国家网络安全宣传周
China Cybersecurity Week

网络安全为人民
Cybersecurity is for the people
网络安全靠人民
Cybersecurity depends on the people

国家网络安全宣传周
China Cybersecurity Week

个人信息安全防护宣传册

PERSONAL INFORMATION SECURITY

前 言
Introduction

随着信息技术应用范围的不断扩大和深入，个人信息安全也面临更加严峻的形势，银行卡在自己手里，钱却被人盗取；手机号码并未随意告知，却总是接到各种骚扰电话；随意晒一晒照片，马上便有人猜出拍照地点；以及近几年频频成为新闻焦点的网络金融诈骗事件等。隐私泄露层出不穷，财产受损现象频繁发生，“我的信息安全吗？”已成为个人隐私关注的焦点。

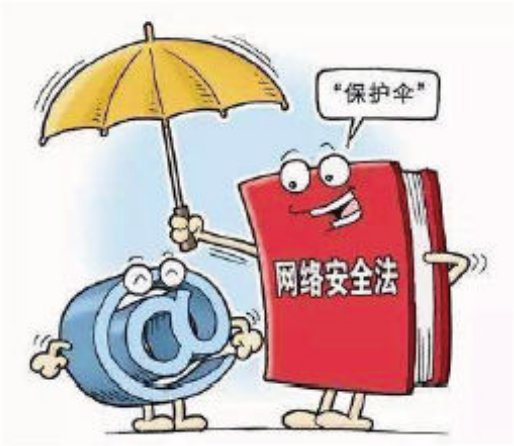
本宣传册结合2017年6月1日正式施行的《中华人民共和国网络安全法》（简称《网络安全法》），围绕个人生活中经常使用的智能工具，用简单易懂的语言重点讲述了电脑、手机、QQ、微信、电子邮件等的安全使用和防护方法，期望让每一位读者能轻松获知个人信息安全防护的基本知识以及相关法律。

目 录
CONTENTS

《网络安全法》是什么？

《网络安全法》全称为《中华人民共和国网络安全法》，是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。

《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法制建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。



违反了《网络安全法》有哪些处罚？

1、窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款；

2、从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，则予以处罚如下：

(1)由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；

(2)情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

公民、组织有哪些义务和责任?

1、遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家破坏国家统一，宣扬恐怖主义、极端主义、宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动；

