瞭解病毒，就不用怕病毒
使用電腦網路的防護基礎

By
Diamond Liu
(劉潯明、劉得民)

Malware vs. Anti-Malware

My first wish is to see this plague of mankind, war, banished from the earth.

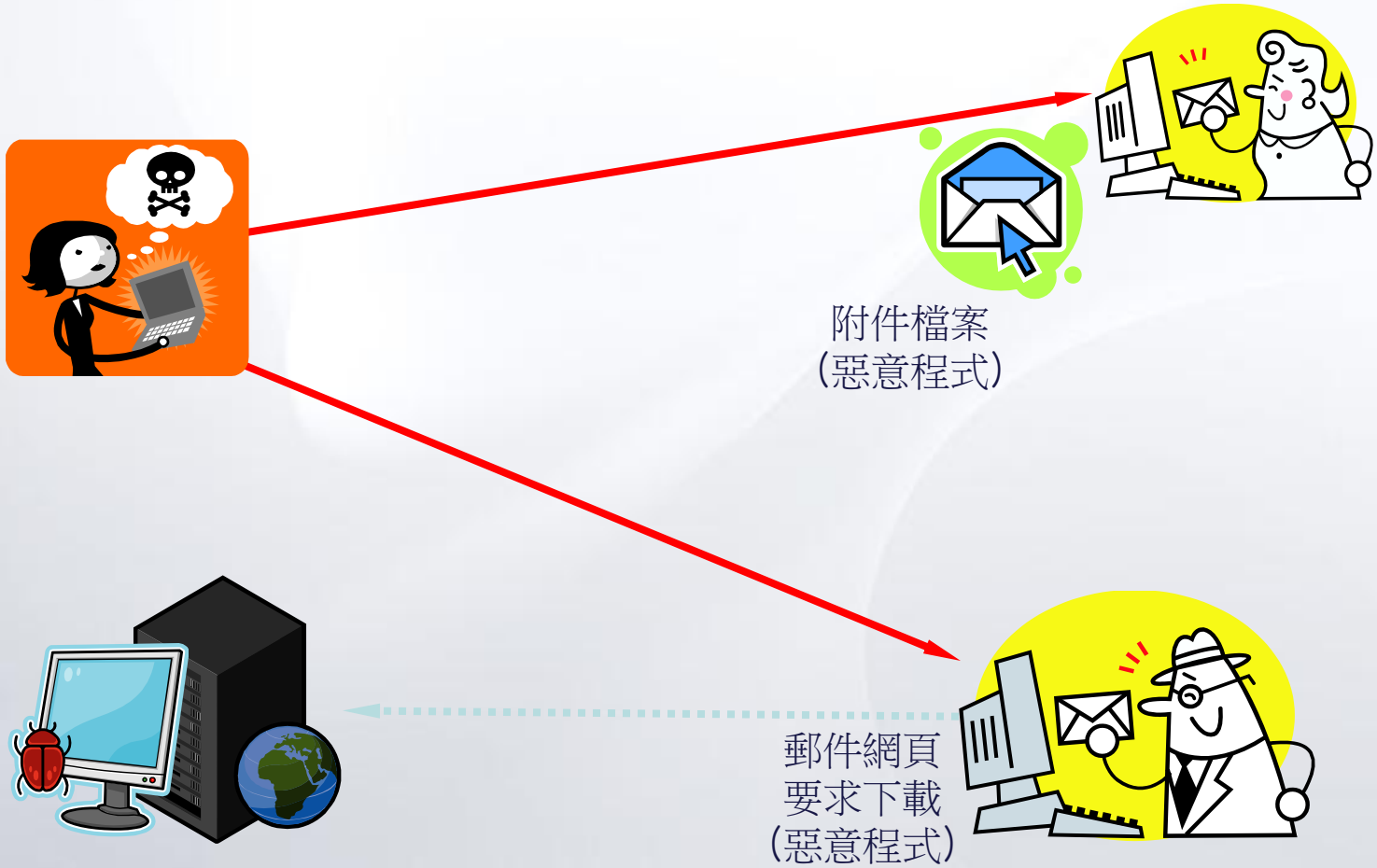
George Washington, 1st US President

瞭解病毒，就不用怕病毒

- 感染病毒木馬的三大途徑
- 親友電郵遭駭 真實案例
- USB隨身碟病毒的感染與防護
- 電子郵件病毒的感染與防護
- 即時通病毒的感染與防護
- Facebook的隱藏憂慮
- 家庭電腦 與公務電腦 的隔離措施
- 個人資料保護法
- 網路安全的三不政策與資安五要
- Q&A

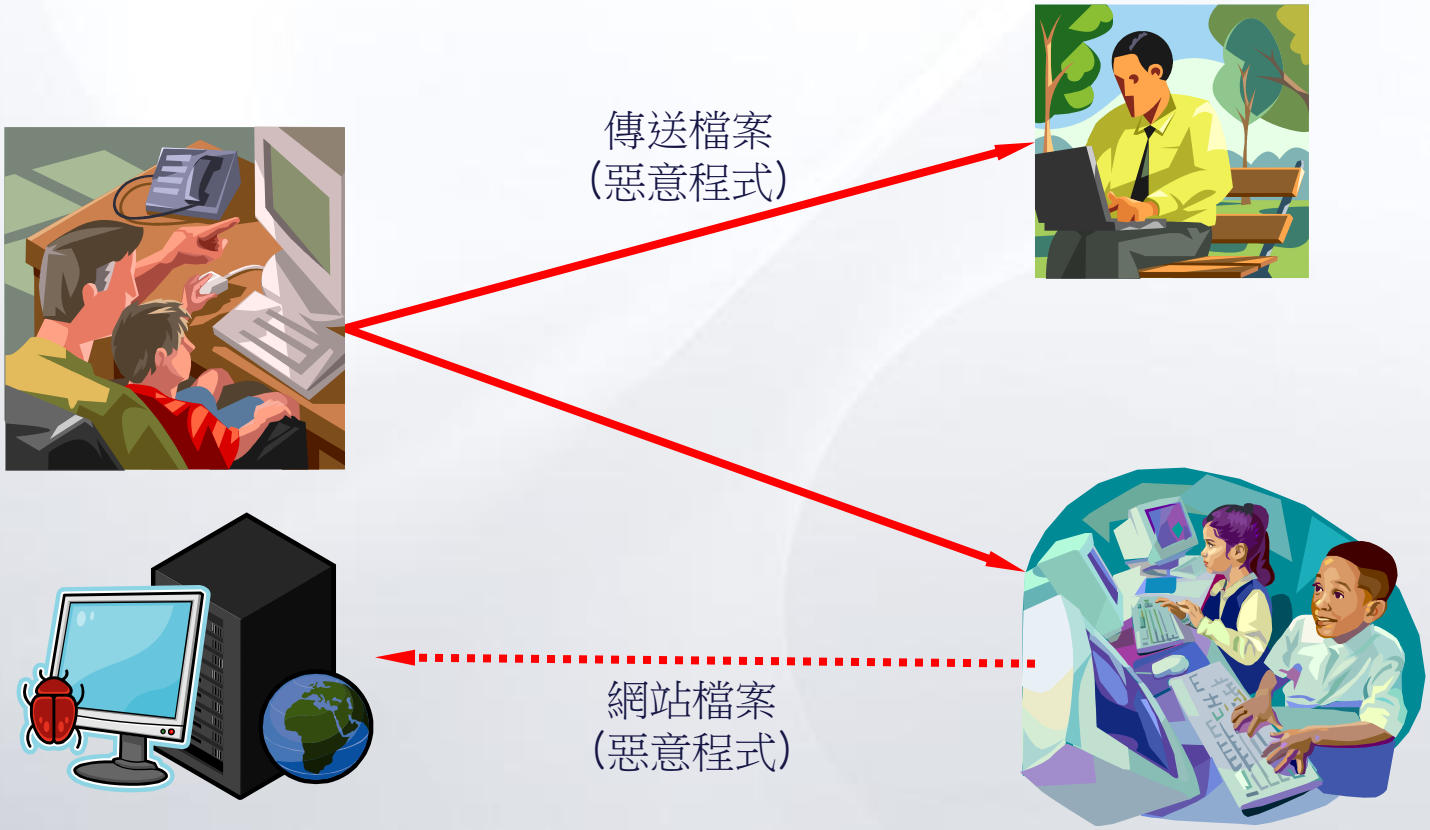
感染病毒木馬的三大途徑之1

1. 透過電子郵件傳送感染
   - 附件檔案　包含病毒木馬檔案
   - 郵件網頁　要求下載安裝檔案



感染病毒木馬的三大途徑之2

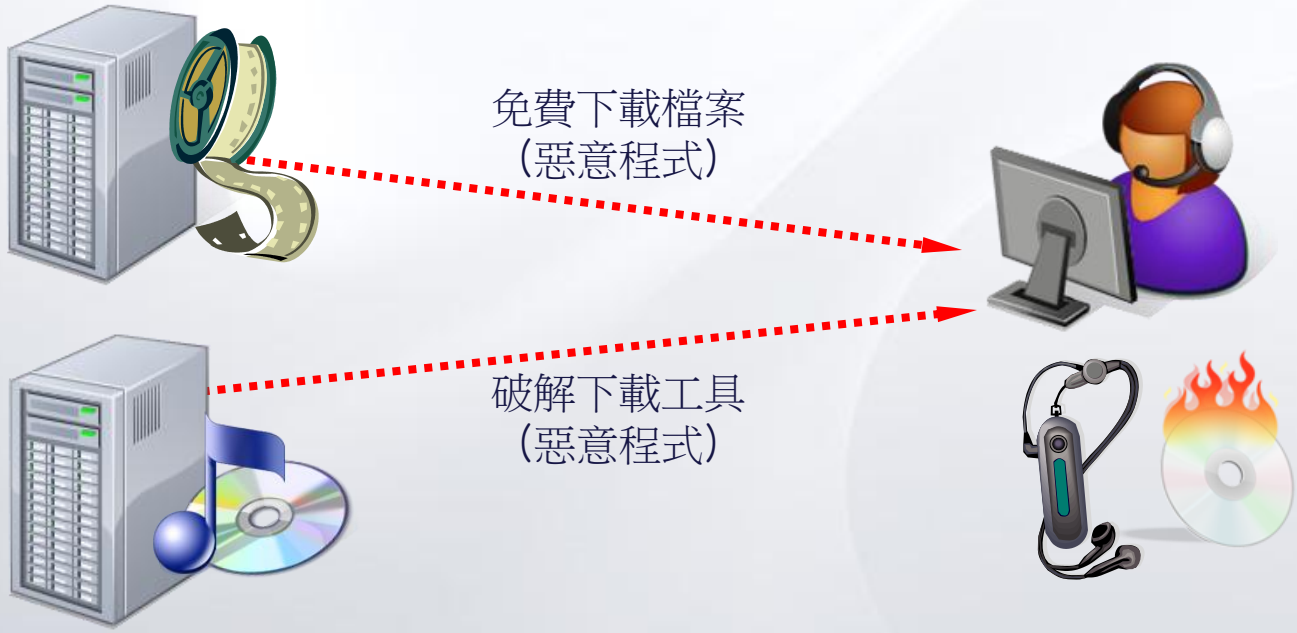
2. 即時通 與 網頁瀏覽
   - 點選網頁超連結　要求下載安裝惡意檔案
   - 即時通用戶傳送病毒檔案　（已經不多見，烤雞病毒）



感染病毒木馬的三大途徑之3

3. 下載軟體
   - 免費工具，盜版軟體
   - 好玩遊戲，可愛圖案，螢幕保護程式

註: USB 隨身碟與USB拇指碟 （它們只是傳播媒介，類似蒼蠅與蚊蟲，不是真正病毒來源）



親友電郵遭駭　真實案例

假冒指導教授發出電郵
大學講師匯款被騙

某大學講師接到以前指導教授的求助電子郵件，內容為老師在國外需要金錢幫助。該名講師隨即按照指示匯了2,800美金到英國，事後才得知老師在國內。

被冒名的教授，曾接到冒充信箱管理員確認帳號的電子郵件，填了相關資料之後不僅資料外洩，電子信箱也一整天都無法使用。

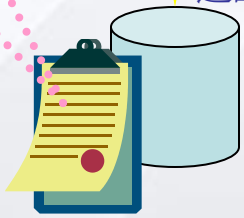
歹徒經由釣魚手法取得這名教授的通訊錄之後，假冒名義向學生發出借錢e-mail，詐騙得逞。

用戶端
被植入
惡意程式

駭客

竊取
電郵
通訊錄

向親友散佈
虛假訊息



電郵詐騙匯款

親友電郵遭駭　真實案例

假藉Facebook名義 入侵電腦

熱門的社群交友機制,Facebook, 許多人都有在其中種菜養魚的經驗，最近有電子郵件假借Facebook帳號通知的名義，該電郵信件內容(中英文皆有)：為了確保帳號安全，要求用戶重新設定Facebook帳號。

若是使用者若想要知道其重新設定的帳號，就必須先開啟郵件中的附件檔案，來誘使Facebook使用者開啟郵件中夾帶檔案。而實際上這個附件檔中隱藏了一個名為「Trojan Bredolab」的木馬程式。


The Facebook Team
To:
Facebook_Password_7a343.zip (23.8 KB)
Facebook Password Reset Confirmation.
Hey ,
Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.
Thanks,
The Facebook Team
The message comes with a .zip file containing a malici
as Trojan.Bredolab.
This variant of Bredolab connects to a Russian domain and the infect
botnet.

