ZERONE
零壹科技

只要你懂，手持裝置就是網站攻擊的神工具

李啟銘　Ken Lee

Agenda

- 近期資安新聞
- 手機攻擊手法介紹
- 郵件攻擊手法介紹
- DDoS攻擊手法介紹
- 如何提升避免遭駭

iOS v.s Android

買手機送惡意程式

特定來源的36款Android裝置被預載惡意程式，小米、華碩Zenfone及三星Note系列都中鏢

受影響的36款Android裝置包含三星的Note 2//3/4/5及Note 8.0與Galaxy Tab平板電腦、華碩Zenfone 2、小米的紅米、米4i等，這些裝置均來自大型的電信業者及跨國技術公司，這些預載至裝置的惡意程式包含竊取資料、廣告網路、行動勒索程式。

文/ 陳曉莉 | 2017-03-14 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 3,899 分享 G+1 22

資料來源:IThome

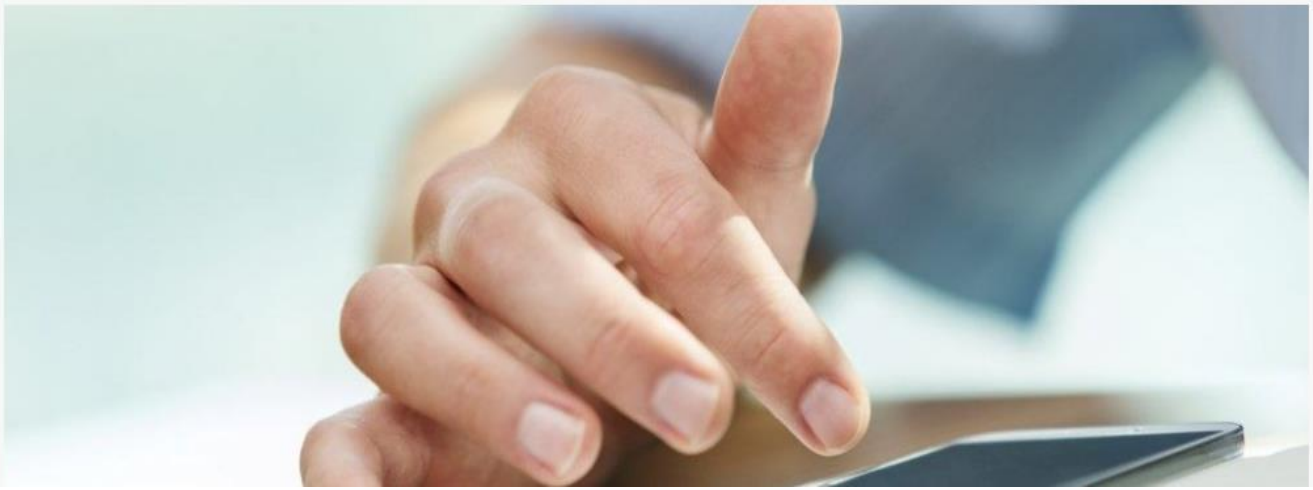
你的手機也可以幫忙駭客賺錢

Check Point：CopyCat感染1400萬台Android裝置，駭客兩個月內賺進150萬美元

Check Point揭露CopyCat主要透過第三方來源感染Android裝置，可取得裝置最高權限，並建立永久性，主要目的為進行廣告詐騙，例如賺取評價、擅自顯示廣告。

文/ 陳曉莉 | 2017-07-07 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 26 分享 G+1 0



資料來源:IThome

Android惡意程式數量高居不下

Android用戶注意 逾800款APP遭植惡意程式

分享 留言 列印 存新聞 A- A+

2017-06-18 19:38中央社 台北18日電 讚 22 分享 傳送

IOS漸漸不再安全

快更新到 iOS 10.1，否則駭客可透過 JPEG 圖片駭入你的手機

作者 T客邦 | 發布日期 2016 年 10 月 28 日 12:05 | 分類 Apple , iOS , iPhone Follow G+1 讚 500 分享

Apple 在 iOS 10.1 版的更新公告中提到，該版更新修正了 CVE-2016-4673 漏洞，不過反過來說，也就是在這個版本之前的 iOS 將曝露於安全風險之下。攻擊者可以利用特殊的 Jpeg 圖片或 PDF 文件，從遠端駭入手機並植入惡意程式，最好的反制方式當然就是趕快把 iOS 升級到 10.1 版囉。

