機密維護常識彙編（98 年 12 月份）

＊網路釣魚，願者上鉤

壹、案例事實：

2007 年1 月有不肖集團以聯X 銀行網站為樣本，製作與聯X 銀行首頁相同的網頁，並以該銀行名義發出數十萬封以「銀行系統轉換，重新登錄」為標題的電子郵件，要求銀行用戶點選郵件末隨附的極相似網址，上網重新確認帳號及個人密碼。當用戶連上該偽冒網站時，即被植入木馬，竊取個人密碼及信用資料；歹徒隨後更利用相關資料盜領存款、盜開支票，甚至複製信用卡詐欺取財。

貳、法律探討：

一、所謂網路釣魚，英文為Phishing，與Fishing 發音相同，主要因為早期是以盜撥電話來詐騙財物，所以將「Phone」和「Fishing」兩字結合為Phishing。現在則是指利用網站連結、電子郵件、即時通訊等工具，誘騙網友進入與企業或組織網站相似的網頁，騙取帳號或是植入木馬程式，更進一步詐取受害人的財物。這類犯罪由於具有經濟上的誘因，已迅速成為目前國內外嚴重的詐欺犯罪態樣。

二、由於資訊化社會的發展，許多的文字或圖像都已經電子化，並相當程度足以表示其用意之證明，法律上即將其擬制為「文書」，適用文書保護之相關規定。以本案為例，行為人以商家名義向不特定多數人發送電子郵件之行為，即可能構成我國刑法的第210 條偽造準文書罪；郵件內含偽造首頁及偽冒網址之行為，即可能違反了著作權法第91 條，侵害網頁著作人重製權，也可能涉及使用他人商標中之文字作為來源之標識，成立商標法第62 條的侵害商標權罪。

三、關於竊取帳號密碼的部分，不論是網友誤入極為相似的網站而輸入帳號密碼，或行為人透過木馬程式竊取，有可能成立刑法第359 條取得電磁記錄罪。最後，行為人以竊得之帳號、密碼進入銀行網站，進而將被害人帳戶內

存款轉走之行為，視行為的階段性，可能成立刑法第358條之無故入侵罪，也可能成立第339-3 條之電腦詐欺罪，分別為3 年與7 年以下的刑責。如歹徒用以製作偽卡，可構成刑法第201-1 條的偽造支付工具罪，可處1 年以上、7 年以下有期徒刑。網路釣魚詐欺多是利用人性弱點進行誘騙，或要求收信人及時回覆、或提供虛假網址連結誤導被害人。面對層出不窮的犯罪手法，消費者對於網路之應用要有所警惕，除應定期更新安全防護軟體及更新瀏覽器漏洞修正外，更要謹慎小心，不要輕信不明的電子郵件，或隨意點擊廣告連結，並儘可能注意加註防釣安全標章(Sign-in Seal)，以確保擁有安全的網路使用環境而免於受騙。

（資料來源：行政院國家資通安全會報技術服務中心）

＊洩密案例

壹、案例事實：

檢舉人「王○○」君向水利署○○河川局檢舉「○○砂石企業股份有限公司於○○溪旁設置砂石廠房、機具盜採砂石等情」，請求該局依法處理。案經該局依據該檢舉指稱事項查證瞭解，發現該○○砂石廠違法部分已於檢舉前主動查處並分別處以罰鍰在案。有關本案處理結果，該局具函函復檢舉人。惟查該函除以正本函復檢舉人外，並以副本抄送相關人員、單位，其中被檢舉之「○○砂石企業股份有限公司」列為副本收受者，亦即本案承辦人未依保密規定，將檢舉人及被檢舉人在同一函並列。

貳、本案研析：

一、刑法第132條第1項，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。第132條第2項，因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。

二、有關檢舉內容(包括檢舉人之身分)對被檢舉對象自屬應秘密之文書，按「本監受理檢舉人身分保密作業注意事項」第10點規定，處理檢舉案件，函覆檢舉人與相關單位之文件，應分別處理；儘量避免正本發文檢舉人，副本抄

送相關單位之併列情形。如確有兩者併列之必要時，應僅列「檢舉人」字樣，以免致生洩密情事。

三、本案因公務員於函復檢舉人時，並另以副本抄送被檢舉人致生洩密事件，實務見解皆認為核有疏失並應負刑責。

參、結語：

有關公務員是否洩密及是否應加處罰，散見於刑法及其他法律，如刑法第 132 條。至於關係他人權利、義務或個人隱私之案件，在未依法公開前，參與辦理過程之人員，亦均有保密義務，以確保行政目的之達成外，亦兼及人民權利之保障。