親友電郵遭駭　真實案例

假藉Facebook名義 入侵電腦

熱門的社群交友
菜養魚的經驗，最
知的名義，該電
帳號安全，要求用

若是使用者若想要
開啟郵件中的附件
郵件中夾帶檔案。
名為「Trojan Br

The Facebook Team
To:
Facebook_Password_7a343.zip (23.8 KB)

Facebook Password Reset Confirmation.

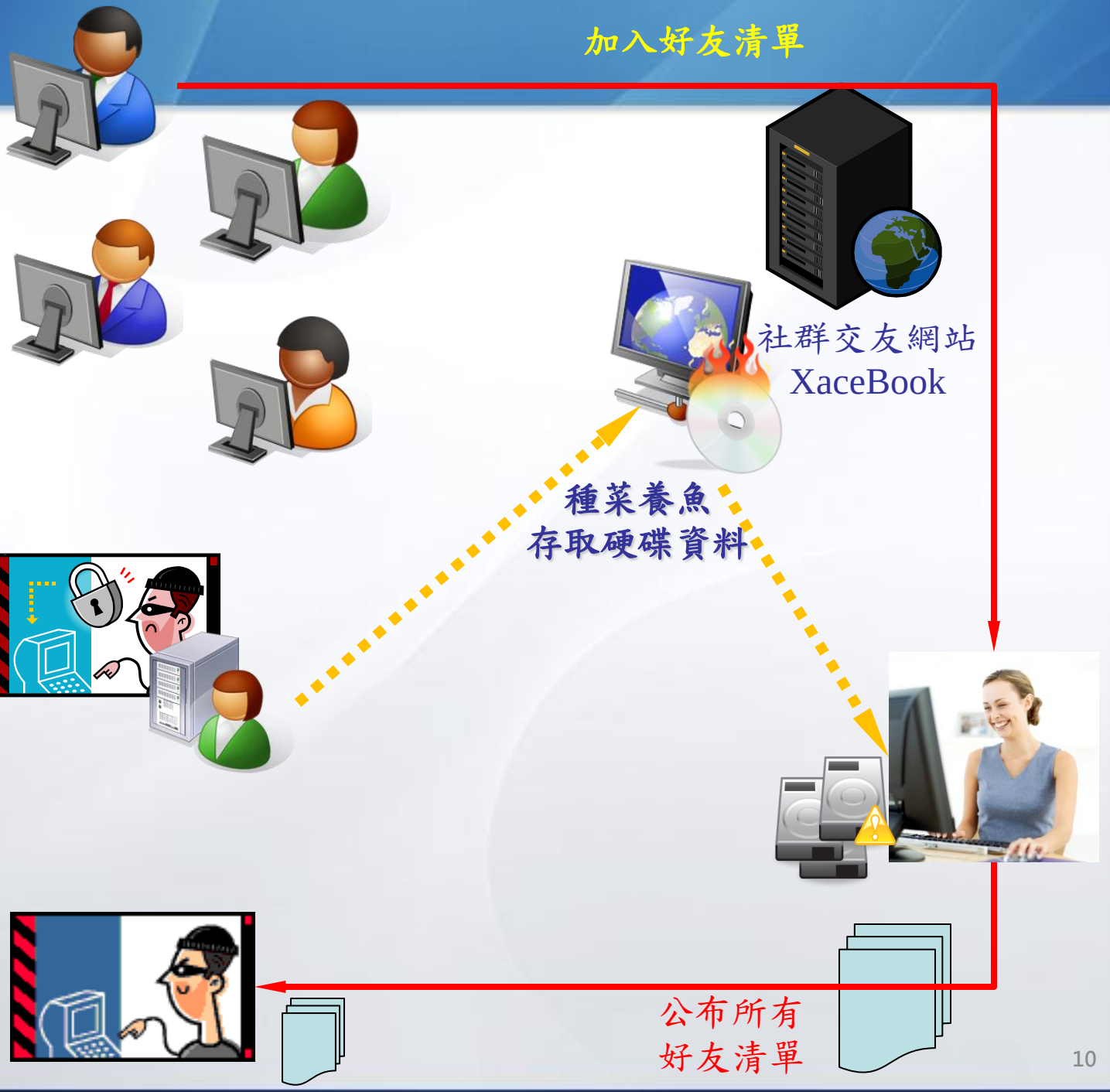
Hey .

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

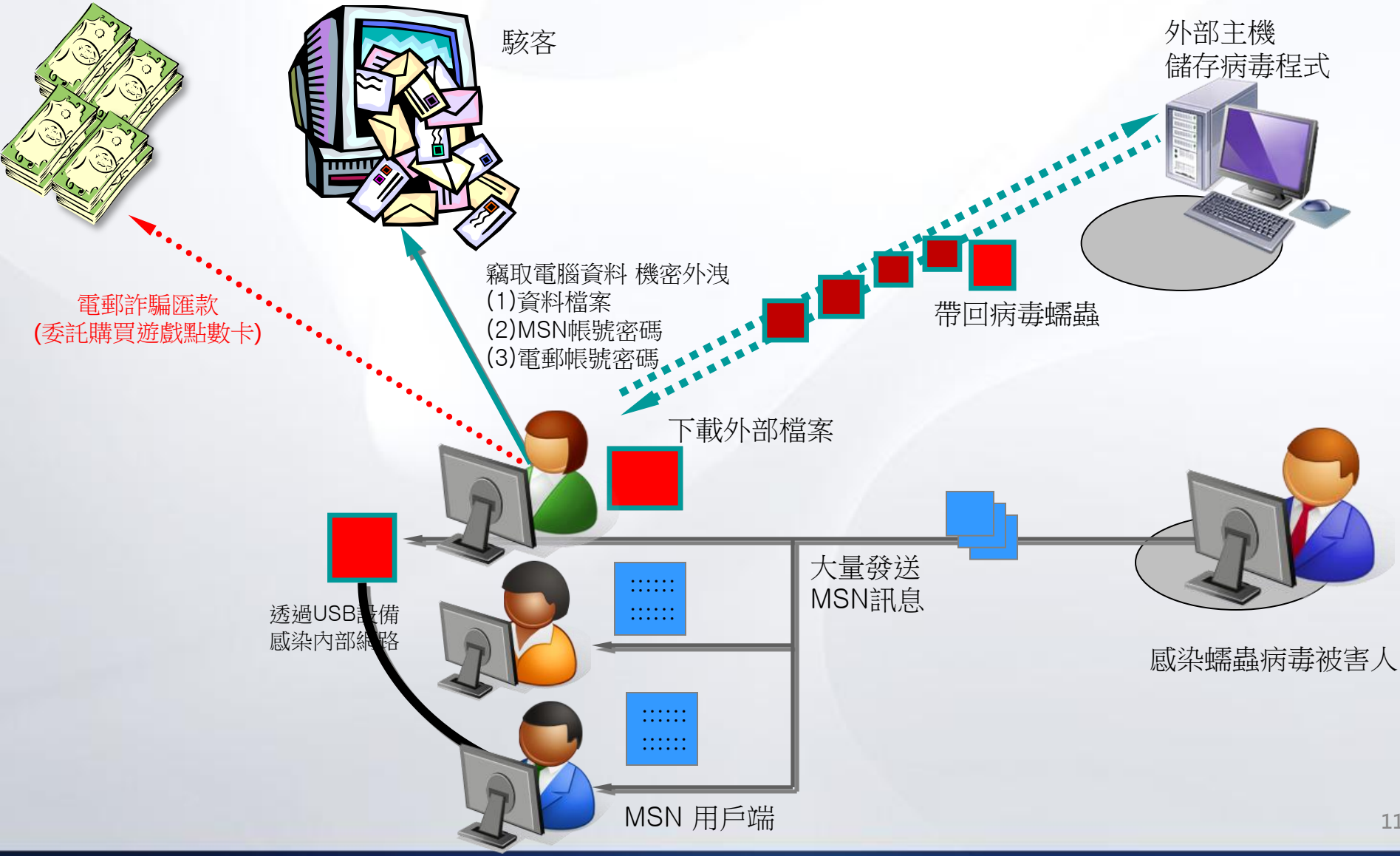
Thanks,
The Facebook Team

The message comes with a .zip file containing a malici
as Trojan.Bredolab.

This variant of Bredolab connects to a Russian domain and the infect
botnet.


加入好友清單
社群交友網站
XaceBook
種菜養魚
存取硬碟資料
公布所有
好友清單

即時通病毒蠕蟲 詐騙親友匯款




我的電子郵件收件匣(B)
傳送立即訊息(E)...
我的狀態(M)
登入(S)
用以下身分登入(I)...
登出(N)
開啓(O)
Windows Messenger - 未登入
我的文件
下午 12:31