變臉詐騙金額屢創新高

FBI網路犯罪報告：小心假冒技術支援的詐騙手法，變臉詐騙讓企業損失最慘重

變臉詐騙鎖定企業，假冒供應商向企業騙取匯款，至於技術支援詐騙則是假冒安全、軟體或網路公司的技術支援人員，誘騙被害者提供遠端存取裝置的權限，竊取資料、進行勒索軟體攻擊或是誘騙金額。

文/ 陳曉莉 | 2017-06-26 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 51 分享 G+1 1

資料來源:IThome

只要能上網就能發動” DDoS”

美國大學遭到DDoS攻擊，「凶手」竟然是校內的自動販賣機、路燈

美國電信商Verizon揭露一所美國大學遭到DDoS攻擊，在追查下竟發現來自校內為數約5000台的物連網裝置，包含連網路燈、自動販賣機等，所幸駭客操控手法不夠高明，校方最後取回這些連網裝置的控制權。

文/ 陳文義 | 2017-02-14 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 2,373 分享 G+1 10

資料來源:IThome

Agenda

- 近期資安新聞
- 手機攻擊手法介紹
- 郵件攻擊手法介紹
- DDoS攻擊手法介紹
- 如何提升避免遭駭

手機使用率超越電腦....將成為下個目標

資料來源:ETNews

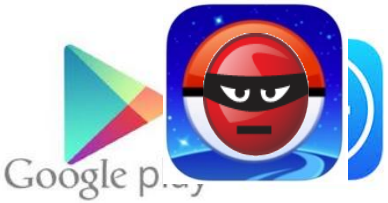
手機為何會被駭??

1.手機系統漏洞

2.誤裝惡意程式

3.誤點惡意連結

手機入侵手法剖析(一):惡意程式



惡意程式開始收集手機上相關資料:

*手機簡訊
*通訊軟體內容
*手機聯絡人資料
*.....

手機詐騙手法剖析:惡意連結

資料來源:內政部警政署

手機入侵實作

Agenda

- 近期資安新聞
- 手機攻擊手法介紹
- ✓ 郵件攻擊手法介紹
- DDoS攻擊手法介紹
- 如何提升避免遭駭

一封郵件能夠做什麼??


THE FOLLOWING PREVIEW HAS BEEN APPROVED FOR
ALL AUDIENCES
THE FILM ADVERTISED HAS BEEN RATED
S
SECURED by IBM
STRONGLY RECOMMENDED FOR
ALL ENTERPRISE BUSINESSES

常見的郵件攻擊類型

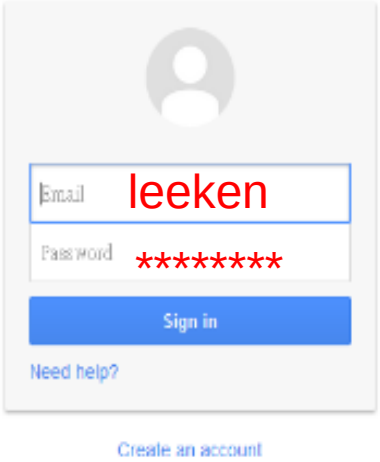
1.垃圾郵件攻擊(Spam)

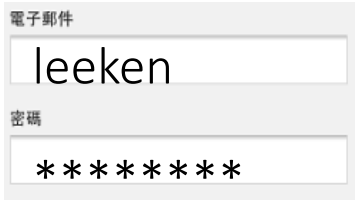
2.郵件釣魚攻擊(Phishing or Spear Phishing)

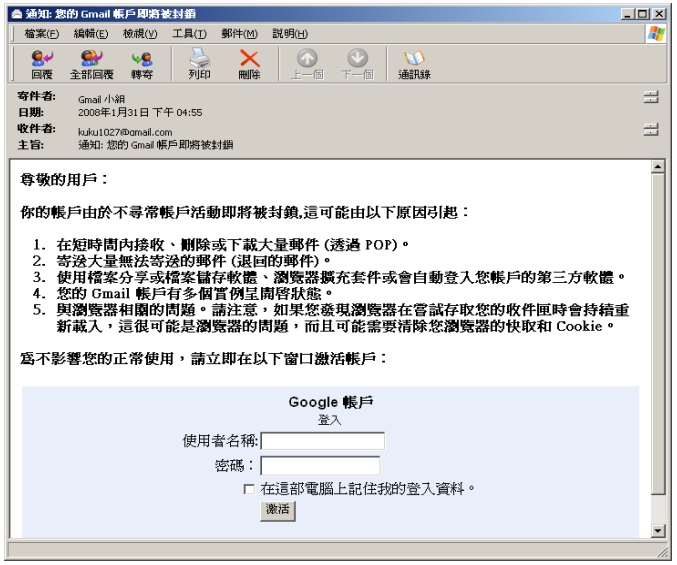
3.郵件APT攻擊(APT For Email)

