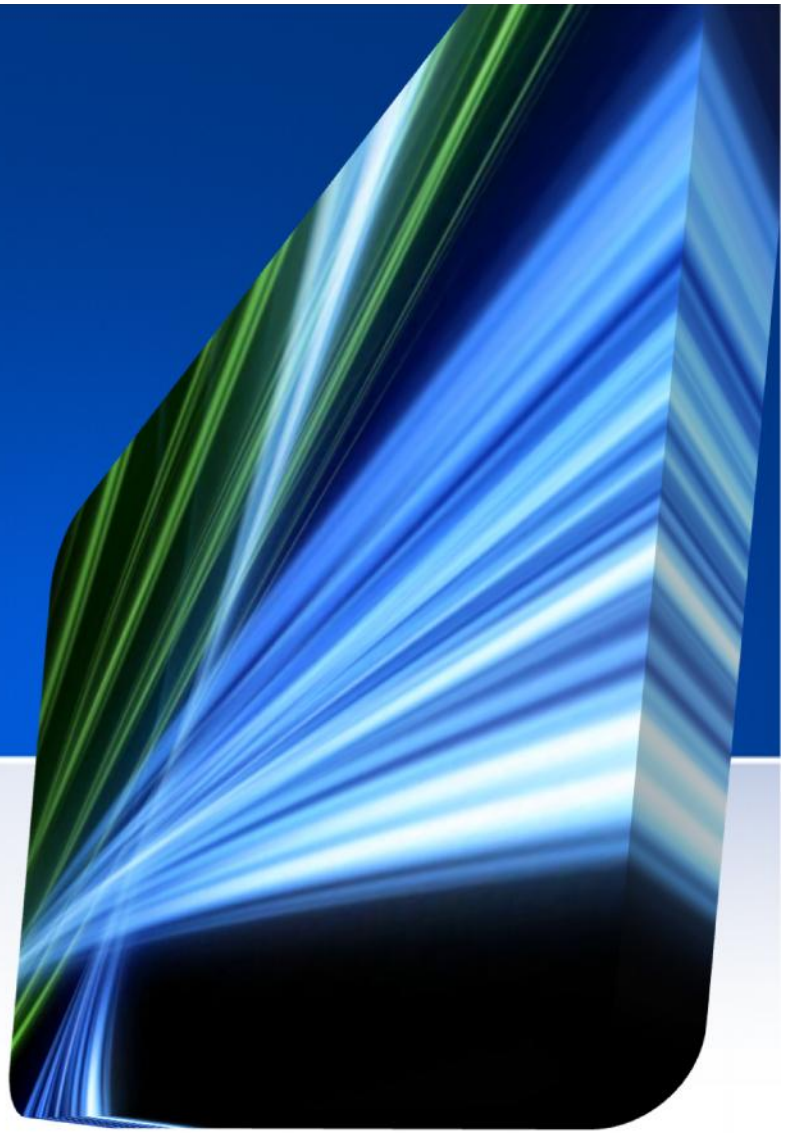
不可不知の社交工程手法

網路管理組
張維廷

May,2012



大綱

- 資安威脅
- 常見手法介紹
- 社交工程演練
- 演練結果分析
- 總結

面對日益嚴重的資安威脅，

您準備好了嗎?

層出不窮的資安事件

- 2012-05-18 英國國防部遭駭客入侵
- 2012-05-03 伊朗石油部遭駭客攻擊
- 2012-04-09 惡意程式使用遭竊憑證
- 2012-03-26 NASA噴氣推進引擎實驗室遭駭客入侵
- 2012-01-03 中國駭客入侵美國商會
- 2011-12-08 駭客攻擊美國自來水供應系統
- 2011-12-07 挪威關鍵企業遭駭客鎖定竊取機敏資訊
- 2011-10-20 美國無人駕駛戰機操作系統感染惡意程式
- 2011-10-13 MySQL 網站遭駭客入侵
- 2011-09-21 DigiNotar 遭駭客入侵
- 2011-09-07 Fidelity 遭駭客入侵
- 2011-09-05 竊取個資Android惡意程式現蹤

中國駭客入侵美國商會
2012-01-03

- 美國商會(U.S. Chamber of Commerce)遭到來自於中國的駭客入侵，讀取該會三百萬會員資料的時間可能長達半年，直到美國聯邦調查局(FBI)於2010/5 調查其他資安事故時才意外發現。
- 駭客於2009/11開始進行入侵，可能是利用魚叉式網路釣魚(Spear Phishing)的手法，誘使該商會員工開啟或瀏覽藏有惡意程式的郵件或連結，逐步取得該商會整個網路之管理者權限。
- 駭客在美國商會網路內置入至少6個不同的後門，並連結至大約300個中繼站網址。
- 目前尚不清楚究竟有多少資料遭到駭客竊取，但根據調查的結果顯示駭客集中大部分攻擊資源於該商會4名處理亞洲事務的員工，其所有電子郵件紀錄均遭複製取走。

挪威關鍵企業遭駭客鎖定竊取機敏資訊
2011-12-07

- 包含石油、天然氣及國防相關產業等多家挪威關鍵企業，在2011/11傳出遭駭客鎖定竊取企業機敏資訊。挪威國家安全管理局(National Security Authority, NSM)發言人向媒體表示，駭客集團藉由寄發附有惡意程式或是帶有釣魚網站網址的社交工程電子郵件，針對特定企業進行攻擊。
- 受害者在開啟惡意程式檔案後，該惡意程式會在系統上執行全硬碟掃描，將所有資料壓縮後回傳至駭客指定的國外中繼站。2011年挪威至少發生10件類似的針對性網路攻擊事故，造成的損害難以估計。
- 但這可能只是冰山的一角，可能有更多的受害企業至今仍不知受害，或是為了企業形象而選擇隱瞞受害事實。

資安威脅新趨勢

- 近來越來越多的提供網路身分認驗證機制廠商遭到駭客組織鎖定入侵。
- 一旦提供網路安全與信任之供應商遭入侵淪陷，整個網際網路就會陷入混亂。
- 當身分認驗證安全機制無法被信任，網際網路秩序就無法維持，其後果將不堪設想。