異常的即時通操作畫面

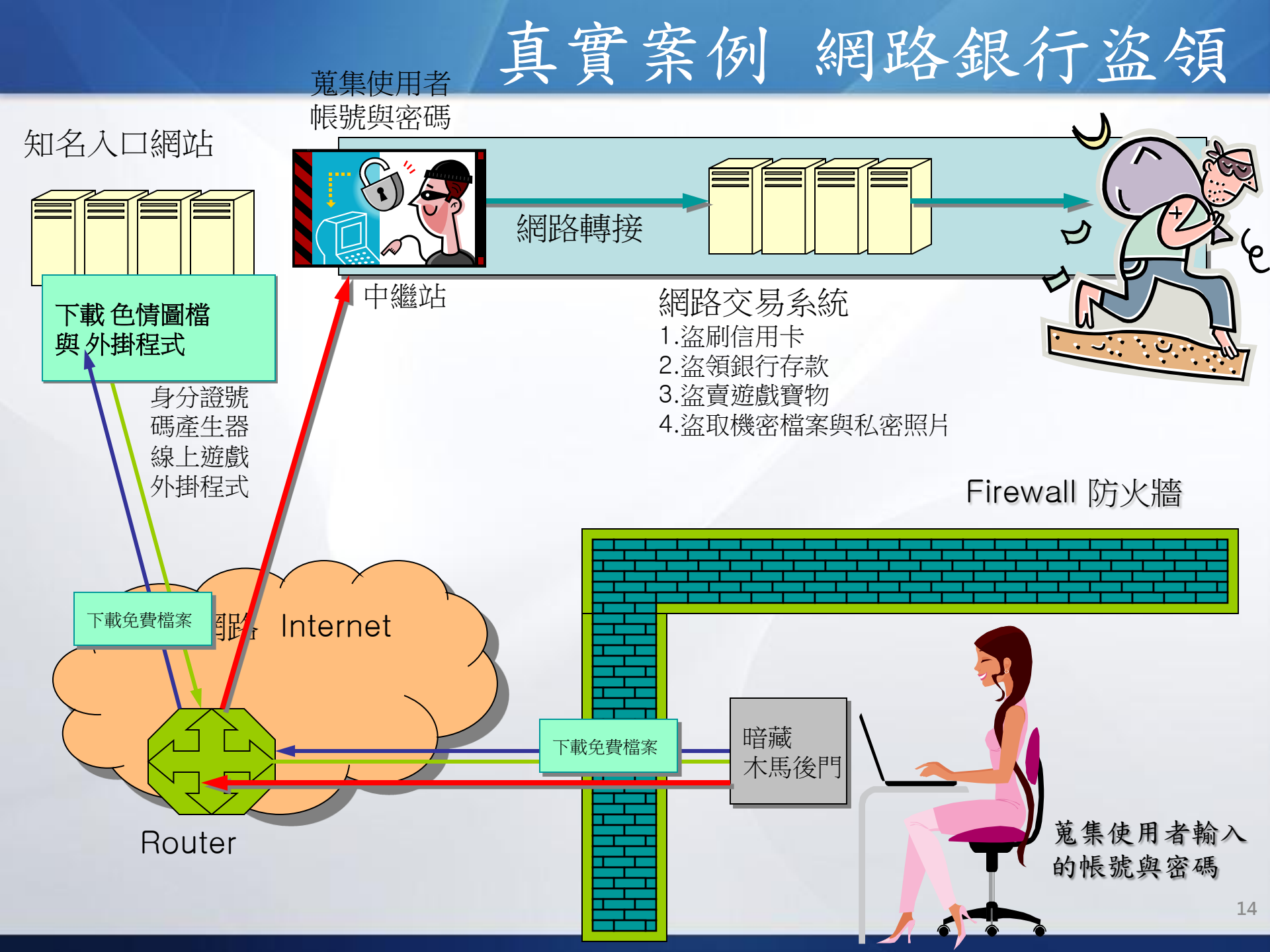
常見即時通的3種駭客社交工程方式

(1)對話當中，對方傳送URL網址

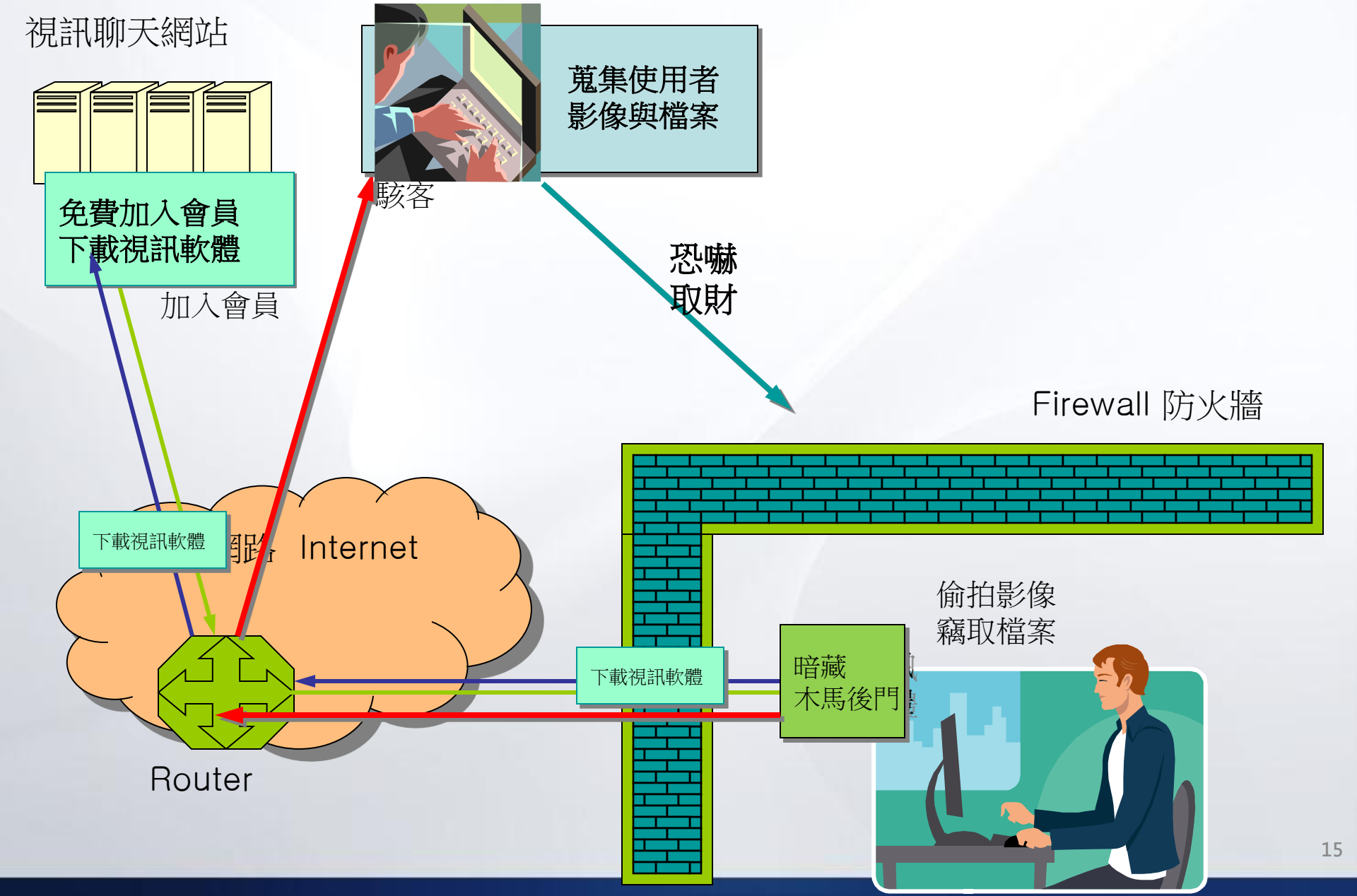
(2)陌生人邀請我們加入好友清單

(3)對方請我們幫忙買遊戲點數卡

真實案例 網路銀行盜領


蒐集使用者
帳號與密碼
知名入口網站
網路轉接
中繼站
網路交易系統
1.盜刷信用卡
2.盜領銀行存款
3.盜賣遊戲寶物
4.盜取機密檔案與私密照片
下載 色情圖檔
與 外掛程式
身分證號
碼產生器
線上遊戲
外掛程式
Firewall 防火牆
下載免費檔案
Internet
下載免費檔案
暗藏
木馬後門
Router
蒐集使用者輸入
的帳號與密碼

真實案例　影音聊天 視訊偷拍



免費聊天

一對多視訊

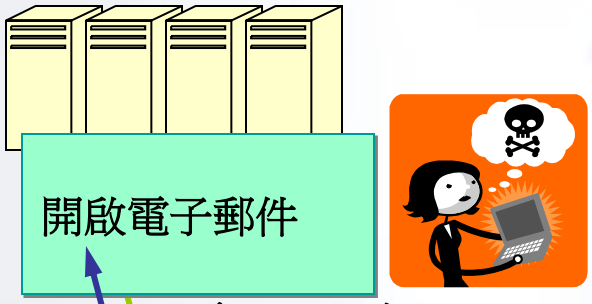
色情網站
暗藏木馬後門!!
個人資料影像
被悄悄偷拍!!

下載視訊軟體

暗藏
木馬後門

偷拍影像
竊取檔案

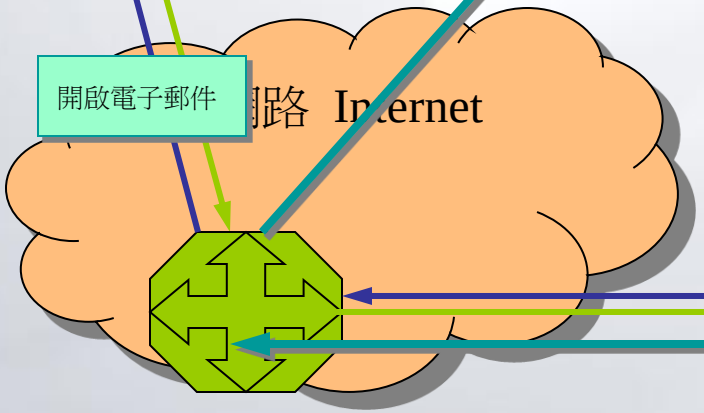
網路駭客 真實案例

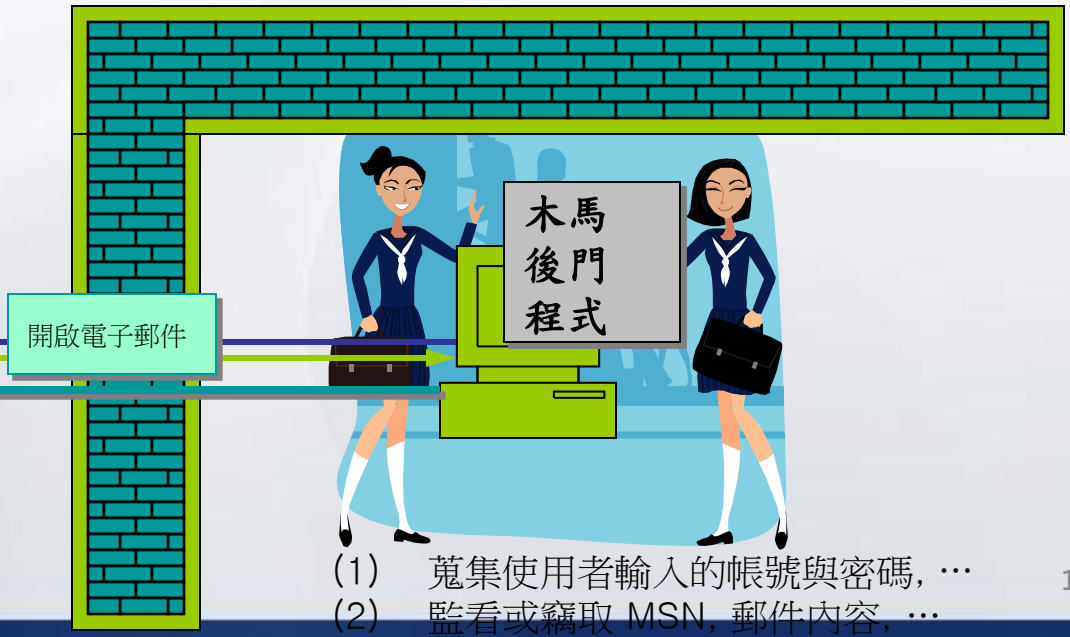



網路駭客


現任男友
或是
“故男友”

