

維護社會安寧
MAINTAIN SOCIAL SECURITY.



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

機關安全與公務機密維護



報告人：

花蓮縣調查站副主任 張進明

2022.1.13



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

報告大綱

01

機關安防介紹

04

資通安全工作

02

防制滲透工作

05

意見交流

03

機密維護工作





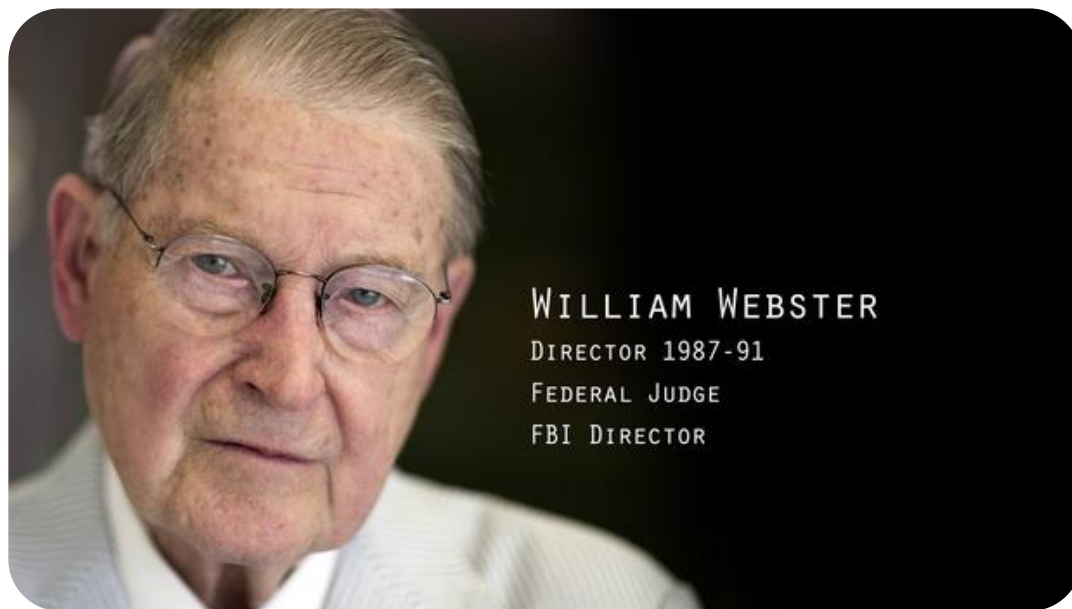
MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

1

機關安防介紹

前中情局長韋伯斯特：
假如逮捕了間諜，表示反情報工作有了問題；
假如沒逮捕間諜，還是表示反情報工作有了問題，你只能**二者擇其一**。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!



機關安全防護

- 機關設施危害之預防及風險管理
- 偶發意外之應變處置



防制滲透工作

- 預防境外敵對勢力的滲透
- 發掘長期埋伏之可疑份子



機密維護工作

- 保護機關公文及資料
- 保護民眾個人資料



資通安全工作

- 機關資訊安全之規劃、教育訓練、推動、執行及稽核





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

全國保防工作會報 法務部調查局關鍵基礎設施安全 防護實施作業要點

- 8大類別324目標
- 含重點目標177個、次要目標147個，著重國家安全
- 與政府運作相關者。
- 建構安全防護網絡、機先蒐報情資

- 結合三大保防體系（機關、軍中、社會）
- 各級政風機構督導



- 各調查處站清查、檢討加強轄區CI目標布置狀況
- 研提相關安全防護缺失及策進作為

- 法源依據：「調查局組織法」、「政風人員設置管理條例」、「全國安全防護會報設置要點」



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!



