資訊安全議題與
資訊融入教學研習

tksu

104.11.25

研習軟體資料請至中正mail ccpsplan下載：
ftp://163.32.193.4/!tools by tksu

全方位防毒防駭新生活

前言：

- 網路犯罪從電影看資安
- 資安案例宣導
  - 移動式裝置防毒防駭與應用
  - 認識p2p軟體
  - 社交工程攻擊
- 網路教育資源應用
- 資安檢查宣導

結語：

全方位防毒防駭新生活

影片欣賞：

2020網路危機 http://goo.gl/aDp6Pi

間諜"袋"著走!?揭發智慧型手機間諜軟體,滲透個人和企業的秘辛

https://www.youtube.com/watch?v=Ze1y1qCWB6U#t=91

APT 攻擊(Advanced Persistent Threats) 真實案例改編

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

萬物聯網的資安問題？

萬物聯網IoE(Internet of everything) & IPv6

智慧型裝置，如嬰兒監視攝影機、smart電視、無線交換器、電燈、自動駕駛、無人機、機器人…等的攻擊，將不斷持續增加。

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、平板、家電電器用品…等)

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：163.32.193.1（IPv4）

DNS：2001:288:827F:1::1(IPv6)

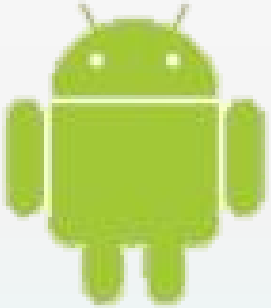
高資教DNS主機

DNS服務架構變更

Server專用DNS主機		User專用DNS主機	
dns.kh.edu.tw	163.28.136.14	uns1.kh.edu.tw	163.28.136.21
	2001:288:8201:1::14		2001:288:8201:1::21
dns1.kh.edu.tw	163.28.136.2	uns2.kh.edu.tw	163.28.136.22
	2001:288:8201:1::2		2001:288:8201:1::22
dns2.kh.edu.tw	163.28.136.10	uns3.kh.edu.tw	163.28.136.23
	2001:288:8201:1::10		2001:288:8201:1::23
ns.ks.edu.tw	163.16.1.12	uns4.kh.edu.tw	163.28.136.24
	2001:288:8401::2		2001:288:8201:1::24
dwb.ks.edu.tw	163.16.1.23		
	2001:288:8401::3		

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



木馬駭台記》 十萬手機個資遭竊--蘋果日報20151013

https://www.youtube.com/watch?v=tyfHEyduiDA

清除也嘸用！ Android手機個資恐曝光 20150525

https://www.youtube.com/watch?v=rMhwT39kqSY

賣手機時要注意個資外洩，尤其是Android系統的用戶。英國劍橋大學研究21款手機發現,使用Android的手機，即使你把手機資料刪光光，破解高手仍然可以看到你的資料，即使回復原廠設定或加密，也沒有用。

蘋果用戶小心!程式有漏洞.個資恐被看光

https://www.youtube.com/watch?v=4Wwm7ZJy4vU

蘋果迷要特別小心了！iPhone居然有資訊安全漏洞!駭客踢爆，而蘋果也承認了，iOS有系統後門，讓蘋果員工可以在用戶不知情的狀況下，獲取訊息與聯絡人資料，消息一出，讓大陸再度槓上蘋果，官方媒體呼籲黨政軍高層，不要用蘋果手機！

蘋果App Store遭入侵　幾百app中招微信有份

https://www.youtube.com/watch?v=2rh_tiypI9I

發佈日期：2015年9月22日

【蘋果報訊】過千款由中國開發的iPhone應用程式（apps）被爆有漏洞，包括WeChat（微信）、滴滴打車等多款大陸apps被惡意修改，有機會盜取用戶的個人資料，甚至操控用戶手機，涉及過億名用戶受影響。事件因部份軟件工程師經非官方渠道下載app開發軟件Xcode，未為意黑客可從中植入惡意程式。有專家建議用戶下載防毒軟件自保。

iCloud被駭 女明星私密照外洩 FBI展開調查

https://www.youtube.com/watch?v=2rh_tiypI9I

發佈日期：2014年9月2日
珍妮佛勞倫斯 撈乳開腿洩60張裸照 珍妮佛勞倫斯裸照被駭FBI調查 FBI調查名人裸照流出事件 iCloud洩美百位女星春光FBI調查 iCloud被駭 大批明星名流私密照外洩 FBI介入2014年9月2日蘋果雲端服務出包，iCloud資料庫被駭客入侵，包括奧斯卡影后珍妮佛勞倫斯在內的一百多位好萊塢明星和名流的私密照片與影片曝光，FBI已經介入。

