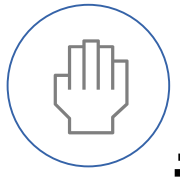
【110年】

# 資安通報演練

基隆市教育網路中心

# 資安通報演練目的



教育部希望透過此次演練檢視所有機關(構)、學校資料更新程度，並了解各區域、縣市網路中心及學校反應能力與熟悉應變流程。

# 資安通報演練期程

一、整備作業自111年8月1日至09月11日止

請更新第一、第二資安聯絡人資料與密碼

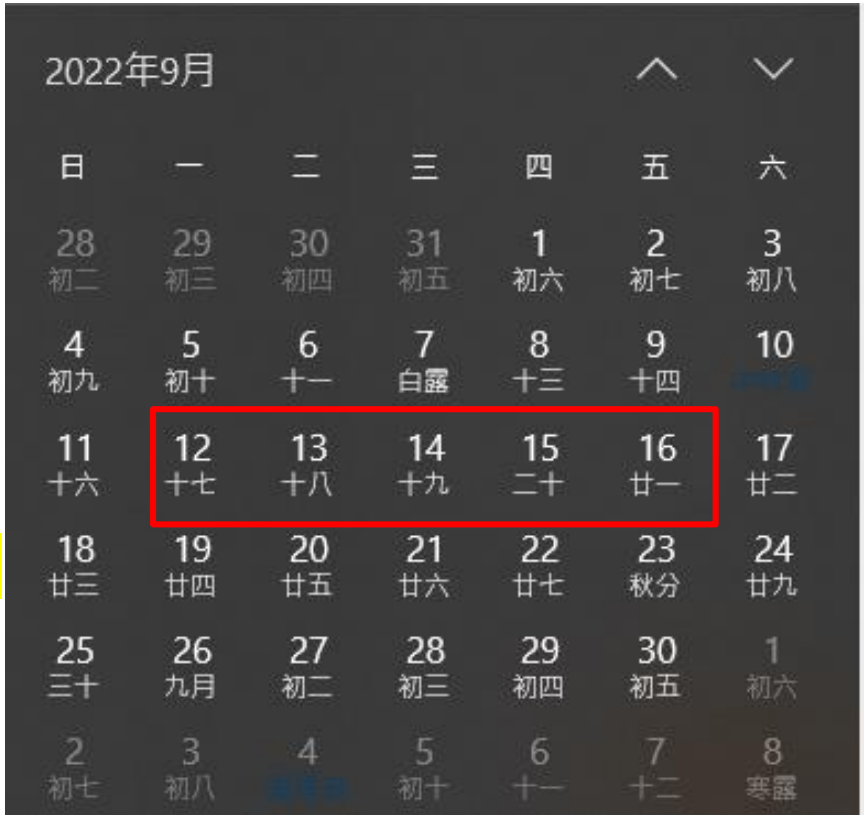
關閉未使用帳號

填寫資安長資料(校長姓名、校長公務EMAIL、校長公務電話)

