦不下載不明程式、不在網咖公用電腦登入LINE等，都是保護帳號的不二法門。

3.近期資安攻擊與防範個案

- (1)「看著這些照片，好懷念以前的日子！」按訊息連結 被詐5千(資料來源：自由時報)
- (2)LINE帳號被盜 一招火速搶回(資料來源：自由時報)
- (3)宅急便病毒化身35種簡訊，一人中鏢好友恐全難逃(資料來源： NOWnews今日新聞)
- (4)電子郵件夾帶病毒(資料來源：衛生福利部中央健康保險署)
- (5)勒索病毒(資料來源：趨勢科技)

3.近期資訊安全攻擊與防範個案

(資料來源： NOWnews今日新聞)

3.近期資訊安全攻擊與防範個案

(資料來源： NOWnews今日新聞)

- 攻擊方式
  - 主要是透過各種引人注目的文字內容，例如「來下載上次聚會的照片」、冒充「新北市政府警察局」的案件處理結果通知單、「張惠妹新歌試聽」等等，在簡訊中放入含有病毒的網址連結，誘使民眾點擊。
  - 被誘導下載「小額支付大盜App」，直接導致金錢損失。
  - 此類病毒可以取得手機通訊錄，因此當一人受害，其通訊錄中的所有人都可能收到詐騙簡訊，導致受害人數暴增。

3.近期資訊安全攻擊與防範個案

(資料來源： NOWnews今日新聞)

- 防範方式
  - 針對此類病毒簡訊氾濫情形，刑事警察局甚至推出防詐騙懶人包，其中提到，若不小心感染了簡訊病毒，可直接恢復原廠設定保障安全，但此舉將使手機中個人資料和安裝的應用程式等個人化資訊消失。
  - 最新版的CM Security免費手機防毒軟體中，已經加入了詐騙簡訊封鎖功能，並針對不明來源的網址連結進行防禦，使用者不須恢復原廠設定，也能保障手機安全。

3.近期資安攻擊與防範個案

- (1)「看著這些照片，好懷念以前的日子！」按訊息連結 被詐5千(資料來源：自由時報)
- (2)LINE帳號被盜 一招火速搶回(資料來源：自由時報)
- (3)宅急便病毒化身35種簡訊，一人中鏢好友恐全難逃(資料來源： NOWnews今日新聞)
- (4)電子郵件夾帶病毒(資料來源：衛生福利部中央健康保險署)
- (5)勒索病毒(資料來源：趨勢科技)

3.近期資訊安全攻擊與防範個案

(資料來源：衛生福利部中央健康保險署)

訊息快報

友善列印　寄給朋友

近日有心人士假本署名義發送健保卡網路報稅電子郵件夾帶電腦病毒，請勿開啟並立即刪除。

近日接獲民眾反應有心人士利用署名「衛生福利部中央健康保險署承保組承保資料科」，發送主旨：『網路報稅「健保卡+註冊密碼」輕鬆搞定』及『報稅囉~~健保卡報稅，輕鬆兩步驟』二份電子郵件夾帶電腦病毒，提醒您本署近日未發送是類電子郵件，請收到上開主旨之電子郵件切勿開啟立即刪除。

更新日期：2016/05/09

3.近期資安攻擊與防範個案

- (1)「看著這些照片，好懷念以前的日子！」按訊息連結 被詐5千(資料來源：自由時報)
- (2)LINE帳號被盜 一招火速搶回(資料來源：自由時報)
- (3)宅急便病毒化身35種簡訊，一人中鏢好友恐全難逃(資料來源： NOWnews今日新聞)
- (4)電子郵件夾帶病毒(資料來源：衛生福利部中央健康保險署)
- (5)勒索病毒(資料來源：趨勢科技)

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

- 勒索病毒攻擊方式
  - 瀏覽之網站藏有惡意廣告，受到「Drive by download」路過式下載攻擊。
  - 瀏覽惡意電子郵件，點選惡意網站連結或附件。