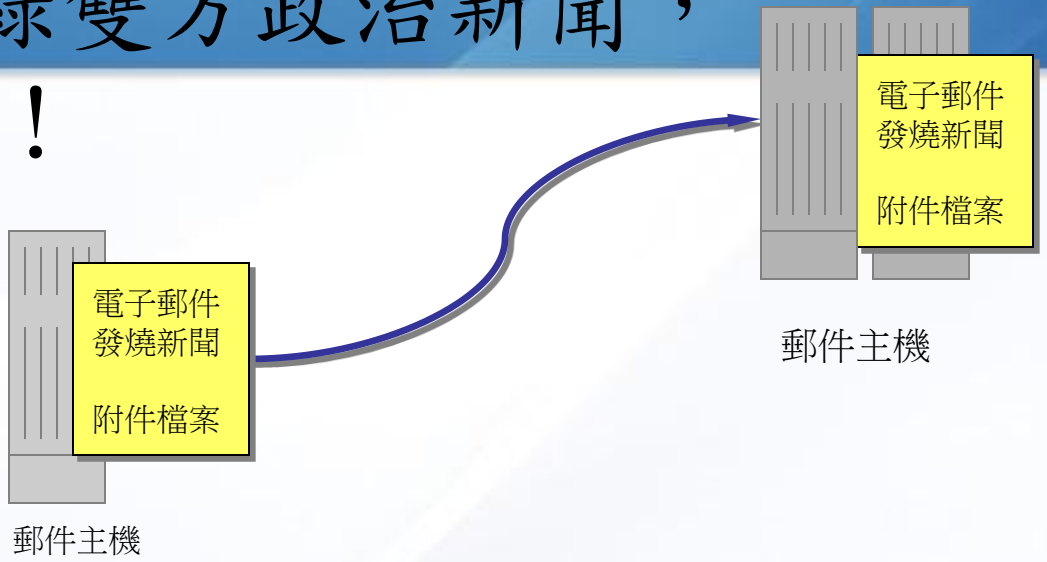
Firewall 防火牆

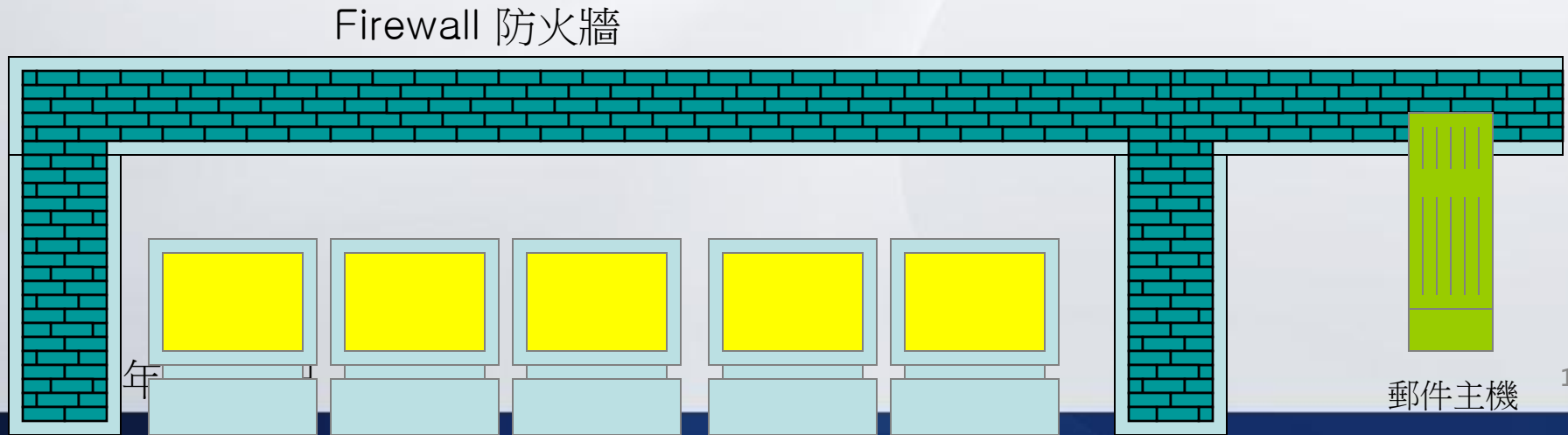




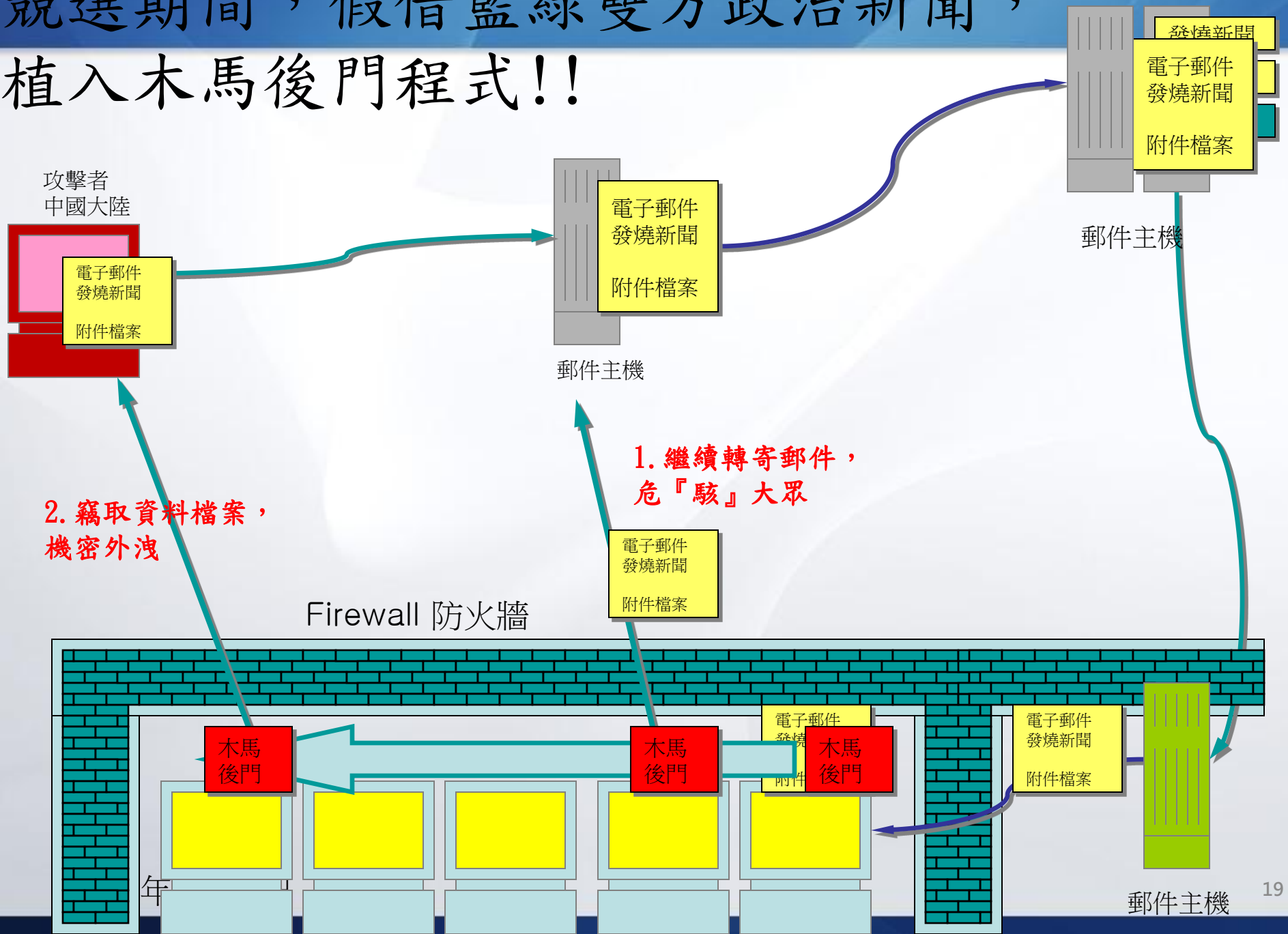
(1) 蒐集使用者輸入的帳號與密碼, …
(2) 監看或竊取 MSN, 郵件內容, …

競選期間，假借藍綠雙方政治新聞，植入木馬後門程式!!





競選期間，假借藍綠雙方政治新聞，植入木馬後門程式!!



你看得出來，誰有問題嗎？

	dmliu@ms4.hine...	[X-Spam]RE: Pharmacy Message 11304	02/11 17:18	2K
	The Code Proje...	[CodeProject] Daily News - Get a free domain...	02/11 13:11	15K
	United Mileage...	My Mileage Plus Summary - February 2009	02/10 20:58	30K
	何[redacted]	^___^你嚇到他了!!!	02/09 14:12	221K
	楊林森	Fw: (有關資訊安全)請檢查一下自己的電腦有沒有不...	02/09 11:10	2K
	[redacted]	知道什麼叫做盪鞦韆嗎？	02/09 10:50	6[redacted]
	Intel (R) Soft...	英特尔(R) C++ 编译器 Windows* 专业版 评估版到期通...	02/09 00:04	4[redacted]
	"Anshuman Prat...	RE: RE: RE: Partnership for Taiwan	02/06 17:56	119[redacted]
	The Code Proje...	[CodeProject] Daily News - The case for supp...	02/06 16:06	15[redacted]
	Intel Performa...	Survey reminder: Intel® IPP Evaluation Vers...	02/06 13:20	3K
	台北市電腦公會	TCA會訊--2009台北國際電玩展，2/12-...	02/05 17:23	25K
	The Code Proje...	[CodeProject] Daily News - The power of pers...	02/05 13:07	15K
	Rossy 黃莉雲	Fw: Micro net	02/04 14:51	2K
	intel.software...	Intel® Evaluation Survey: Intel C++ Compile...	02/03 21:35	4K
!	Richy Huang	合作:採購重要資訊通知~廣得利貿...	02/02 11:13	450K
	何[redacted]	**~~sorry~~**	**01/31 23:58**	**230K**
	何[redacted]	迷你女郎圖片	01/31 18:09	6K
	[redacted]	在無名上看到的 現在的年輕人阿	01/26 07:07	221K
	[redacted]	**安安.....**	**01/25 14:39**	**6K**
	[redacted]	**朋友就要像你這樣的...**	**01/25 03:42**	**5K**
	[redacted]	**眞滴很麻煩你勒~~太需要你的幫忙...**	**01/25 01:21**	**6K**
	st.huang	**我瘦下來啦...趕緊告訴妳小撇步**	**01/24 19:30**	**192K**

何[redacted] ~~sorry~~

[redacted] 安安.....

[redacted] 朋友就要像你這樣的...

[redacted] 眞滴很麻煩你勒~~太需要你的幫忙...

st.huang 我瘦下來啦...趕緊告訴妳小撇步

何[redacted] ^___^你嚇到他了!!!

何[redacted] 迷你女郎圖片

[redacted] 在無名上看到的 現在的年輕人阿

照樣有毒!!

Windows Live Hotmail - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛

網址(D) http://bl125w.blu125.mail.live.com/mail/InboxLight.aspx?n=1678258151 移至 連結

Windows Live™ 首頁 Hotmail Spaces OneCare | MSN 郵件 網頁 dmliu99999@hotmail.com 登出

收件匣 (21)
垃圾郵件
草稿
寄件備份
已刪除的郵件 (1)
管理資料夾

首頁
郵件
連絡人
行事曆

新增 回覆 全部回覆 轉寄 刪除 垃圾郵件 置於資料夾 選項

FW： （我是德明的王姿懿，這是病毒信） [7 10急件] 我訂婚了

寄件者： 王姿 (wendy76802@yahoo.com.tw)
寄件日期： 2008年8月2日 下午 03:55:41
回覆地址： wendy76802@yahoo.com.tw
收件者： dmliu99999@hotmail.com
自拍婚紗.zip (202.3 KB)

下載時執行安全性掃描 TREND MICRO

--- 08/8/2 (星期六)，姿 <wendy520yaya@yahoo.com.tw> 寫道：

寄件者: 姿 <wendy520yaya@yahoo.com.tw>
主旨: FW： [7 10急件] 我訂婚了
收件者: "Liuyi" <wendy76802@yahoo.com.tw>
日期: 2008 8 2 星期六 下午 11:56

--- 08/7/11 (星期五)，Fang Shan Chang <fsc510@yahoo.com.tw> 寫道：

寄件者: Fang Shan Chang <fsc510@yahoo.com.tw>
主旨: [7 10急件] 我訂婚了
收件者: wendy520123@yahoo.com.tw
日期: 2008 7 11 星期五 上午 3:18

7 10
好久沒有聯絡了 我訂婚了 給我祝福吧 發張婚紗照給你 看看你能不能認出我
7 10

總會在某些時刻，突然想起舊情人？他 現在過得還好嗎？- 馬上搜尋！

Microsoft Internet Explorer

檔案 (自拍婚紗.zip) 受到未知病毒的感染，因此下載檔案是不安全的。

確定

完成 網際網路

Windows Live Hotmail - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛

網址(D) http://bl125w.blu125.mail.live.com/mail/InboxLight.aspx?n=1678258151 移至 連結

Windows Live™ 首頁 Hotmail Spaces OneCare | MSN 郵件 網頁 dmliu99999@hotmail.com 登出

收件匣 (21)
垃圾郵件
草稿
寄件備份
已刪除的郵件 (1)
管理資料夾

首頁
郵件
連絡人
行事曆

新增 回覆 全部回覆 轉寄 刪除 垃圾郵件 置於資料夾 選項

FW： （我是[redacted]，這是病毒信） [6 27急件] 別了 朋友們

寄件者： [redacted] (wendy76802@yahoo.com.tw)
寄件日期： 2008年8月2日 下午 03:55:17
回覆地址： [redacted]
收件者： dmliu99999@hotmail.com
我的遺書.zip (173.8 KB)

下載時執行安全性掃描 TREND MICRO

--- 08/8/2 (星期六)，[redacted] 寫

寄件者: [redacted]
主旨: FW： [6 27急件] 別了 朋友們
收件者: [redacted]
日期: 2008 8 2 星期六 下午 11:56

--- 08/6/27 (星期五)，[redacted] 寫道：

寄件者: [redacted]
主旨: [6 27急件] 別了 朋友們
收件者: [redacted]
日期: 2008 6 27 星期五 上午 4:44

6 27
這個世界已經沒什麼值得我眷戀了 永別了 朋友們
這是我給你們的訣別信
6 27

Microsoft Internet Explorer

檔案 (我的遺書.zip) 受到未知病毒的感染，因此下載檔案是不安全的。

確定

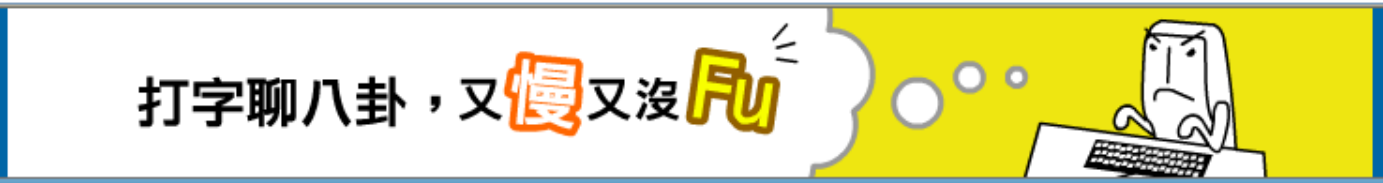
完成 網際網路

Windows Live Hotmail - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

上一頁 搜尋 我的最愛

網址(D) http://bl125w.blu125.mail.live.com/mail/InboxLight.aspx?n=1678258151 移至 連結



Windows Live™ 首頁 Hotmail Spaces OneCare | MSN 郵件 網頁 dmliu99999@hotmail.com 登出

收件匣 (21)
垃圾郵件
草稿
寄件備份
刪除的郵件 (1)
管理資料夾

首頁
郵件
連絡人
行事曆

新增 回覆 全部回覆 轉寄 刪除 垃圾郵件 置於資料夾 選項

FW： （我是[redacted]，這是病毒信）想找新工作

寄件者： [redacted] (wendy76802@yahoo.com.tw)
寄件日期： 2008年8月2日 下午 03:47:37
回覆地址： [redacted]
收件者： dmliu99999@hotmail.com
讚讚讚--拜託拉!...zip (98.3 KB)

下載時執行安全性掃描 TREND MICRO

--- 08/7/12 (星期六)， [redacted] 寫道

寄件者: 張綺綺 <chi19880316@yahoo.com.tw>
主旨: 想找新工作
收件者: s81750@yahoo.com.tw, mei900420@yahoo.com.tw, a_tzu_1020@yahoo
wendy76802@yahoo.com.tw, rita01230@yahoo.com.tw, w9034834@yahoo.com.
ruby198710302000@yahoo.com.tw, g90238@yahoo.com.tw, c22631030@yahoo
alexmax234@yahoo.com.tw, clse0359@yahoo.com.tw, winnie33k@yahoo.com.tw
jackson29449935@yahoo.com.tw, kyo76823@yahoo.com.tw, lovehu1013@yaho
s22616227@yahoo.com.tw, saya-@yahoo.com.tw, turtle90332@yahoo.com.tw
日期: 2008 7 12 星期六 上午 3:00

親愛ㄉ朋友好久不見----我想換工作了如果有甚麼好工作徵人可以幫我留意

總會在某些時刻，突然想起舊情人？他 現在過得還好嗎？- 馬上搜尋！

總會在某些時刻，突然想起舊情人？他 現在過得還好嗎？- 馬上搜尋！

檔案下載

是否要開啓或儲存這個檔案?

名稱: 讚讚讚--拜託拉![1]...zip
類型: WinRAR ZIP archive，126 KB
來自: 65.55.172.39

開啓(O) 儲存(S) 取消

雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。有什麼樣的風險?