4.郵件變臉詐騙(Business Email Compromise)

釣魚郵件攻擊手法

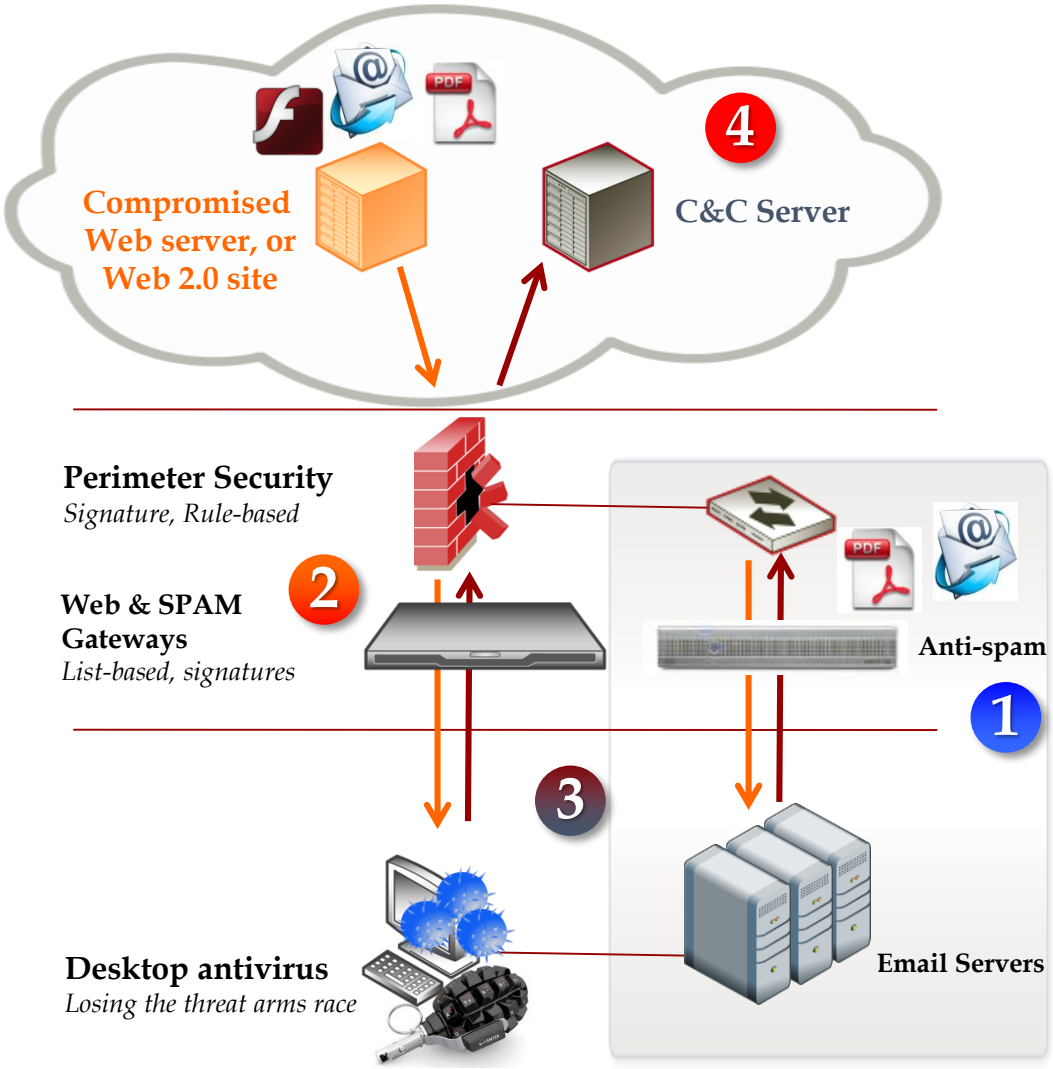

Email
leeken
Password
****
Sign in
Need help?
Create an account


電子郵件
leeken
密碼
****


通知: 您的 Gmail 帳戶即將被封鎖
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄
寄件者: Gmail 小組
日期: 2008年1月31日 下午 04:55
收件者: kuku1027@gmail.com
主旨: 通知: 您的 Gmail 帳戶即將被封鎖
尊敬的用戶：
你的帳戶由於不尋常帳戶活動即將被封鎖,這可能由以下原因引起：
1. 在短時間內接收、刪除或下載大量郵件 (透過 POP)。
2. 寄送大量無法寄送的郵件 (退回的郵件)。
3. 使用檔案分享或檔案儲存軟體、瀏覽器擴充套件或會自動登入您帳戶的第三方軟體。
4. 您的 Gmail 帳戶有多個實例呈開啓狀態。
5. 與瀏覽器相關的問題。請注意，如果您發現瀏覽器在嘗試存取您的收件匣時會持續重新載入，這很可能是瀏覽器的問題，而且可能需要清除您瀏覽器的快取和 Cookie。
爲不影響您的正常使用，請立即在以下窗口激活帳戶：
Google 帳戶
登入
使用者名稱:
密碼：
在這部電腦上記住我的登入資料。
激活

惡意郵件APT攻擊手法

1. **透過漏洞進行攻擊 (Exploit)**
   - 郵件中夾帶惡意檔案
2. **持續與總部持續建立後門連線 (Callback to C&C)**
   - 完成主機連線
   - 下載相關惡意程式工具
   - 使用 80 or 443連線 (SSL)
3. **透過網路下載惡意程式 (Binary Download)**
   - 連線指定主機
   - 下載惡意未知程式
   - 未知型檔案
4. **完成資料竊取或破壞 (Data Exfiltration)**



變臉詐騙比勒索軟體更好賺??

