103 資訊安全與網路資源研習

tksu

103.10.15

研習軟體資料請至中正mail ccpsplan下載：
ftp://163.32.193.4/!tools_by_tksu/103-4U

大綱

前言：資訊倫理與資訊安全

- 網路犯罪社交工程APT攻擊
- IoE vs IPv6
- 資安案例宣導
- 網路教常資源
- 電腦節能與保健
- 資安檢查宣導

結語：

萬物聯網IoE(Internet of everything) VS IPv6

影片欣賞：2020網路危機 http://goo.gl/aDp6Pi

從高雄輕軌、機器人大展談萬物聯網的資安問題？

隨著居家環境越來越智慧化，新的安全挑戰也逐漸形成。過去一年，我們看到針對家用智慧型裝置，如嬰兒監視攝影機、電視、無線交換器、電燈等等的攻擊不斷持續增加。

就在智慧型電視遭駭客入侵引起大家更加關注萬物聯網（Internet of Everything，簡稱 IoE）的議題沒多久後，靠群眾集資成立的新創公司 LIFX 所生產的連網燈泡也被發現有可能洩漏 Wi-Fi 網路的密碼漏洞。

LIFX生產的連網燈泡，是一個具有WiFi功能，多色彩可以使用 iPhone或Android 智慧手機app控制的LED省電燈泡 。

這款「可變換顏色的省電 LED 燈泡」會經由標準的「6LoWPAN 」網狀網路（mesh network）廣播 Wi-Fi 密碼，這種網路是最適合低功率無線裝置（如燈泡）的一項通訊標準。

白帽駭客發現了一個可讓其進入主燈泡以及其他相連燈泡的漏洞。駭客接著又在屋主不知情的狀況下，向網狀網路索取該 Wi-Fi 網路的詳細資料。透過這個方法，駭客就能在離其中一個燈泡 30 公尺的距離內取得其加密後的密碼。

手機洩漏個資？3大品牌旗艦機驚爆13資安漏洞

http://www.setnews.net/News.aspx?PageGroupID=7&NewsID=29941

不要用？

不可能！

那就小心用！

Why IPv6?

IPv4位址不夠

現行IPv4位址最大可以定義約四十多億個IP位址，但全球目前人口已超過六十億，每人平均可分配量不到一個，而未來需上網的設備平均每人又不只一個(如手機、PDA、iPad、家電電器用品等)

IPv6

- 於一九九五年一月發表的RFC 1752。
- 在RFC 1752發表後，有三種版本經過討論後，決定選擇SIPP(Simple Internet Protocol Plus)。
- 最後, 將新的協定命名為「IPv6, InternetProtocol version 6」。

IPv6 誕生

Version 4 即為現在常見的IPv4所用。

Version 5已經被用在保留另一個Stream協定(Protocol)。

Version 6 順勢保留給下一代IP所用，因此可用的版本號為6，IPv6 就這樣誕生了。

- Version7、8、9也都被定義了，下一版就會是IPv10。

- IPv6 位址表示法(native)

IPv6使用128Bit的位址空間，也就是最高可有2^128的位址空間，以16進位(2^4)表示，可寫成32組十六進位數字。

20010288827f0001000000000000000001

太長容易記錯！

IPV6

- 2001:0288:827f:0001:0000:0000:0000:0001
- (分為八段，以冒號:分隔,好多了！)
- 2001:288:827f:1::1(簡寫，這樣才好記！)
- 簡寫規則:
- 每32Bit如開頭之4bit表示為0，即可省略，若32Bit全為0，則可簡寫為0。
- 若連續完整之32Bit段落皆為0000，則可全省略，簡寫為::，但以一次為限。

高市苓雅區中正國小IPV6網段

中正路由器SRX240-ccps相關設定(103.10.07)