二、演練作業111年09月12日至09月16日止

主要為前三日，9月12日至9月14日

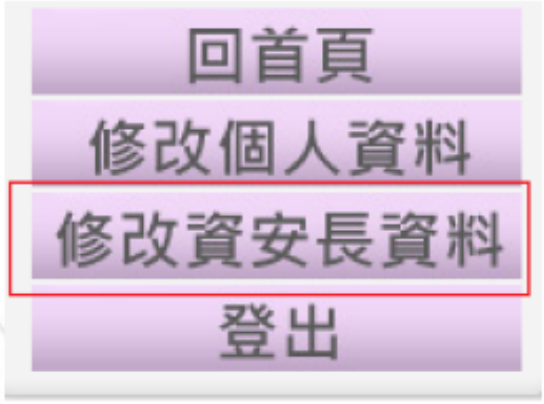
請上資安通報”演練”平台進行通報與應變

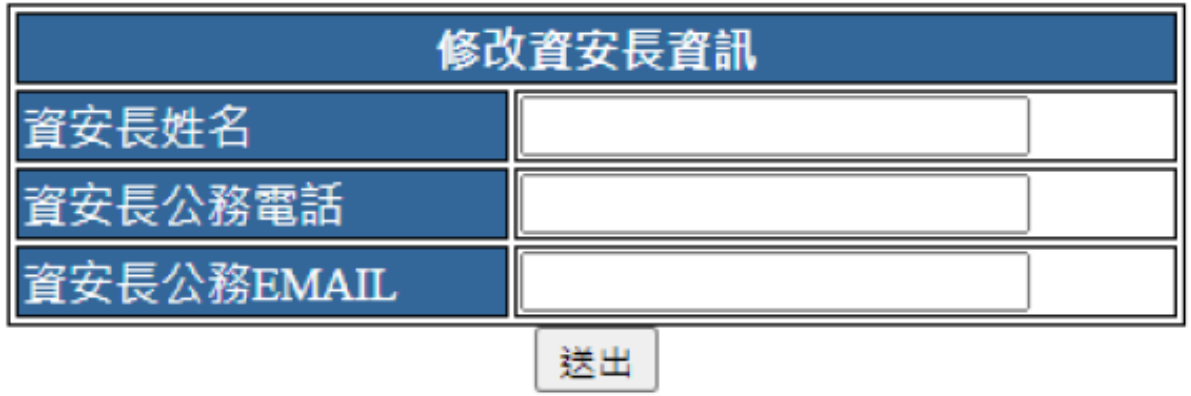


# 新增資安長資訊

資通安全管理法 第2章第11條規定

公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。



# 會員登入

- 使用OID及密碼登入
- 一個單位最多有五位連絡人
- 每個連絡人OID及密碼可不同

**各校帳號請詳公文附件**

# 各校帳號請詳公文附件

| 1. 請第一及第二聯絡人務必於8/1-9/11間變更密碼<br>2. 請填寫資安長資料（校長姓名、校長公務EMAIL、校長公務電話） | | | | |
|---|---|---|---|---|
| 本次是否參與演練 | 演練單位名稱 | 第一聯絡人登入(帳號) | 第二聯絡人登入(帳號) | 第三聯絡人登入(帳號) |
| 是 | 財團法人基隆市輔大聖心高級中學 | 2.16.886.104.100870.100002 | 2.16.886.104.100870.100002.1 | |
| 是 | 財團法人基隆市輔大聖心國民小學 | 2.16.886.104.100870.100001 | 2.16.886.104.100870.100001.1 | |
| 是 | 財團法人崇右影藝科技大學 | 2.16.886.104.101346.100000 | 2.16.886.104.101346.100000.1 | |
| 是 | 國立基隆女子高級中學 | 2.16.886.111.100201 | 2.16.886.111.100201.1 | |
| 是 | 國立基隆特殊教育學校 | 2.16.886.111.100304 | 2.16.886.111.100304.1 | |
| 是 | 國立基隆高級商工職業學校 | 2.16.886.111.100267 | 2.16.886.111.100267.1 | |
| 是 | 基隆市七堵區七堵國民小學 | 2.16.886.111.90001.90006.100000 | 2.16.886.111.90001.90006.100000.1 | |
| 是 | 基隆市七堵區五堵國民小學 | 2.16.886.111.90001.90006.100002 | 2.16.886.111.90001.90006.100002.1 | |
| 是 | 基隆市七堵區尚仁國民小學 | 2.16.886.111.90001.90006.100006 | 2.16.886.111.90001.90006.100006.1 | |
| 是 | 基隆市七堵區長興國民小學 | 2.16.886.111.90001.90006.100007 | 2.16.886.111.90001.90006.100007.1 | |
| 是 | 基隆市七堵區堵南國民小學 | 2.16.886.111.90001.90006.100003 | 2.16.886.111.90001.90006.100003.1 | |
| 是 | 基隆市七堵區復興國民小學 | 2.16.886.111.90001.90006.100005 | 2.16.886.111.90001.90006.100005.1 | |
| 是 | 基隆市七堵區華興國民小學 | 2.16.886.111.90001.90006.100001 | 2.16.886.111.90001.90006.100001.1 | |
| 是 | 基隆市七堵區瑪陵國民小學 | 2.16.886.111.90001.90006.100004 | 2.16.886.111.90001.90006.100004.1 | |
| 是 | 基隆市中山區中山國民小學 | 2.16.886.111.90001.90005.100001 | 2.16.886.111.90001.90005.100001.1 | |
| 是 | 基隆市中山區中和國民小學 | 2.16.886.111.90001.90005.100006 | 2.16.886.111.90001.90005.100006.1 | |
| 是 | 基隆市中山區中華國民小學 | 2.16.886.111.90001.90005.100003 | 2.16.886.111.90001.90005.100003.1 | |

