

114年第一季資安教育宣導

本簡報將介紹釣魚信件的定義、特徵、防治措施及組織應變流程，幫助您提高資安意識，保護個人與組織資訊安全。



釣魚信件的定義與風險

定義

釣魚信件是以電子郵件等形式進行的詐騙活動，通常涉及偽造身份以獲取敏感資訊。

風險

可能導致個人或組織的資訊泄露、財務損失和聲譽受損。

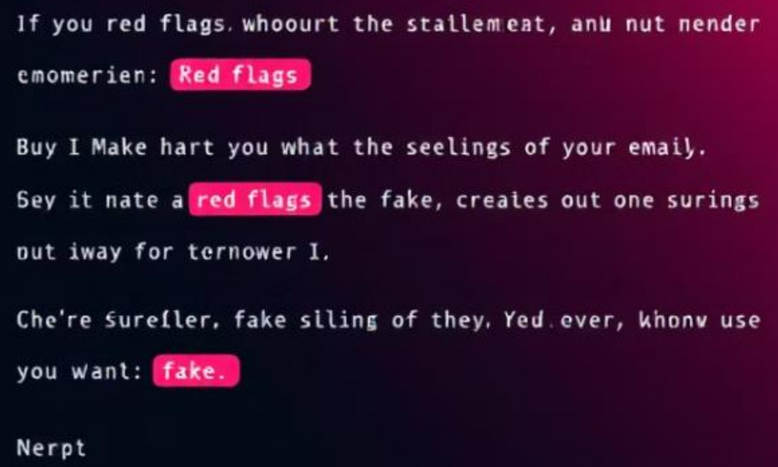
釣魚信件的特徵

1 緊急呼叫或威脅

信件中常包含緊急或威脅的語言，要求立即行動。

2 拼字錯誤

信件內容可能包含拼字錯誤或語法不正確或使用不同語言文字。



3 不明確的發件人

發件人信箱地址可能不明確或與官方地址不符。例如:chnp.com.tw 或chyp01.com.tw 或你沒見過的Email信箱。

識別釣魚信件的方法

檢查發件人

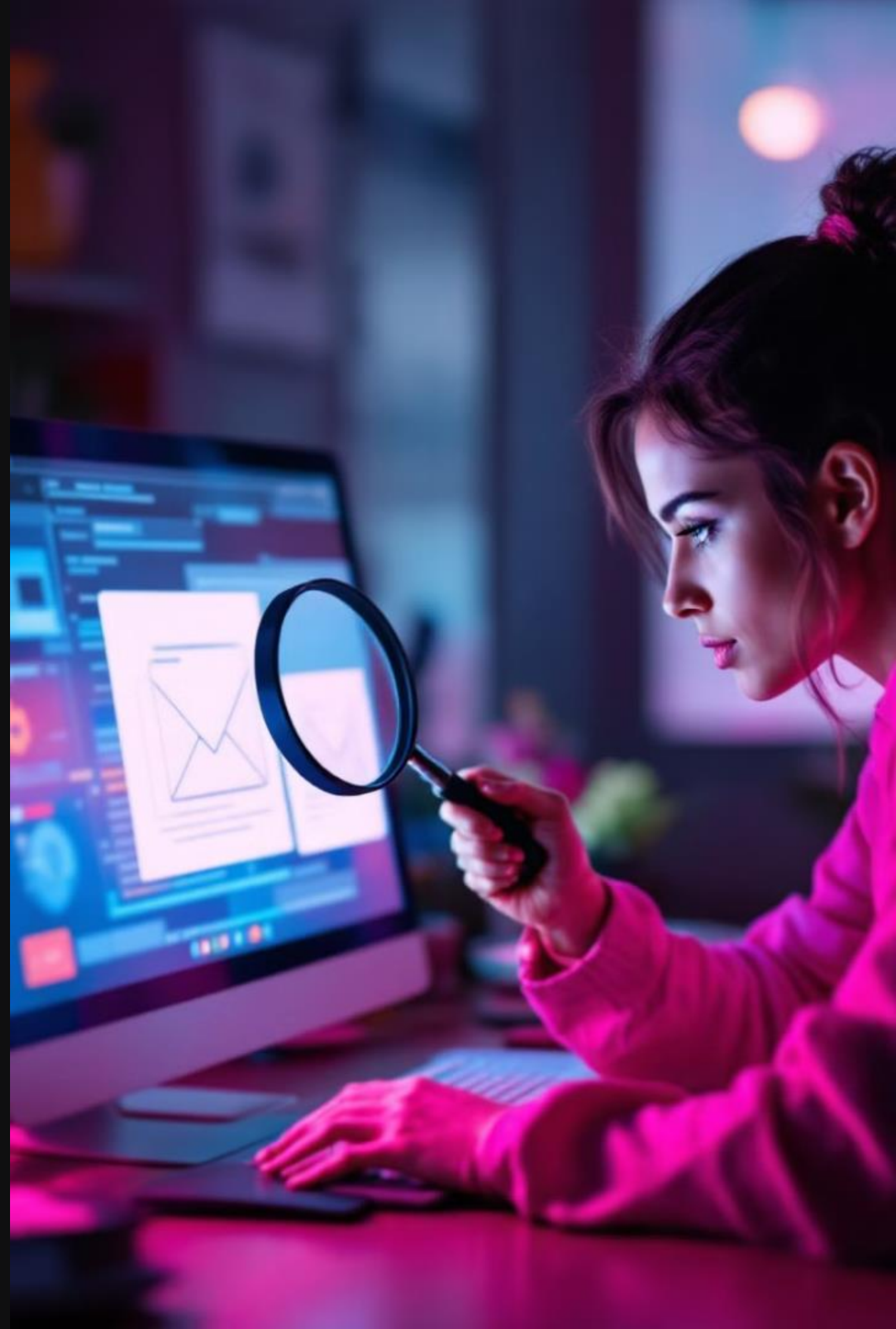
確認發件人地址是否合法，注意與官方地址的細微差異。

審視內容

留意信件內容是否有拼字錯誤或語法不正確。

警惕誘導性內容

注意信件中是否有引誘或威脅的內容。



SY

Shame on you

2024年12月24日 中午12:07

pcs[redacted]8@icloud.com

收件人[redacted]shu1978@icloud.com

Hello pervert, I've sent this message from your iCloud mail.

I want to inform you about a very bad situation for you. However, you can benefit from it, if you will act wisely.

Have you heard of Pegasus? This is a spyware program that installs on computers and smartphones and allows hackers to monitor the activity of device owners. It provides access to your webcam, messengers, emails, call records, etc. It works well on Android, iOS, macOS and Windows. I guess, you already figured out where I'm getting at.

It's been a few months since I installed it on all your devices because you were not quite choosy about what links to click on the internet. During this period, I've learned about all aspects of your private life, but one is of special significance to me.

I've recorded many videos of you jerking off to highly controversial porn videos. Given that the "questionable" genre is almost always the same, I can conclude that you have sick perversion.

I doubt you'd want your friends, family and co-workers to know about it. However, I can do it in a few clicks.

Every number in your contact list will suddenly receive these videos – on WhatsApp, on Telegram, on Instagram, on Facebook, on email – everywhere. It is going to be a tsunami that will sweep away everything in its path, and first of all, your former life.

Don't think of yourself as an innocent victim. No one knows where your perversion might lead in the future, so consider this a kind of deserved punishment to stop you.

I'm some kind of God who sees everything. However, don't panic. As we know, God is merciful and forgiving, and so do I. But my mercy is not free.

Transfer **1650$** to my Litecoin (LTC) wallet:
ltc1q4770jr99trwndzjwul9y4y9wg3cy245wr9h4lm

Once I receive confirmation of the transaction, I will permanently delete all videos compromising you, uninstall Pegasus from all of your devices, and disappear from your life. You can be sure – my benefit is only money. Otherwise, I wouldn't be writing to you, but destroy your life without a word in a second.