port1 ipv6路由網路閘設定

- 163.32.193.0/24 port2→ 2001:288:827f:1:209:fff:fe85:f2aa

port3 ipv6路由網路閘設定

- 192.168.0.0/24 port4→ 2001:288:827f:3:209:fff:fe85:f2ac

port4 ipv6路由網路閘設定

- 192.168.1.0/24 port3→ 2001:288:827f:4:209:fff:fe85:f2ad

port5 ipv6路由網路閘設定

- 192.168.2.0/24 port3→ 2001:288:827f:5:209:fff:fe85:f2ae

port6 ipv6路由網路閘設定

- 192.168.3.0/24 port3→ 2001:288:827f:6:209:fff:fe85:f2af

苓雅區中正國小主機網址建置及維護

WWW：163.32.193.100（IPv4）

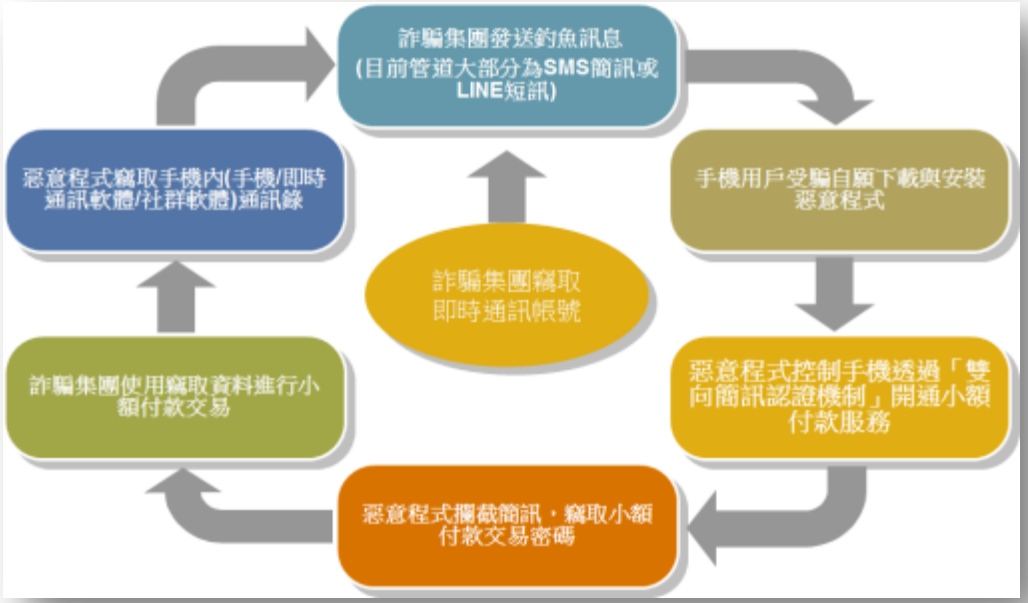
WWW：2001:288:827F:1::100（IPv6）

- http://[2001:288:827f:1::100]
- http://www.ccps.kh.edu.tw
- http://www.ipv6.ccps.kh.edu.tw

DNS: 2001:288:827F:1::1

資安案例宣導一

手機簡訊與LINE。 手機傳訊詐騙流程如下圖所示：



資料來源：[行政院國家資通安全會報]

行動裝置資通安全注意事項

- 防護建議

  1. 限制惡意程式的安裝

  設定手機不允許安裝非市集中的應用程式。

  設定手機，取消勾選「設定」內的「安全性」/「應用程式設定」中「未知的來源」。

- 2.加強LINE的安全性

(1)開啟「阻擋訊息」功能，設定LINE→其他→設定→隱私設定→勾選「阻擋訊息」，就不會收到非好友的訊息，降低收到釣魚訊息的機率。

(2)不公開個人ID，取消勾選LINE→其他→設定→個人資料→公開ID，避免被陌生人與詐騙集團加為好友

(3)沒有使用電腦版 LINE的用戶，取消勾選LINE→其他→設定→「我的帳號」中「允許自其他裝置登入」，避免駭客取得的帳密後從電腦登入。

- 3.取消電信小額付款機制

  請透過手機撥打電信業者客服，告知客服人員取消服務。
- 相關客服電話：
- 中華電信：800;
- 台灣大哥大：188;
- 遠傳電信：888;
- 亞太電信：999,
- 威寶：123。

  （目前各家電信公司已預設小額付費為取消狀態）

- 4.養成良好使用習慣

(1)使用任何通訊軟體與社群軟體，切勿使用懶人密碼。

(2)絕對不要點選傳送來的訊息裡面的連結。如果是好友送來的訊息，建議改用另外的方式(打電話、email)與對方聯絡，確定這個連結是安全、沒有問題的之後再開。

(3)不隨意提供個人資訊，也不轉知簡訊收到的密碼。

(4)需要使用小額付款的使用者，應啟用「即時消費通知」，若發現詐騙發生，請務必報警，才可當作是被詐騙證明，要求電信業者不能列入帳單或是可到臨櫃辦簽結退款。

(5)安裝手機防毒軟體。

資安案例宣導二

- 想看 iCloud被駭明星影片,請先分享到fb?! 搜尋被駭明星關鍵字,當心病毒守株待兔
- 隨著整個網路因為 iCloud 被駭導致A 咖女星私密照外流事件 而鬧得沸沸揚揚 - 超過一百位明星的照片被放上網路 - 網路罪犯利用這事件來進行社交工程（social engineering ）誘餌只是遲早的事情。所以也真的發生了，針對尋找上述外流照片使用者的特製新騙局。