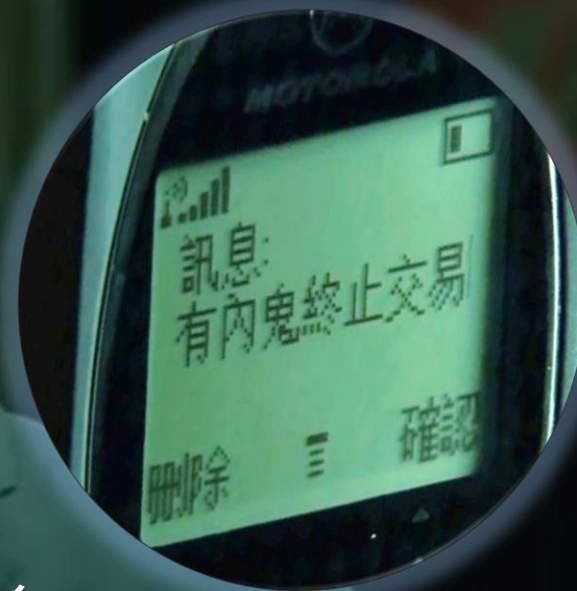
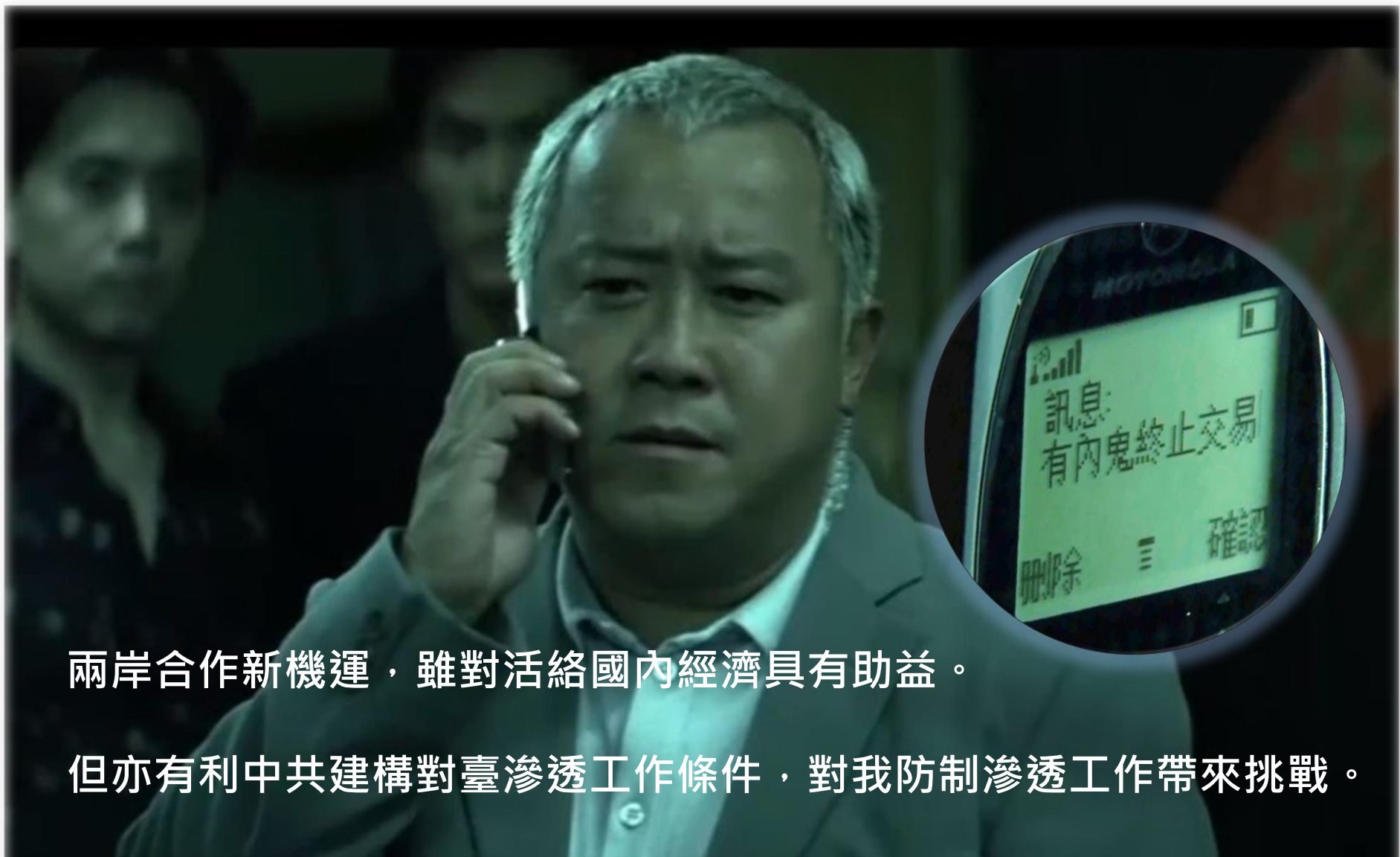
2

防制滲透工作



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!



兩岸合作新機運，雖對活絡國內經濟具有助益。

但亦有利中共建構對臺滲透工作條件，對我防制滲透工作帶來挑戰。



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!