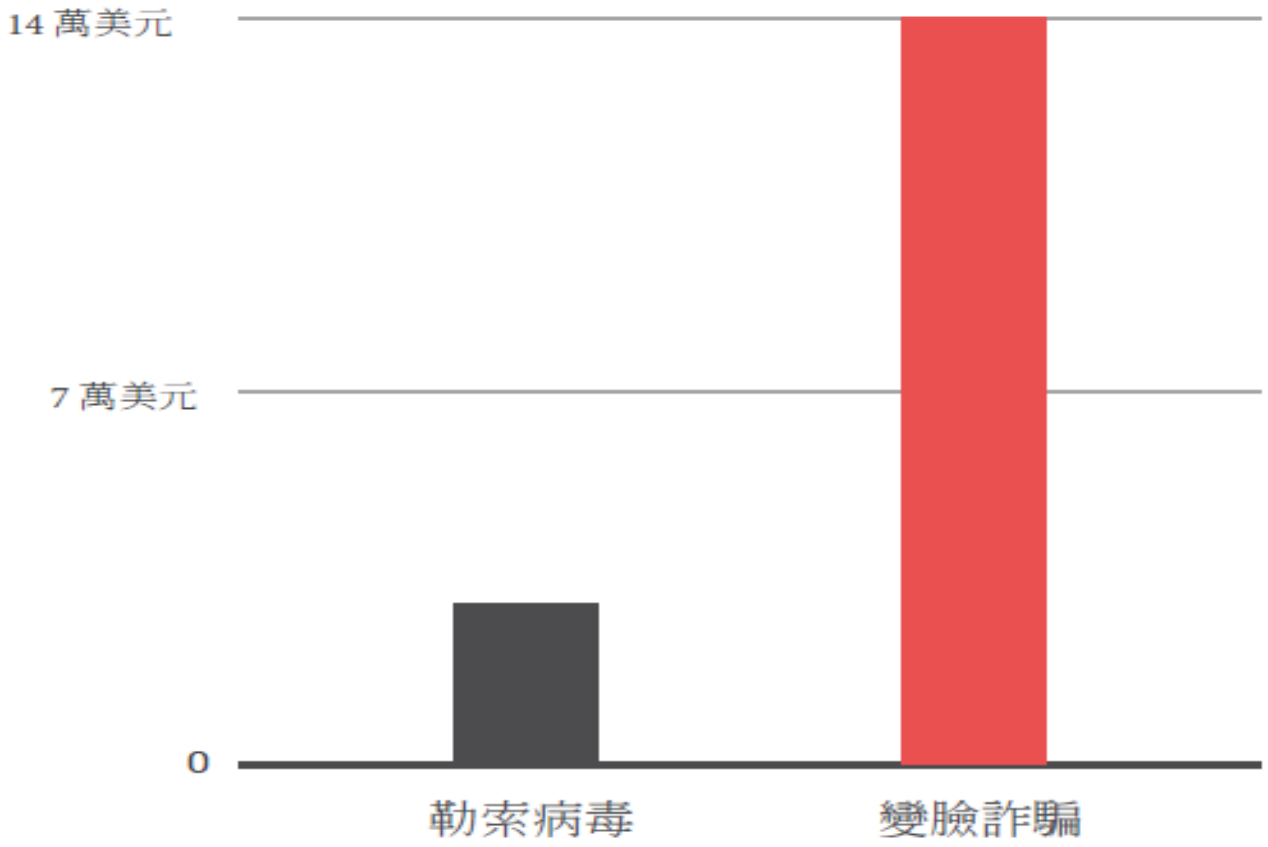


圖 3：勒索病毒攻擊與變臉詐騙企業平均損失金額比較。

資料來源:趨勢科技

何謂變臉詐騙??

變臉詐騙攻擊又稱為商務電子郵件入侵(Business Email Compromise，簡稱 BEC)專門針對那些經常需要匯款給外部供應商的企業機構

變臉詐騙駭客手法


偽冒報價單及匯款帳戶騙取客戶匯款