小米回送個資到北京！ 還有多少資安漏洞

https://www.youtube.com/watch?v=2c051m6iP1Q

發佈日期：2014年8月16日

智慧型手機隱私，竟然被送到北京！儘管小米已經發聲明並且道歉，不過，又被踢爆，根本就是「假更新，真連線」，究竟是怎麼回事？而雲端網路時代，從即時通訊，到雲端儲存，消費者怎麼保護自己的隱私權不被侵犯？新聞最聚焦，我們帶您從小米機送使用者個資到北京看起，一起來關心，到底還有多少的資安漏洞。

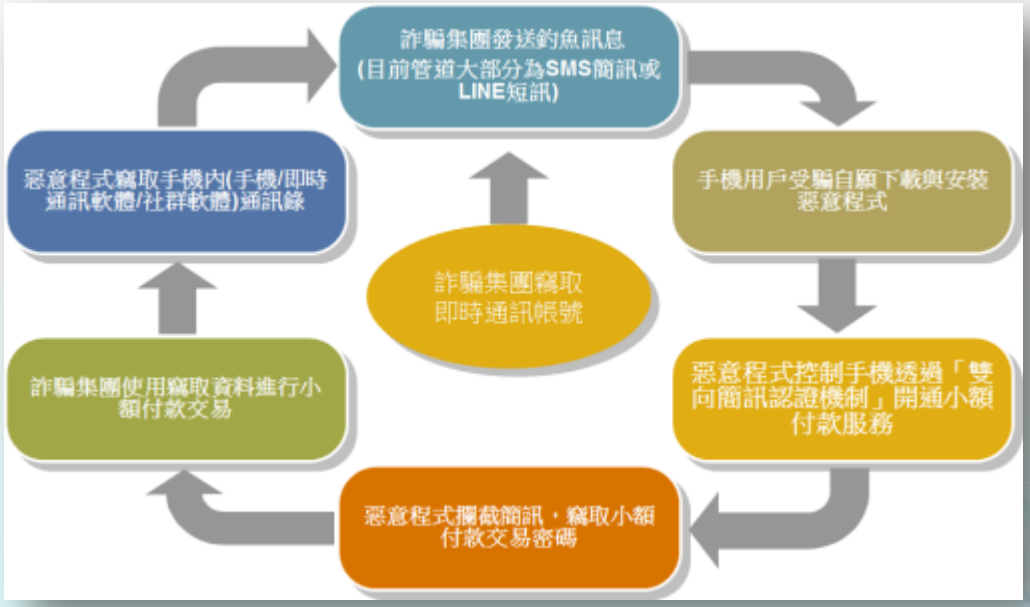
不要用？

不可能！

那就小心用！

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。

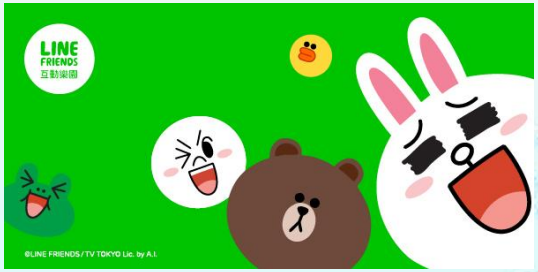
設定手機，取消勾選「設定」內的「安全性」/「應用程式設定」中「未知的來源」。

- 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.小心或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。