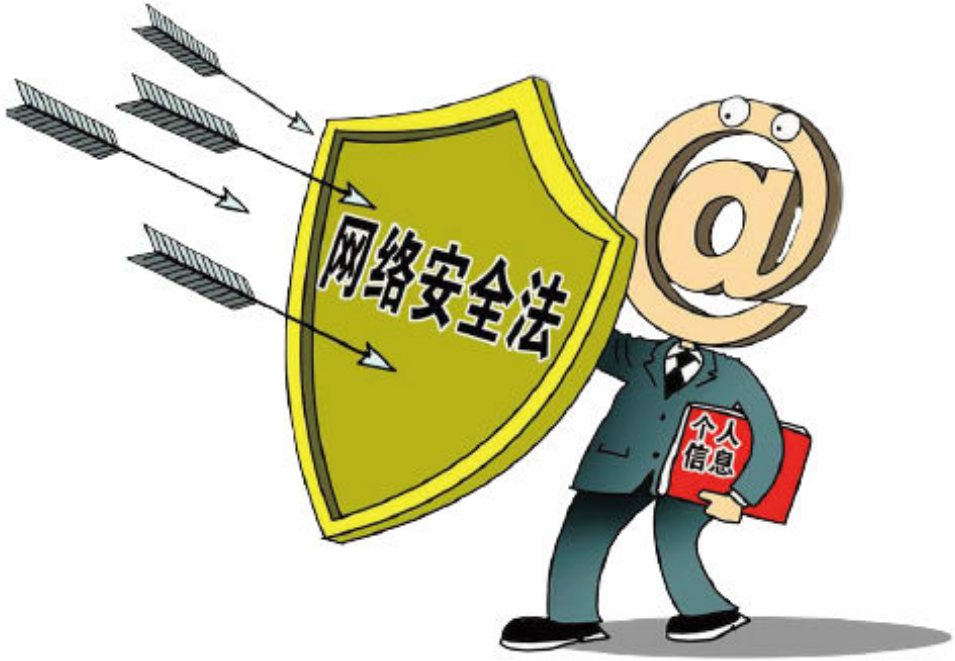
2、不得从事危害网络安全的活动，亦不得为之提供程序、工具和帮助；

3、不得设立用于实施违法犯罪活动的网站、通讯群组，不得利用网络发布涉及违法犯罪活动的信息；

4、在电子信息、应用软件中，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息；

5、国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及、提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动；

6、对危害网络安全的行为有权向网信、电信、公安等部门举报。



伪基站的防范

市民郑女士收到"10086"发来的一条短信，称郑女士有大量积分，可以兑换一笔金额不小的话费。郑女士随后点击了短信上的网址链接，进入了一个兑换话费的网页，并按提示输入了自己的支付宝账号密码和银行卡密码。郑女士等了几天，说好的话费却迟迟没有到账，更蹊跷的是，她发现自己在支付宝上绑定的三张银行卡内资金莫名减少，共被转走2.7万元。

事后追查，郑女士是中了"伪基站"的诈骗圈套。

安全解读：

"伪基站"即假基站，不法份子利用现代计算机与通讯技术伪装成运营商的基站，向"伪基站"周边一定范围内的手机发送信息。伪装的号码多为银行、运营商、党政部门的官方号码。伪基站设备运行时，用户手机信号被强制连接到该设备上，导致手机无法正常使用运营商提供的服务，手机用户一般会暂时脱网8～12秒后恢复正常，部分手机则必须重启才能重新入网。

在排除周边信号不好或者存在信号死角之外，当通话中信号突然中断时，很可能是被伪基站强制吸走，信号被"切断"。

安全小贴士：

1、不打开不明短信链接；
2、发现手机信号突然中断的时候，提高警惕；
3、遇到中奖、抽奖等字样时格外警惕；
4、在手机上被要求输入银行、支付宝等账号及密码时要格外小心，尽量不要在非官方APP或网页上进行操作。

钓鱼Wi-Fi的防范

公共场所免费Wi-Fi越来越多，人们进入酒店、餐馆、商场等公共场所后习惯先打开Wi-Fi功能，看一下是否有免费的Wi-Fi信号，甚至在家也有"蹭网"的习惯。

南京市民张先生使用公共场所的Wi-Fi后，电脑被黑客入侵，在U盾、行卡均未丢失的情况下，网银被他人在两天内盗刷69次，卡上的6万多元仅剩下500元，与此同时他的手机也被黑客做了手脚，接收消费提醒短信的功能被屏蔽，所发生的69次交易他根本没收到任何短信提示，钱在不知不觉中被转走了。

安全解读：

钓鱼Wi-Fi的成本很低，黑客一般只需几百元便可以设置一个钓鱼Wi-Fi 并在公共场合部署，而且在名称上与免费Wi-Fi相似。

例如：咖啡厅的正规Wi-Fi信号叫 coffee-free，钓鱼Wi-Fi信号有可能取名叫coffee-free2等等。受害者访问钓鱼Wi-Fi时，他的所有数据信息都可能会被钓鱼Wi-Fi记录下来，从而盗取QQ账号、微信账号、游戏密码等个人隐私信息，甚至导致严重的财产损失。

警惕钓鱼WiFi 安全使用公共WiFi

安全小贴士：

1、关闭手机自动连接Wi-Fi的功能；
2、在公共场所，不要连接未知的Wi-Fi；
3、不要将自己家的Wi-Fi密码共享，定期修改密码；
4、在未知的Wi-Fi信号下不要输入QQ、微信、游戏、银行、支付宝等密码。