拋棄式郵件信箱
正常往來信件
進口商 買家
出口商 賣家
客戶接收駭客通知匯款被騙
業務郵件遭鎖定、竄改

Agenda

- 近期資安新聞
- 手機攻擊手法介紹
- 郵件攻擊手法介紹
- DDoS攻擊手法介紹
- 如何提升避免遭駭

什麼是DDoS攻擊??

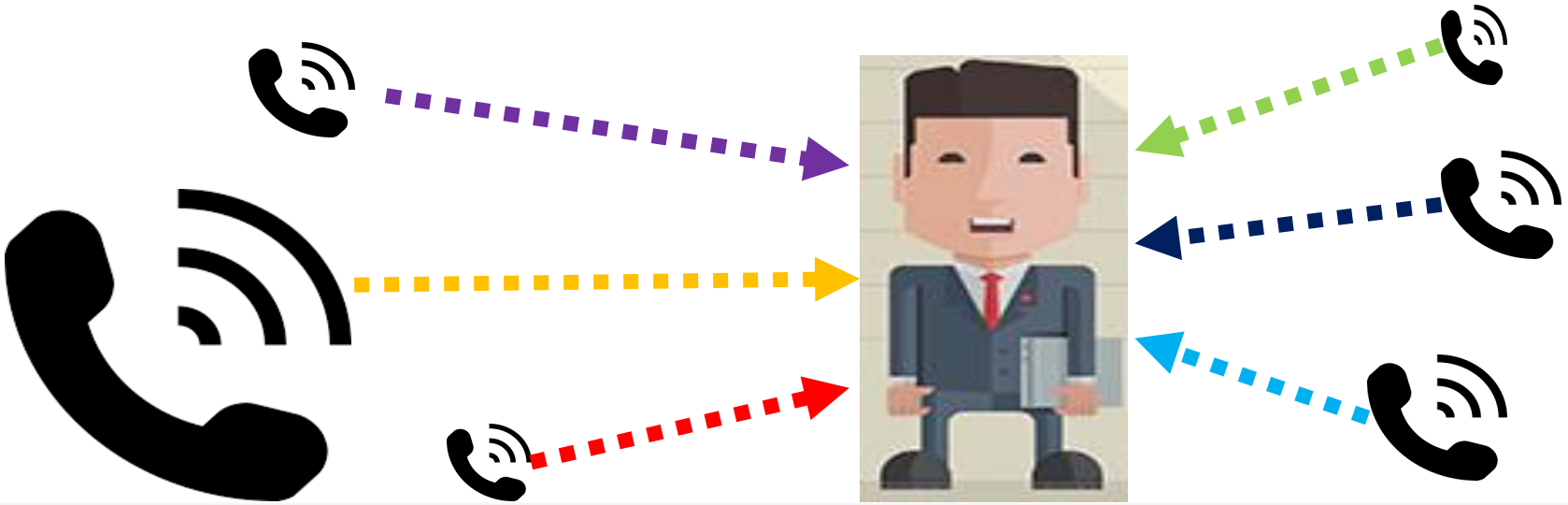
請你想像一下...

