

公務機密維護宣導

114年5月

強化社交工程（電子郵件、行動裝置簡訊） 攻擊防範意識宣導

社交工程(Social Engineering)係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破個人、企業或政府機關的資通安全防護；這種攻擊方式並非利用技術漏洞，而是直接操縱受害者，使其洩露個人資訊或採取不安全的行為。

預防社交工程攻擊，可留意以下事項：

- 1.社交工程攻擊喜歡用「聳動標題、公務資訊、結合時事新聞、財金、健康、打折優惠促銷活動...等吸引注意力、好奇心及混淆人心之事件」，誘騙使用者點擊釣魚信件或簡訊，騙取用戶個人資訊、密碼或下載惡意程式、檔案等，造成機敏資料外洩或遭勒索病毒攻擊等資安事件發生。
- 2.請關閉電子郵件預覽功能。
- 3.開啟郵件前，請確認主旨與本身業務相關，或與承辦人、寄件人確認來信。
- 4.不任意點閱郵件或簡訊中之超連結網址、附加檔案。
- 5.公務郵件與私人郵件應區隔，請勿將公務郵件地址用於註冊、認證其他非公務平台。
- 6.不隨意輸入帳號密碼資訊：輸入帳號密碼前應再三確認其正當性，避免遭假冒網站竊取。
- 7.若有可疑信件、簡訊或相關問題，請洽單位資訊或資安人員。



台灣自來水股份有限公司
第九區管理處政風室