(2013後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。

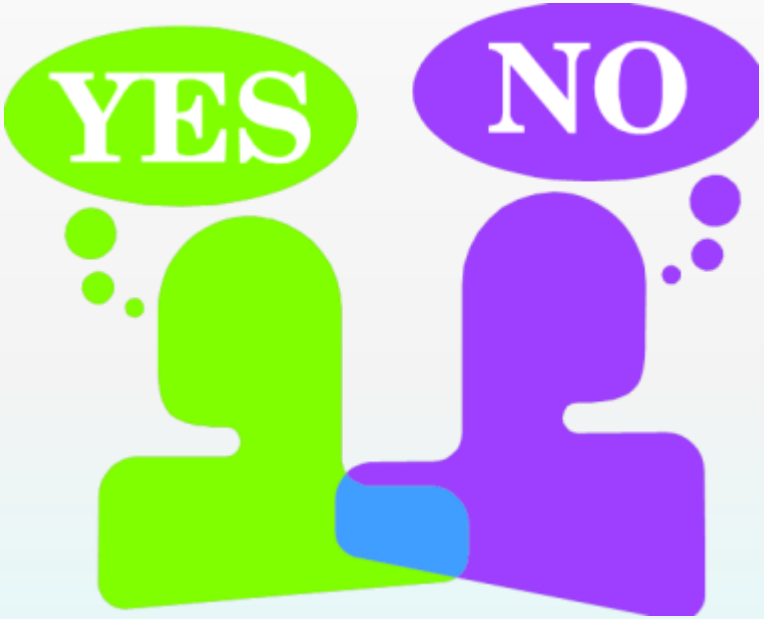
(2)絕對不要點選傳送來的訊息裡面的連結。如果是好友送來的訊息，建議改用另外的方式(打電話、email)與對方聯絡，確定這個連結是安全、沒有問題的之後再開。

(3)不隨意提供個人資訊，也不轉知簡訊收到的密碼。

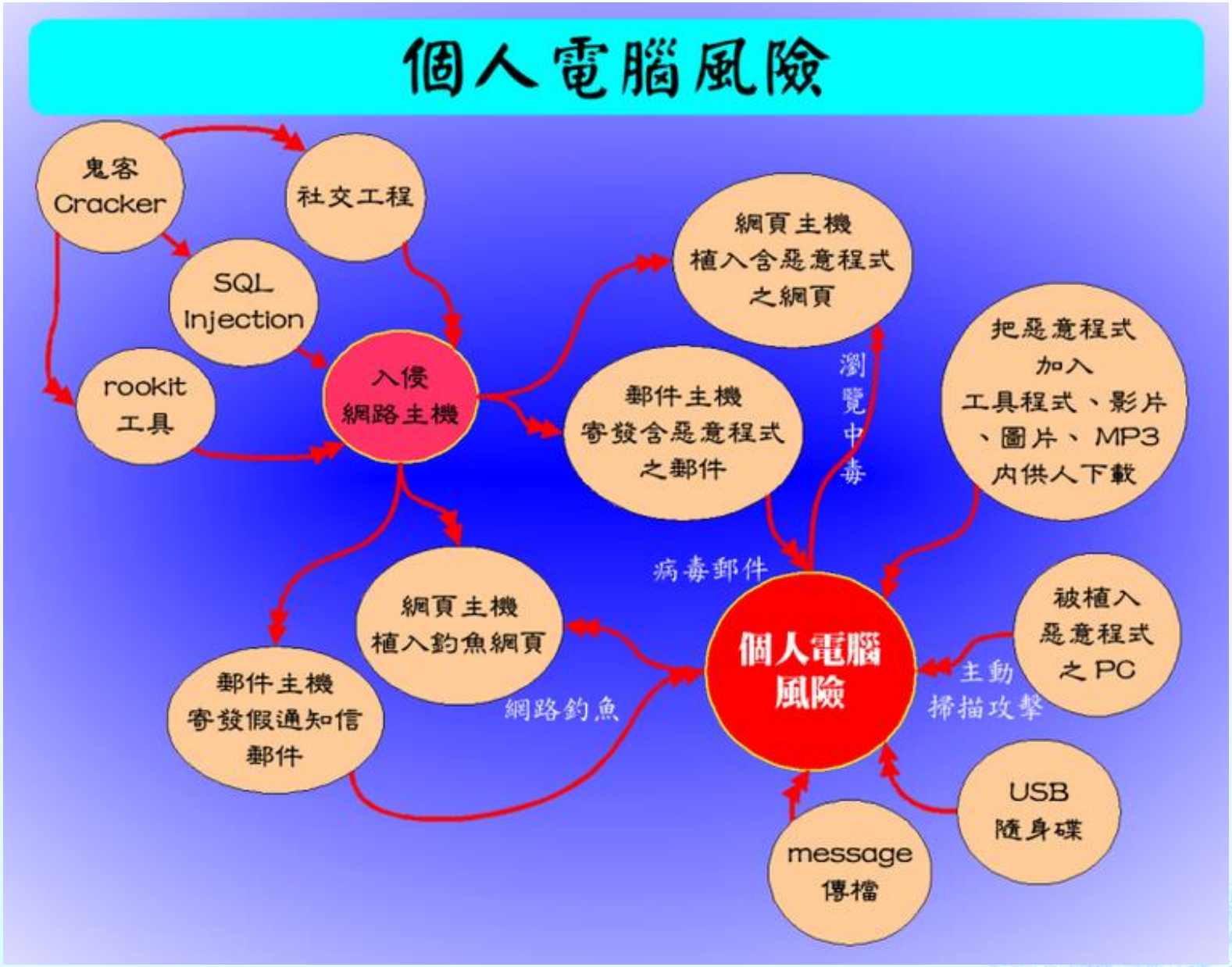
(4)需要使用小額付款的使用者，應啟用「即時消費通知」，若發現詐騙發生，請務必報警，才可當作是被詐騙證明，要求電信業者不能列入帳單或是可到臨櫃辦簽結退款。