今天你正被另一半
用 LINE奪命連環call

會發生什麼事呢？

你會發生以下狀況:

- 你沒辦法接其他人的來電 (網路資源消耗型攻擊)
- 你沒辦法用 LINE 回覆訊息(應用資源消耗型攻擊)
- 手機被 Call 到當機了 (系統資源消耗型攻擊)



Agenda

- 近期資安新聞
- 手機攻擊手法介紹
- 郵件攻擊手法介紹
- DDoS攻擊手法介紹
- 如何提升避免遭駭

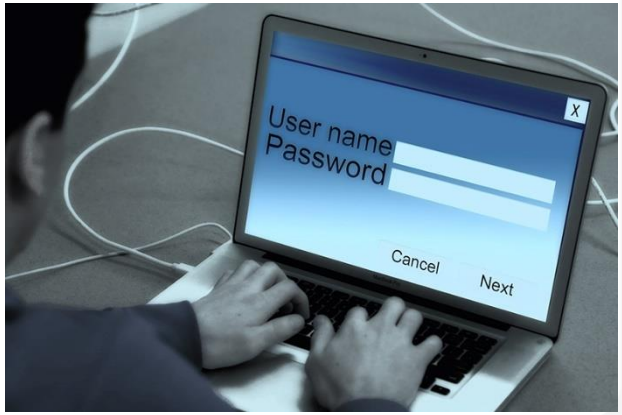
個人電腦安全概念

- 安裝**最少的系統元件** (降低被入侵的風險)
- **遠離來路不明的軟體**，檔案，磁片及光碟；並隨時注意電腦異常狀況
- **設定一組強而有力的密碼**
- **定期更新系統修補程式(Hotfix)**
- 定期**備份**

  3-2-1 原則(三份備份、二種儲存媒體、一個不同存放地點)
- 安裝**防毒軟體**：定期更新病毒碼、掃毒引擎及程式

你是否也用這些密碼?

2015年	2016年
123456	123456
password	123456789
12345678	qwerty
qwerty	12345678
12345	111111
123456789	1234567890
football	1234567
1234	Password
1234567	123123
baseball	987654321



密碼長度	26 英文字母	26 英文字母+10 數字	52大小寫英文字母	96可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9天	4 個月	23 年
8	24 天	10.5個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21萬9000年
10	45 年	1159 年	45838 年	2100萬年

密碼安全的守則

密碼是保護電腦的第一防線，**密碼安全**的守則

- 使用**長度超過10 個字元**的密碼，越長越好。
- 將某些**字母換成數字和/或標點符號**。
- 最好**用三個無意義的字**所組成的密碼。
- **使用不連續的數字**。避免使用重要的日期，例如你的生日。
- **切勿重複使用相同的密碼**。**花點時間為每一個帳號建立各自的密碼**。
- 採用**隨機組合的密碼**並且超過 10 個字元。而且，不能用於一個以上的帳號。
- **密碼提示問題的答案,網路上找不到**。使用與問題完全不相干的答案。某些網站會讓你建立自己的密碼提示問題。
- 遠離網路釣魚攻擊。網路釣魚是一種歹徒誘騙你提供登入帳號密碼的手法。**切勿開啟可疑的訊息或點選不明來源的連結**。
- 整頓你的數位生活。**刪除不再需要的帳號**。這樣可以消除你舊帳號與新帳號之間的連結。
- 仔細篩選你在社交網路上所分享的資訊。你或許透漏太多私人生活的細節，這有可能對你不利。

如何在上網瀏覽時保持安全?

- 採用具備安全防護功能的應用程式
- 持續定期更新
- 按下連結時應提高警覺
- 禁止非必要的通訊協定進入企業網路
- 定期更新作業系統
- 建置多面向的多層式安全防護解決方案
- Web Threat Protect (WTP)避免電腦被傀儡網路控制

手機防護六大要領

1.安裝App停看聽

2.JB 、Root 不可行

3.天下沒白吃的午餐(Android)

4.安全機制不可少(複雜密碼、指紋辨識)

5.定期更新版本與備份

6.安裝防護軟體煩惱少

社交網路安全使用守則

1. 熟悉社交網站的隱私權設定與安全政策
2. 千萬不要照實填寫全部填寫所有的欄位
3. 回應別人的文章時,你發表的內容是公開的
4. 重設密碼要小心你的「安全提示問題」
5. 切勿在不同的網站使用相同的密碼
6. 如果你收到不認識的人所發的請求，請先直接和那個人連絡，再決定要不要將該人加入你的好友圈
7. 將朋友社群組,只挑選某些朋友分享
8. 盡量減少你所安裝或者能夠存取你帳戶的協力廠商應用程式與服務
9. 請當心”怪怪”或”好康”的訊息或塗鴉牆貼文當中的連結
10. LINE 簡訊詐騙要當心

