@所有人，這些網路安全“漏洞”，你堵好了嗎？

15-10-2021　　珠海市消委會

2021 年網路安全宣傳周來啦！對網路安全“漏洞”，每天上網的你瞭解多少？知道怎樣保護自己的個人資訊嗎？今天來為大家科普網路安全知識，向安全性漏洞、風險隱患 say no！

漏洞一個人敏感資訊隨意外泄

一張照片就能洩露全部家庭成員資訊，容易給不法人員創造行騙、行竊的機會，尤其是老人、小孩的資訊，更要注意保護，包括姓名、幼稚園和學校的地址等。

01 曬娃要注意

有些愛曬孩子的家長沒有關掉微信中“附近的人”這個設置，騙子通過微信搜索“附近的人”，輕易就能獲取孩子的資訊。

02 行程要保密

外出時，排程、行蹤等資訊要注意保密，不要給犯罪分子行竊的機會。所以，外出期間能夠顯示姓名、身份證號的車票、護照、飛機票等不要“曬”。

03 保護好隱私

儘量不要在照片中出現特徵明顯的東西，例如你的家門鑰匙、車牌號碼，以及身份證、駕照和護照等證件。

漏洞二密碼過於簡單或所有帳戶使用同一密碼

對於密碼我們都不陌生，每當我們登錄論壇、郵箱、網站、網上銀行或在銀行取款時都需要輸入密碼，密碼的安全與否直接關係到我們的工作資料、個人隱私及財產安全。

以下幾點要注意：

1.不要所有帳戶使用同一密碼

2.重要的帳戶應使用更為安全的密碼

3.偶爾登錄的論壇可以設置簡單的密碼

4.日常使用的電子郵箱、網上銀行、公司資訊系統需設置複雜的密碼

5.不要把論壇、郵箱、網上銀行、資訊系統帳戶設置成相同密碼

下面幾個竅門教給大家

第一式 短語拼接

自己熟悉的短語，最好有數位有字母，大小寫結合；如“5G 時代@”轉換密碼“5Gshidai@”

第二式 整句化散詞

使用喜愛的詩詞拼音首字母加上數位與特殊符號組成密碼;如“天生我材必有用” 首字母加數位與特殊字元組成密碼“tswcbyy@6”

第三式 數字換文字

可以將漢字替換成對應的阿拉伯數字如“二月春風似剪刀”轉換成密碼“2ycfsjd@”

第四式 中英文匹配

選擇熟悉的一句話，部分用拼音其餘用英文單詞代替，並加上數位與特殊字元進行組合。如“我愛工作”“wo love work@7”

漏洞三使用沒有密碼的公共 Wi-Fi

為了滿足線民手機上網需求,現在不少商家都配備 Wi-Fi 來吸引消費者。“公共 Wi-Fi”雖然方便，卻也有不少安全隱患。駭客們喜歡在“公共 Wi-Fi”裡設置埋伏,線民一不小心就會中招,輕則損失錢財,重則個人資訊全洩露。

手機如何安全使用“公共 Wi-Fi”？下面幾招教給你：

1.手機設置禁止自動連接 Wi-Fi

2.拒絕來源不明的 Wi-Fi

3.使用安全軟體檢測 Wi-Fi

4.不使用陌生 Wi-Fi 進行網購

5.警惕同一地區多個相同或相似名字的 Wi-Fi

漏洞四放鬆對“熟人”釣魚郵件的警惕

釣魚郵件是指駭客偽裝成同事、合作夥伴、朋友、家人等用戶信任的人，誘使用戶回復郵件、點擊嵌入郵件的惡意連結或者打開郵件附件以植入木馬或惡意程式，進而竊取使用者敏感性資料等的一種網路攻擊活動。

防範釣魚郵件要做到“五要”：殺毒軟體要安裝；登錄口令要保密；郵箱帳號要綁定手機；公私郵箱要分離；重要文件要做好防護。

另外，不要輕信寄件者位址中顯示的“顯示名”。因為顯示名實際上是可以隨便設置的，要注意閱讀發件郵箱全稱；不要輕易點開陌生郵件中的連結；不要放鬆對“熟人”郵件的警惕。如果收到了來自信任的朋友或者同事的郵件，你對郵件內容表示懷疑，可直接撥打電話向其核實。

漏洞五掃描來路不明的網站或 APP 上的二維碼

移動支付時代，掃描二維碼已經成為我們生活中最稀鬆平常的事兒。可是，這些二維碼看起來方便，但是一不小心，你可能就要付出錢財損失的代價。

以下是常見的幾種二維碼詐騙伎倆

01 在商場購物時，遇到稱“掃二維碼”就能免費贈送商品的“推銷員”，大家決不能抱著“不要白不要”的想法順手掃碼。有些不法分子利用了這種心理，通過各種方式誘導受害者掃描二維碼。受害人在不知情的狀態下登錄預設網站自動下載木馬病毒，導致個人資訊、網銀密碼被竊取。

02 有不法分子會通過微信向大家發送一個二維碼，謊稱掃描二維碼幫忙刷一下淘寶店的信譽，還能得到傭金。市民一旦輸入了手機號和銀行帳號，不久後微信錢包裡的餘額會被轉走。

03 有人在車窗上看到“違法停車單”，單子底部附有一個二維碼，如果車主掃二維碼進入，螢幕上就會出現一個 200 元的轉帳介面。該手段比傳統詐騙有較強的迷惑性，群眾容易上當受騙，社會危害相當大。

所以，一定要慎重甄別網路虛擬身份，切不可相信來路不明的二維碼，填寫帳號、密碼時，一定要驗明對方身份真假，謹防受騙。一旦發現錢款被轉走，及時報警。