MJIB
法務部調查局

軍情局上校羅奇正、國人羅彬案

調查局，守護你的安全！
MJIB, Protects Your Life!



羅奇正遭中共吸收後，每3至4個月攜帶儲存情報局機密之隨身碟或光碟，交付羅奇攜往大陸，圖為渠等在臺北捷運昆陽站1號出口，遭本局當場逮捕情形。

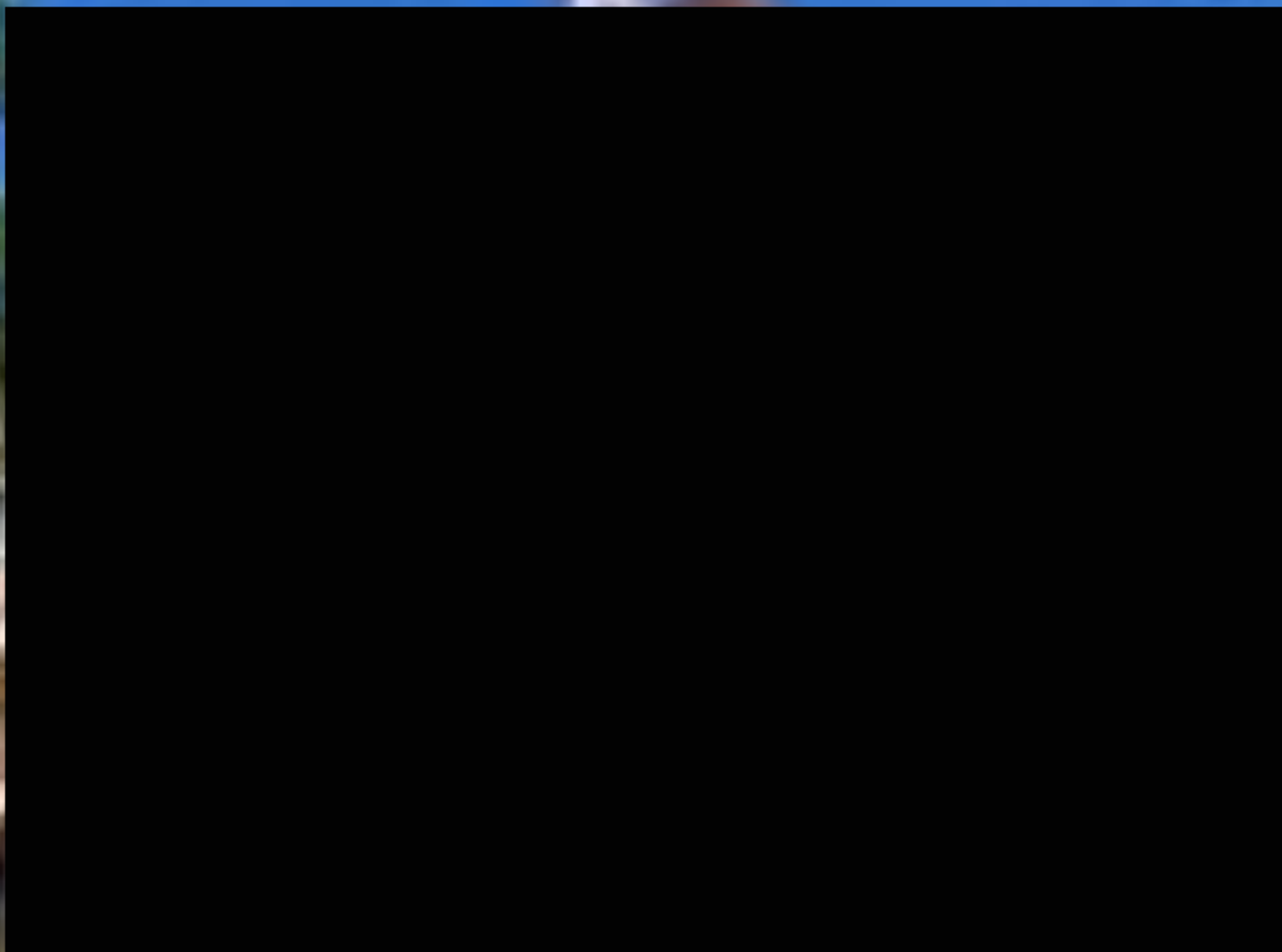




MJIB
法務部調查局

影片：違規赴陸

調查局，守護你的安全！
MJIB, Protects Your Life!