完成 網際網路

科技 CEO 防毒 欺騙

Google 搜尋　好手氣

ZDNet Taiwan - 趨勢CEO陳怡樺：防毒產業騙了客戶20年- 新聞- 企業 ...
www.zdnet.com.tw/news/.../0,2000085678,20130359,00.htm - 頁庫存檔
2008年7月2日 – 趨勢科技（Trend Micro）執行長陳怡樺對於防毒產業過去20年來的效能有一番 ... 在防毒產業，我們已經騙了客戶20年了，大家都以為防毒軟體可保護 ...

誰騙了你20年@ 就是資安:: 痞客邦PIXNET ::
cyrilwang.pixnet.net/blog/post/25637117-誰騙了你20年 - 頁庫存檔
這一陣子，有一個還算蠻震撼的新聞，就是趨勢科技的CEO陳怡樺說了「防毒產業騙了客戶20年」這麼一句話。這一句話，不但打翻了趨勢科技自己一直以來的產品，也 ...

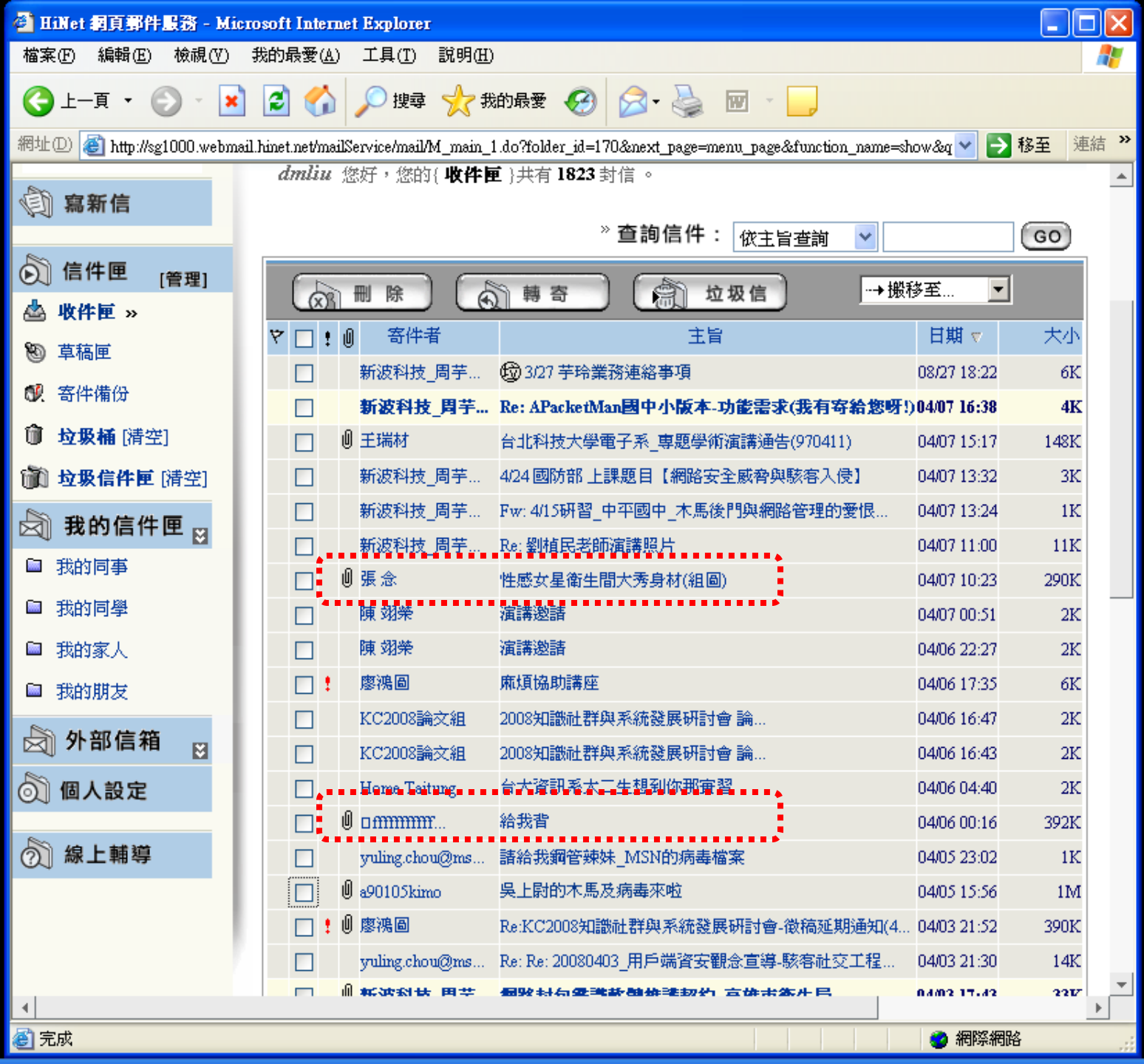
誤打誤撞的驚人發現~~~~~~防毒產業騙了客戶20年!!!!!
www.wretch.cc/blog/lf260703/24269005 - 頁庫存檔
2010年11月1日 – 看到一篇趨勢科技CEO一篇爆炸性發言：防毒產業騙了客戶20年，可是讓我好奇不已，看完整篇新聞卻有種莫名的情感交織，轉貼重點如下： ...

趨勢CEO陳怡樺：防毒產業騙了客戶20年- iT邦幫忙::IT知識分享社群
ithelp.ithome.com.tw/question/10005614 - 頁庫存檔
23 個答案 - 2008年7月3日
趨勢科技（Trend Micro）執行長陳怡樺對於防毒產業過去20年來的效能有一番 ... 在防毒產業，

@ 網路暨遊戲安全防護哈啦板 ...

防毒產業過去20年來的效能有一
毒軟體可保護 ...

在防毒產業，我們已經騙了客戶20年了，
大家都以為防毒軟體可保護他們，
但其實我們不可能完全擋住病毒。


HiNet 網頁郵件服務 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://sg1000.webmail.hinet.net/mailService/mail/M_main_1.do?folder_id=170&next_page=menu_page&function_name=show&q
移至 連結
寫新信
信件匣 [管理]
收件匣 »
草稿匣
寄件備份
垃圾桶 [清空]
垃圾信件匣 [清空]
我的信件匣
我的同事
我的同學
我的家人
我的朋友
外部信箱
個人設定
線上輔導
dmliu 您好，您的{ 收件匣 }共有 1823 封信 。
» 查詢信件： 依主旨查詢 GO
刪 除 轉 寄 垃圾信 --→搬移至...
寄件者 主旨 日期 大小
新波科技_周芋... 3/27 芋玲業務連絡事項 08/27 18:22 6K
新波科技_周芋... Re: APacketMan國中小版本-功能需求(我有寄給您呀!) 04/07 16:38 4K
王瑞材 台北科技大學電子系_專題學術演講通告(970411) 04/07 15:17 148K
新波科技_周芋... 4/24 國防部 上課題目【網路安全威脅與駭客入侵】 04/07 13:32 3K
新波科技_周芋... Fw: 4/15研習_中平國中_木馬後門與網路管理的愛恨... 04/07 13:24 1K
新波科技_周芋... Re: 劉植民老師演講照片 04/07 11:00 11K
張 念 性感女星衛生間大秀身材(組圖) 04/07 10:23 290K
陳 翊榮 演講邀請 04/07 00:51 2K
陳 翊榮 演講邀請 04/06 22:27 2K
廖鴻圖 麻煩協助講座 04/06 17:35 6K
KC2008論文組 2008知識社群與系統發展研討會 論... 04/06 16:47 2K
KC2008論文組 2008知識社群與系統發展研討會 論... 04/06 16:43 2K
Hong Taitung 台大資訊系大二生想到你那實習 04/06 04:40 2K
□fffffffff... 給我背 04/06 00:16 392K
yuling.chou@ms... 請給我網管辣妹_MSN的病毒檔案 04/05 23:02 1K
a90105kimo 吳上尉的木馬及病毒來啦 04/05 15:56 1M
廖鴻圖 Re:KC2008知識社群與系統發展研討會-徵稿延期通知(4... 04/03 21:52 390K
yuling.chou@ms... Re: Re: 20080403_用戶端資安觀念宣導-駭客社交工程... 04/03 21:30 14K
完成
網際網路

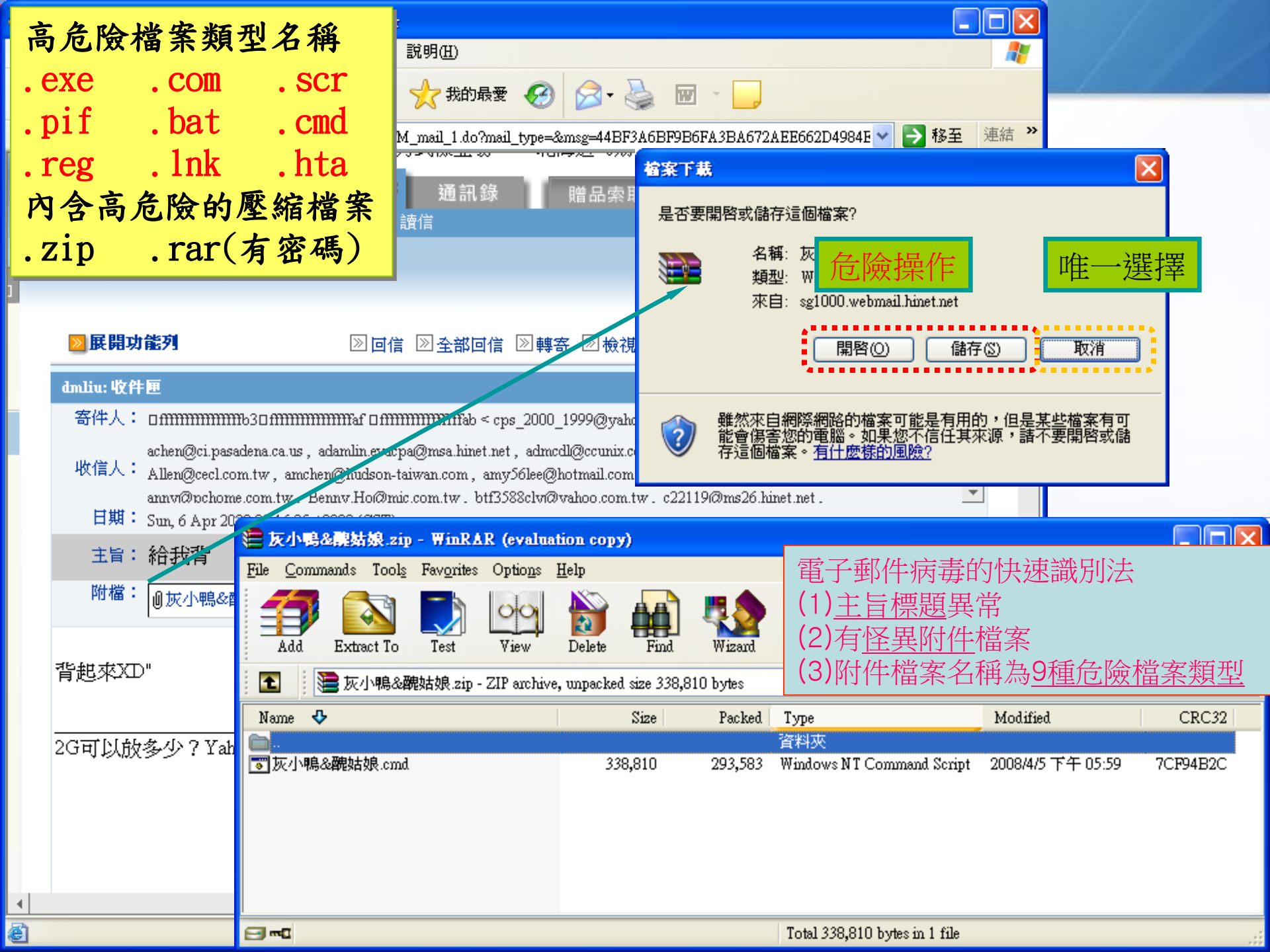
甚麼是 衛生間？ 廁所是也！ 此為 老共用語！

※推論1: 使用台灣專用的繁體中文，該病毒為老共專門為台灣調製的木馬

※推論2: 區域病毒(Local Virus)，國際掃毒軟體找得到它嗎？

※再次說明，掃毒軟體告訴妳：電腦沒有中毒。

只代表它沒有掃到毒，不表示電腦檔案是乾淨的環境！


高危險檔案類型名稱
.exe .com .scr
.pif .bat .cmd
.reg .lnk .hta
內含高危險的壓縮檔案
.zip .rar(有密碼)
檔案下載
是否要開啓或儲存這個檔案?
名稱: 灰
類型: W
來自: sg1000.webmail.hinet.net
危險操作
唯一選擇
開啓(O)
儲存(S)
取消
雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啓或儲存這個檔案。有什麼樣的風險?
展開功能列
回信
全部回信
轉寄
dmliu: 收件匣
寄件人：
收信人：
日期：
主旨：給我背
附檔：灰小鴨&
背起來XD"
2G可以放多少？Yah
灰小鴨&醜姑娘.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
灰小鴨&醜姑娘.zip - ZIP archive, unpacked size 338,810 bytes
Name
Size
Packed
Type
Modified
CRC32
資料夾
灰小鴨&醜姑娘.cmd
338,810
293,583
Windows NT Command Script
2008/4/5 下午 05:59
7CF94B2C
Total 338,810 bytes in 1 file
電子郵件病毒的快速識別法
(1)主旨標題異常
(2)有怪異附件檔案
(3)附件檔案名稱為9種危險檔案類型