不可不知的社交工程手法

常見手法

- 系統入侵
- 網站掛碼
- 網路釣魚
- 圖片中的惡意程式
- 偽裝系統修補程式
- 即時通訊軟體
- 在電子郵件中隱藏未知陷阱

新一代的網路攻擊手法

- 進階持續性滲透攻擊-Advanced Persistent Threat, APT
- 魚叉式網路釣魚-Spear phishing

APT-進階持續性滲透攻擊

- 簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。

- 以往駭客發動的APT攻擊雖然以政府為主，但從2010年開始企業成為駭客鎖定竊取情資的受駭者越來越多，RSA和Sony是 2011年最大的兩個APT攻擊的目標。他們失去了數百萬客戶的資料，光是完成修復就花費了鉅資。

APT 攻擊特色

- 鎖定特定目標

  針對特定政府或企業，長期間進行有計劃性、組織性竊取情資行為,可能持續幾天，幾週，幾個月，甚至更長的時間。

- 假冒信件

  針對被鎖定對象寄送幾可亂真的社交工程惡意郵件，如冒充長官的來信,取得在電腦植入惡意程式的第一個機會。

- 低調且緩慢

  為了進行長期潛伏,惡意程式入侵後,具有自我隱藏能力避免被偵測,伺機竊取管理者帳號、密碼。

- 客製化惡意元件

  攻擊者除了使用現成的惡意程式外亦使用客制化的惡意元件。

- 安裝遠端控制工具

  攻擊者建立一個類似 Botnet 的遠端控制架構會定期傳送有潛在價值文件的副本給命令和控制伺服器（C&C Server）審查。

- 傳送情資

  將過濾後的敏感機密資料，利用加密方式外傳

魚叉式網路釣魚（Spear phishing）

- 只針對特定目標進行攻擊的網路釣魚攻擊。

- 當進行攻擊的駭客鎖定目標後，會以電子郵件的方式，假冒該公司或組織的名義寄發難以辨真偽之檔案，誘使員工進一步登錄其帳號密碼，使攻擊者可以藉機安裝惡意軟體，竊取機密；或於員工時常瀏覽之網頁中置入病毒自動下載器，並持續更新受感染系統內之變種病毒，讓使用者防不勝防。

- 由於魚叉式網路釣魚鎖定之對象並非一般個人，而是特定公司、組織之成員，故受竊之資訊已非一般網路釣魚所竊取之個人資料，而是其他高度敏感性資料，如智慧財產權及商業機密。

魚叉式網路釣魚（Spear phishing）

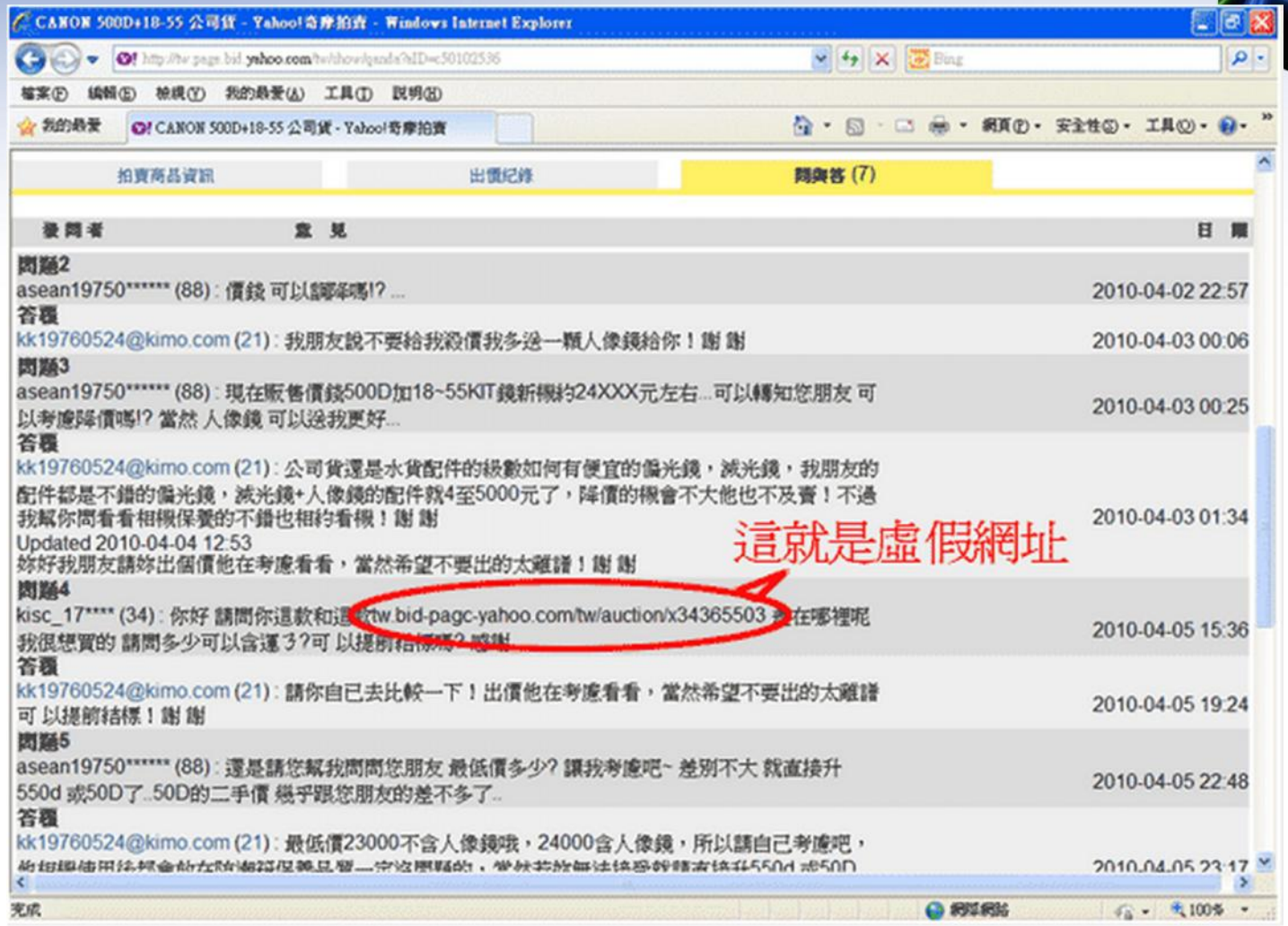
- 混合式的網路釣魚
- 經過萃取過的、潛在威力更強大的網路釣魚
- 針對特定的目標在不安全的網路上放置釣餌，進行誘捕，而非針對廣大的不特定群眾
- 魚叉式網路釣魚比一般的網路釣魚更難偵查。偽造的 email 與網站不僅更像真實的版本的複製，並且還能夠夠過受害者現存的人際關係進行滲透
- 魚叉式網路釣魚不是一般的駭客所為，而是那些更急於得到資金收入、商業祕密、或是軍事情報的老練團體所為

