



南投縣教育網路中心 資安防護種子教師培訓研習課程

防範電子郵件社交工程

蔡和燁

Hoyeh_tsai@kh.ringline.com.tw

大綱

- ➔ **社交工程**
- ➔ 社交工程 - 網路篇
- ➔ 如何防範

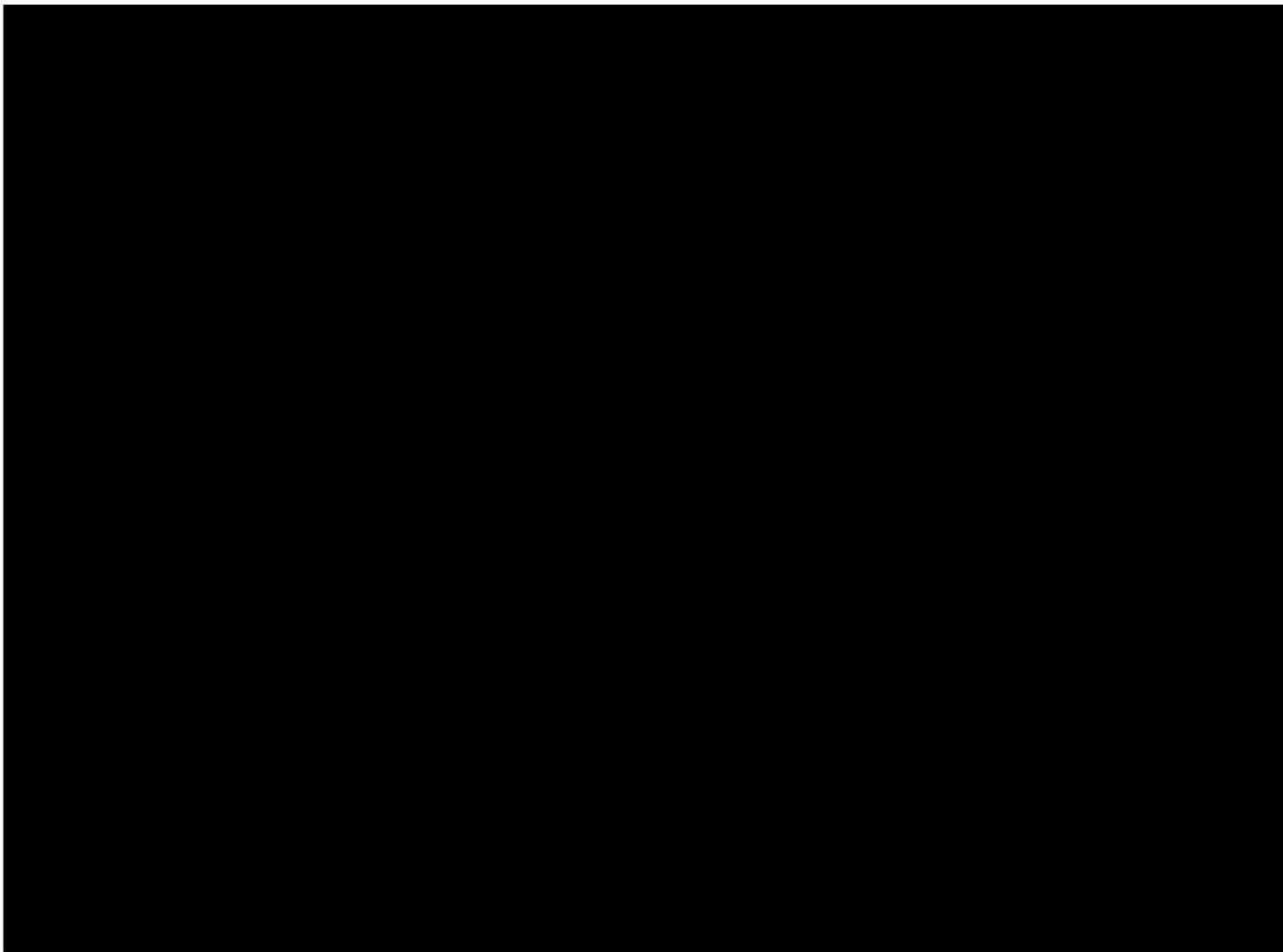


何謂社交工程

- ◆ 社交工程，英文為 Social Engineering
- ◆ 是以影響力或說服力來欺騙他人以獲得有用的資訊
- ◆ 社交工程利用人性容易相信而上當的弱點