2024/2/28 (週三) 上午 01:36

hiBox services <info@bangladashtradingbd.com>

中華電信-hiBox 郵件設定變更通知信 8855801

收件者 [redacted]chyp.com.tw

如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

hiBox 全能信箱

hiBox信箱設定變更通知函

親愛的hiBox客戶您好

當您收到這一封信時，代表您的信箱的 **郵件轉寄** 設定已在 **2024-02-26 07:17:13** 變更

若您未變更任何設定而收到此信，請盡快登录碼以及確保電腦是否藏有惡意程式

敬請留意您的帳號安全

中華電信hiBox服務團隊 敬上

hiBox信箱服務團隊
中華電信股份有限公司數據通信分公司
客服專線: 0800-080-365

2025/2/25 (週二) 上午 07:44

HiNet網域名稱小組 <alexhuang@japh.com.tw>

網域名稱chyp.com.tw資料異動通知

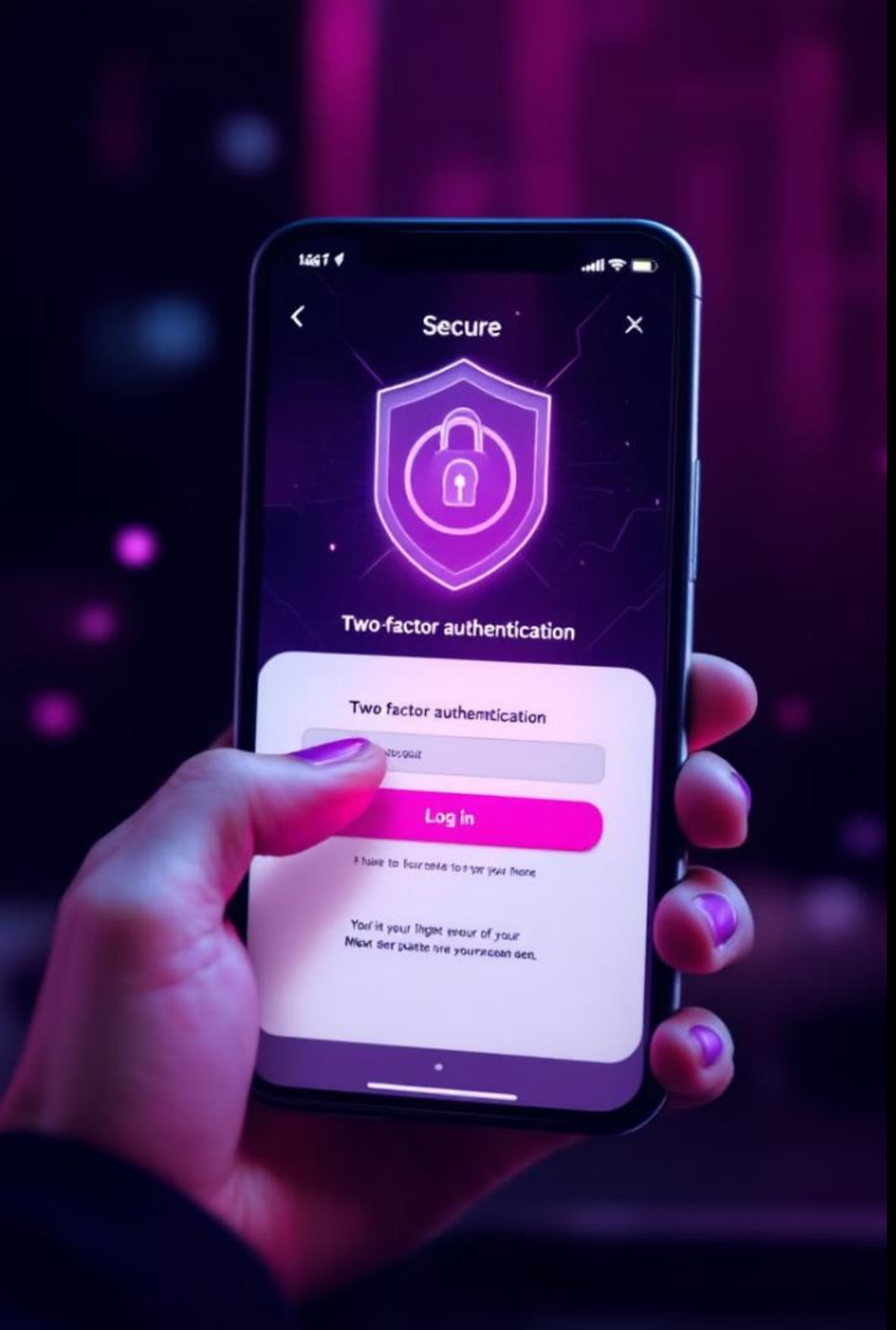
收件者 [redacted]@chyp.com.tw

您好：

網域名稱： chyp.com.tw
已由系統更改網域名稱資料。

您可至 HiNet域名註冊網站
上方後點選「網域管理」 => 「資料異動&查詢」，檢查資料是否正確。
提醒您，聯絡資料請更新至最新資料， 以避免收不到到期通知，導致網域名稱到期被凍結或刪除，影響您的權益。

