
# 屏科大教職員生
# 電子郵件安全管理冊

電子計算機中心 教學研究組

電子計算機中心 Computer Center / NPUST

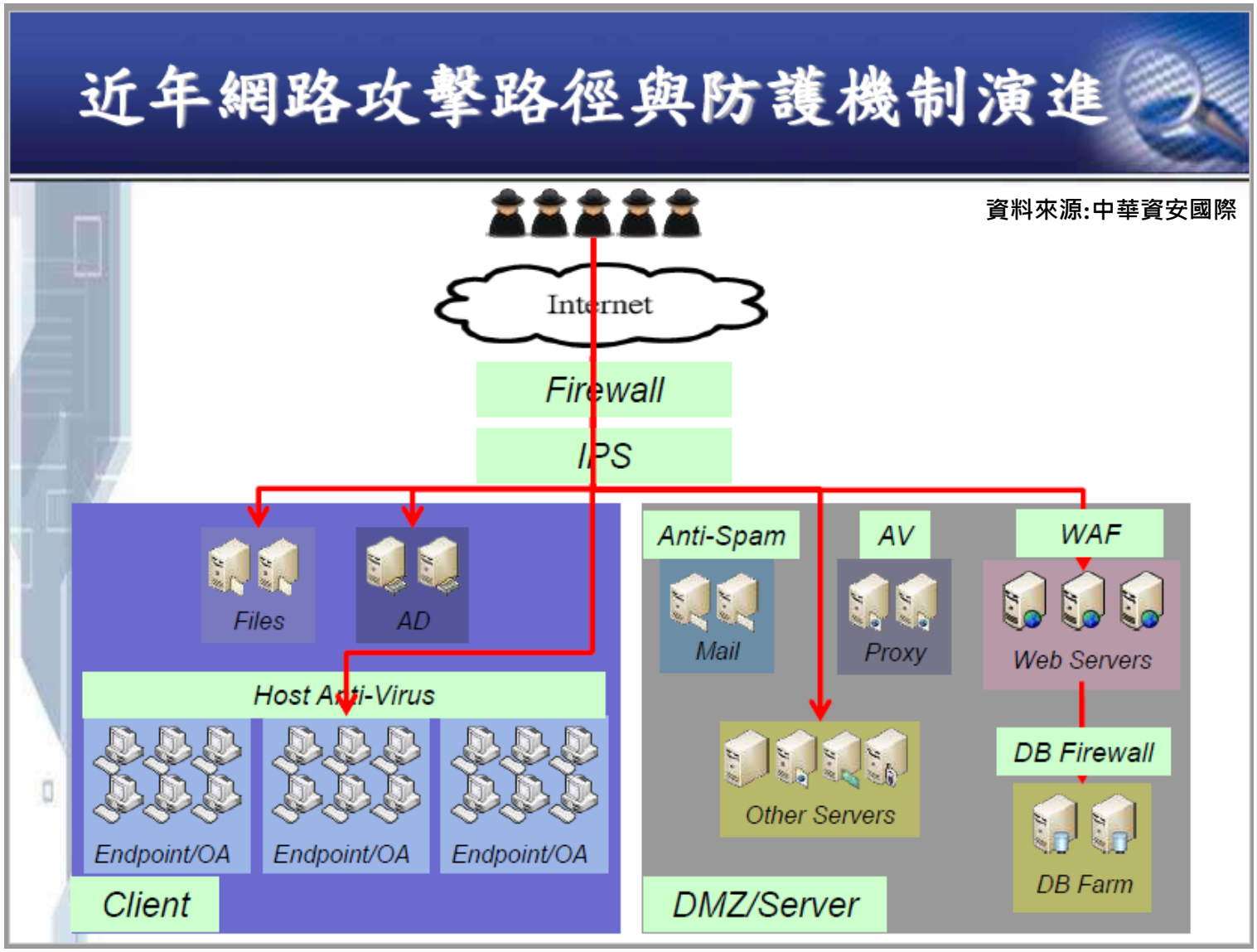
# 源由及目標：

- 參與教育部函每年於**日期約為6月及10月**，針對各校施行兩次電子郵件社交工程演練，進行各校資安風險評比。
- **提升本校教職員生**電子郵件安全管理能力。