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

公務員赴陸現行相關規定

「臺灣地區公務員及特定身分人員進入大陸地區許可辦法」

(依兩岸人民關係條例第9條第9項授權訂定，
簡稱：**許可辦法**)

「簡任第十職等及警監四階以下未涉及國家安全機密之公務員及警察人員赴大陸地區作業要點」

(依兩岸人民關係條例第9條第3項授權訂定，
簡稱：**作業要點**)



應於返臺上班後一星期內填報，送交**政風**業務部門。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

3

機密維護工作





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

公務洩密主要類型





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例研析(資料保管不當)

- **案情說明：**兵役處理疏失，意外讓役男愛滋感染身分曝光，造成家庭關係緊張，險被掃地出門！【中國時報 99/11/09】
 - 剛大學畢業準備投入職場的某甲因感染愛滋而辦理免役，但有一天竟接到母親電話，泣責他感染愛滋卻不告知。原來是地方里幹事在兵役體位判定書上註明「後天免疫缺乏症候群」，原應由本人親自領取，卻透過大樓管理員轉交母親，讓甲頓時啞口無言，導致親子關係緊張。
 - **個資法第6條**「有關醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。」本案例中之敏感個人資料，係公務機關執行法定職務所必要，不應輕易傳遞或洩漏予他人。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例研析(公務家辦洩密)

■ 案情說明：某技正為圖一時之便，公務家辦導致資訊外流！

- 某縣政府技正，基於私誼協力執行「○○專案」預算執行成效，因進度落後，為求時效，未經核准以個人隨身碟儲存相關資訊，攜返家中電腦作業，復因家中電腦連網遭植入惡意程式擷取檔資，致生公務資訊外流情事。
- 該名技正係因對資安相關規定認知不足，且為求作業時效，雖明知嚴禁公務家辦、私攜移動式儲存媒體等規定，然心存僥倖，致衍生疏漏所致。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例研析(委辦業務失當)

- **案情說明：**某環保單位委外辦理業務之廠商，因人員及資訊管理不足，導致公務資料外流！
 - 某環保單位委外辦理「柴油車排煙檢測站檢驗計畫」業務，因承包廠商同仁所使用之電腦遭植入木馬病毒，致電腦檔案中「全縣車齡9年以上車輛通知到檢名單及總清單」公務資料，因委辦廠商之資安缺失而外洩。
 - 環保單位委外辦理業務甚多，未能訂定管理辦法及罰則，又未切實負起督導責任，對委辦廠商無法適當管制，公務電腦未設定使用權限，委辦廠商均能任意使用公務電腦，員工資訊保密訓練不足，嚴重缺乏機密維護警覺。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例研析(網路管理疏失)

- **案情說明：**○○局地方行政研習中心的網站，日前突然出現大量身分證字號【聯合報104/10/03】
 - 該網站架設目的，原是給初任公務員註冊累積研習時數用的開放式交流平台，公務員只要申請帳號、密碼，都可以進入論壇、發表意見，身分證字號僅作為帳號使用，且會員得隨時更改帳號。
 - 資訊平台對使用者帳戶密碼的保管，應有完整的維護系統和安全防護，以避免使用者資訊的外洩。另方面可透過宣導、教育及訓練，讓使用者可以更清楚使用上的風險，以期可以達到最合適的控管。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

影片：無心之錯





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

4

資通安全工作



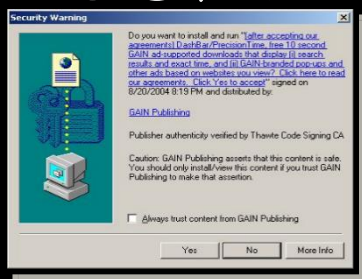


MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

網路攻擊態樣

惡意軟體



螢幕監看



勒索病毒



網路釣魚



身分竊取



鍵盤側錄



駭客攻擊



間諜軟體





案例分享—1111人力銀行案



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

1111人力銀行接獲民眾反映個資遭外洩，新北地檢署循線查出原來是1111客戶「**台灣宅經濟商務股份有限公司**」違反約定，洩露人才查詢系統專屬帳號、密碼，供富邦人壽業務員竊取2萬多筆個資。





案例分享－手機隱形偵探木馬案



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!