人類的弱點: 免費吃麥當勞



麟瑞科技
RING LINE CORPORATION



何謂社交工程

- ◆ 惡意人士不需要具備頂尖的電腦專業技術
- ◆ 只要使用人員對於防範詐騙沒有足夠的認知，就可以輕易地避過了單位的相關軟、硬體安全防護系統
- ◆ 可輕易騙取到各項帳號密碼、個人資料、財務資料或單位重要資料等資訊



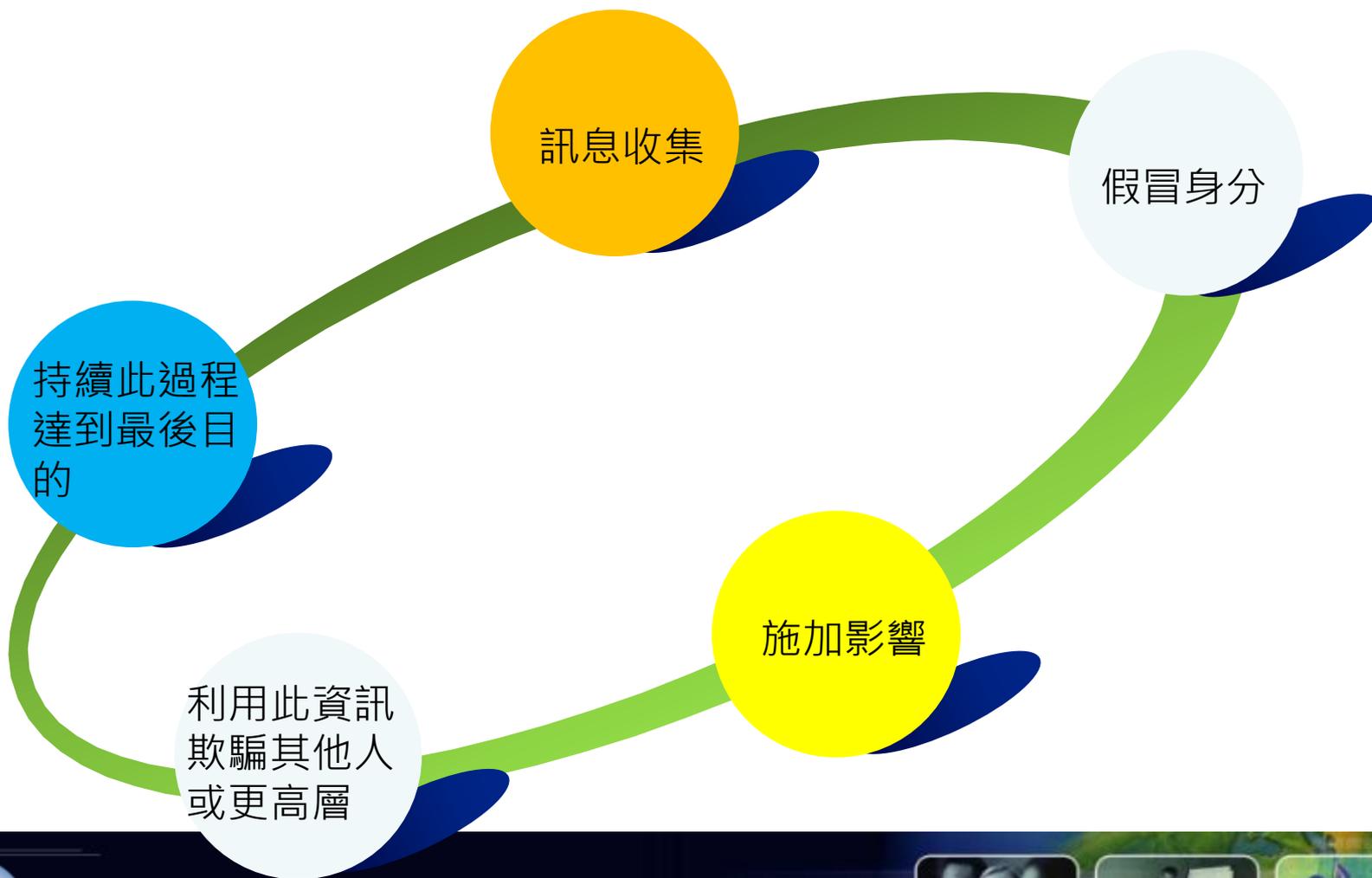
達到最終目的 不用任何電腦技能



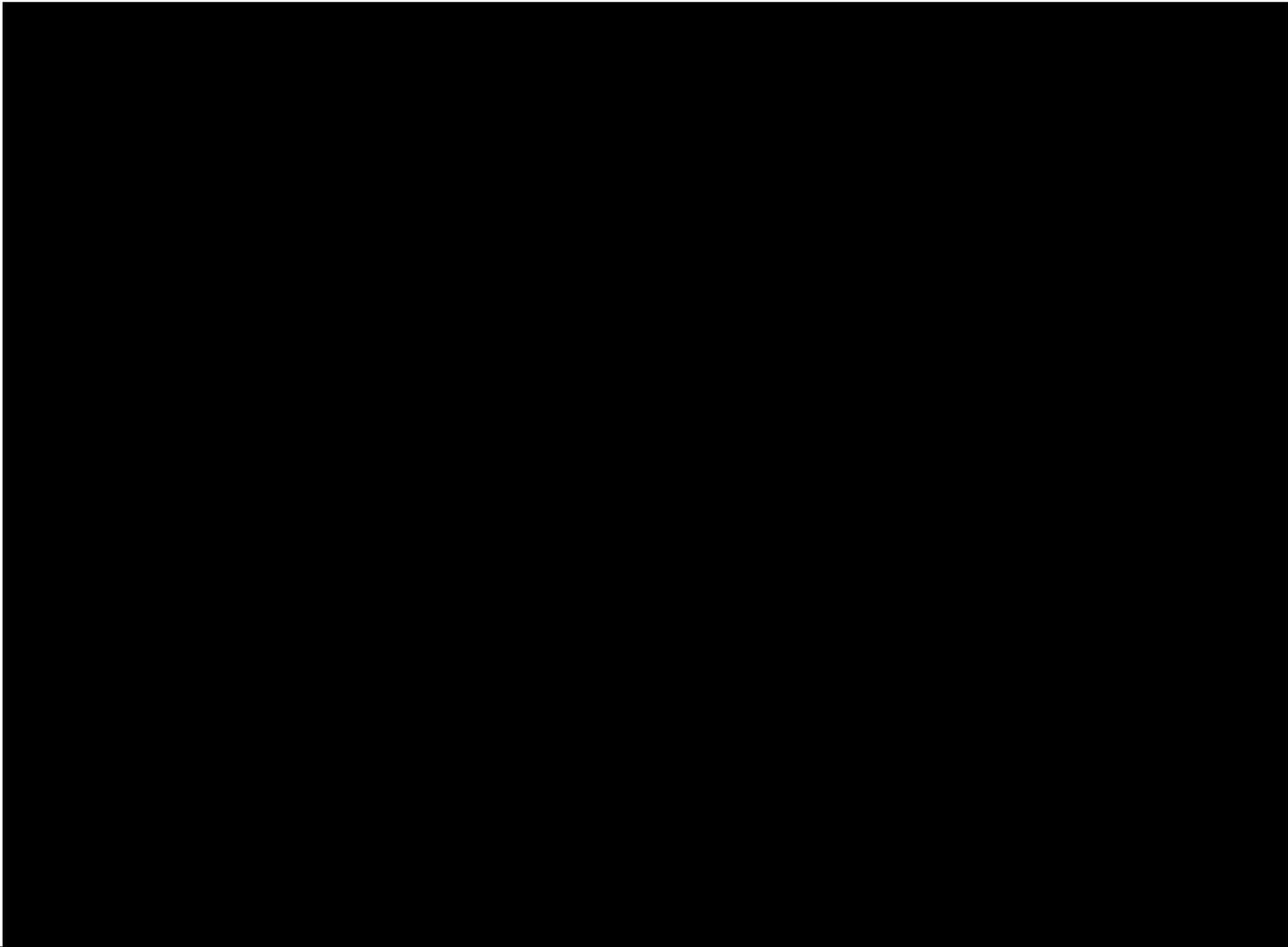
麟瑞科技
RING LINE CORPORATION



社交工程攻擊步驟



收集資料 – 從最不起眼的地方開始



麟瑞科技
RING LINE CORPORATION



為什麼要假冒身份？

- ◆ 假冒身份說白了就是「包裝」。
- ◆ 包裝成你會信任的角色



假冒身分要達到什麼效果？

◆ 博取信任

➤ 攻擊者會利用之前得到的『不敏感訊息』來證明自己是機構內的人，從而得到信任。

◆ 博取好感

➤ 如果對方產生了好感，攻擊者就便於提出更進一步的要求。

◆ 博取同情