不是只有 A 咖女星,才該擔心個資成公開秘密

- https://www.youtube.com/watch?v=61_ry3D_9hU

✔確定您的密碼複雜而不易猜測，並且混合使用大小寫字母、數字和標點符號。

✔切勿在多個帳號重複使用相同密碼，不然就使用一套密碼管理軟體。

歡迎免費啟用密碼管理通http://www.trendmicro.com.tw/edm/Trac...

✔用來重設密碼的安全提示問題，確定只有您自己知道答案。

您的答案不必是真的，只要是您記得住的就行。

✔隨時留意那些專門用來騙您提供使用者名稱和密碼的網路釣魚郵件。

還有，若是任何線上服務提供了額外的安全機制，例如透過手機進行雙重認證，請務必將它啟用。

✔不要再拍了！

怪客手法：

- 透過「忘記密碼？」的機制、鍵盤側錄程式、利用使用者其他已被破解的帳號密碼，或者使用暴力破解方式，來試圖進入雲端帳號以取得資料。
- 操作簡訊、信件及社群軟體fb、line出現短網址及超連結，小心木馬藏在裡面。

設定密碼常見的錯誤

髒話密碼

罵人的話也通常都在暴力破解字典的前端,使用髒話當密碼有加倍的壞處，不僅因為這是種弱密碼，而且當密碼外流時也會讓使用者丟臉。用罵老闆的話當成密碼，可能會讓你需要用LinkedIn去找另一份工作！

網站名稱關連詞

密碼跟網站有關是種糟糕的作法。從LinkedIn 案例來看，「link」、「work」、「job」、「connect」和「career」在分析裡排在常見密碼的前20位。而且如果你用七個字母的相關單字做密碼，而平均密碼長度是八個字母時，你就糟糕了

宗教聯想詞

講到密碼時，別碰宗教是件好事。像是「god」、「angel」和「jesus」是前15名的常用單字。當人們在宗教附屬網站選擇密碼時，常常會落入這一模式。

社交工程攻擊方式有哪些?應如何防範?

http://ycorpblog.tumblr.com/post/62406380438

http://blog.trendmicro.com.tw/?p=4703

社交工程（Social Engineering）係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破校園的資通安全防護，遂行其非法的存取、破壞行為。

常見的社交工程攻擊方式如下：

●利用電話佯裝資訊人員，騙取帳號及通行碼。

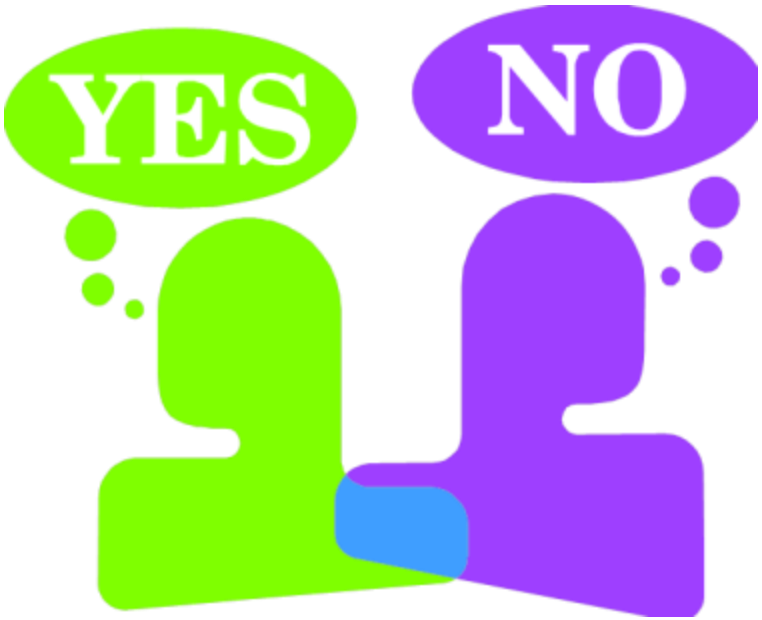
●偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。