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

– 什麼是「Drive by download」路過式下載攻擊

- 「Drive by download」路過式下載（或稱為隱藏式下載、偷渡式下載、強迫下載）,這是一個在未經用戶同意(或用戶未知的情況下)自動下載到用戶電腦上的惡意程式, 另外,由於遭到植入惡意連結的網頁，多數會導向下載木馬程式，故俗稱網頁掛馬。
- 「Drive by download」路過式下載是利用系統、應用程式和瀏覽器的漏洞植入惡意程式的一種攻擊手段。網友即使只是瀏覽網站,也會在不知不覺中被迫下載惡意程式。

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

台灣的網頁掛馬攻擊

- 從2015年十月開始在台灣劇烈活動
- 第四季的攻擊總數有3.5倍的成長
- 從Q3的43,015次至Q4的152,929次

台灣的網頁掛馬攻擊,從去年底開始大幅成長,光去年第四季就成長3.5 倍

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

Q：瀏覽合法的官方網站也會感染上勒索病毒！？

A：是的，如果電腦有軟體的修補程式沒有更新的話，遇到「Drive by download」路過式下載攻擊，瀏覽惡意網頁或惡意廣告就會中毒，台灣也傳出相關案例。

Q：Cerber勒索病毒透過惡意廣告散播，主要集中在台灣，只要不點擊廣告就不會中招？

A：惡意廣告是勒索病毒傳播的主要途徑之一，大多數人對於惡意廣告有著很大的誤解，就是要有點擊的動作才會受到危害，事實上，惡意廣告的攻擊並不需要使用者的點擊，只要瀏覽器或裝置顯示出惡意廣告，使用者就會受到攻擊。

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

Q：網路追劇也有可能遇到勒索病毒嗎？

A：很多網友因為在網路追劇中毒，因為有些廣告會在影片播放前顯示，網路犯罪集團會經由這類廣告來散布惡意程式。這就是所謂的「惡意廣告」，除了勒索病毒,它們也利用軟體漏洞在系統暗中植入一些可竊取帳號密碼、銀行資訊和個人資料的惡意程式。

Q：CryptXXX勒索病毒受害者回報瀏覽過內容農場網站後出現中毒症狀，所以大型網站比較安全嗎？

A：在台灣傳出大量災情的 CryptXXX(RANSOM_Waltrix)勒索病毒主要利用 Flash/SilverLight/IE的漏洞進行攻擊，據受害者反映，瀏覽新聞網站、入口網站以及文章常在 Facebook 臉書上被分享的一些內容農場網站之後，開始出現感染勒索病毒的情況。許多高知名度的網站，因為他們的廣告網路在不知情下成為網路犯罪市場的幫兇。報導指出網頁廣告成勒索軟體散播溫床，紐約時報、BBC、MSN 皆中招，文中指出”攻擊者透過廣告聯盟及軟體漏洞，透過大型網站如《紐約時報》、BBC 、MSN 等的廣告，藉此安裝勒索病毒。

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

- 勒索病毒防範方式
  - 趨勢科技建議，若作業系統或是應用程式有提供修補程式或更新程式，應該要盡快更新，並使用防毒軟體，如此一來就能大幅度地減少威脅。

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

- 勒索病毒攻擊方式-2
  - 部分變種會透過email寄送office文件檔案,開啟文件時會要求開啟巨集的功能。
  - 此封信件也可能是一封封量身訂做的社交工程信件,比如針對人事部門的假冒應徵者履歷表。
  - 提醒您若收到這類信件或附檔，請不要任意開啟巨集以避免中毒。

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

– 勒索病毒曾經使用過的網路釣魚主旨或手法包含:

- 退稅通知
- 電子帳單/電子發票
- Google Chrome 和 Facebook 重大更新和通知訊息
- 假冒com 訂單出貨通知
- iPhone中獎通知
- 求職信/履歷表
- 電子訃聞
- 誘騙使用者連到看似真正銀行或政府機構網站的假網頁
- 輸入驗證碼（CAPTCHA，一種防止機器人的程序）
- 您的帳戶欠款已過期!

3.近期資訊安全攻擊與防範個案

(資料來源：趨勢科技)

- 勒索病勒索病毒防範方式-2

簡報結束

感謝聆聽