(5)安裝手機防毒軟體。

您今天更新了嗎?



勒索病毒Crypt0L0cker



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

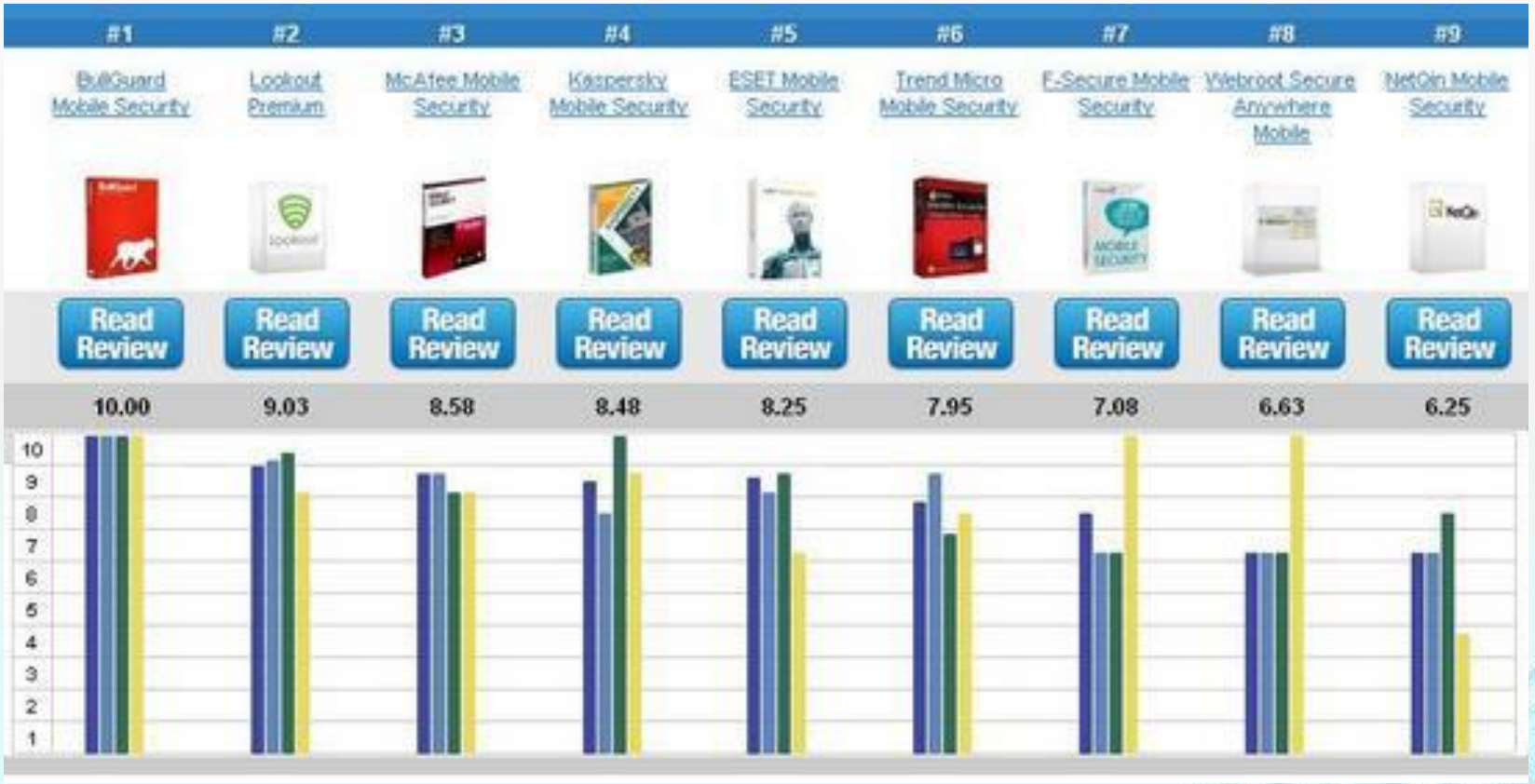
Compare Antivirus Software 2015

Rank	1st Place	2nd Place	3rd Place	4th Place	5th Place	6th Place	7th Place	8th Place	9th Place	10th Place
Score	96%	92%	91%	85%	84%	83%	83%	80%	75%	72%
Overall Protection	Best Overall Antivirus Software of 2015									
Antivirus Software (All Software Available for Instant Download)	VIPRE Antivirus	ESET Antivirus	Bitdefender Antivirus	Kaspersky Anti-Virus	AVG Anti-Virus	avast Antivirus	Avira Antivirus	Norton Antivirus	Trend Micro Antivirus	Panda Antivirus
	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now	Read More / Buy Now
Price	~~$39.99~~	$39.99	~~$39.95~~	$39.95	~~$39.99~~	~~$39.99~~	$44.99	$49.99	$39.95	~~$39.99~~
Discount Price	$29.99	No discount available	$31.96	No discount available	$31.99	$34.99	No discount available	No discount available	No discount available	$31.99
Screenshots										
Real-time Antivirus	Excellent	Excellent	Excellent	Excellent	Excellent	Very Good	Very Good	Excellent	Good	Good