# 修改個人資料-更新第一、第二聯絡人資料與密碼

需於111/8/1至9/11期間更新


**修改個人資料**

| | |
|---|---|
| 機關名稱 | 中山大學營運團隊 |
| 帳號 | v2.16.886.111.100008.2 |
| 單位電話 | 07-5250211 * |
| 傳真 | |
| 地址 | 高雄市鼓山區蓮海路70 * |

**聯絡人資料(1)**

| | |
|---|---|
| 聯絡人姓名 | 張明達 * |
| 職稱 | 研究助理 * |
| 聯絡人電話 | 07-5250211 |
| 聯絡人手機號碼 | 09XXXXXXXX * |
| 聯絡人E-MAIL | service@cert.tanet.edu.t * |

**變更密碼**

| | |
|---|---|
| 目前密碼 | * |
| 新密碼 | * |
| 確認密碼 | * |

送出 重填

| 連絡人順序 | 連絡人名稱 | 連絡人EMAIL |
|---|---|---|
| 第二連絡人 | 第二連絡人 | service@cert.tanet.ed |
| 第三連絡人 | | |
| 第四連絡人 | | |
| 第五連絡人 | | |

個人基本資料區

密碼變更區

以大小寫英文、數字、符號至少擇其二種組合成8碼以上之密碼

單位其他連絡人資料區

# 忘記帳號密碼流程

需於111/8/1至9/11期間更新

1. 帳號不知道：請先致電教網中心詢問 (02)24591311#836

1. 忘記密碼：
   1) 若已知舊的第一(二)聯絡人相關資料
      →請直接致電「資安通報平台」詢問密碼。(07)525-0211
      →因為該平台承辦人會與您核對目前系統內「舊的」第一(二)聯絡人之姓名、電話、email等資料後，會重設密碼，改將重設密碼寄給新承辦。
   2) 若未知舊的第一(二)聯絡人相關資料
      →可致電教網中心先行詢問舊資料供核對。(02)24591311#836
      →再行致電「資安通報平台」詢問密碼。(07)525-0211

**各校帳號請詳公文附件**

# 帳號管理-關閉未使用者帳號(第三到第五)

# 資安通報演練作業

111年09月12日至111年09月16日止

## 演練方式

- 本次演練將以郵件及簡訊傳送「資安演練事件通知單」形式進行
  - 通知信的E-Mail：service@cert.tanet.edu.tw 設為白名單，避免接收不到重要演練通知
  - 簡訊號碼為0911516652、0903447787、0907173177、0961231612，此為網路平台發送，故請確認手機號碼是否有取消「阻擋廣告簡訊服務」，避免收不到重要簡訊通知。
- 事件單編號皆以「DRILL」開頭進行編碼。
- 模擬之10種情境樣本以亂數方式分別發送至所有演練學術單位
- 演練學術單位於收到mail及簡訊通知後，應於1小時內至演練平台完成事件通報流程與應變處理並結案。

資安通報演練平台　https://drill.cert.tanet.edu.tw

# 資安通報演練作業

## (一、二級事件)模擬之10種情境樣本 111年09月12日至111年09月16日止

| 模擬狀況編號 | 攻擊事件說明 |
|---|---|
| 1 | 單位網站被置入詐騙網頁，誘導使用者至釣魚網站 |
| 2 | 單位電腦被入侵，而成為BotNet所控制的Bot主機 |
| 3 | 單位內電腦被入侵，並被利用來進行遠端桌面(RDP)暴力攻擊 |
| 4 | 單位電腦被入侵，並利用散佈電子郵件 |
| 5 | 單位內 IoT 設備使用預設帳號密碼，遭駭客入侵 |
| 6 | 單位內網站具有跨網站腳本攻擊(Cross site scripting ，簡稱 XSS) 的漏洞，可能造成瀏覽者的危害 |
| 7 | 單位內主機被植入勒索病毒，系統資料遭到加密 |
| 8 | 發現單位電腦系統被植入惡意程式，並對外進行APT 攻擊 |
| 9 | 發現單位電腦系統被入侵，並進行挖礦惡意行為 |
| 10 | 單位人員誤將個人資料置於公開網路上，導致外部人員可下載相關資訊 |

# 資安通報演練作業

111年09月12日至111年09月16日止

## (三、四級事件)演練模擬重大資安事件情境樣本

此次演練為配合教育部內針對資訊安全3級與4級事件通報流程演練，將於各梯次抽選單位進行3級與4級事件派發，收到之單位依演練流程完成通報應變作業。

| 模擬狀況編號 | 重大事件說明 |
| --- | --- |
| 1 | 單位含有學生個資 (姓名、身分證字號等 )被置於網站上，並造成 個資外洩。 |
| 2 | 攻擊者利用合法帳號密碼以單位VPN主機做為跳板，取得資料庫之相關敏感個人資料，造成個資外洩事件。 |