釣魚網站-1　虛構網站

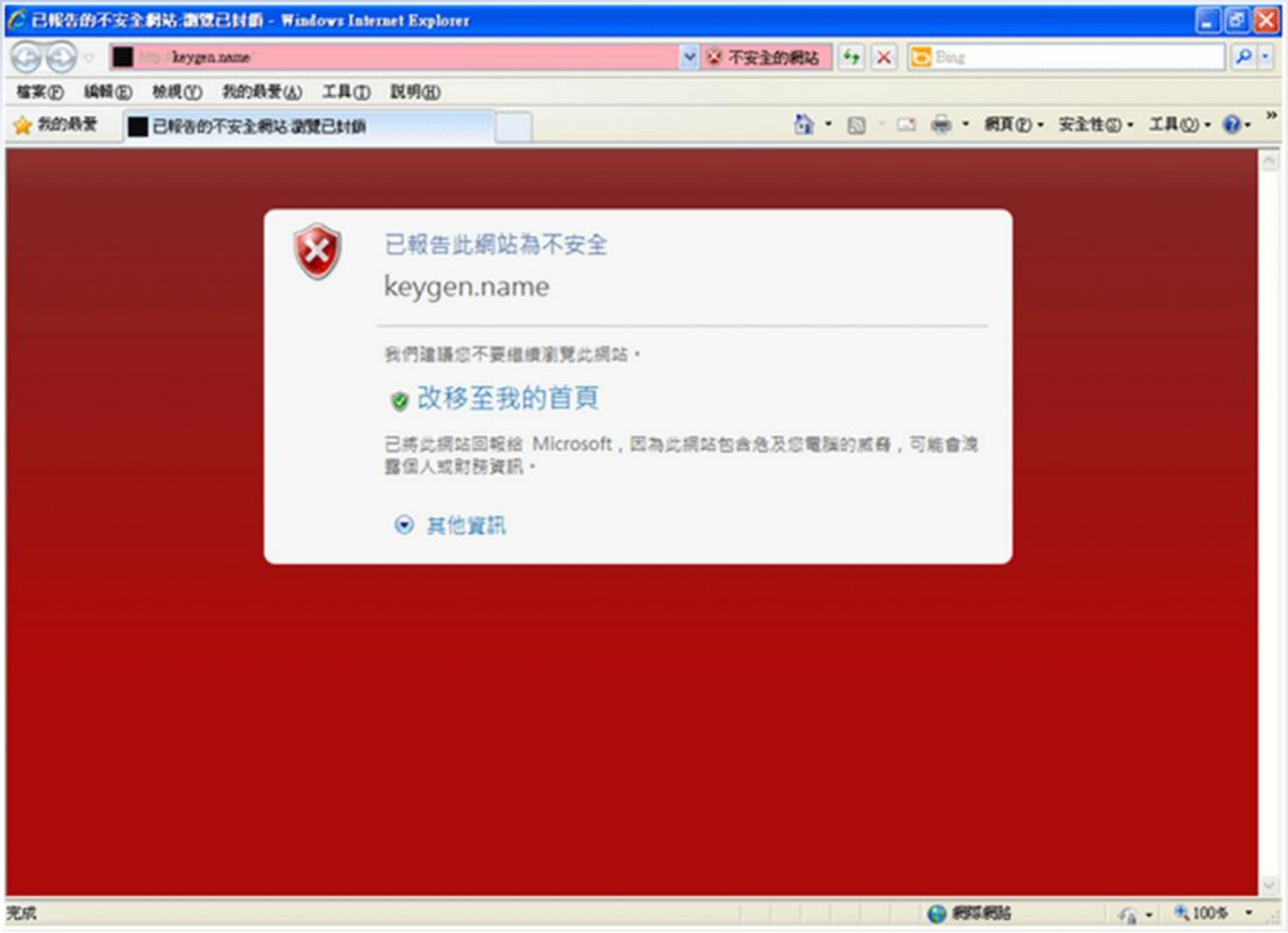
- https://login.yahoo.com/config/mail?.intl=tw

- https://login-yahoo.com/config/mail?.intl=tw

釣魚網站-1　虛構網站


CANON 500D+18-55 公司貨 - Yahoo!奇摩拍賣 - Windows Internet Explorer
拍賣商品資訊
出價紀錄
問與答 (7)
發問者
意見
日期
問題2
asean19750****** (88) : 價錢 可以講嗎嗎!? ...
2010-04-02 22:57
答覆
kk19760524@kimo.com (21) : 我朋友說不要給我殺價我多送一顆人像鏡給你！謝 謝
2010-04-03 00:06
問題3
asean19750****** (88) : 現在販售價錢500D加18~55KIT鏡新機約24XXX元左右...可以轉知您朋友 可以考慮降價嗎!? 當然 人像鏡 可以送我更好...
2010-04-03 00:25
答覆
kk19760524@kimo.com (21) : 公司貨還是水貨配件的級數如何有便宜的偏光鏡，減光鏡，我朋友的配件都是不錯的偏光鏡，減光鏡+人像鏡的配件就4至5000元了，降價的機會不大他也不及賣！不過我幫你問看看相機保養的不錯也相約看機！謝 謝
Updated 2010-04-04 12:53
妳好我朋友請妳出個價他在考慮看看，當然希望不要出的太離譜！謝 謝
2010-04-03 01:34
這就是虛假網址
問題4
kisc_17**** (34) : 你好 請問你這款和這個tw.bid-pagc-yahoo.com/tw/auction/x34365503 在哪裡呢 我很想買的 請問多少可以含運3?可 以提前結標嗎? 感謝
2010-04-05 15:36
答覆
kk19760524@kimo.com (21) : 請你自已去比較一下！出價他在考慮看看，當然希望不要出的太離譜 可 以提前結標！謝 謝
2010-04-05 19:24
問題5
asean19750****** (88) : 還是請您幫我問問您朋友 最低價多少? 讓我考慮吧~ 差別不大 就直接升550d 或50D了..50D的二手價 幾乎跟您朋友的差不多了..
2010-04-05 22:48
答覆
kk19760524@kimo.com (21) : 最低價23000不含人像鏡哦，24000含人像鏡，所以請自已考慮吧，
2010-04-05 23:17
完成
100%