刪 除
轉 寄
檢舉垃圾信
寄件者
主旨
Home Taitung 地震天母房子如何
Tofer 型錄
朱瑄淳 NII課程測驗題-請老師提供
Tofer s-monitor 進度
SearchSecurity... Expert guidance on app layer security; con
姿汶 公司的系統欄位-MONICA 02/25 09:38 450K
The Code Proje... [CodeProject] Daily News - The top 3 clo
RFID基礎應用技... RFID 晶片設計教師研習會【歡迎參...
Mike 祝您今年虎虎生威阿~
a90105kimo 網咖剛認識的美眉.
a90105kimo 愛情測試.副件密碼520
a90105kimo 男士請進.MM勿入.嘿嘿~.~副件密碼6
Advanser 迎春納福,前展顧問祝大家虎年行大運發
張國 Re: 關於Diamond group meeting 2月20日
逸凡科技行銷部 逸凡科技陳逸文跟 您拜年！
張國 Re: 關於Diamond group meeting
Mike 謝謝各位百忙之中抽空前往!!
宋茂深 請教找木馬病毒之DOS指令
林啟瑞 RE: 很榮幸今天能與您見到面~
Mike Fw: 很榮幸今天能與您見到面~
Mike Re: 很榮幸今天能與您見到面~
新波科技 FW: 資安研討會主題及大綱
主旨： 網咖剛認識的美眉.
附檔： 網咖剛認識的美眉.rar(81.1K)
前幾天去網咖新認識的美眉....長的像不像明星黃圣依~.~副件密碼520
主旨： 愛情測試.副件密碼520
附檔： 愛情測試.rar(81.3K)
測試下你們愛情是不是能地老天荒.讓你了解對方....更能了解自己.....
主旨： 男士請進.MM勿入.嘿嘿~.~副件密碼668
附檔： 男士請進.MM勿入.嘿嘿.rar(81.1K)
如果你淪落到一個荒島上.你會選擇那條魚....看帖就要回哦.不回後果自負!!!!!

Toyota再創騎蹟 買就送! 年前最殺降價好屋!快搶 可愛小熊螢幕擦!

網頁郵件 通訊錄 心理測驗

現在位置： 網頁郵件 > 讀信

讀取信件

WEBMAIL@HINET 登出

搬移至...

展開功能列 回信 全部回信 轉寄 檢視信件原始檔 友善列印 下載信件 刪除

dmliu: 收件匣 下一封 | 返回 | 另開視窗閱讀信件

寄件人： 何 < honhungmen@yahoo.com.tw > 加入通訊錄 檢舉垃圾信

收信人： aglowdzi@gmail.com

日期： Thu, 14 Jan 2010 16:36:30 +0800 (CST)

主旨： 聽說你最近心情好差?

附檔： 自己好過些.rar(48.8K)

【字體】 【語系】

如果今天的你不能比昨天的你更喜歡自己， 那麼明天對你來說，又有什麼意義？

寄件人： 何 < honhungmen@yahoo.com.tw > 加入通訊錄 檢舉垃圾信

收信人： aglowdzi@gmail.com

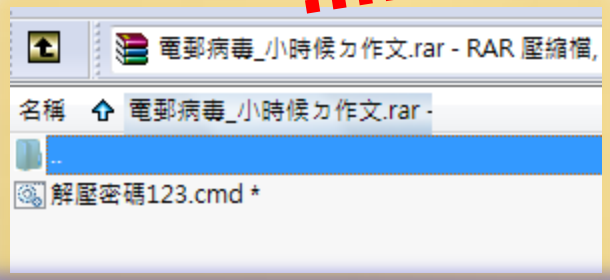
日期： Thu, 14 Jan 2010 00:54:03 +0800 (CST)

主旨： 看看吧~~我國中時寫ㄉ作文

附檔： 小時候ㄉ作文.rar(48.8K)

天啊~~看我小ㄉ時候多糗``^ - ^

夾帶----->小時候ㄉ作文



加密碼的壓縮檔案，危險類別.cmd

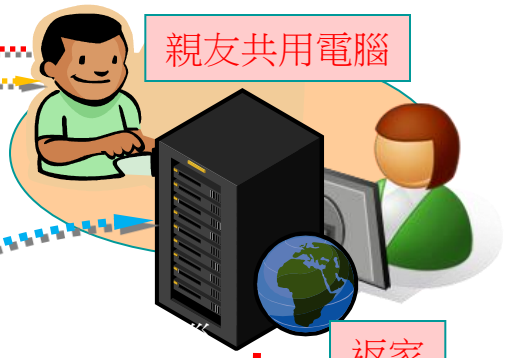
主旨： 好倒楣!我摔倒ㄉ..不能出去玩

附檔： 可憐受傷ㄉ我.rar(48.9K)