# 資安通報演練作業

111年09月12日至111年09月16日止

發送之演練簡訊及電子郵件之告知訊息範例如後：

(一) 簡訊格式與範例：

格式：(告知通報演練)[受測單位],[事件類型]警訊,[事件編號],請盡速至平台完成事件處理。

範例1：(告知通報演練)[國立XX大學],[入侵攻擊]事件警訊,[15],請盡速至平台完成事件處理。

範例2：(告知通報演練)[國立YY大學],[網頁攻擊]事件警訊,[16],請盡速至平台完成事件處理。

(二) 電子郵件主旨格式與範例：

郵件主旨欄格式：(事件單編號： DRILL-2021-XX( 告知通報演練)[事件類型 ]事件警報

範例1：(事件單編號：DRILL-2021-15)(告知通報演練)入侵攻擊事件警報)

範例2：(事件單編號：DRILL-2021-16)(告知通報演練)網頁攻擊事件警報)

# 告知通報表單填寫


**聯絡資訊**

| | |
|---|---|
| 機關名稱:基隆市教育網路中心<br>使用者:陳莞華 | 教育機構資安通報應變小組<br>聯絡電話:07-525-0211<br>E-Mail:service@cert.tanet.edu.tw |

回首頁
修改個人資料
登出

通報
事件審核
新進告知通報
事件單處理狀態
逾時事件單
歷史通報
事件附檔下載
資安預警事件

| 事件單編號 | 單位名稱 | 通報時間 | 應變時間 | 距通報時間(小時) | 流程 |
|---|---|---|---|---|---|

Page 1/1

# 告知通報表單填寫


新進告知通知報圖例。

點擊工單編號(數字)後會出現通報流程表單，

◆ 表單分為兩大項：

第一項是發生資安事件之機關聯絡資料(毋須填寫，會自動顯示)

第二項是因外在因素產生資安事件時的通報事項

**新增【確認時間】**

新增「確認時間」並於事件確認後**一小時內**完成通報流程。(所以事件通報應變時效不因新增確認時間而改變)

## 4. 資通安全事件：基本資料

事件分類：

INT（入侵攻擊）：
- 系統被入侵(資訊設備遭惡意使用者入侵)
- 對外攻擊(對外部主機進行攻擊行為)
- 針對性攻擊(針對特定個人的資訊洩漏與身分盜取)
- 散播惡意程式(主機對外進行惡意程式散播)
- 中繼站(主機成駭客之中繼站，接收惡意程式連線)
- 電子郵件社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
- 垃圾郵件(Spam)(資訊設備從事Spam Mail散播行為)
- 命令與控制伺服器(C&C)(主機疑似為駭客之Botnet C&C Server)
- 殭屍電腦(Bot)(資訊設備疑似成為駭客所控制之Botnet成員)
- 其它類型的入侵攻擊

DEF（網頁攻擊）：
- 惡意網頁(網頁遭駭客置換或放置不當內容)
- 惡意留言(網頁遭駭客放上惡意留言)
- 網頁置換(網頁遭駭客置換)
- 釣魚網頁(主機遭駭客置入釣魚網頁)
- 個資外洩(主機遭個資外洩)
- 其它類型的網頁攻擊

破壞程度：(文字勿超過200中文字，標點符號請用全形)

經Tanet Cert告知本校IP：xxx.xxx.xxx.xxx疑似成為Bot的成員。經查xxx.xxx.xxx.xxx為本校無線認證閘道器，疑似下轄的電腦受BotNet入侵。

事件說明：(文字勿超過200中文字，標點符號請用全形)

經Tanet Cert告知本校IP：xxx.xxx.xxx.xxx疑似成為Bot的成員。經查xxx.xxx.xxx.xxx為本校無線認證閘道器，疑似下轄的電腦受BotNet入侵。

**破壞程度**
**事件說明**
**填寫相同即可**

**影響範圍及損失評估**

**5. 資通安全事件：影響等級及說明**

1. 事件等級：取底下三個欄位中最高等級當成最後之事件等級
2. 第3、4級事件係屬於重大資安事件，教育部各長官需親自督導進度
3. 若有3、4級事件，請立刻電話告知您所屬的主管機關
4. 如果您無法確定如何填寫時，請電話連絡您所屬的主管機關請求協助
5. 等級0之資安事件教育部另有規範，請至少填入等級1