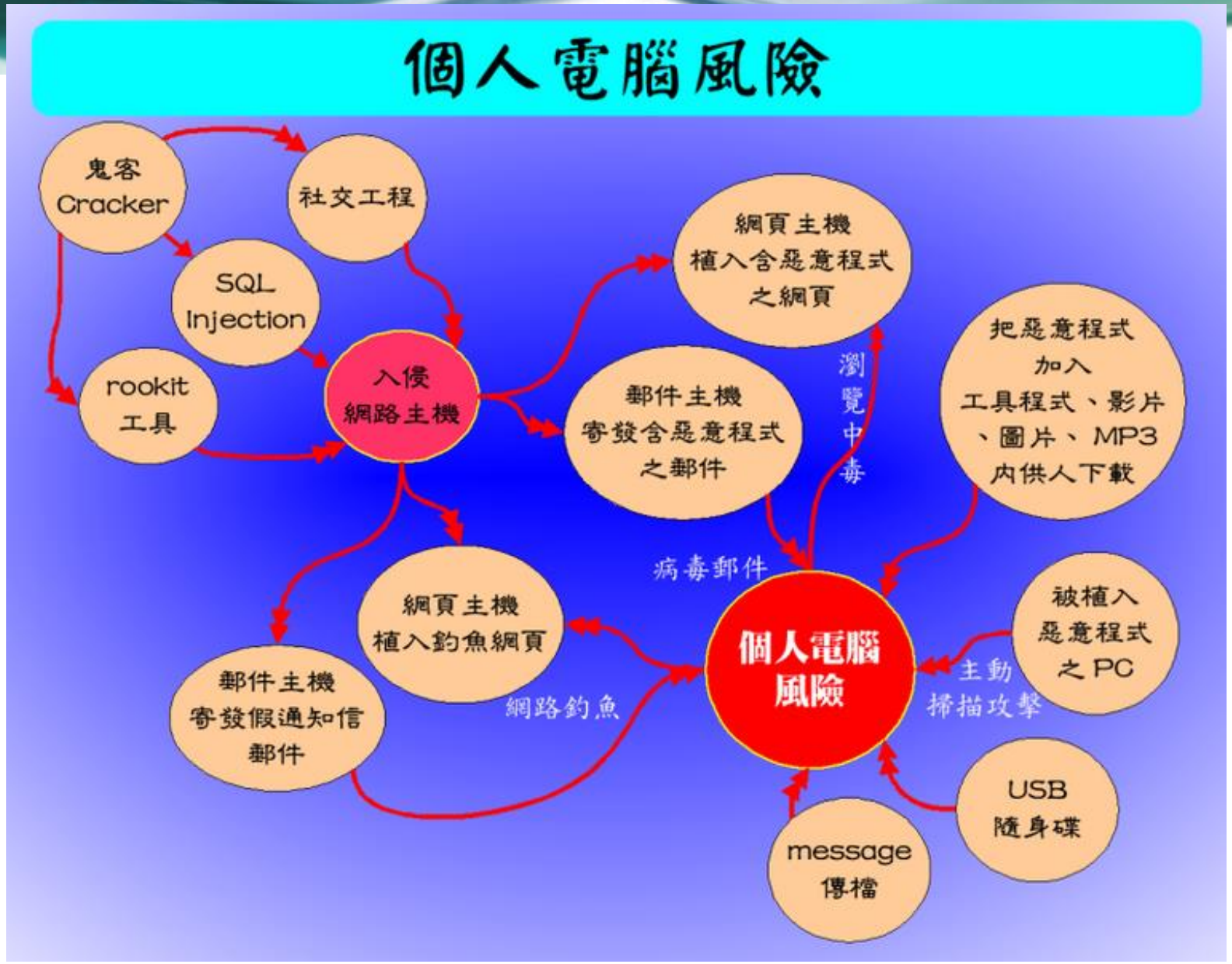
●利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。

●利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。
●利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式 、 p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。
●利用即時通訊軟體如 MSN ，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，不未經確認即提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害。