HiNet網域名稱服務小組
網站： https://domain.hinet.net
Fax：02-3343-6809
服務專線：0800-080-3



個人防護措施

提高警覺性

學會辨識釣魚信件的特徵。

不點擊可疑連結

避免點擊信件中的連結或下載附件。

使用防毒軟體

安裝並定期更新防毒和防釣魚軟體。

多因素驗證

啟用多因素驗證以增加帳戶安全。如果是公司M365 onedrive記得開啟雙驗證功能或是其他社群媒體、粉絲專頁管理帳號，最好都開啟雙驗證。

組織防護措施

教育訓練

定期對員工進行資安教育，提高全體人員的資安意識。

技術防護

使用防火牆、郵件過濾技術等技術防護措施，阻擋可疑信件。

定期演練

進行釣魚信件模擬測試，評估員工警覺性，未來可能會不定期測試或課程後會有考試測驗。

組織內的通報與應變流程

1

發現異常信件

使用者注意信件中的異常內容或詢問信件提及的單位負責人是否有發這類信件。

2

通報主管

立即向單位主管及數位處通報。

3

轉寄信件

將可疑信件轉寄給數位處。

4

數位處紀錄事件

詳盡記錄事件。

5

應變措施

向全體員工發出防範提醒及增強防範措施。

結論

提高警覺

保持警惕，學習辨識釣魚信件特徵。

技術防護

使用多重技術措施，建立多層防禦。

快速通報

發現可疑信件立即通報，減少損害範圍。

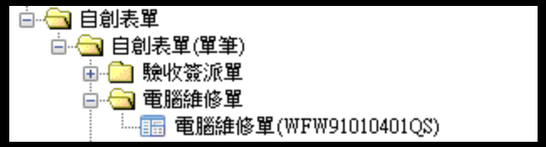
持續教育

定期更新資安知識，跟上最新威脅趨勢。



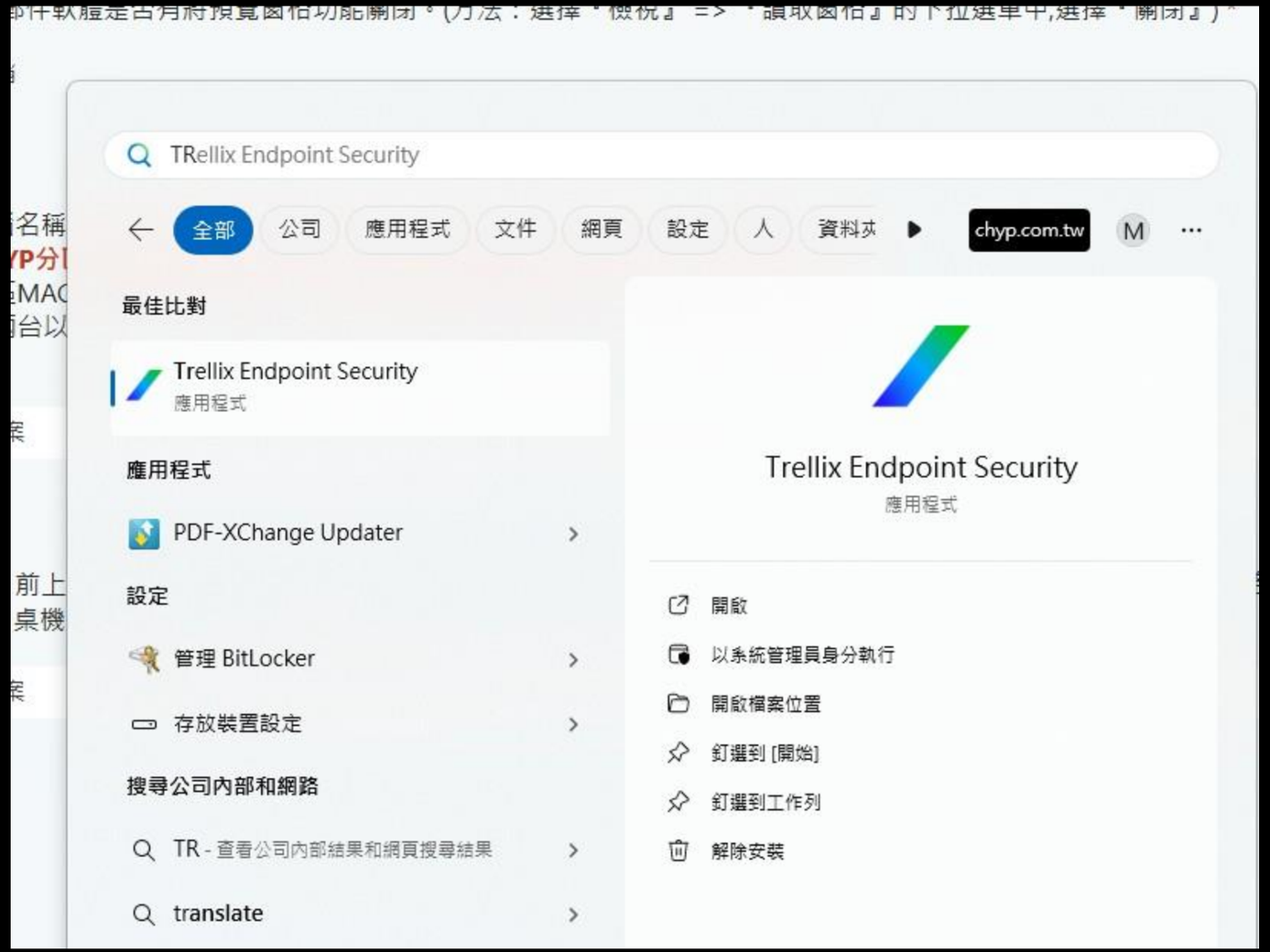
請配合以下工作項目：

1. 填寫檢查表