通信诈骗的正确防范

通信诈骗近年来发展快速，涉及面广，后果严重。山东临沂大一新生徐玉玉，开学前接到一通声称有一笔2600元的助学金要发给她的电话，当天是最后一天，要求她通过ATM机将9900元学费汇入自己的账号，助学金连同学费将会在半小时内一起汇款回来。当她完成操作后，对方电话已经关机。反应过来自己受骗的徐玉玉万分难过，两日后遗憾离世。清华大学一名教师也被"冒充公检法"的人员要求其将钱款打入"安全账号"，结果被诈骗卷走1760万元。

安全解读：

通信诈骗是近年来比较普遍的一种新型网络犯罪行为。不法分子通常使用任意显号软件、网络电话等技术，利用电话、短信、QQ、微信、微博公众号等社交工具，冒充公检法机关，医保、社保、救助等政府部门和运营商、房东等，以牵涉司法事宜、资助金领取、电话欠费等进行诱拐或恐吓威胁，骗取受害人汇转资金。

安全小贴士：

1、凡是谈到银行账户信息，一律挂掉；
2、凡是谈到中奖了，一律挂掉；
3、凡是短信让点击链接的，一律删掉；
4、凡是微信发来的莫名链接，一律不点；
5、凡是谈到"电话转接公检法"，一律挂掉；
6、凡是自称领导、同事要求汇款的，一律不管；
7、凡是告知"家属"出事需要先汇款的，一律举报；
8、如不幸受骗：

(1) 保存好汇款或转账时的凭证并立即拨打110报警，或到当地公安刑警队、派出所报案；

(2) 向警方说清被骗经过，准确提供受害人姓名、受害人转出现金的账户及开户行信息；

(3) 向警方准确提供骗子的账号、账号用户名及账户开户行（银行柜台及银行客户均可以帮助查询）；

(4) 向警方提供汇款凭证或电子凭证截图。

二维码的正确扫描

二维码已经在我们的生活中扮演着相当重要的角色，只要掏出手机扫一下别人，或者被别人扫一下，我们就可以做到吃饭不带钱，认识好友不带名片，偶尔还可以领取不要钱的小礼品。

泰兴市民倪女士在淘宝网上经营一家网店。前不久，一位淘宝买家购物后，利用旺旺与其交流，就在准备支付时，对方发来了一个消息，希望倪女士通过扫描二维码方式结算。倪女士为了得到对方的"好评"，便同意了对方的要求。掏出手机扫了对方发来的二维码，可等了一分钟左右也没显示成功，手机网页也变得很卡。倪女士觉得不对劲，马上用电脑登录支付宝账户，支付宝密码已被修改。随后发现网银上的9万元已被转走。

经调查发现，倪女士扫描的二维码被植入木马类病毒，手机中毒后服务密码被窃取。

安全解读：

不法分子通常虚拟伪装一个网站，并生成二维码，实际上这个网站带有木马病毒。受害人扫描该二维码后，不法分子通过云端软件获取了倪女士的身份证号、银行账号、手机号码等重要信息，并截取淘宝平台发来的信息如验证码等，便可轻松转走受害人卡里的钱。有的还将这些个人信息再次出售给其它渠道，从中二次获利。

安全小贴士：

1、不要贪图便宜随便扫描未知二维码；
2、扫描后若要求填写个人账户信息，应当坚决拒绝，不要犹豫；
3、手机安装正规防病毒软件，定期扫描手机安全性。

快递单的正确处理

随着电子商务的快速发展，“淘宝”、“京东”等各大电子商务平台均受到大家的青睐，网络购物日益成为一种流行的消费形式。

厦门市民夏女士，习惯把快递包装盒随意丢弃，包装盒上的快递单未经处理，泄漏了个人住址、联系方式等信息。不法分子通过掌握相关信息假扮快递公司员工，骗取夏女士信任，入室实施抢劫。该事件公布后，某网站发起“你平时乱丢网购包装吗?”的调查，有1.8万名网友参与调查，其中10526名网友表示“我经常乱丢网购包装，以后要注意个人信息”。