調查局臺南市調查處於107年5月22日，破獲兩岸三地最大手機木馬程式販售網站「**隱形偵探**」(網址：<http://www.ez-xspy.com>)，於高雄市林園區及小港區，查獲擔任在臺唯一代理人龔姓女子，扣押龔女用以聯繫其他共犯之手機及客戶名單，經查已有上百人透過該網站購買竊取程式。



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例分享一 TWDDoS網站及第一金控勒索案

日期: 2016/09/22 上午 11:22

主旨: Re: 你的网站正在遭受到 DDoS 攻击

攻擊公務、金融機關2萬次 TWDDOS網站管理者遭搜索



你的网站正在遭受到 DDoS 攻击

把此重要电邮交给公司内有经营权决议者阅读
来自于 F-DaY-Cn .

于12个小时内支付 50 Bitcoins (比特币)
(北京时间 9月22日 21:00 前)

F-DaY-Cn @ 比特币钱包位置:

15ejRjsypPw4H81Rz1rAskJw5hggAyYh

当如果在时间内没有收到 50 比特币

我们将对于你的线上服务进行DDoS攻击中止
届时你的用户全部无法进行你提供的项目

我们来证明一下我们是否为真实的信件

你们目前的部分线上服务正在遭受我们的DDoS

<https://ebank.firstbank.com.tw/>

<http://ewinner.ftsi.com.tw/etrade/weblogin.html>

这只是我们小小的一部分，

时间内没有收到50个BTC则增加至70个BTC

拖延一天则每日增加20个，直到支付完成我们才会停止DDoS



2018-05-30 19:02

〔記者謝君臨 / 台北報導〕TWDDOS網站成員，號稱以分散式阻斷服務（DDoS）對中華電信、中央銀行等公務、金融機構進行2萬餘次攻擊，並製作機關遭攻擊影片供人瀏覽，以招攬會員購買攻擊服務；台北地檢署28日指揮調查局搜索主嫌處所，查扣犯案手機、電腦及比特幣等證物，本案亦為首次查獲從事比特幣非法交易之案件。



北檢指揮調查局搜索TWDDOS網站管理者處所，查扣犯案手機、電腦及比特幣等證物。
（記者謝君臨攝）

調查局指出，TWDDOS網站自稱是台灣首家最強阻斷式攻擊服務提供者，提供穩定且強大的攻擊流量，強調司法單位無法追查，有意購買攻擊服務者，需將比特幣轉至國外比特幣代收機制的指定帳戶。

調查局發現，主嫌為吸引感興趣的網友加入會員，除提供45秒免費攻擊試用，更為證明攻擊效果，再於日前對國內外網站發動2萬餘次攻擊，分別攻擊中央銀行、多所大學、國高中等學校、中華電信、電信業者機房、遊戲公司及金控公司等，造成網站短暫停止服務，嚴重影響網路正常運行。





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例分享—手機誤傳資料 1

北市政風處主秘上班炒股 LINE誤傳柯P被記過

19:58 2015/09/09 | 集團連線報導 | 張潼、黃麗蓉



政風處主秘林惠琴今早上班時，誤傳「6269台郡買三張，分批，上市零組件」訊息到台北市政府LINE群組。（張潼翻攝）

政治熱門新聞

- 1 【陸鳳梨禁令】項 林佳新：綠 - 政治
- 2 蔡政府2月最新眼鏡 - 政治
- 3 【陸鳳梨禁令】翻天 最新民調
- 4 陸鳳梨禁令 胡諷諷萬狀 民進黨
- 5 交涉日方增加捐 廷這樣回應 - 政
- 6 薩礁連署年輕人 大學生總召吐責
- 7 【陸鳳梨禁令】有蹊蹺 媒體人5 因 - 政治
- 8 王金平到底想幹 多次現身背後目
- 9 黃曙光屆退 張 政治要聞 - 中
- 10 新聞早班車》台 從5成跌至5凱 -