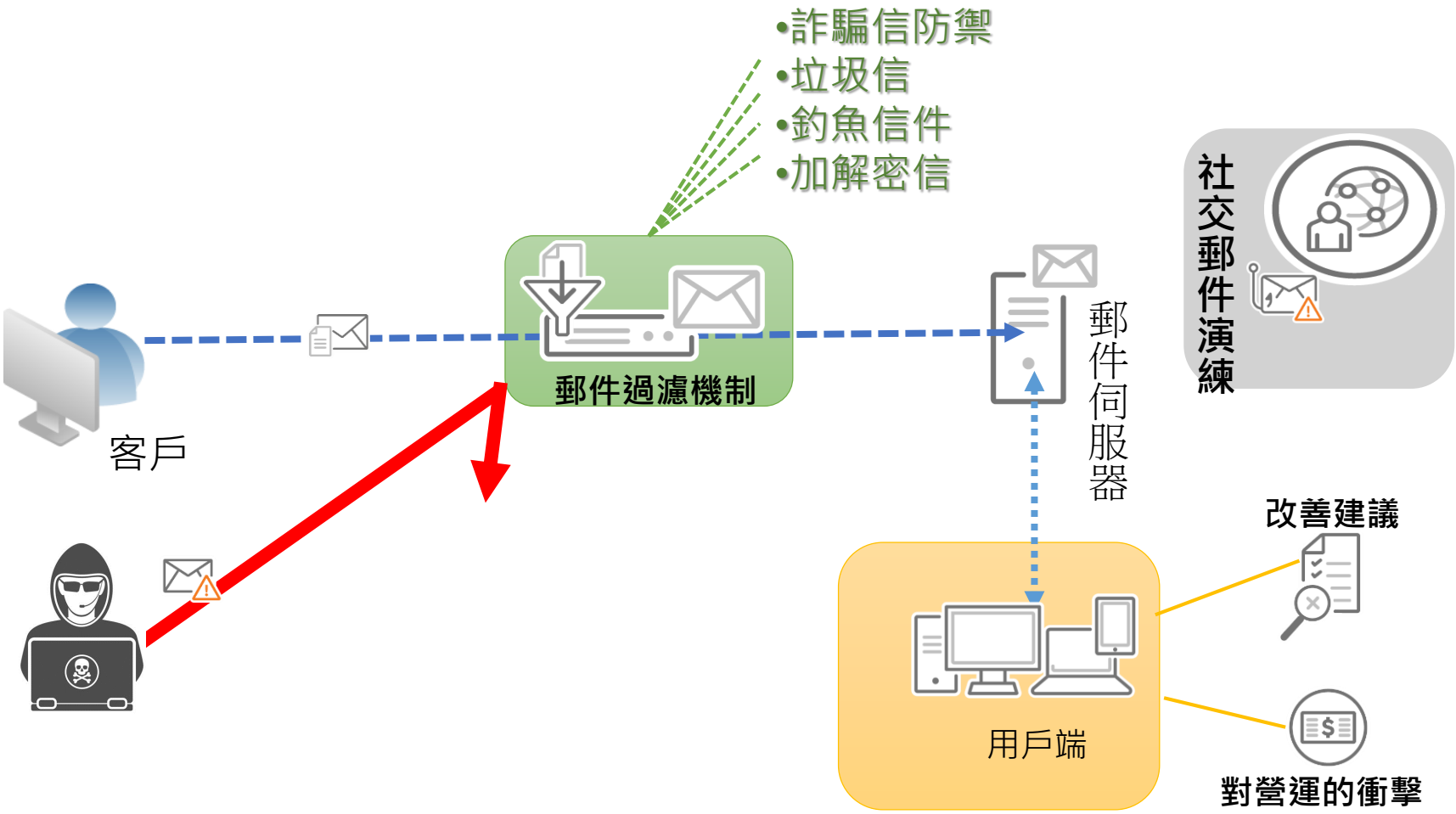
Line 的自救術 – 關閉允許其他裝置登入

防範社交工程郵件重點

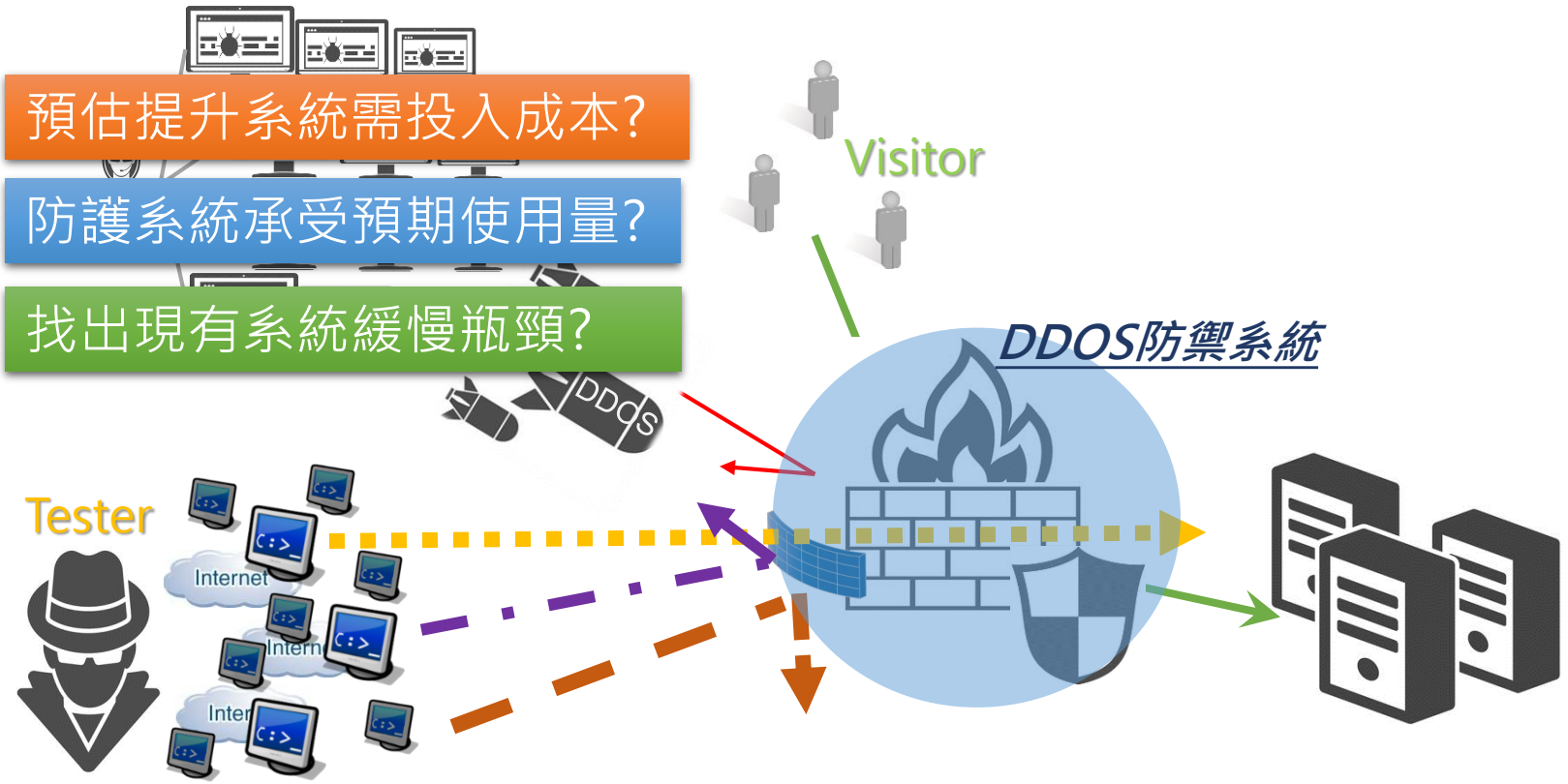
- 不是所屬業務信件一律不開
- 陌生郵件一律不開!!!
- 不要太八卦, 怪怪的郵件不要再轉寄!!
- 注意連結與附檔
  - Com
  - Exe
  - Scr
  - Lnk
  - Bat

可疑檔案掃瞄網站 https://www.virustotal.com/en-gb/
可疑網址檢查網站 http://global.sitesafety.trendmicro.com/

除了防禦還需要提升意識-社交工程演練



提升網站安全防護-DDoS演練



專業服務 邁向卓越

We Commit To Excellence