釣魚網站-2　放置惡意程式碼



釣魚網頁分辨測試

- 哪一個是釣魚網站

關於密碼的二三事

- 密碼是抵禦網路犯罪的第一道防線。
- 為每個重要帳戶挑選安全強度高的密碼以及定期加以變更，是非常重要的事。
- 密碼原則
- 強度測試

電子郵件社交工程

電子郵件是最適合做社交工程攻擊的工具

- 可偽裝寄件者
- 低成本且可大量發送
- 容易使用，無技術門檻
- 可輕易利用被害者協助攻擊他人的電子郵件(轉寄電子郵件給親友、同事)

詐騙信件-1

Posta kutunuz, yönetici tarafından belirlenen 2GB depolama sınırını aştı
Şu anda 2.30GB çalışan ve yeni göndermek veya almak mümkün olmayabilir
o kutunuza doğrulayın kadar yollayın. Posta kutunuza tekrar doğrulamak.

Gerekli bilgileri doldurun ve e-posta göndermek için aşağıdaki
(1) E-posta:
(2) Kullanıcı Adı:
(3) Şifre:
(4) Şifre:

teşekkür ederim
sistem yöneticisi

詐騙信件-2

- 您的郵箱已超出存儲限制由管理員設置到2GB
  2.30GB目前的工作，無法發送或接收新
  請在您的郵箱發送，直到驗證它。重新驗證您的郵箱。

  填寫以下所需信息發送電子郵件
  （1）電子郵箱：
  （2）用戶名：
  （3）密碼：
  （4）密碼：

  謝謝
  系統管理員

社交工程演練

電子郵件社交工程演練

- 測試成功定義

- 信件預覽
  - 偵測受測者於收到警覺性測試信件後，預覽信件圖片或內容。

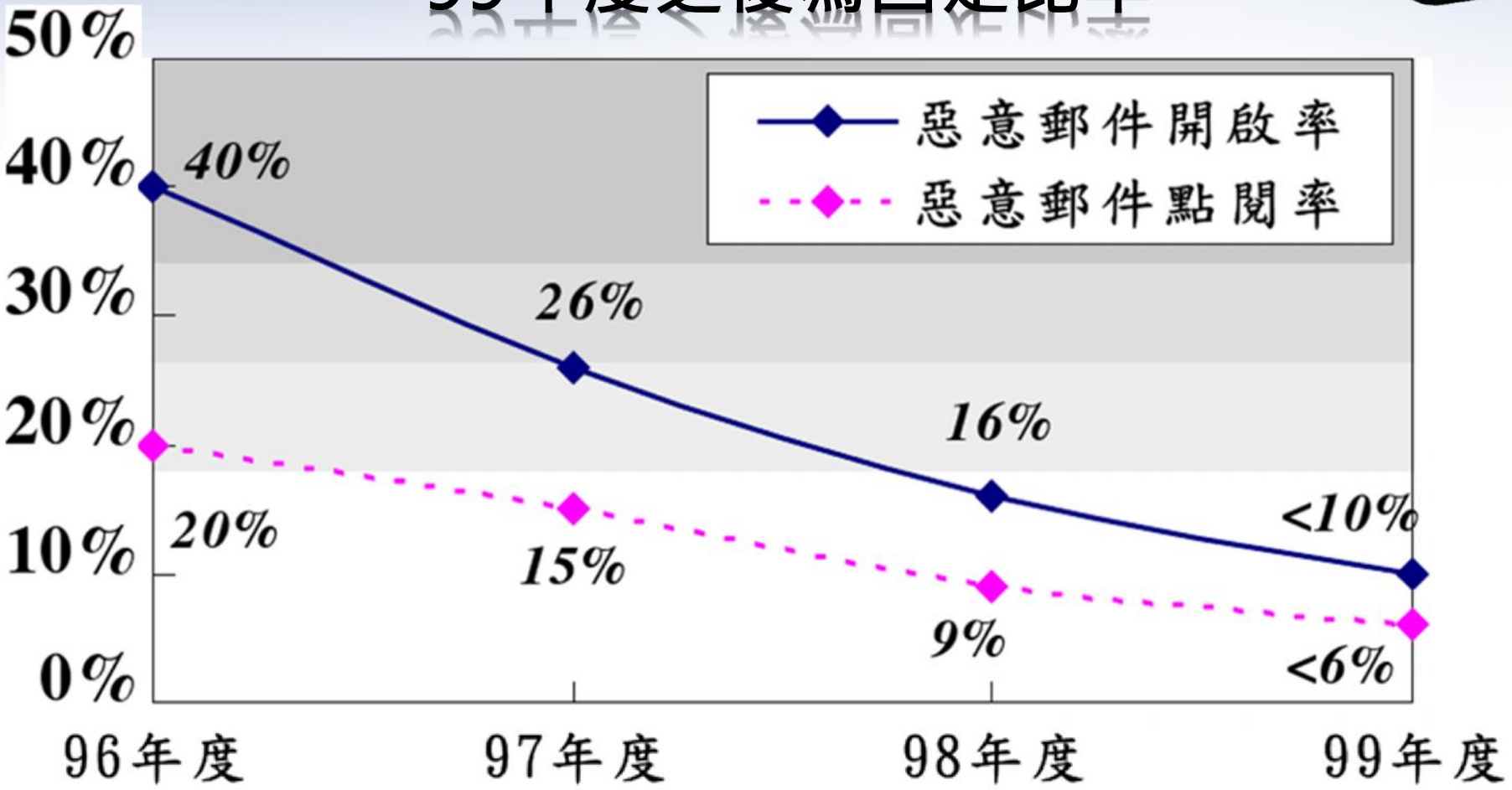
- 連結點選
  - 偵測受測者於收到警覺性測試信件後，開啟信件並點擊信件中之URL連結或附檔。

教育部測試信件分類

編號	信件類別	信件標題
Letter 1	旅遊圖片類	【HiNet 旅遊網】深度旅遊團 超低價好康!!
Letter 2	生活類	五月報稅天 網路報稅讓麻煩省一半！
Letter 3	知識類	超重要！不要再相信網路謠言「生命三角」
Letter 4	科技類	台灣之光！日內瓦展 我發明奪42金 世界第一！
Letter 5	美女類	大陸美女-范冰冰 為了拍 MV 露點也願意！
Letter 6	美容類	完美牙齒整型 五大注意事項
Letter 7	旅遊類	騎鐵馬逛八里 便道成車道 車友爭相樂活
Letter 8	時事類	從日本核災看輻射線對眼球的影響！
Letter 9	財經類	凍漲七年 軍公教終於要加薪了！
Letter 10	健康類	外食族 如何吃得更健康？超商減肥法！
Letter 11	新奇類	巨無霸高麗菜 重 30 台斤超吸睛！