➤ 某些攻擊者會刻意示弱，從而讓對方產生一些同情心，然後藉機提出一些要求。

◆ 樹立權威性

➤ 很多人都會對權威人物有一種輕信和盲從。樹立權威性助於攻擊者後續的「施加影響」。



網路是最容易的身份包裝



聊天容易有好感



麟瑞科技
RING LINE CORPORATION



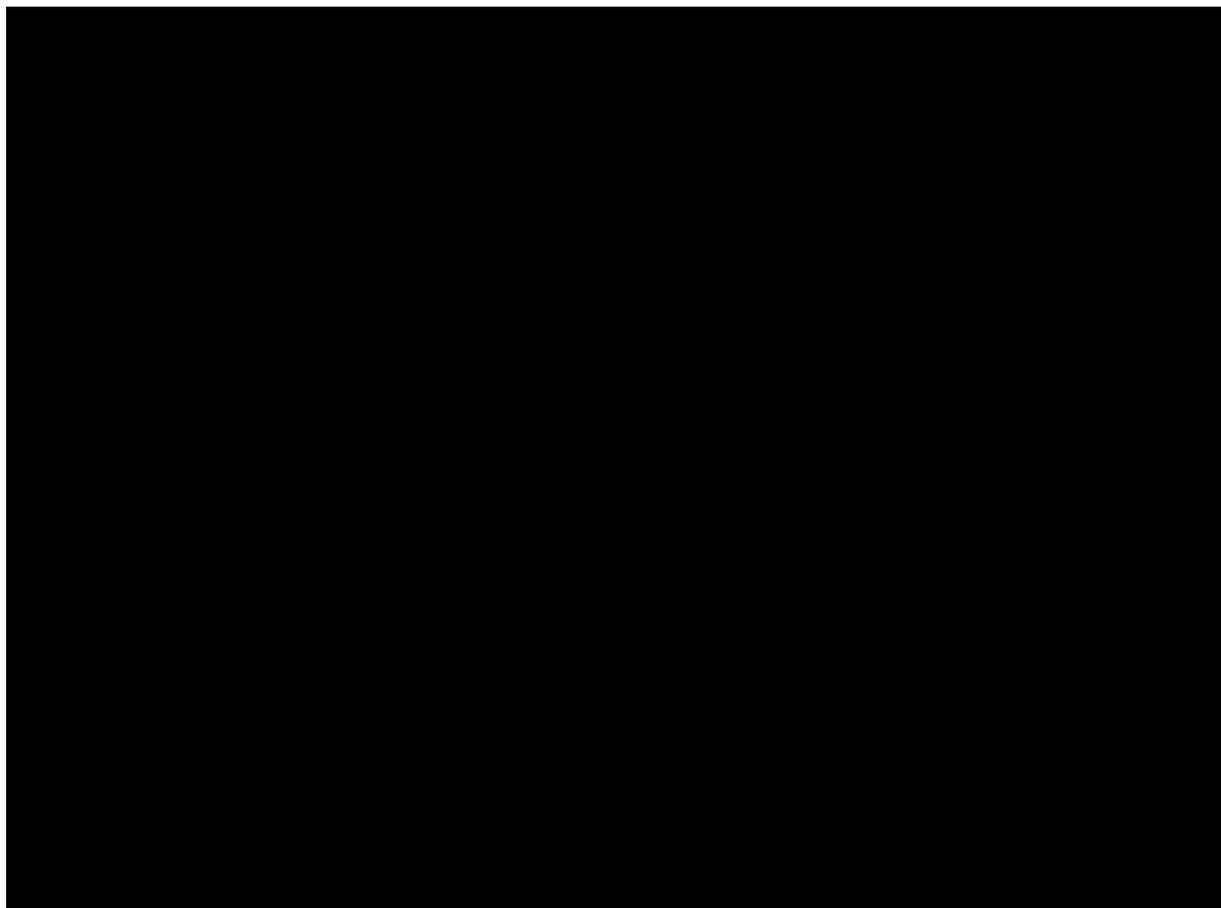
通過互惠原理來騙取好處



麟瑞科技
RING LINE CORPORATION



通過權威來施加壓力 – 虎三小



麟瑞科技
RING LINE CORPORATION



除了包裝人 還可以包裝...

這是一台完全被偽裝的提款機，您辨識的出來嗎？



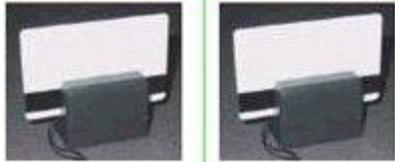
麟瑞科技
RING LINE CORPORATION



Yahoo就有在賣

犯罪者可以透過網路就可合法地購買讀卡機或寫卡機。

上圖為國外網站，下圖為台灣拍賣網站資料。

	Two Portable Readers	\$510
(mini123) Portable Magnetic Card Reader USB	(mini123) Portable Magnetic Card Reader USB	