前幾天我摔倒ㄉ..現在有好點但不能出去玩.只好寫信給你
並怕幾張受傷包紮後ㄉ相片給你看看

家庭電腦 與 公務電腦 的交互感染

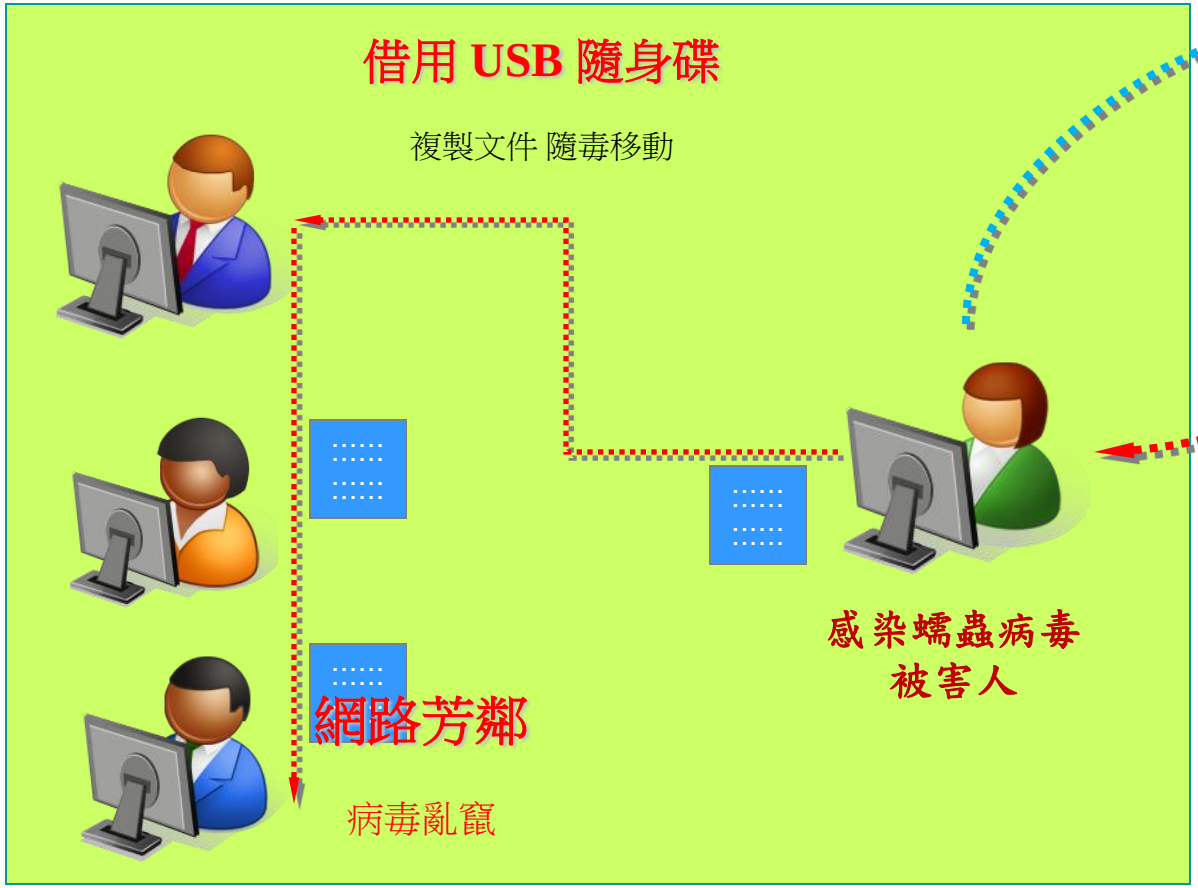
下載影音檔案與程式



返家

攜帶 USB 隨身碟

複製文件 隨毒移動



USB 隨身碟的資安防範

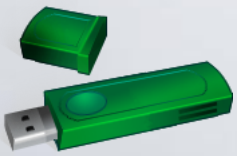
USB儲存設備感染病毒後，不容易清除，因為…

1. 隨身碟，拇指碟，MP3播放器，手機，數位相機，記憶卡等等都可能已經感染 USB病毒，到處傳染其他電腦。

2. 常見USB儲存設備病毒有兩種，

A. 自動執行方式 ➔ Autorun.inf （容易對付）

B. 隱藏文件方式 ➔ 正式文件.doc.exe 或是 目錄名稱.exe



原始檔案目錄 A

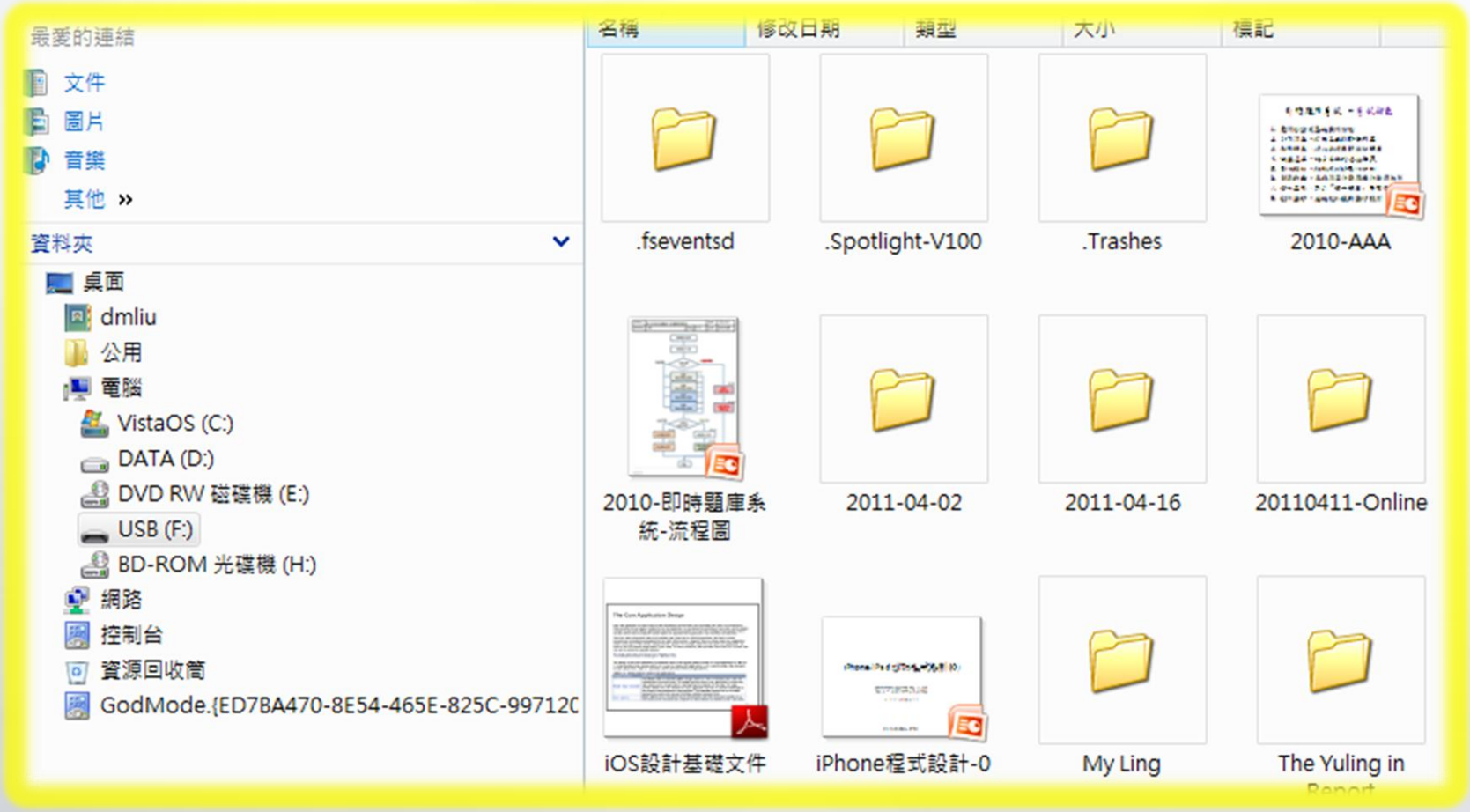
隱藏檔案目錄 A

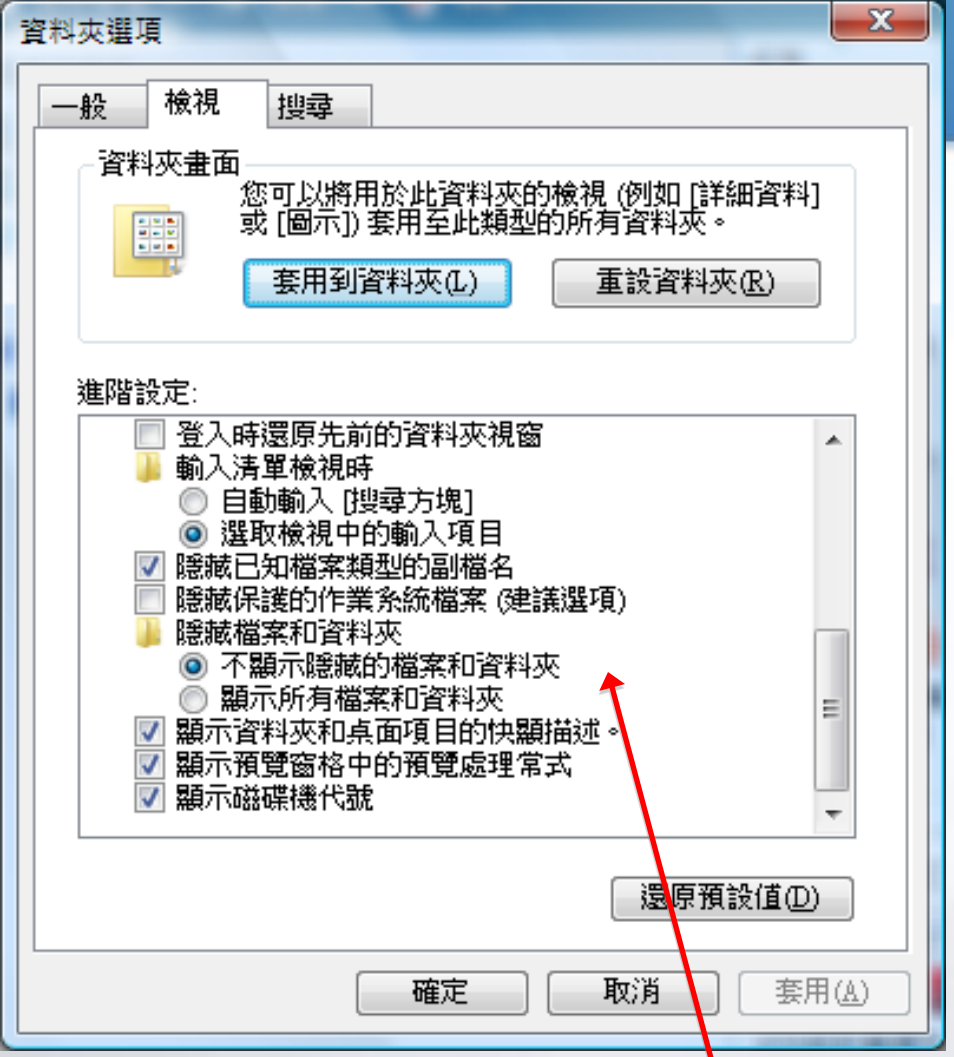
隱藏顯示已知檔案類型

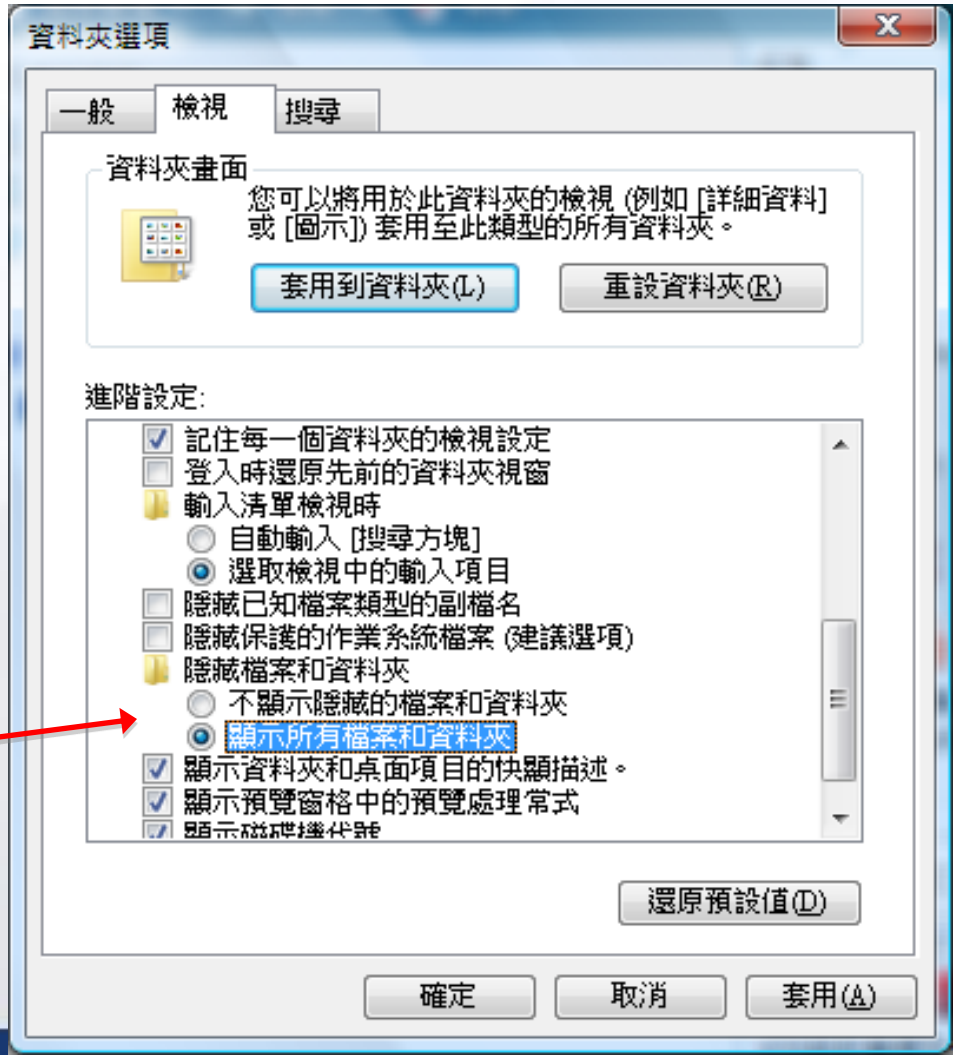
病毒檔案目錄 A.exe

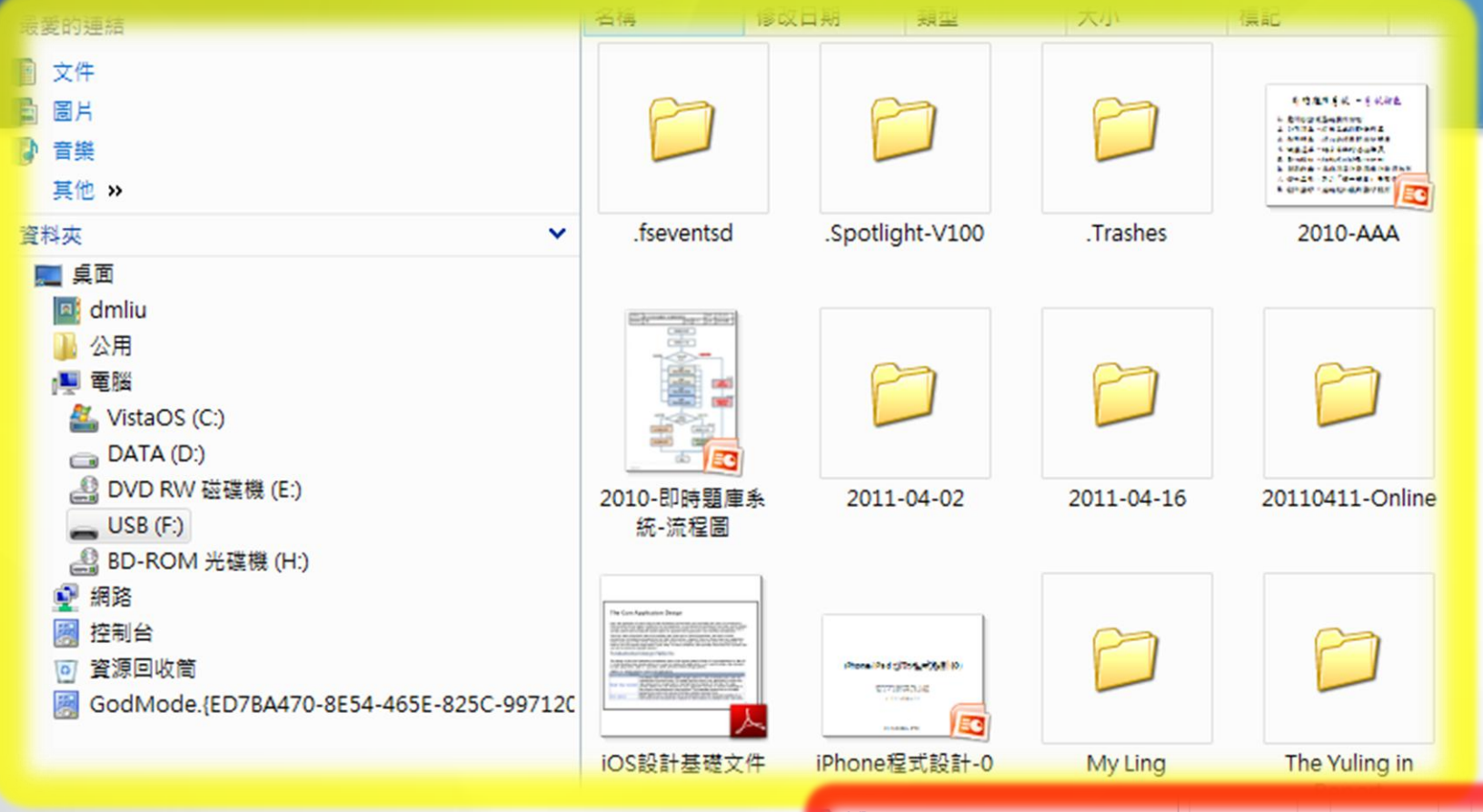
31

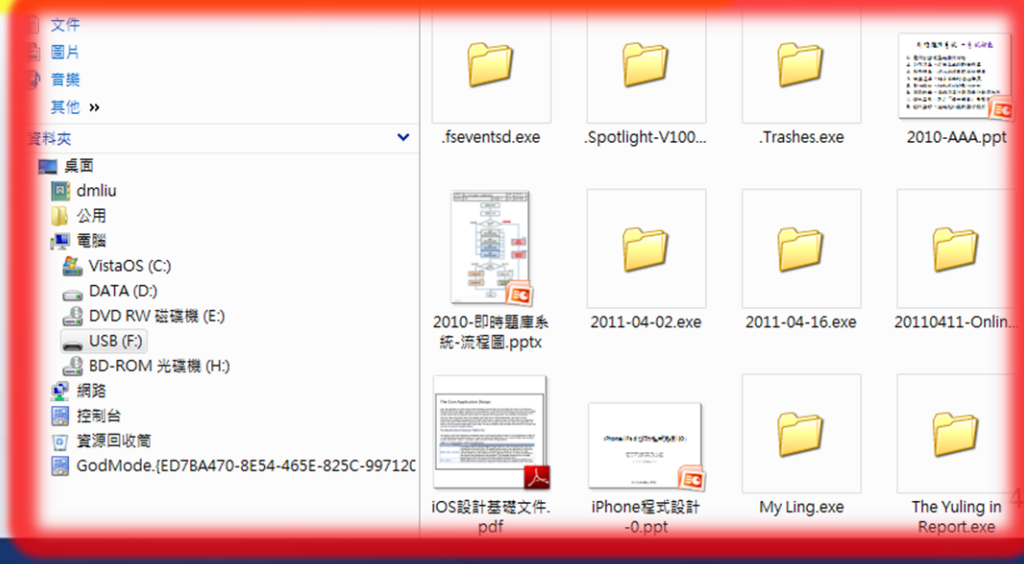
看得出來？這個USB-F碟，有毒嗎？



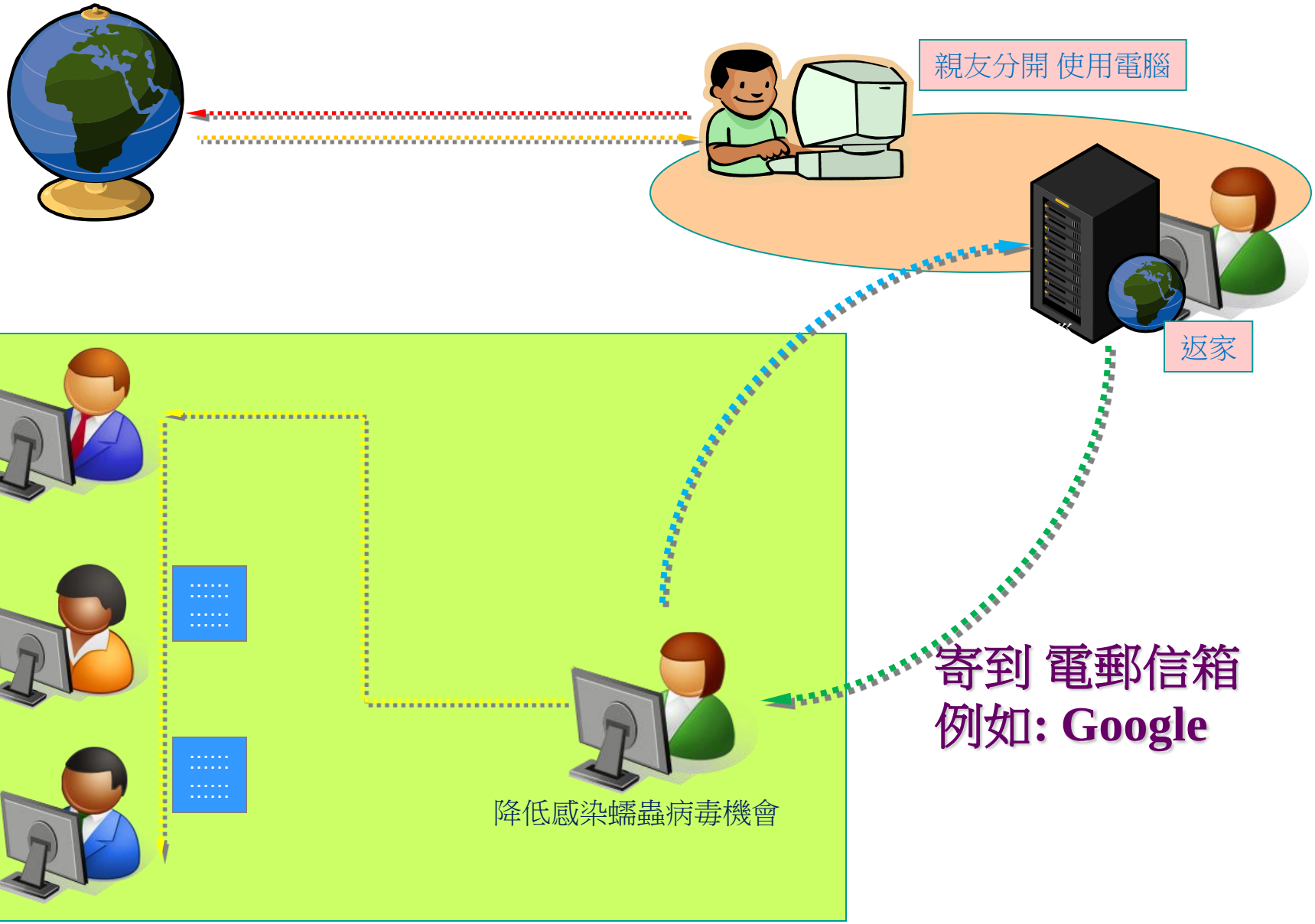

資料夾選項
一般
檢視
搜尋
資料夾畫面
您可以將用於此資料夾的檢視 (例如 [詳細資料] 或 [圖示]) 套用至此類型的所有資料夾。
套用到資料夾(L)
重設資料夾(R)
進階設定:
登入時還原先前的資料夾視窗
輸入清單檢視時
自動輸入 [搜尋方塊]
選取檢視中的輸入項目
隱藏已知檔案類型的副檔名
隱藏保護的作業系統檔案 (建議選項)
隱藏檔案和資料夾
不顯示隱藏的檔案和資料夾
顯示所有檔案和資料夾
顯示資料夾和桌面項目的快顯描述。
顯示預覽窗格中的預覽處理常式
顯示磁碟機代號
還原預設值(D)
確定
取消
套用(A)


資料夾選項
一般
檢視
搜尋
資料夾畫面
您可以將用於此資料夾的檢視 (例如 [詳細資料] 或 [圖示]) 套用至此類型的所有資料夾。
套用到資料夾(L)
重設資料夾(R)
進階設定:
記住每一個資料夾的檢視設定
登入時還原先前的資料夾視窗
輸入清單檢視時
自動輸入 [搜尋方塊]
選取檢視中的輸入項目
隱藏已知檔案類型的副檔名
隱藏保護的作業系統檔案 (建議選項)
隱藏檔案和資料夾
不顯示隱藏的檔案和資料夾
顯示所有檔案和資料夾
顯示資料夾和桌面項目的快顯描述。
顯示預覽窗格中的預覽處理常式
還原預設值(D)
確定
取消
套用(A)


最愛的連結
文件
圖片
音樂
其他 »
資料夾
桌面
dmliu
公用
電腦
VistaOS (C:)
DATA (D:)
DVD RW 磁碟機 (E:)
USB (F:)
BD-ROM 光碟機 (H:)
網路
控制台
資源回收筒
GodMode.{ED7BA470-8E54-465E-825C-99712C
名稱
修改日期
類型
大小
標記
.fseventsd
.Spotlight-V100
.Trashes
2010-AAA
2010-即時題庫系統-流程圖
2011-04-02
2011-04-16
20110411-Online
iOS設計基礎文件
iPhone程式設計-0
My Ling
The Yuling in

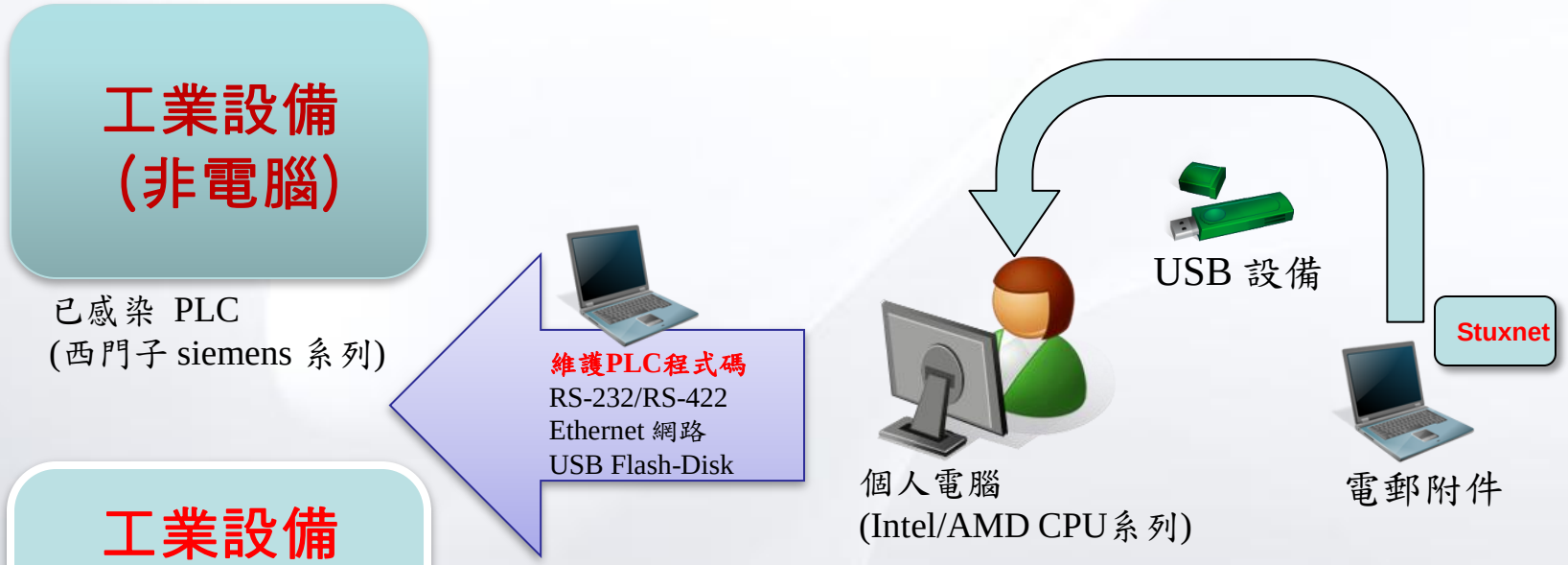

文件
圖片
音樂
其他 »
資料夾
桌面
dmliu
公用
電腦
VistaOS (C:)
DATA (D:)
DVD RW 磁碟機 (E:)
USB (F:)
BD-ROM 光碟機 (H:)
網路
控制台
資源回收筒
GodMode.{ED7BA470-8E54-465E-825C-99712C
.fseventsd.exe
.Spotlight-V100...
.Trashes.exe
2010-AAA.ppt
2010-即時題庫系統-流程圖.pptx
2011-04-02.exe
2011-04-16.exe
20110411-Onlin...
iOS設計基礎文件.pdf
iPhone程式設計-0.ppt
My Ling.exe
The Yuling in Report.exe

家庭電腦 與公務電腦 的隔離措施



Stuxnet – 歷史新發展