Manual Virus Scanning	Excellent	Good	Excellent	Excellent	Very Good	Very Good	Good	Excellent	Excellent	Good
Virus Removal	Excellent	Very Good	Excellent	Excellent	Excellent	Very Good	Average	Excellent	Very Good	Good
USB Virus Scanning	Excellent	Excellent	Excellent	Excellent	Average	Poor	Average	Average	Poor	Average
Anti-Spyware	Very Good	Excellent	Very Good	Very Good	Good	Good	Good	Good	Very Good	Very Good
Installation	Excellent	Excellent	Very Good	Very Good	Very Good	Very Good	Good	Excellent	Average	Average
Resource Usage	Excellent	Very Good	Excellent	Good	Good	Excellent	Very Good	Very Good	Excellent	Good
User Interface	Excellent	Very Good	Excellent	Very Good	Very Good	Very Good	Very Good	Good	Average	Average
Tech Support	Excellent	Excellent	Good	Average	Average	Poor	Excellent	Average	Average	Poor

- 第一名：VIPRE Antivirus
- 第二名：ESET Antivirus
- 第三名：Bitdefender AntiVirus(下載 Bitdefender 免費版)
- 第四名：Kaspersky Anti-Virus
- 第五名：AVG Anti-Virus(下載 AVG 免費版)
- 第六名：Avast AntiVirus(下載 AVAST 免費版)
- 第七名：Avira Antivirus (下載小紅傘免費版)
- 第八名：Norton Antivirus
- 第九名：Trend Micro Antivirus
- 第十名：Panda Antivirus (下載 Panda 免費版)