	One Writer	\$440
	Card Writer (Serial and USB)	
Priced Separately		\$950
Software		FREE
100 HI-CO cards		FREE
SPECIAL discount		-\$140



門禁管理
 用餐及收費管理
 考勤管理
 搭配POS收銀機



麟瑞科技
 RING LINE CORPORATION



不要讓信用卡離開視線

想像去餐廳吃飯，吃完將信用卡交給服務生，
該服務生手中有這台讀卡機的狀況？

或是他利用下方這台可即時傳送文字的讀卡機讀取？



讀卡機內建電池、512K記憶體(約刷2500次記憶量)



這些讀卡機會放在哪？

- 藏於提款機內
- 置於免費清卡機
- 置於儲值機



微型讀卡、清卡機



讀卡的規格

網路販售的規格:

可刷**2000~3000**筆資料，並有**512K**記憶體儲存，再透過**USB**介面進行傳輸。

size	2.25" x 1.80" x 0.75"
memory	512k
tracks	1, 2, & 3
swipes stored	2000 - 3000
color	black
computer interface	USB
software	yes
msr206 software support	yes
weight	1.9 oz



側錄按鍵自己做

在螢幕背版鐳上晶片，再把各按鍵接到晶片上，
只需直流**5V**電壓就可傳輸資料



真實案例 –

右圖，那不勒斯警方照片，圖中螢幕上方藏有針孔攝影機錄取使用者密碼



左圖為另一種隱藏方式，置於傳單盒側邊，下次提款前多加確認。



下次提款前請確認



螢幕上方是否多一個塑膠盒？

螢幕前方是否有宣傳盒？

讀卡機

鍵盤



麟瑞科技
RING LINE CORPORATION



回顧

- ◆ 社交工程
 - 利用人性弱點，從收集、偽裝、利用達到目的。
- ◆ 收集資料
 - 為了下一步偽裝做準備
- ◆ 不是只有技術
 - 許多社交工程，沒有技術背景，不要僅留意技術部份。
- ◆ 其它偽裝
 - 提款機也可能成為偽裝的一部份。



Q & A

Hoyeh_tsai@kh.ringline.com.tw



麟瑞科技
RING LINE CORPORATION