演練目標

99年度之後為固定比率



本校演練結果及合格標準

測試日期	信件開啟率	連結點選率	合格信件開啟率	合格連結點選率
200905	10.22%	0.67%	< 16.0%	< 9.0%
200909	31.87%	16.48%	< 16.0%	< 9.0%
201005	2.44%	0%	< 10.0%	< 6.0%
201009	0%	0%	< 10.0%	< 6.0%
201105	0%	0%	< 10.0%	< 6.0%

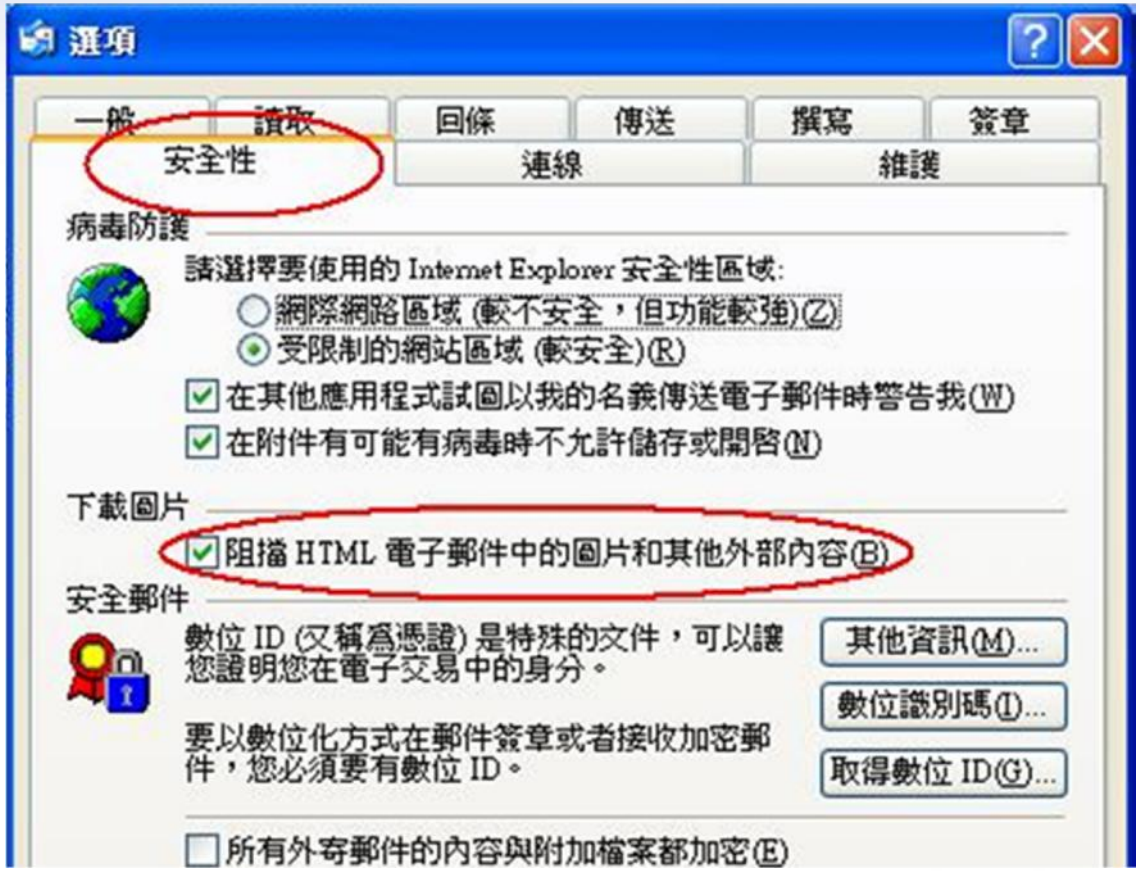
演練結果分析-1

- 不經意的點閱郵件
  - 讀信軟體自動點閱
    - 軟體設定為自動檢閱外部內容
    - 解決之道：關閉外部內容下載。
  - 不經意點選開啟信件檢閱內容
    - 檢視信件時外部內容未呈現，使用者點選『顯示內容』。
    - 解決之道：不點選『顯示內容』。