- 資料來源：PC Antivirus reviews

2014手機防毒排名


#1
BullGuard Mobile Security
Read Review
10.00
#2
Lookout Premium
Read Review
9.03
#3
McAfee Mobile Security
Read Review
8.58
#4
Kaspersky Mobile Security
Read Review
8.48
#5
ESET Mobile Security
Read Review
8.25
#6
Trend Micro Mobile Security
Read Review
7.95
#7
F-Secure Mobile Security
Read Review
7.08
#8
Webroot Secure Anywhere Mobile
Read Review
6.63
#9
NetQin Mobile Security
Read Review
6.25
10
9
8
7
6
5
4
3
2
1

手機免費防毒防駭

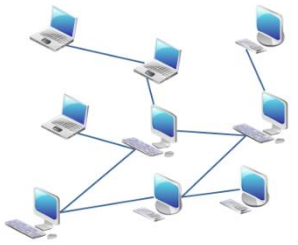
Lookout 手機安全（防毒，防盜，定位）

avast! 手機安全軟體

CM Security 免費防毒、App鎖、輸錯密碼自動拍照

資安案例宣導二-P2P軟體是什麼？

- P2P 為 Peer-to-Peer的簡寫，意思就是參與其中的所有角色皆是平等互惠的，而非傳統主從式架構。
- 在傳統架構中必須要有人扮演服務提供者，負責架設 HTTP 或 FTP 伺服器提供檔案下載；但在 P2P 架構中則由所有的使用者直接互相分享，各有所得、各取所需。



一、 P2P軟體說明

- Peer to Peer(點對點通訊傳輸工具)
- 傳統HTTP/FTP傳送檔案方式，採用戶與主機的通訊模式(Client-Server Mode)
- 新制P2P檔案傳送，採取用戶與用戶的通訊模式，可以同時連接多個下載點，分散式下載檔案。
- P2P可以快速完成檔案下載的目標。

一、 P2P軟體說明

- 檔案分享是目前 P2P 最主要的一種應用，P2P 檔案分享軟體本身是合法的，合不合法 則是在分享的檔案。
- 目前美國的八大影片公司、台灣的 BSA 商業軟體聯盟、 台灣的IFPI 國際唱片業交流基金會等機構對其 所屬成員的著作權很重視， 而且警方也配合加強取締 ，故請勿下載 非法檔案以免官司上身。

P2P社群

早期主流的 P2P 社群可概分為三大類：

第一類是 BitTorrent(BT)，較具代表性的軟體有BitComet、比特精靈等。

第二類是 eDonkey2000，以 emule 軟體為主流。

第三類則是偏重 MP3 音樂下載，例如 ezPeer 與 Foxy。

二、常見的P2P軟體種類

BitTorrent系列(BT)
BitComet、 BitLord 、BitSpirit比特精靈、BitTorrent、clubbox 、 uTorren、Vuze箭毒藍蛙…

eDonkey系列：eDonkey、eMule…

Gnutella系列： ezPeer、Foxy 、Gnutella、 Mxie…

FastTrack系列：FastTrack、 KaZaA…

WinMx系列：WinMx、 Winny、 NapMx…

其他：
1kxun千尋影視、Ares Galaxy、Azureus、BearShare、Blubste、DC (Direct Connect)、exeem lite、Fileguri/Freechal、Fpsetup、Gnucleus、Grokster、Groove Virtual Office、Hamachi、iMesh、kkbox、Kuro、LimeWirer、Lphant、Morpheus、Mutella、OpenLITO、PeerEnabler、Phex、Piolet、愛奇藝PPS影音、 Pruna、RockItNet、Shareaza、Soribada、SoulSeek、Swapper、Thunder、xfplay影音先鋒、XoloX等。

P2P軟體可能影響的網路安全問題

2007年4月23日，CA公司發表資安警訊，指出Foxy、BitComet、eDonkey、µTorrent、Ares、Azureus、BearShare、Lphant、Shareaza、Hamachi、exeem lite、Fpsetup、Morpheus、iMesh等14個P2P軟體都存在安全威脅，這些P2P軟體的潛在威脅來源包括可能會覆寫檔案、為檔案重新命名、刪除檔案、被第三方植入惡意程式等。