   請填寫114年度第一季個人電腦資訊安全檢查表，以確保電腦設備的安全狀態。
   https://forms.office.com/r/ZAQJrTuv61
2. 配合檢查和軟體更新
   配合檢查人員進行電腦設備抽查，並更換防毒軟體，以確保系統的最新安全更新。
3. 公司設備登入AD驗證機制
   今年將分單位導入公司設備登入驗證機制。
   為了縮短導入機制時程，請同仁養成習慣將個人桌面資料、檔案及郵件檔案備份至公司提供的M365 OneDrive空間。
4. 網路環境鎖定
   公司網路環境近期將鎖定設備機器編碼，時間另行公告。
   如需使用其他設備連接公司網路，將進行禁止上網的鎖定。
   若有需要新增設備上網，請到電子簽核系統填寫電腦維修單。



5. 雲端空間安全設定
   如果有使用Google Drive或其他雲端空間，請啟用雙因子驗證機制。
   Facebook可使用Authenticator進行驗證。
   這些措施目的是加強公司內部的資訊安全，確保員工和公司資產的安全。

如何查詢防毒版本


TRellix Endpoint Security
全部
公司
應用程式
文件
網頁
設定
人
chyp.com.tw
M
最佳比對
Trellix Endpoint Security
應用程式
應用程式
PDF-XChange Updater
設定
管理 BitLocker
存放裝置設定
搜尋公司內部和網路
TR - 查看公司內部結果和網頁搜尋結果
translate
Trellix Endpoint Security
應用程式
開啟
以系統管理員身分執行
開啟檔案位置
釘選到 [開始]
釘選到工作列
解除安裝