演練結果分析-2

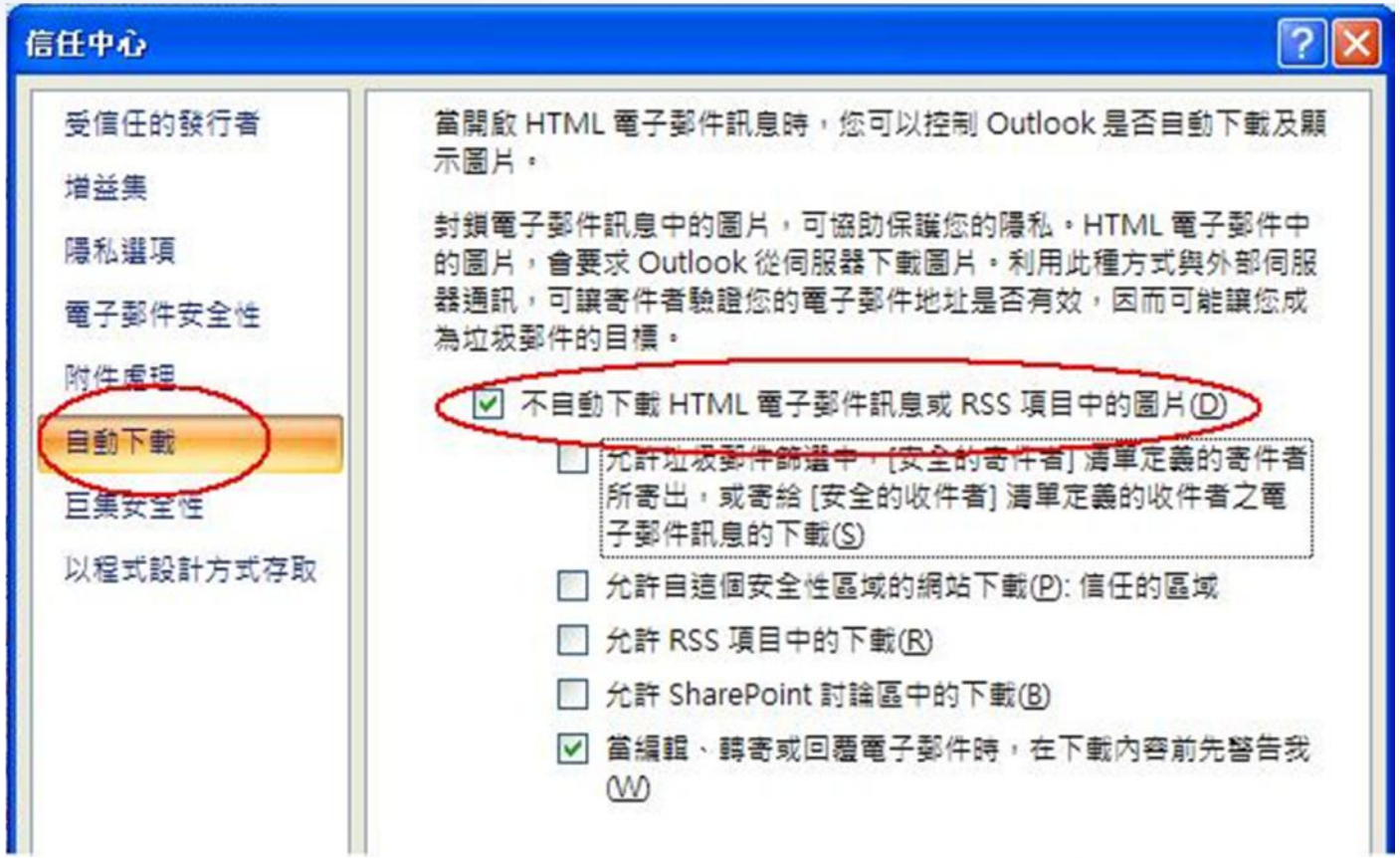
軟體安全性設定-1

- Outlook Express：選擇[工具]->[選項]



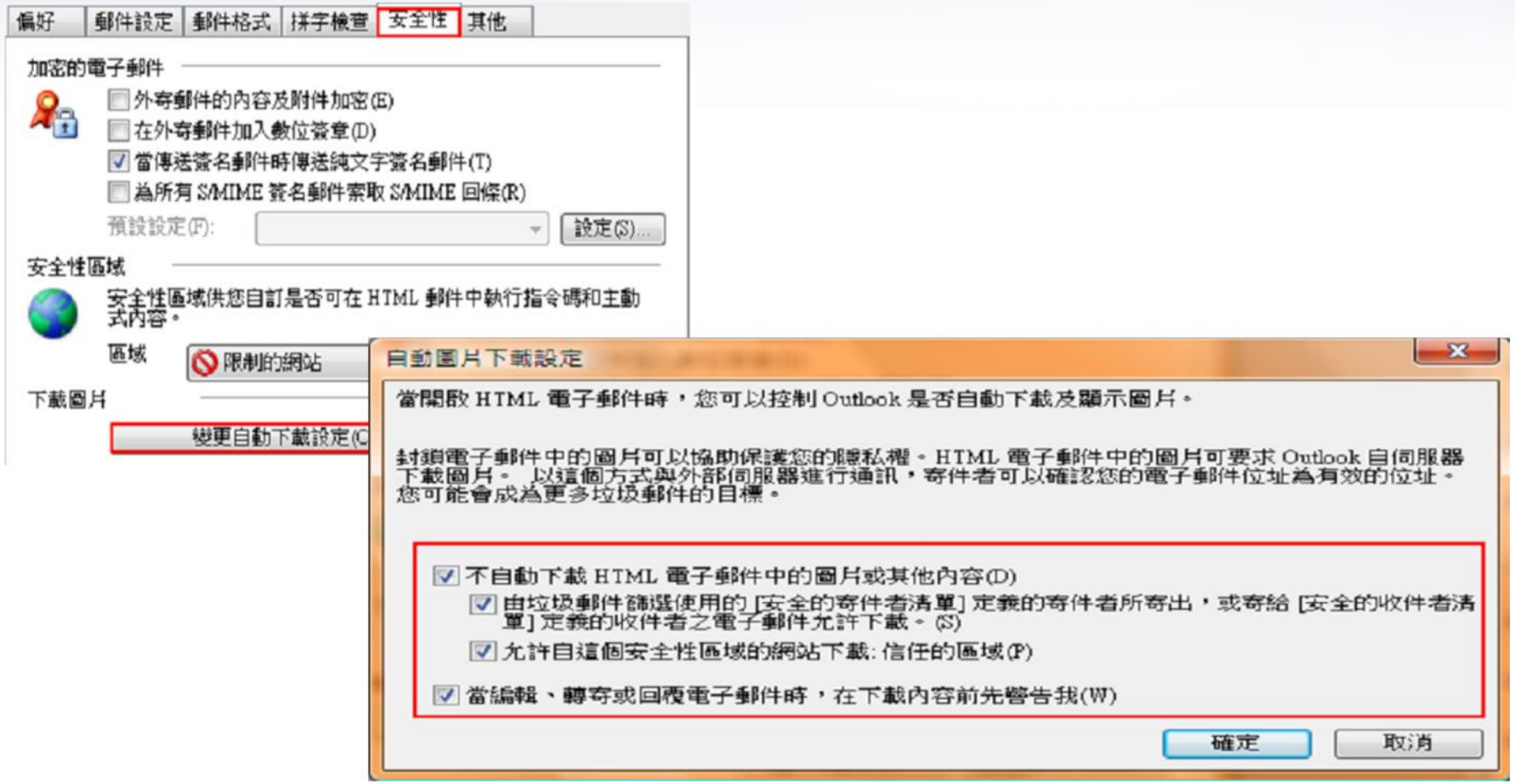
軟體安全性設定-2

- Outlook 2007：選擇[工具]→[信任中心]→[自動下載]