糗！誤傳裸照到司改LINE群 男檢察官驚慌：怎刪

編輯 徐子婷 報導

發佈時間：2017/10/13 22:03

最後更新時間：2017/10/13 22:03



圖／擷取自網路



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

案例分享－手機誤傳資料 2



花蓮縣某警員上傳有關該單位109年度業務費經費編列、使用、剩餘、分配情形之簽稿併陳公文檔案至LINE私人群組。



北市某派出所副所長將新冠肺炎確診者姓名、年籍、行蹤、接觸史拍照，以LINE傳送予友人，而後遭網路瘋傳。





MJIB
法務部調查局

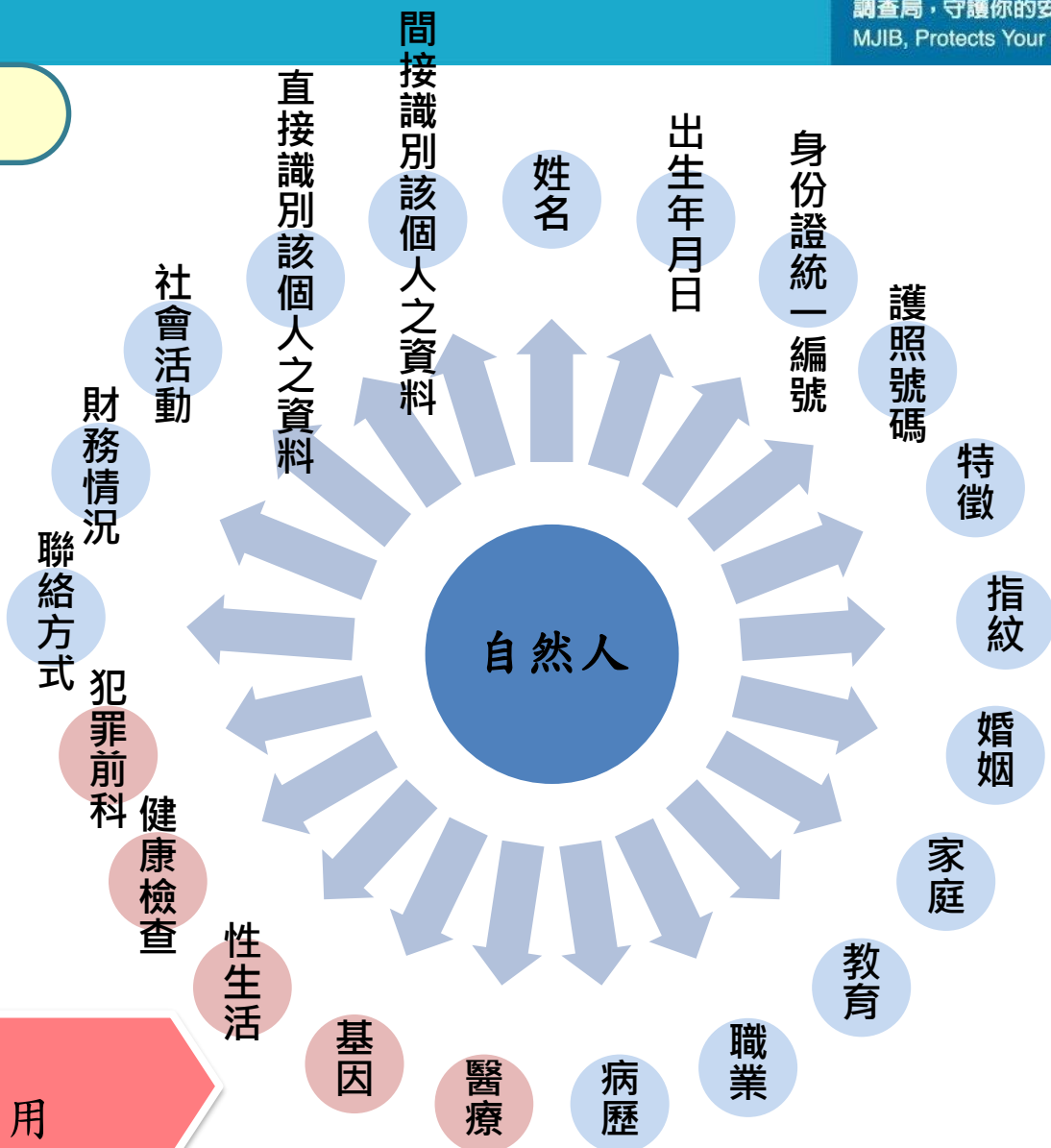
調查局，守護你的安全！
MJIB, Protects Your Life!

個人資料保護法範疇

除非符合下列情形之一：

1. **法律明文規定**
2. 公務機關執行法定職務或非公務機關履行**法定義務所必要，且有適當安全維護措施**
3. **當事人自行公開**或其他已合法公開之個人資料
4. 公務或學術研究機構基於醫療、衛生或犯罪預防之目的，為**統計或學術研究而有必要，且經一定申請程序**

特種個資：
不得蒐集處理或利用





我國「數位發展部」即將成立



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

立院三讀 數位發展部將成立

2021/12/29 05:30

讚 3



立法院長游錫堃，昨敲槌三讀通過數位發展部數位產業署組織法。（記者王藝菘攝）

自由時報

數位發展部組織法三讀過關，外界期待2022年520前能掛牌，新成立「資通安全署」與「數位產業署」

因應行政院組改規定，數發部三讀通過後，現有的科技部將調整為國家科學及技術委員會；現有行政院資安處將升格為三級機關「資通安全署」，同時新成立一個「數位產業署」，負責數位經濟產業政策規畫與執行