為什麼會有那麼多P2P軟體？

P2P 的實作方式各家廠商皆有所不同，彼此相互競爭，因而造就了許多不同的 P2P 網路（或稱 P2P 社群）。而不同的 P2P 社群往往只允許使用者以特定軟體參與其中，便因此誕生了許多不同的 P2P 軟體。

為什麼使用 BT 下載檔案的時候網路會變得很慢？

- 因為當您在使用 BT 下載檔案時，您也同時在上傳檔案，若您的上傳頻寬被 BT 完全佔用，整個網路速度就會變得非常的慢。您可以至各 ISP 的連線速率測試網站進行測試，以瞭解自己的連線速率為何。
- 一般而言，若只是單純的上網瀏覽網頁，那麼只要將 BT 的最大上傳頻寬設定為你的線路最大上傳頻寬的一半即可；但若您有在玩線上遊戲的話可能需要再調低一些。

P2P軟體影響的網路安全問題

許多P2P網路一直受到懷有各種目的的人的持續攻擊。

例子包括：

- 中毒攻擊（提供內容與描述不同的檔案）
- 拒絕服務攻擊（使網路執行非常慢甚至完全崩潰）
- 背叛攻擊（吸血）（使用者或軟體使用網路卻沒有貢獻出自己的資源）
- 在資料中插入病毒（如下載或傳遞的檔案可能被感染了病毒或木馬）
- P2P軟體本身的木馬（如軟體可能含有間諜軟體）
- 過濾（網路業者可能會試圖禁止傳遞來自P2P網路上的資料）
- 身分攻擊（如，跟蹤網路上使用者並且進行不斷騷擾式的或者是用合法性地攻擊他們）
- 垃圾資訊（如在網路上傳送未請求的資訊，不一定是拒絕服務攻擊）

個人使用P2P軟體的網路安全問題

1. P2P工具包，可能被惡意人員放置木馬後門程式，與病毒蠕蟲。

2. P2P軟體本身的漏洞，造成駭客入侵。

3. 使用P2P軟體，誤將本機目錄開放共享。

4. 使用P2P軟體下載影音檔案，多半為mp3、mpeg與avi等檔案，可能造成侵權行為。

P2P軟體資安應對策略

1. 下載任何工具軟體，從原廠官方網站取得。

2. 不要在公眾或公務電腦下載P2P軟體或檔案。

3. 使用P2P工具，要縮短暴露在網際網路的時間。

4. 使用任何網路工具(包含P2P檔案下載工具)，不應侵害他人權益，入侵他人電腦或是侵害著作權。

5. P2P技術是技術潮流，不是反對P2P發展，而是『反對在辦公室與校園，使用P2P檔案下載』。

參考資料

P2P軟體對網路安全的威脅講義

資安案例宣導

- 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！

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。

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。

網際資源運用


dns、ftp、mail、ww、nas(限校內網芳)、防毒等服務
OpenID認證暨教育資源
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

AdwCleaner 移除廣告軟體、解除首頁被綁架
Daemon tools 個人虛擬光碟
EduCase 教育百寶箱，提供教師1TB大空間
Everynote 不會忘記事情的大象
Fillzilla 免費ftp軟體
Mobizen 手機與電腦雙向同步程式
Picpick 方便好用的螢幕截圖
Stellarium 模擬實際星空的虛擬天象館軟體
VoiceTube 《看影片學英語》
天下雜誌群資料庫 天下雜誌影音、康健雜誌
奇美古典樂 奇美博物館古典音樂
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)
維基百科 人人可編輯的自由百科全書

電腦節能與健康

- 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)

建議電腦電源管理可做下列的設定：

- 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)

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：

政府機關：A、B、C級

學術機構：A、B、C級

C級：(1)各學院、專科學校及高級中等以下學校。

國（公）營事業、醫療機構及其他

C級：(1)各學院、專科學校及高級中等以下學校

C級作業名稱：

防護縱深-防毒、防火牆、郵件過濾裝置。

ISMS推動作業：自行成立推動小組規劃作業。

稽核方式：依主管機關規定。

資安教育訓練：

1. 依各主管機關規定資安人員(資訊人員)資安專業課程訓練或資安職能訓練要求
2. 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

資安宣導：

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。
（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)。


Thank You!