＊高科技機密外洩案例評析

國內台積電十二吋晶圓製程機密資料「外傳」中國事件，國內資訊專家指出，市面上已有現成的硬體鎖定加密技術，可將機密資料文件「鎖定」在特定的電腦硬體上，因此既使該資料外流到他處，也無法順利開啟瀏覽，除非將電腦一併帶走，所以只要應用該資料加密技術，台積電的機密資料外洩事件，就可防患未然。

據國內資訊安全專家分析，以電腦 bios（基本輸入輸出系統）技術見長的 Phoenix 公司即已發表一套「硬體鎖定加密」技術，可以將某加密資料文件與特定電腦「配套」，也就是說，要看該檔案，就只能在該電腦開啟，如果資料被「有心人士」外傳，在別台電腦上根本無用武之地，所以機密就無從外洩了。

＊洩漏應保密資料觸法案例

壹、案例事實：

某甲係某電腦及資訊兩家公司實際負責人，不久前該電腦公司取得某公家機關原始資料之電腦登錄建檔工作，依雙方所訂合約第十條規定「登錄之資料，應以機密文件處理，電腦公司並應採必要之保密措施」，某甲在取得該機關原始資料後，明知依合約不得洩漏予他人，卻意圖為自己不法之利益，於建檔期間將其持有之電腦建檔機密資料，私自拷貝存檔或列印報表後，夾帶回公司重新建檔，事後再利用資訊公司名義，連續販售機密資料予相關廠商寄發推銷商品，某甲因此獲利達新台幣五百六十餘萬元，在

檢調單位獲報查證後始破獲全案。

貳、本案研析：

洩密人雖非公務人員，但受公署委託電腦建檔，且與受委託機關訂有合約，「登錄之資料，應以機密文件處理，電腦公司並應採必要之保密措施」，案經檢察官將洩密部分，依刑法第132條第3項「非公務員因職務或業務知悉或持有第一項之文書、圖畫、消息或物品，而洩漏或交付之者，處一年以下有期徒刑、拘役或三百元以下罰金] 罪嫌偵辦。

參、結語：

本案係典型電腦資料洩密案件，洩漏國防以外應秘密之文書，受法律制裁，因此，在平日即應落實電腦、文書、通信等各項保密措施，對易滋弊端及有損民眾權益之事項，應嚴格管制作業流程，預估可能洩密管道，機先妥訂週延之防制作為，以杜絕洩密於未然。

＊洩漏國防以外之秘密罪

壹、案例事實：

甲○○自民國95年9月8日起，任職於行政院勞工委員會勞工保險局（下稱勞保局）承保處公司行號科第二大組商五組練習員，負責公司員工勞保加、退保資料建檔等工作，為依據勞工保險局組織條例及辦事細則從事公務之人員，依其職務雖可查詢全國勞工保險相關資料，然此等資料查詢必須透過一定程式，即需主動告知投保單位之保險證號，始得以電話詢問方式或親赴櫃臺查詢保險相關資料，而前述資料查詢並非其所執掌業務且均屬職務上應秘密事項，甲○○竟基於洩露此等機密內容之故意，自96年1月至97年1月15日間，由一自稱「王靜欣」之大陸地區女子，經由勞保局總機轉至甲○○分機2519，陸續來電要求甲○○代為查詢勞工保險證號資料，甲○○明知透過電話查詢取得勞工保險證號資料並不符合作業程式，仍使用代號KL754之電腦，輸入帳號A70317及密碼，由「王靜欣」以電話傳達身分證號資料，使甲○○由電腦得知勞工保險證號，並透過電話告知之方式，陸續

洩漏共計約6380筆之投保單位保險證號相關資訊，致「王靜欣」取得該等保險證號後，即可據此透過勞保局全球資訊網之「投保單位應繳保費查詢」或「勞退作業應繳提繳查詢及補列繳款單」之系統，輸入投保單位之保險證號，進而得知被保險人最新任職之公司行號名稱，而洩漏中華民國國防以外之秘密。

貳、觸犯法條：

一、刑法第132條第1項，公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處3年以下有期徒刑。

二、臺灣○○地方法院97年10月31日97年度簡字第3523號刑事簡易判決主文：

甲○○公務員洩漏關於中華民國國防以外應秘密之消息，處有期徒刑壹年陸月，緩刑肆年，並應向公庫支付新台幣拾萬元。

（以上二則資料摘自於臺灣宜蘭監獄政風室）