- 2010-06，歷史上，第一個從個人電腦感染工業(醫療)控制器的跨系統(攻擊型)電腦病毒，相當於生物界的『異種』感染病毒。



NSS researcher Dillon Beresford reported finding "multiple vulnerabilities" in Siemens programmable logic controllers (PLCs) used in plants worldwide to automatically regulate temperatures, pressures, turbine speeds, robot arms and more.

"This is a global problem," NSS chief executive Rick Moy told AFP. "There are no fixes to this right now," he continued. "Bad guys would be able to cause real environmental and physical problems and possibly loss of life."

個資法對公務人員的影響

1. 個人資料保護法的影響

- 個人資料是指自然人的姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情況、社會活動及其他足資識別該個人之資料。
- 外洩民眾個人資料的處罰刑責為五年。

2. 資安防護,從自己做起,養成資安好習慣

- 不要將公務資料(個人資料)帶回家登打。
- 公務電腦檔案要加密，不要用簡單密碼。
- 公務電腦的檔案與帳號密碼，必須與私用帳密分開使用。
- 禁止攜帶個人隨身碟或USB儲存裝置到公務電腦使用。
- 部要在公務電腦使用任何私人活動。

3. 不要過度相信任何資安防護工具

- 任何號稱100%的防護,都是科學的錯誤(行銷的誇大言詞)
- 養成電腦防護的好習慣，才是真正的資訊安全『王道』。

網路安全的三不政策

- 駭客會採用最熟悉的方式欺騙被害人。 包括有 ： 熟悉的朋友電郵帳號、常用的同事電郵帳號、最近的會議活動名稱等等，其中的電郵附件檔案就是病毒木馬的檔案。

- 不自行下載軟體程式（政府網站除外）
  - 如果要下載程式，請至官方網站(Official Web)。
  - 不要相信入口網站的下載資料。
  - 不執行外部來源程式（學校寄送除外）
  - 不要執行(開啟)電子郵件的附件檔案(exe, pif, com, scr, …)。
  - 不要自行安裝私帶的程式。(包括免費軟體, 螢幕保護程式)
  - 不要安裝破解版的電腦程式或防毒軟體。
- 家裡電腦檔案不要複製到公務電腦，反之亦然
  - USB設備已經成為電腦病毒溫床，不要將任何檔案帶回家。
  - USB設備(拇指碟、隨身碟、文件照片、影音檔案)
  - 不要攜帶私人電腦設備，更不宜連接公務網路環境
- 不要相信公眾網路的安全機制
  - 無線上網與飯店網路的資料洩漏機會很大
  - 不要在有疑慮的網路環境，處理個人機敏資料(帳號密碼、金融事務) 。
  - USB設備(拇指碟)已經成為病毒溫床，不要帶回家。

網路安全的 資安五要

- 網路視訊有漏洞，平常要關閉
  - 木馬後門會進行『視訊偷拍』
  - 不用WebCam視訊的時候，要將它『停用』。
- 網路照片要謹慎保管好(切勿交給別人保管)
  - 許多知名部落格都有漏洞，私密照片不要上傳。
  - 現任男友，也許會成為『歷史遺跡』，私密照片要加密。
  - X 不要自拍裸照、不要用電腦做「害羞的事」...
  - X 如果男友要求你跟他自拍害羞的照片，休掉他！
- 電腦送修前要先備份重要資料，並刪除私密檔案
  - 不要讓維修廠商複製電腦檔案的機會。
  - 現任男友，如果是電腦高手，他也可能會幫你安裝木馬後門
  - (安裝木馬後門只要5秒鐘，就可以監控msn, 開啟WebCam)
- 網路交友要謹慎，網路是最好的偽裝機制
- 要經常參加各類資安研討會，獲悉最新資安防護方式

Q&A

- Name : Diamond Liu (劉浔明、劉得民)
- Email : dmliu@ms4.hinet.net
- MSN : dmliu99999@hotmail.com
- Address: Diamond InfoTech.
- Taipei, Taiwan, R.O.C.

My first wish is to see this plague of mankind, war, banished from the earth.

George Washington, 1st US President