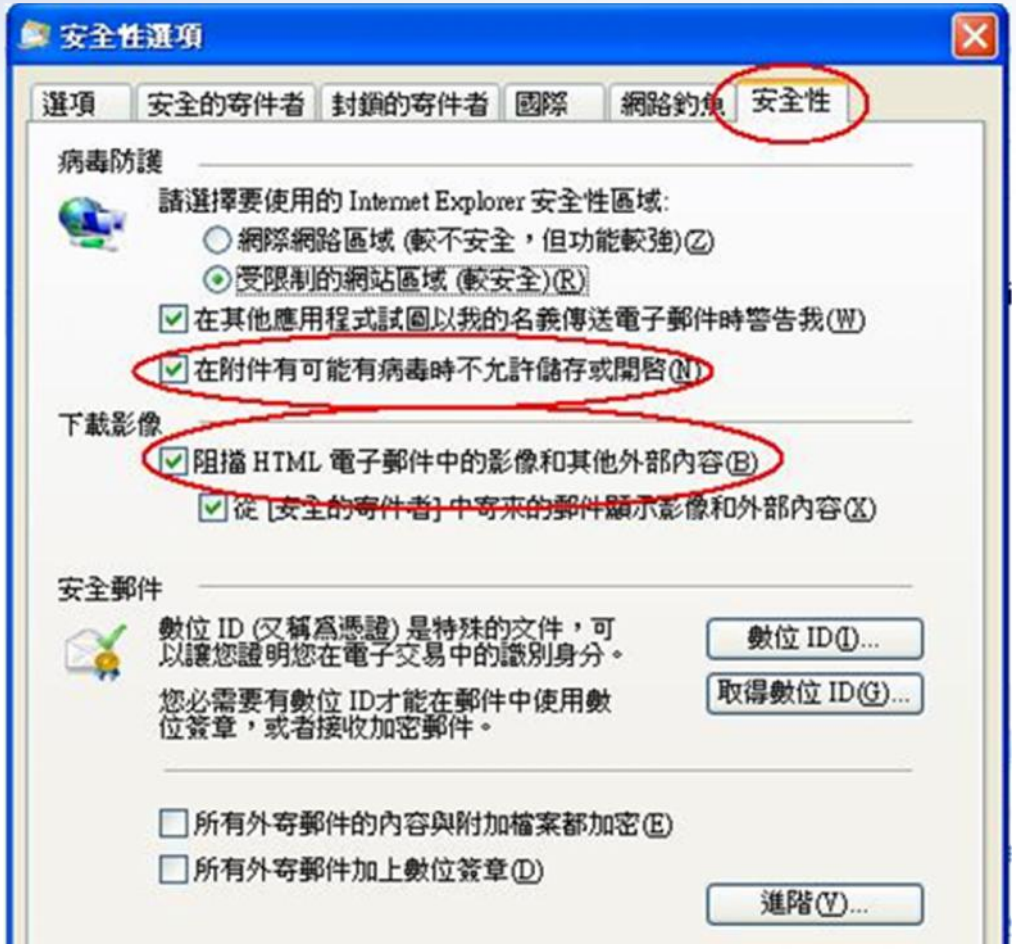
軟體安全性設定-3

- Outlook 2003：選擇[工具]→[選項]→[安全性]點選[變更自動下載]



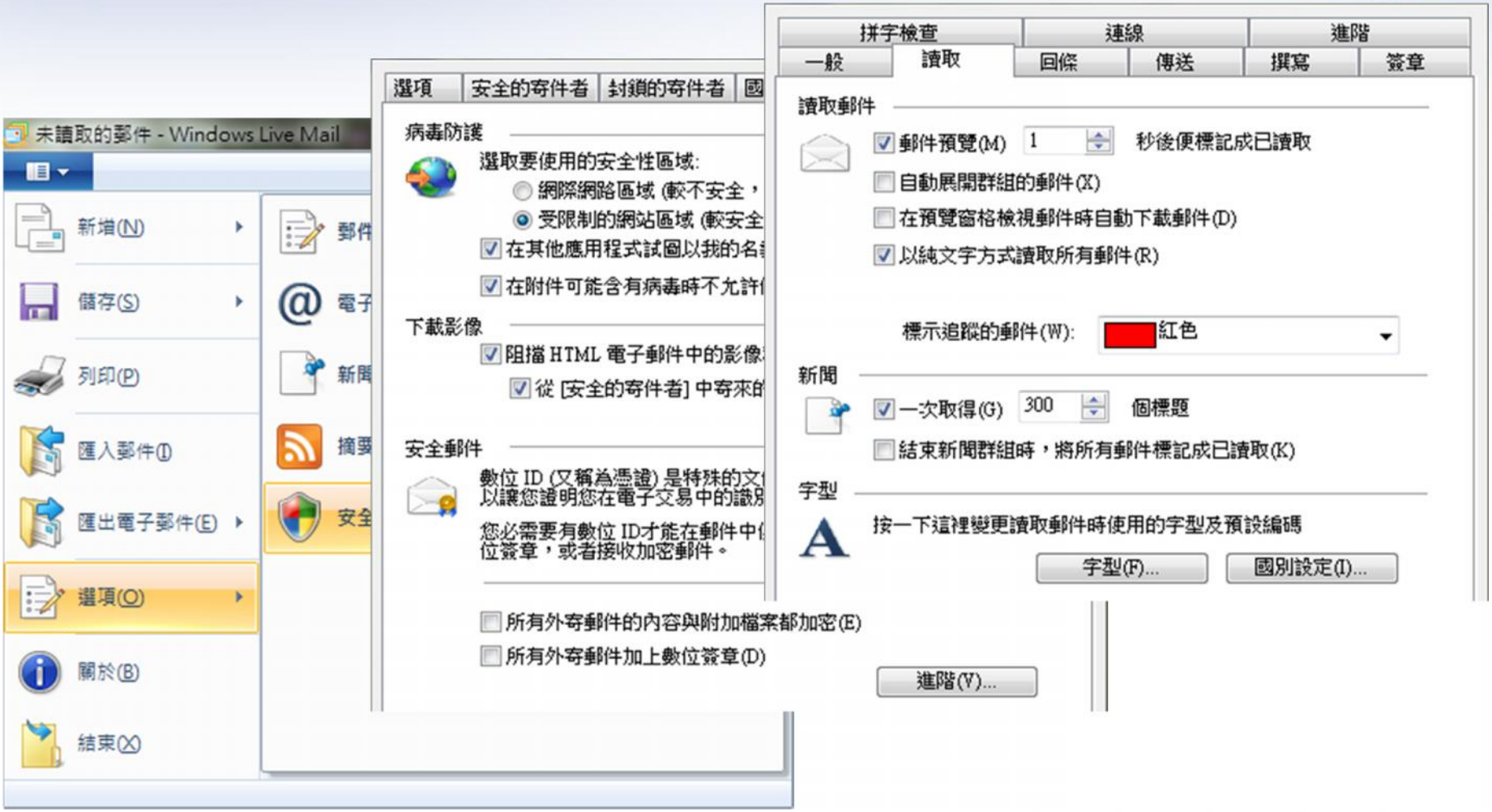
軟體安全性設定-4

- **Live Mail** ：選擇[工具]->[安全性選項]