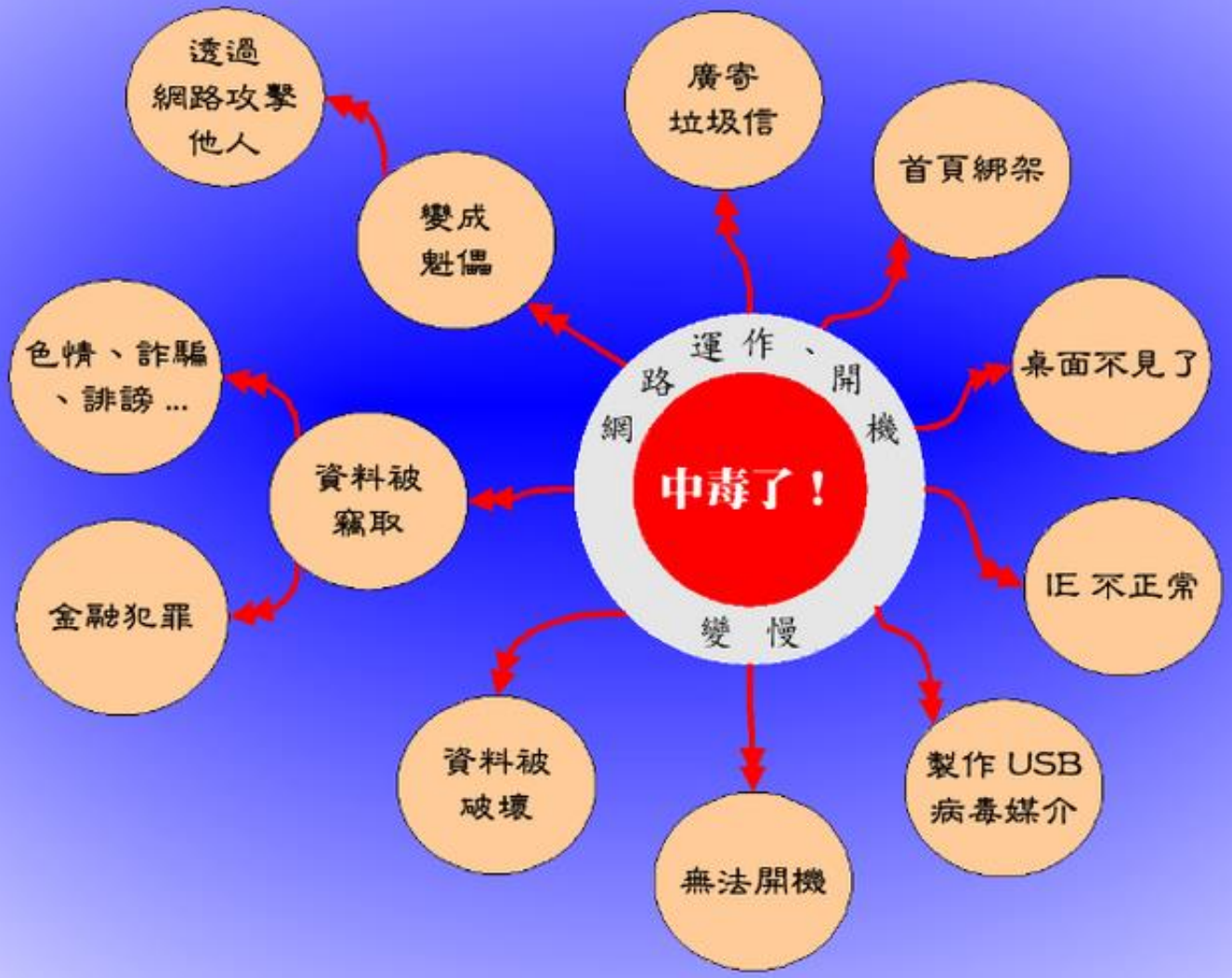
您享有資訊安全嗎?