讚 6.8 萬

按讚加入iThome粉絲團

讚 236

分享

文/ 黃彥霖 | 2021-12-28 發表



圖片來源: iThome



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

駭侵主流--社交工程攻擊

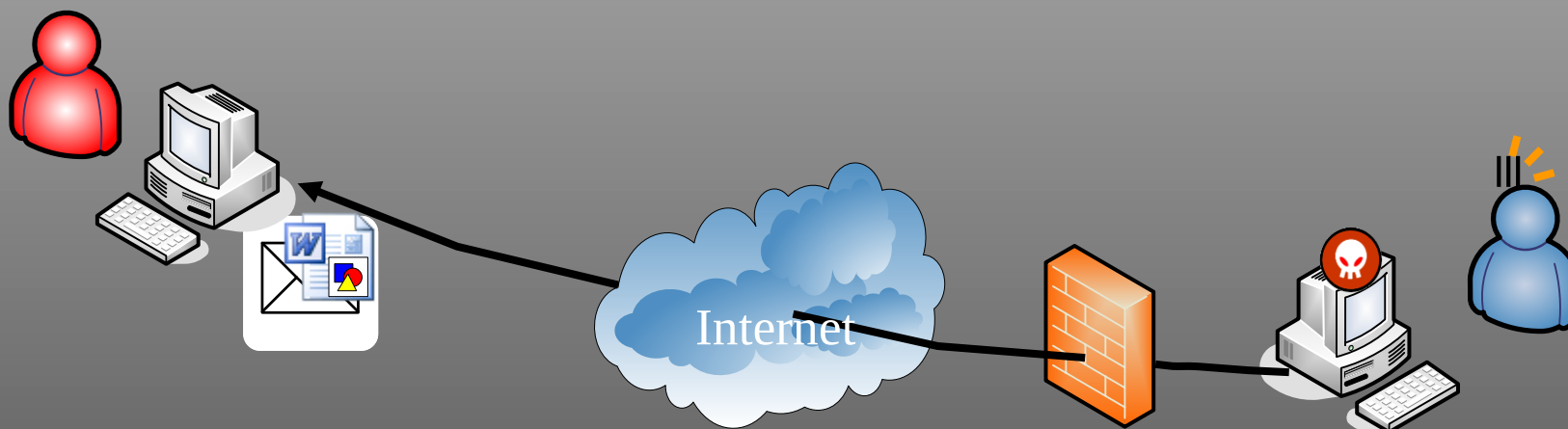
- ◆ 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法。
- ◆ 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊。
- ◆ 透過電子郵件進行攻擊之常見手法
 - 假冒寄件者
 - 使用與業務、時事相關或令人感興趣的郵件內容
 - 含有惡意程式的附件
 - 利用應用程式之弱點(包括所謂零時差攻擊)



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

社交工程攻擊流程



1. 駭客設計攻擊陷阱程式(如特殊 Word 檔案)
2. 將攻擊程式埋入電子郵件中
3. 寄發電子郵件給特定的目標

4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，並被植入後門程式

6. 後門程式逆向連接，向遠端駭客報到
7. 遠端駭客進行資料竊取



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

資安防護「停 看 聽」1

停 使用任何電子郵件軟體前，必須先確認以下設定

- 必須安裝防毒軟體，並確實更新病毒碼
- 審慎開啟郵件及其附件或連結
- 必須取消郵件預覽功能，避免無意開啟郵件
- 設定過濾垃圾郵件機制
- 建立電子郵件驗證機制(推動電子識別證)