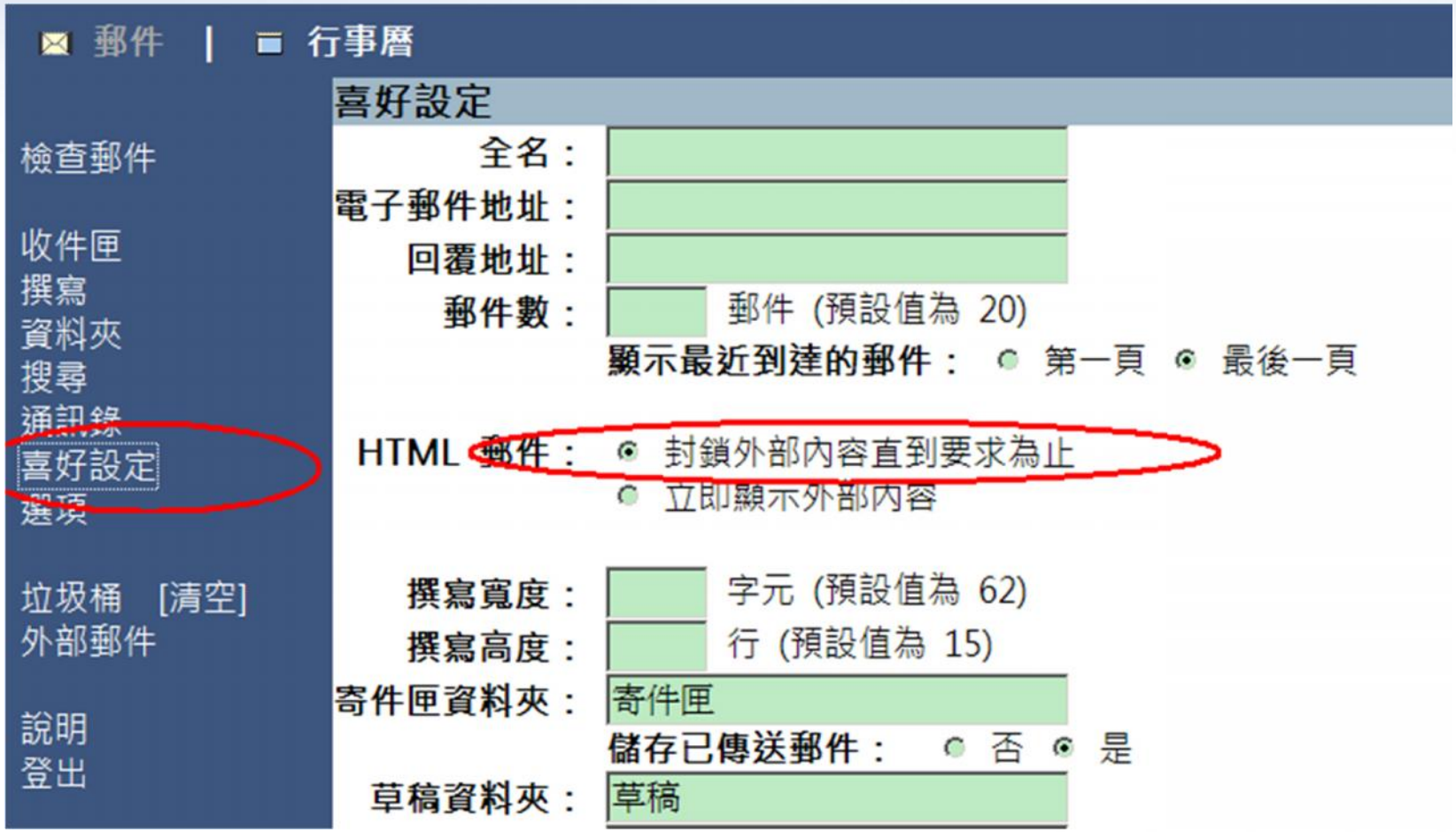
軟體安全性設定-5

- **Live Mail 2011**



軟體安全性設定-6

- 本校Webmail(標準版):點選[喜好設定]



校內模擬演練

本校電子社交工程演練

- 日期：101年5月～ 101年6月
- 實施項目：
  - 教育訓練
  - 實際演練
  - 統計結果
  - 未達目標重複以上步驟直至達成目標為止
- 目標：點閱率<10%、點擊率<6%

本次演練的信件標題

- Dear Email Account User
- 我家有小車神~七歲展現停車特技的小女孩！
- 騎鐵馬逛八里 便道成車道 車友爭相樂活
- 真的哦~ 最近的究表研示 漢字序順並不定一影閱響讀
- 長隧道自保之道 逆行至橫行坑、導坑避難

魚兒上鉤?

淡江大學電子郵件社交工程演練

注意!! 您收到的這封信是模擬的釣魚信

- 勿開啟不明來源信件之連結或附檔。

使用電子郵件應有的警覺性觀念：

1.我為何會收到這封郵件？(寄件者是誰？我認識他嗎？但需注意『寄件者名稱』和『寄件者郵件地址』也是可以假造的！)
2.我是不是應該收到這封郵件？(這封信是不是跟我有關聯？內容是否合理？有沒有威脅利誘的字眼？有沒有詐騙的可能？)
3.我是不是有必要開啟附件或點選連結？
真正危害的動作是開啟附件或點選連結讓電腦被植入惡意程式

- 所有資訊中心發出的通知信都是以中文書寫，並會附上聯絡電話。
- 若收到可疑信件，或對信件內容有疑慮，請先以校內分機查證。

淡江大學資訊中心關心您
ipc@mail.tku.edu.tw

Note: This site is used for email social engineering exercise of Tamkang University.

上級命令

- 行政副校長指示：

全校所有人員必須

將電子郵件軟體設定為安全性設定

總結

- 網路安全必須是一種習慣與文化，而不能只是一種技術與專業。