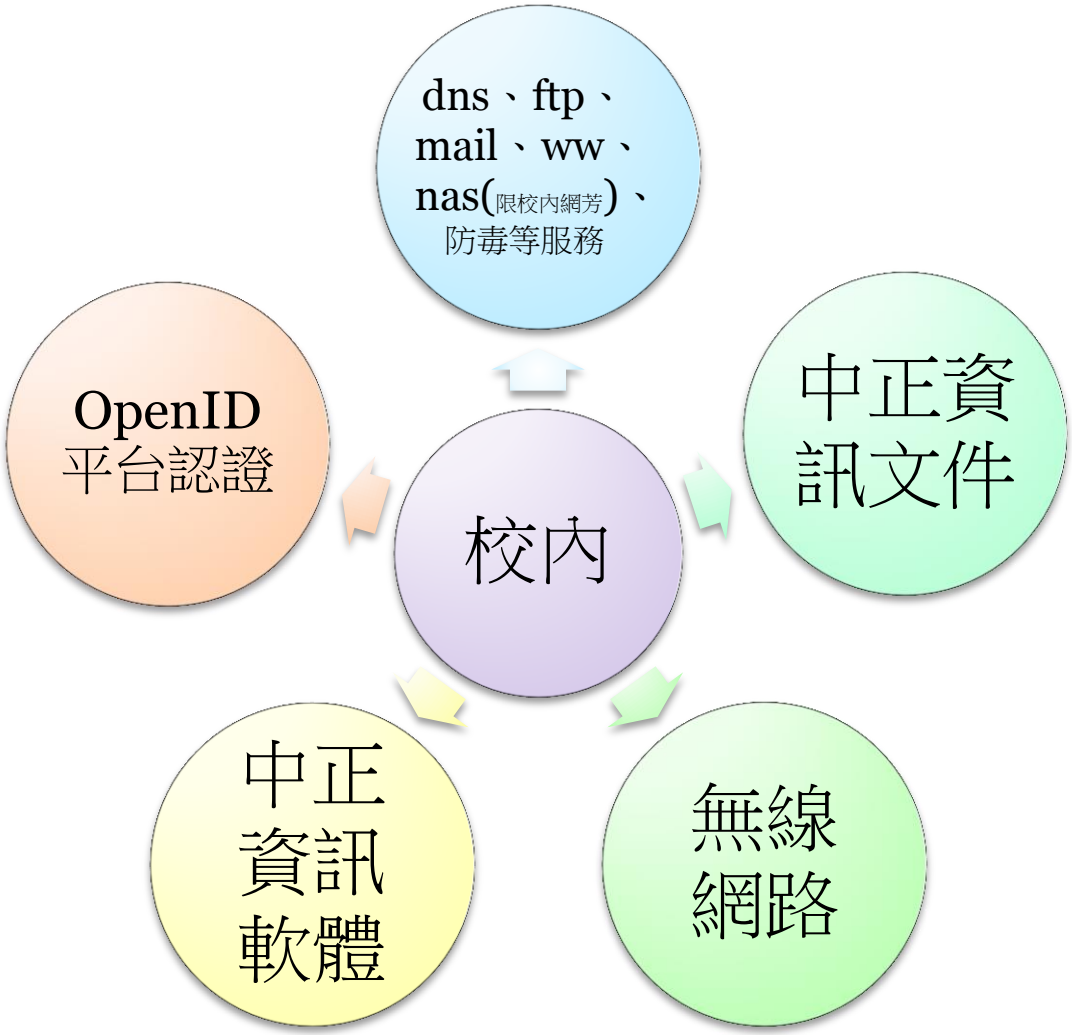
http://myip.tw/itsmw/index.php?title=%E6%AA%94%E6%A1%88:Pc_risk_800.png

淪陷後的症狀



http://myip.tw/itsmw/index.php?title=%E6%AA%94%E6%A1%88:Pc_infected_800.png

網際資源運用


dns、ftp、
mail、ww、
nas(限校內網芳)、
防毒等服務
OpenID
平台認證
中正資
訊文件
校內
中正
資訊
軟體
無線
網路

高市教無線網路

- 因應教育部加入Eduroam漫遊計畫，原有SSID:KH-guest 於1030701已改為TANetRoaming。

- KH與KH-ccps開放測試使用dove-name認證

- 各SSID流量限制如下:
- TANetRoaming：5Mbps/device
- KH：10Mbps/device
- KH-ccps：不設限
- 目的：鼓勵校內儘量使用KH-ccps，跨校儘量使用KH，而TANetRoaming留給跨區(縣市)user使用。

- iTaiwan無線網路使用原則：

- 僅開放校門口穿堂附近AP使用，校內AP不開放使用
- 增加SSID: iTaiwan • 流量限制: 1M/device
- 使用時間為下班時間：
- 上班日16:30-22:30
- 例假日08:00-22:30
- 原則：避免一般民眾進到教學區；學生無法利用iTaiwan上無線網路