資安事件判斷：

(1) 機密性衝擊 -

- 無（0級）
- 1級-非核心業務資料遭洩漏
- 2級-非屬密級或敏感之核心業務資料遭洩漏
- 3級-密級或敏感公務遭洩漏
- 4級-國家機密資料遭洩漏

(2) 完整性衝擊 -

- 無（0級）
- 1級-非核心業務系統或資料遭竄改
- 2級-核心業務系統或資料遭輕微竄改
- 3級-核心業務系統或資料遭嚴重竄改
- 4級-國家重要資訊基礎建設系統或資料遭竄改

(3) 可用性衝擊

- 無（0級）
- 1級-非核心業務運作遭影響或短暫停頓
- 2級-核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作
- 3級-核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作
- 4級-國家重要資訊基礎建設運作影響或系統停頓，無法於可容忍中斷時間內回復正常運作

資安事件綜合評估等級：1級：一般資安事件

可能影響範圍及損失評估（文字勿超過200字，標點符號請用全形）

本校對外網路頻寬可能受影響。

**6. 是否需要支援?**

- 是
- 否:通報單位自行解決

你的上層機關負責人為: 王言俊
聯絡電話:02-2459-1311
E-mail:AA4220@mail.kl.edu.tw
期望支援方式:
電話告知 Email告知

**建議通報流程與應變流程一起完成。**

7. 是否同時進行通報流程與應變流程?

是 (請繼續完成 II.應變流程之作業)　否 (會先完成 I.通報流程 並結束，後續時間請儘快完成 II.應變流程)

## 應變流程

1. 緊急應變措施：已中斷網路連線，待處理完成後再上線 / 已停止伺服器之服務，待處理完成後再上線 / 直接處理完成，解決辦法詳見【解決辦法】 / 其它

2. 解決辦法：(文字勿超過200中文字, 標點符號請用全形)

全面清查xxx.xxx.xxx.xxx下轄的電腦，如有異常則先行下線，待重新安裝作業系統後才上線。

**解決辦法**

3. 解決時間：

## 改善措施

改善辦法：(文字勿超過200中文字,標點符號請用全形)

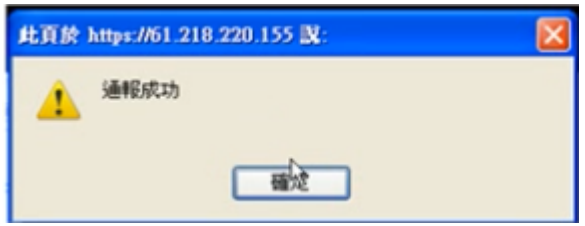
依資通安全相關管理規範進行改善措施

改善時間：2019-05-24 14:37:36

發布通報

**新增【改善措施】**

各連線單位於完成通報應變後，針對事件提出相關改善措施，以完備事件處理流程及預防事件重複發生。



# INT事件填寫範例(僅供參考)

| 事件類型 | 破壞程度/事件說明 | 影響範圍與損失 | 解決辦法 |
|---|---|---|---|
| 系統被入侵 | xxx.xxxx.xxx.xxx疑似受駭客入侵。 | xxx.xxxx.xxx.xxx主機無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 對外攻擊 | xxx.xxxx.xxx.xxx疑似受惡意程式感染，對外攻擊其它主機。 | 本校對外網路頻寬可能受影響。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 針對性攻擊 | xxx.xxxx.xxx.xxx疑似被駭客植入後門程式，針對特定主機進行攻擊。 | 本校暫時無損失 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 散播惡意程式 | xxx.xxxx.xxx.xxx疑似受惡意程式感染，對外散佈惡意程式。 | 本校對外網路頻寬受影響。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 中繼站 | xxx.xxxx.xxx.xxx受BOTS感染而成為中繼站。 | 本校對外網路頻寬受影響。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 電子郵件社交工程攻擊 | xxx.xxxx.xxx.xxx電子郵件伺服器疑似受駭客入侵，對外大量散佈社交工程郵件。 | xxx.xxxx.xxx.xxx郵件主機無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新清查帳號及修補系統漏洞後才上線。 |
| 垃圾郵件SPAM | xxx.xxxx.xxx.xxx電子郵件伺服器疑似受駭客入侵，對外大量散佈垃圾郵件。 | xxx.xxxx.xxx.xxx郵件主機無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新清查帳號及修補系統漏洞後才上線。 |
| 命令與控制伺服器(C&C) | xxx.xxxx.xxx.xxx受BOTS感染而成為C&C伺服器。 | 本校對外網路頻寬受影響。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 殭屍電腦BOT | xxx.xxxx.xxx.xxx受BOTS感染而成為殭屍網路(BOTNET)的一員。 | 本校對外網路頻寬受影響。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 其它類型的入侵攻擊 | 以上隨便填一個 | 以上隨便填一個 | 以上隨便填一個 |