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

資安防護「停 看 聽」2

看 收到郵件後，必須先注意

- 郵件主旨是否與本身業務相關
- 其餘郵件不建議開啟，如需開啟應先確認來源

聽 若懷疑郵件來源，必須進行確認

- 透過電話或電子郵件向寄件人於開啟前確認真偽



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

個人行動裝置的5不5要



不要自行破解行動裝置的安全機制



要用Pin Code或密碼鎖定手機螢幕



不要連接不信任的無線網路基地台



要安裝遠端安全服務：如遠端鎖定、清除資料或GPS定位



不要安裝不信任的APP



要記得定期備份資料



不要假設行動裝置比電腦安全



要儘可能加密



不要等待，立即回報安全問題



要定期更新系統與APP



MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

十大資訊安全好習慣

1. 不明人士要盤查

2. 社交工程要小心

3. 電腦不用要登出

4. 機密資料要保護

5. 密碼設定要穩固

6. 重要資料要備份

7. 電腦防毒要更新

8. 應用系統要更新

9. 瀏覽網路要提防

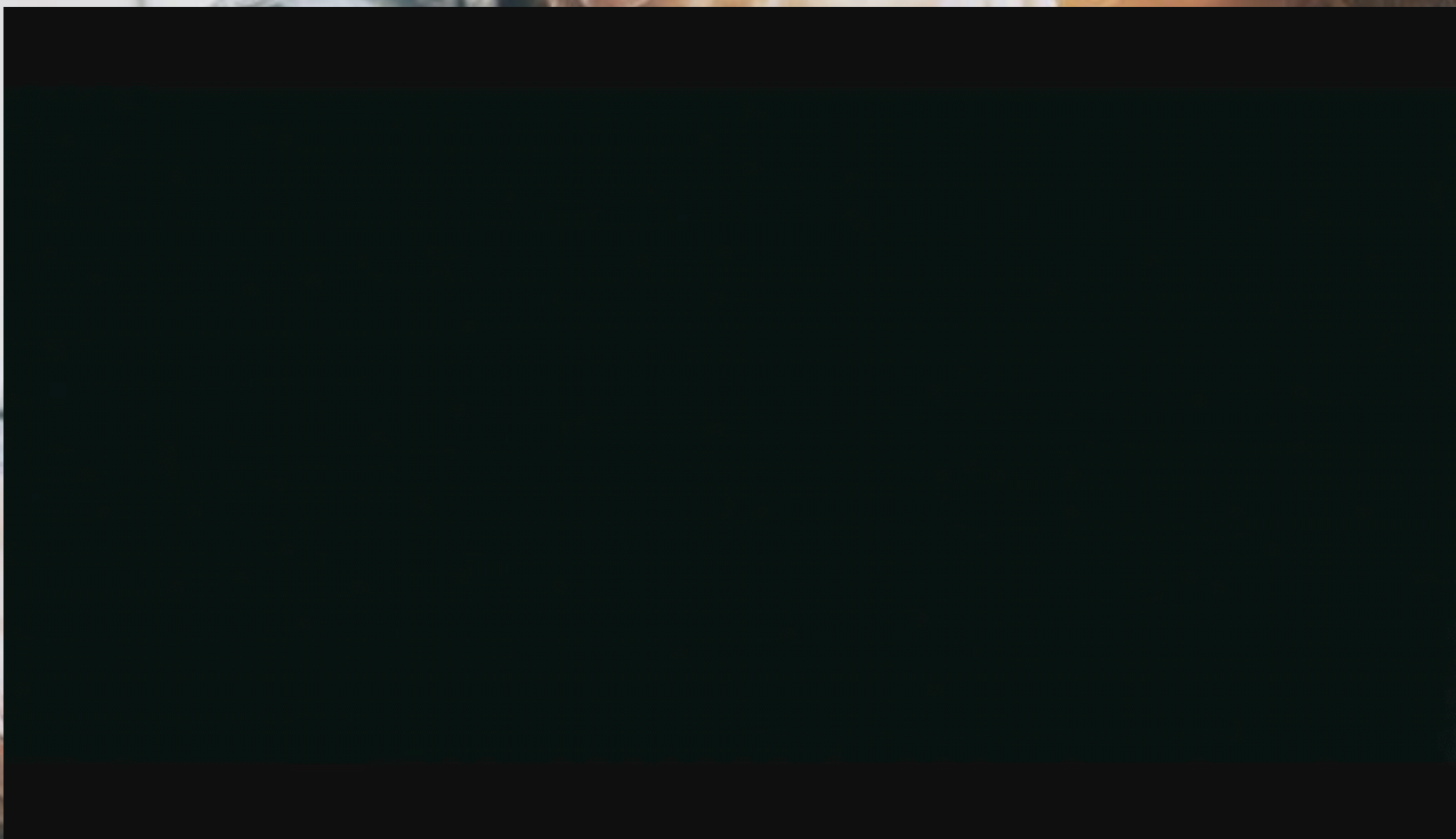
10. 電子郵件要過濾



MJIB
法務部調查局

影片：資安防護

調查局，守護你的安全！
MJIB, Protects Your Life!





MJIB
法務部調查局

調查局，守護你的安全！
MJIB, Protects Your Life!

報告完畢 敬請指教

報告人：副主任 張進明