教學資源運用搜出好創意

Picpick 方便好用的螢幕截圖
Everynote 不會忘記事情的大象
VoiceTube《看影片學英語》
Fillzilla 免費ftp軟體
Stellarium 模擬實際星空的虛擬天象館軟體
Daemon tools 個人虛擬光碟
EduCase 教育百寶箱，提供50G大空間
高市影音網 資訊軟體百視達
高市圖庫系統 授權創意圖庫(限校內)

教學資源運用

- 免費螢幕畫筆程 pointofix
- Google 瀏覽器+YouTube downloader(青禾動畫、YouTube)
- 雲端運算線上同步備份：Live@edu(OneDrive)、Asus WebStorage、dropbox、EduCase教育百寶箱
- 線上聽歌：千千靜聽、奇美博物館、黨客、Mear…
- 線上翻譯：dictionary.net 、靈格斯、奇摩翻譯字典…
- 線上計算機：免費的網路計算機 eCalc
- Google服務：
- Google地圖、測量距離工具應用、規劃路線、Google地球
- \\NAS2009.ccps.kh.edu.tw、校園圖庫館、中正mail、維基百科
- 智慧型手機Wifi 暨無線上網認證

- 詳見CCPS2公布欄

電腦與健康

- 正確的姿勢
- 良好的使用習慣：使用電腦30分鐘，休息10分鐘
- 勤運動保健
- 電腦節能救救北極熊！

電腦節能拯救氣候行動(Climate Savers Computing Initiative, CSCI)

建議電腦可做下列的設定：

- 螢幕/監視器休眠：15分鐘之內
- 關閉硬碟/硬碟休眠：15分鐘之內
- 系統待命/休眠：30分鐘之內

「正負2度C」的話題正紅，正在上網的你，能為地球和台灣做些什麼呢？

- 依據主計處調查國內電腦數量約有一千萬台，如果每台電腦每天少開1小時，每台每年可省40度電。也就是說每年全國可省下約4億度電(10億元)， 等於減少約25萬公噸CO2 排放。

- 「電腦節能小助理」
- 下載電腦節能小助理：(要先註冊才能下載)
- 1.單機版(http://ecolife.epa.gov.tw/powersaving/download/1)
- 2.企業版(http://ecolife.epa.gov.tw/powersaving/download/2)

相關網站

- 教師網路素養與認知網
  網址：http://eteacher.edu.tw/
- 台灣終止童妓協會web547-網路色情檢舉
  網址：http://www.web547.org.tw/
- 台北市少年輔導委員會
  網址：http://jcc.tmpd.gov.tw/
- 財團法人台灣網站分級推廣基金會
  網址：http://www.ticrf.org.tw/

政府機關（構）資訊安全責任等級分級作業施行計畫

資安等級區分方式：

1、政府機關：A、B、C、D級

2、學研機關（構）： A、B、C、D級

D級（一般）：各高中職（含）以下學校。

D級：防護縱深防火牆、防毒、郵件過濾裝置，推動ISMS觀念宣導，稽核方式自我檢視，檢測機關網站安全弱點每半年至少乙次。

資安教育訓練：

一般主管 1h、資訊人員 4h、資安人員 8h、

一般使用者 2h資安專業訓練。

1. 依個人資料保護法，禁止在校內外將教職員師生個人資料置放於伺服器供人瀏覽下載，若違反將負刑責責任。遵守個人資料保護法，避免洩漏個人資料。

2. 校內禁止使用未經授權之電腦軟體。

3. 請勿任意下載或安裝來路不明、有違反法令疑慮（如版權、智慧財產權等）或與業務無關的電腦軟體。

4. 密碼至少每三個月更換一次，密碼長度應至少8 碼。

5. 電腦設備不可任意架站或做私人營利用途。

6. 使用外來檔案應先掃毒，請勿任意移除或關閉防毒軟體。

7. 個人電腦應適時軟體更新、修補漏洞，勿自行關閉系統自動更新程式。

8. 電子郵件軟體應關閉收信預覽功能，請勿任意開啟不明來源的電子郵件。

9. 電腦可使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 10 分鐘以內，下班時應依正常程序關機。

10. 請勿隨意未設權限即開啟網路芳鄰分享目錄與檔案，並停用Guest 帳號。

11. 校內禁止使用點對點互連(P2P)軟體及 tunnel 翻牆相關工具下載或提供分享檔案。

12. 電腦內重要資料文件應定期備份，避免資料損毀。機密性敏感性檔案資料應進行實體隔離(與外部網路隔絕)。


隱私
分享

敬請指教！