# DEF事件填寫範例(僅供參考)

| 事件類型 | 破壞程度/事件說明 | 影響範圍與損失 | 解決辦法 |
|---|---|---|---|
| 惡意網頁 | xxx.xxxx.xxx.xxx疑似受駭客入侵，植入惡意網頁。 | xxx.xxxx.xxx.xxx網站無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 惡意留言 | xxx.xxxx.xxx.xxx網站討論區受XSS攻擊。 | xxx.xxxx.xxx.xxx網站討論區無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx討論區關閉，待修補程式漏洞後才上線。 |
| 網頁置換 | xxx.xxxx.xxx.xxx疑似受駭客入侵，網頁內容遭置換。 | xxx.xxxx.xxx.xxx網站無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 釣魚網頁 | xxx.xxxx.xxx.xxx疑似受駭客入侵，遭植入釣魚網頁。 | xxx.xxxx.xxx.xxx網站無法正常運作。 | 暫時將xxx.xxxx.xxx.xxx主機離線，待重新安裝作業系統後才上線。 |
| 個資外洩 | xxx.xxxx.xxx.xxx疑似受駭客入侵或使用者不慎，將個資外洩。 | 本校可能面臨法律責任。 | 暫時將xxx.xxxx.xxx.xxx主機離線，並保存相關證據，交檢調機關處理 |
| 其它類型的網頁攻擊 | 以上隨便填一個 | 以上隨便填一個 | 以上隨便填一個 |

# 注意事項

1. 演練期間還是會有真實事件發生
   - 將「演練事件」填到「資案通報演練平台 」https://drill.cert.tanet.edu.tw
   - 將「真實事件」填到「資案通報平台 」https://info.cert.tanet.edu.tw
2. 建議9/12-9/14在學校期間，請切記手機不要離身（上課時間可調震動）。
3. 依據往年經驗，演練非隨機抽考，各校幾乎都會收到演練通報。
4. 收到簡訊或信件，請逕行登入演練網站進行演練。

✔建議可以用收到的mail進行連結，再行通報比較不會有錯

✔如果你連到的網站，找不到簡訊或是Mail中的事件單就代表你連錯網站了! 請不要點擊自行通報。

# 演練事件通知單內容範例

**範例　　教育機構資安通報【演練平台】**

教育機構資通安全演練事件通知單

演練事件類型：入侵事件警訊

演練事件單編號：DRILL-INT-2022-xx

| | | | |
|---|---|---|---|
| 原發布編號 | DRILL-INT-2022-xxxx | 原發布時間 | 2022-09-xx xx:xx:xx |
| 演練事件類型 | 中繼站 | 原發現時間 | 2022-09-xx xx:xx:xx |
| 演練事件主旨 | 單位內主機[XXX.XXX.XXX.XXX] 遭受殭屍(Bot)惡意程式感染，對外進行攻擊。 | | |
| 演練事件描述 | 該主機可能被植入 Bot 程式而成為殭屍網路(BotNet)中的一員而受到惡意攻擊者的控制。並持續以 IRC（Internet Relay Chat）封包持續與惡意的 C&C(Command and Control)伺服器連線，<br>而被入侵偵測系統所偵測。 | | |
| 手法研判 | 由於該主機具有 MS08-067 弱點，可能受到殭屍(Bot)惡意程式利用而被感染 | | |
| 建議措施 | 建議立即採取下列步驟：<br>1.檢查該系統上是否有不明程式正大量對外建立網路連線(如 TCP Port 139、445)。<br>2.主機之管理者/使用者查明來源主機的發起攻擊行為之原因為何，若為非預定安裝程式所引發，建議直接移除該程式，並詳加檢測貴單位主機是否有任何的異常狀況。<br>3.進行該主機全系統病毒掃描後，安裝最新的系統安全修正程式。 | | |
| 此演練事件需要進行通報，請 貴單位資安聯絡人登入資安通報演練平台進行通報應變作業 | | | |
| 如果您對此通告的內容有疑問或有關於此演練事件的建議，歡迎與我們連絡。 | | | |

# THANKS !