安全解读：

为了保证能收到快递，快递单往往要求准确填写收、寄件人的姓名、电话、收货地址、工作单位等信息。收件人收到快递后，如果不对快递单上的个人信息进行擦除或撕毁等处理，这些信息往往给不法分子留下可乘之机。

安全小贴士：

1、填写收货人地址时应注意相关内容；

2、丢弃包装时应先清除快递包装盒上的个人信息。

充电宝的安全使用

随着掌上互联网的兴起，掌上移动电子设备成了人们日常生活中必不可少的工具，充电宝作为这一类的衍生物，也占据了举足轻重的位置。可许多人并不清楚，充电宝也能泄密。

成都市民任女士工作常有出差安排。某次出差途中，任女士手机没电了，恰巧周围没有充电插口，只得借用一名男士的充电宝。次日，任女士便接到一通陌生电话，对方称手里有任女士手机中的所有信息，包括一些重要的客户资料，如不拿出3000元赎金，将要如何如何……经调查，任女士的信息泄露源头居然就是随意借用他人的充电宝导致的。

安全解读：

市面上有一种被植入木马程序的"病毒充电宝"，手机一旦连上它充电，病毒就会通过USB接口自动读取手机信息，不法分子就可以借助电脑连接的互联网将此前收集到的个人信息隐蔽传输至任何地方，从而达到自己的非法意图，给受害者带来损失。

安全小贴士：

1、从正规渠道购买移动充电设备；
2、尽量不借用他人充电设备；
3、最好使用直充电源，谨慎使用公共场所提供的免费充电接口；
4、手机在连接"问题"充电宝后，不要点击提示的"信任"选项。

淘汰手机的安全处理

新款手机层出不穷，更换手机的频率大大加快，许多人选择卖掉或者丢弃废手机，殊不知废弃手机变成了个人信息泄露的罪魁祸首。

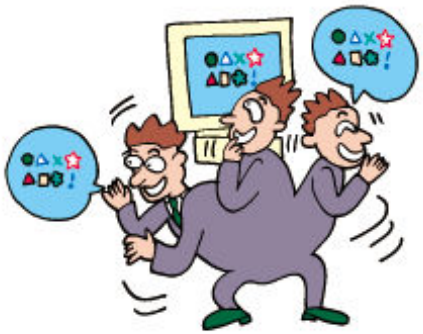
深圳市民张女士新买手机后将旧手机卖掉，在出售旧手机时通过"恢复出厂设置"方式清除手机信息。但令人震惊的是，一周后张女士收到一条名为"我手上有你的艳照，如要赎回，立马转账2万元"的消息，短信内还附了一张张女士的生活照片。

安全解读：

删除手机数据相当于拆房子，被删除的数据就像是写上了"拆迁"两字的旧房子，只是做了一个标记，在房子真正被推倒之前，我们都能从旧房子里获取到一些信息。手机上的数据删除后只要储存路径没有被覆盖，都能通过软件恢复。即便使用手机自带的"恢复出厂设置"功能，也无法彻底删除全部数据。现在网上也有一些手机数据恢复软件，甚至还有详细的教程，只要下载软件和参照教程，任何人都可以进行数据恢复。

