**如何安全地使用手机**

随着移动互联网和智能终端的不断发展，手机、平板电脑等早已成为人们工作、生活和娱乐不可或缺的“利器”，如影随形。也正因其功能强大，稍有不慎，“伤”到自己的情况也较为普遍。网络钓鱼、木马病毒、敌特机关精心设计的陷阱大量充斥在无形的网络空间，用户稍有不慎，便会跌入其中且难以察觉。笔者总结了手机使用过程中的10个注意事项，身处特殊重要岗位和涉密程度较高的人员应当尤为注意。

**不要过于详细地记录联系人信息。**随着人们交际活动的不断增多、朋友圈的不断壮大，手机通讯录的厚度也会相应增加。为了弄清“谁是谁、在何处、什么单位”等情况，一些人便在通讯录中增加了备注信息，或直接将这些信息加在联系人的姓名后，如：张三，北京，××局局长；李四，××部队团长……殊不知，此做法在方便自己区分的同时，也方便了敌特分子和诈骗人员。一旦手机丢失或被植入木马，极易造成隐私和敏感信息外泄，种下失泄密和安全隐患。为此，大家在存储手机号码时切莫过于详细，如若想方便区分，可添加一些易于自己记忆的代号或记录在纸质通讯录中。

**不要轻易将智能终端操作系统破解。**这里所说的破解，即通常我们说的“越狱”（IOS系统）、“ROOT”（安卓系统）等提高权限的操作。通过破解系统可实现软件自由（免费）安装、内置程序卸载、系统权限和资源自由分配等功能。然而，在系统被破解后，系统更新通常也无法正常运行，以致系统BUG和安全漏洞无法修补，严重影响智能终端安全。以苹果产品为例，“越狱”后的苹果产品，表面上摆脱了苹果软件商店的束缚，可安装第三方提供的免费破解软件。然而，这也大大增加了遭遇恶意程序和木马病毒的风险，且病毒同样可以获得系统最高权限。一旦中招，你的声音、图像和手机里的一切信息将“被分享”。倘若不会分辨、不加甄别，便更容易中招。为此，在没有特殊需求的情况下，尽量不要破解系统或将手机系统刷成非官方的系统。

**不要轻易连接免费Wi-Fi和无加密防护的Wi-Fi网络。**天下没有免费的午餐。使用免费或没有加密防护的Wi-Fi网络，除极易被“钓鱼”外，通信内容也极易被监听和篡改。若是连上了“黑”Wi-Fi，手机还可能遭到攻击和被植入木马。特别要说明的是，使用像“Wi-Fi万能钥匙”“免费Wi-Fi”等软件并不安全，其相当于一个公用数据库，收集和分享大家掌握的WiFi网络和密码，若使用，你所掌握的Wi-Fi密码自然也有可能被与人分享。若被别有用心的人由此连上了你的路由器并监听其中数据，那么，你的网络访问便也毫无安全可言。

**不要轻易打开GPS定位系统。**手机的GPS模块一方面，可以方便我们导航、出行和娱乐．另一方面，也可能暴露我们的位置信息。当用户的位置信息积累到一定量，通过分析很容易推断出用户的工作地点、工作性质、家庭住址、生活规律等。目前，市面上有许多软件也都会访问和收集用户的位置信息，如一些社交类软件、导航类软件，甚至影音娱乐软件等。央视就曾曝光过苹果手机未经用户许可，窃取用户位置信息的丑闻。我们关闭定位功能后，系统中的许多软件将无法获取用户终端的位置信息，这在一定程度上提高了手机的安全性，所以，在平时应尽量将GPS开关置于关闭状态。

不要轻易扫描来路不明的二维码。扫描二维码是一种便捷的操作手段，可实现商品信息快速查询、链接快速跳转、网络购物、手机支付、产品推广等功能。然而，单从二维码本身并看不出其中隐藏了什么内容，这也正好成了一些别有用心之人可钻的空子。他们将恶意程序和木马病毒制作成二维码在网络上大肆传播，一旦用户扫描，手机便会在后台自动下载并安装病毒程序，从而威胁你的隐私和财产安全。因此，扫描二维码前一定要确定其来源，必要时，可使用一些二维码安全鉴别软件来识别恶意二维码。

不要随意乱拍照。看到这点，你可能很诧异：拍照和信息安全有什么关系呢？现在的智能终端都具有拍照功能，并且像素非常高，手机也是如此，它已然成为许多入的相机和“记事本”，工作时拍几张、吃大餐时拍几张，甚至一些文件资料和证件都用手机拍下来，以方便使用。殊不知，在拍照的同时，手机会将你拍摄的时间和空间信息存于其中，如若保管不当或设置不当，照片外流，很可能给你的隐私和文件资料安全造成威胁。因此，在没有需求的情况下，最好关闭相机的位置标签功能和GPS开关，在敏感、涉密场所或处理特殊公务时不要用手机拍照，更不要用手机拍摄涉密、敏感的文件资料和重要证件。尤其值得注意的是，即便手机拆下电池，也不能带入重要涉密场所。

不要把手机当U盘使用。现在的智能手机存储空间都相对较大，许多人喜欢什么资料都存入其中，方便携带和使用。其实，这样做存在安全隐患：一方面，手机与其他设备频繁连接，增加了交叉感染木马病毒的可能性；另一方面，手机连接网络，被植入木马病毒或是丢失极易造成信息泄露。特别应注意的是，不要将手机连接在涉密计算机上充电，如此，相当于建立了一座涉密计算机通向互联网的桥梁，应格外注意。

不要轻信、乱传网络上的“段子”。前几年，微博、微信上充斥着许多夸张、吸引眼球的不实信息和谣言。伴随着网民素质的提高，这些负能量的转发大量减少。然而，一些“新伎俩”频频现身，即把谣言和负能量以“白十黑”的模式化妆起来，让人看起来像真理、正能量，以蒙混过关，达到传播负面信息的目的。比如，笔者近期就曾收到过关于“抵制日本贞子电影”的段子，其前文呼吁中国人不要去影院看贞子电影，后文又称“5·12”是南京大屠杀纪念日，大家应牢记历史！实际上“5·12”是汶川特大地震发生的时间，而南京大屠杀纪念日是12月13日。像这样的信息显然不属实。倘若网友不加甄别地转发，那么许多不明真相的人便会错记国难、国耻日，这对于一个民族来说，实属可悲！所以，网络中的段子不可轻信、乱传。

不要轻易使用“云备份”功能或开启自动备份开关。目前，几乎所有品牌的智能手机都有“云备份”功能，该功能主要是将用户的通讯录、短信、照片等数据上传至云端，以实现节省本地空间、易于转移调用、方便故障恢复等目的。然而，无论是手机生产商，还是软件商提供的“云备份”，用户都需要承担传输信息安全和存储信息安全的风险，且信息上传到云服务器后，谁又能保证这些数据是否会被丢失、浏览或篡改呢？所以重要数据资料还是备份在自己手中为好，如U盘、移动硬盘等。

不要轻易出售废旧手机。废旧手机及存储卡通常存储有用户的通讯录、短信文电和图文数据，即便删除，也极易运用软件恢复，从而威胁用户的隐私、财产和数据安全。所以，废旧手机还是谨慎处理的好。