# 社交工程釣魚信件型態及現況

- 電子郵件社交工程演練型態從以前的掃網式社交工程演練，近年演變為**針對式的社交工程釣魚信件**，即一對一釣魚信件攻擊(如圖一)，
- 一旦點選釣魚信件(包括開啟郵件、開啟連結與開啟有木馬程式的附檔)有可能駭客利用使用者電腦，遠端執行任意程式碼(例如使用者電腦被當成跳板勒索其他電腦)，此類型信件後續將被教育部通報為資訊安全入侵事件。
- **校內電子郵件過濾系統(Mailgateway)無法自動攔阻針對式釣魚信件，因此教職員需具備電子郵件安全管理能力。**

# 圖一


近年網路攻擊路徑與防護機制演進
資料來源:中華資安國際
Internet
Firewall
IPS
Files
AD
Host Anti-Virus
Endpoint/OA
Endpoint/OA
Endpoint/OA
Client
Anti-Spam
Mail
AV
Proxy
WAF
Web Servers
Other Servers
DB Firewall
DB Farm
DMZ/Server

# 提昇電子郵件安全管理策略作法

## 三方面落實電子郵件優化

- 面對各種瞬息萬變的社交工程郵件樣態的釣魚信件，為落實電子郵件系統優化需**政策面**、**管理面**、**與使用者面**(如圖二)雙管齊下才能從「有做」提升到有效。

造成學校主機被列入黑名單


系統主動攔截大量發信帳號並封鎖 → 中心確認使用者安裝防毒軟體與修改密碼 → 此帳號納入社交工程演練名單 → 辦理資訊安全宣導

# 提昇電子郵件安全管理--「政策面」作法

- **遵循「教育體系電子郵件服務與安全管理指引」：**

1. **各單位辦理公務業務或核心業務時，應使用單位配發之電子信箱收發公務所需資訊，不得使用非公務信箱進行公務郵件收發等事宜。**
2. 參與教育部函每年於**日期約為6月及10月**，針對各校施行兩次電子郵件社交工程演練，進行各校資安風險評比。

# 如何因應教育部工程演練評比

- 教育部評比方式及流程：
  - 由各校提供名單給教育部後，教育部將依各校給名的名單，發送約10個有問題的信件進行演練。
  - **問題信件標題如下**：標題的平易近人，導致使用者無從判斷是否為問題信件。

- 其它學校作法：
  - 教育部IP主機攔截
  - 提供安全名單給教育部

# 如何因應教育部工程演練評比

- 屏科大的作法:

  **1.如何提供安全名單給教育部**

  **2.從政策面、管理面、與使用者落實電子郵件系統優化**

- 名單的提供邏輯：
  - 1.一級主管名單
  - 2.不常使用E-mail名單
  - 3.剔除上一期社交演練問題名單

| 類別 | 項次 | 問題次數 |
|---|---|---|
| 主管 | 1 | 0 |
| 主管 | 2 | 0 |
| 主管 | 3 | 0 |
| 主管 | 4 | 0 |
| 主管 | 5 | 1 |
| 主管 | 6 | 0 |
| 一般人員 | 7 | 0 |
| 主管 | 8 | 2 |
| 一般人員 | 9 | 0 |
| 一般人員 | 10 | 0 |
| 一般人員 | 11 | 0 |
| 一般人員 | 12 | 1 |
| 一般人員 | 13 | 0 |
| 一般人員 | 14 | 2 |

# 提昇電子郵件安全管理--「管理面」作法

## 2. 主動攔截問題發信帳號：

- 由電算中心於電子郵件系統前設置廣告過濾系統攔截大量發信帳號，**對電子郵件特徵（來源IP、寄件人電子郵件地址與信件內容等)實施必要檢查，以強化電子郵件服務安全。**

# 提昇電子郵件安全管理--「管理面」作法

## 2. 建立常見信件功擊範例

- 於電算中心官網(網址：ccnews.npust.edu.tw)建立使用電子郵件最常遇到的信件攻擊範例，供教職生查閱，提高警覺高風險信件。

## 3. 建立有問題的廣告信帳號

- 將曾大量發送廣告信帳號列入次年社交工程演練模擬名單，作為每次辦理社交工程演練教育訓練參考。

## 4. 加強宣導防毒軟體的安裝及更新

- 新進教職員同仁申請電子郵件帳號前需自我確認個人電腦是否已安裝防毒軟體，且定期更新病毒碼，防止病毒攻擊及擴散。

# 提昇電子郵件安全管理--「使用者端」作法

1. 使用者定期參與電算中心辦理的社交工程演練說明會
2. 使用者端須配合定期(180天)登入Mail系統(https://mail.npust.edu.tw)修改密碼(如圖三)
3. 提醒使用者關閉信件預覽功能(以Outlook為例，如圖四)
4. 不隨意開啟來路不明信件與電子郵件附檔或信件內容的連結

# 圖三 定期修改密碼


寫信
信件匣
通訊錄
雲端硬碟
信箱服務
個人設定
信箱安全
登入記錄
密碼設定
舊密碼：
新密碼：
確認密碼：
請再輸入相同的密碼。
密碼提示：
您忘記密碼時給您的提示訊息。
設定密碼
取消

# 圖四 關閉郵件預覽功能


增加多一點說明：登入Outlook後點選「檢視」➔「讀取窗格」➔「關閉」

# 使用者若收到疑似釣魚信件，請切記停看聽三個原則:

**停**

請勿急著開啟來路不明信件

**看**

查看寄件者是否為認識親友，**寄件者名稱是否與寄件者email相符**

**聽**

打電話聯絡電算中心(分機6043)，確認是否為釣魚信件

- 最後提醒使用者若不慎點選釣魚信件，請先不要驚慌，麻煩立即修改電子郵件密碼並離線(隨身硬碟不要插在電腦上)，保存備份重要資料。

- 電子計算機中心關心您，來電請撥校內分機6043吳小姐

# 電子郵件最常遇到的信件攻擊範例

# 範例(一)：信件內有不明超連結

**From:** xx[mailto:xx@mail.npust.edu.tw]
**Sent:** Tuesday, December 24, 2019 5:58 PM
**To:** xx
**Subject:** 安全通知。有人可以访问您的文件。

你好！

您可能已经注意到，我从您的帐户发送了一封电子邮件。这意味着我可以完全访问您的设备。

我已经看了好几个月了。事实是，您通过您访问过的成人网站感染了恶意软件。

如果您对此不熟悉，我会解释。我创建了高质量的间谍软件。它允许我获得对您设备的完全访问权限和控制权。
这意味着我可以在屏幕上看到所有内容，打开相机和麦克风，但您不知道。

我也可以访问您的所有联系人和所有通信。

为什么您的防病毒软件没有检测到恶意软件？回答：：我的恶意软件使用驱动程序，我每4小时更新一次签名，以便您的防病毒软件无声。

我制作了一个视频，展示了你如何在屏幕的左半部分让自己满意，在右半部分，你会看到你观看的视频。
一键！ 您在电子邮件和社交网络中的所有联系人都将收到此视频！ 你的生活将永远改变！我还可以发布您使用的所有电子邮件通信和信使的访问权限。

如果你想阻止这个，将955美元的金额转入我的比特币地址（如果您不知道如何做到这一点，请写信给Google："购买比特币"）。

我的比特币地址（BTC钱包）是：16Wnc2ZhXihhrvD8wuXZVnN3RatYf2Lk7j

收到付款后，我将删除该视频，您将永远不会再听到我的声音。
我给你50个小时（超过2天）付款。我收到了这封信的通知，当你看到这封信时，计时器会起作用。

在某处提交投诉没有意义，因为无法像我的比特币地址那样跟踪此电子邮件。我没有犯任何错误。

如果我发现您与其他人分享了此消息，则视频将立即分发。

祝你好运，再见！

# 範例(二)：寄件者不明

From: mail.npust.edu.tw Virus Protection [mailto:support@autoservice.host]
Sent: Wednesday, January 29, 2020 9:12 PM
To: huangkL@mail.npust.edu.tw
Subject: Virus Warning: Info <info@mail.npust.edu.tw>

**From:**paul.miller@crediserv.net<paul.miller@crediserv.net>
**To:**??<??>
**Date:** Wed, 16 Jan 2019 04:51:45
**Subject:** Your personal discount

Cialis Super Active
**$2.24** per pill
20% OFF

Select pack

SHOW MORE PRODUCTS

The only place where your dream becomes impossible is in your own thinking.

The difference between stumbling blocks and stepping stones is how you use them.

There are two ways of spreading light: to be the candle, or the mirror that reflects it.

All you can change is yourself, but sometimes that changes everything!

Best Regards

**From:**paul.miller@crediserv.net<paul.miller@crediserv.net>
**To:**??<??>
**Date:** Wed, 16 Jan 2019 04:51:45
**Subject:** Your personal discount

Cialis Super Active
**$2.24** per pill
20% OFF

Select pack

SHOW MORE PRODUCTS

The only place where your dream becomes impossible is in your own thinking.

The difference between stumbling blocks and stepping stones is how you use them.

There are two ways of spreading light: to be the candle, or the mirror that reflects it.

All you can change is yourself, but sometimes that changes everything!

Best Regards

# 範例(三)：熟悉的寄件者.....

- 寄件者姓名與寄件的email不符