安全小贴士：

1、在出售旧手机之前务必删除个人信息，拔出手机卡及存储卡；
2、找专业人士帮助清除手机信息；
3、解除手机应用软件所关联的服务。

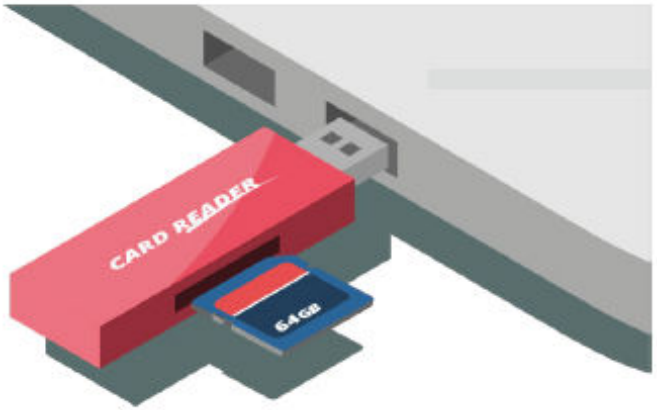


移动存储介质的正确使用

U盘、移动硬盘、内存卡等移动存储介质，在为我们工作带来便利的同时，也带来了不容忽视的信息安全隐患。

市民王先生，在家办公将相关工作资料拷贝到U盘中，带到公司继续工作。在U盘插入电脑一分钟后，电脑突然死机，再次开机后显示该电脑已中病毒。

事后调查发现，王先生的U盘在家使用时已被植入恶意病毒。



安全解读：

借助U盘传播病毒早已成为病毒传播的主要方式。U盘病毒通常是利用Windows系统的自动播放功能进行传播，当用户打开U盘浏览内容的同时，病毒便会自动运行。

安全小贴士：

1、保管好移动存储介质，防止被盗、丢失造成泄密；
2、工作用与生活用的移动存储介质区分，减少在多台电脑上的交叉使用；
3、采用正规的杀毒软件经常对电脑、移动存储介质进行病毒查杀；不定期更换不同的防病毒产品进行查毒；
4、关闭移动存储介质的自动播放功能，先查杀病毒再使用。

云盘网盘的安全使用

随着信息化的快速发展，云存储服务出现了，在线存储的容量更大功能更丰富更具吸引力。于是，网盘（云盘）成为办公、生活、娱乐的重要存储方式。网盘又称网络U盘、网络硬盘，可提供文件的存储、访问、备份、共享等文件管理功能。不管是在家中、单位或者其他任何地方，只要连接到因特网，就可以管理、编辑网盘里的文件。不需要随身携带，更不怕遗失。因此，使用人群也越来越广泛。

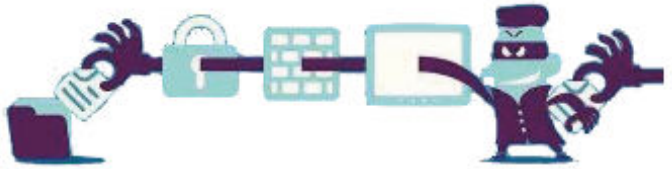
近日，某知名在线数据管理网站被发现其文件共享机制存在安全风险，导致许多企业的部分机密数据和文件可以被谷歌、必应等搜索引擎直接检索。

安全解读：

专家测试后表示，许多网盘在进行数据上传和下载的过程中，客户端和服务器传输的数据是没有经过加密的明文，攻击者（黑客）可以直接截取数据包。同时，黑客还能够利用窃取到的用户历史访问数据，适当修改文件名和路径，对用户的所有数据进行读取和删除操作。给网盘使用者带来重大损失。

安全小贴士：

1、尽量不要用网盘存储私密信息，以防止信息泄露；
2、网盘里的储存内容一定要在本地备份，避免被不法人士删除、修改；
3、使用网盘传输文件后，应做出删除之类的处理。



路由器的正确使用

移动互联网时代，路由器几乎成为家庭网络的标准配置。市民何先生从不"蹭网"，家里的上网密码也只有家人才知道。然而何先生家的网络突然无法使用，显示密码不正确。

经调查，何先生家的路由器遭到不法分子的攻击，何先生的个人信息被盗取，路由器的登录密码也被修改。

安全解读：

由于路由器的产品特性，用户往往会忽视对路由器使用安全的管理防范，比如设定简单的密码，长时间使用同一密码等。不法分子利用这些"漏洞"入侵家用网络，可实时掌握用户利用该网络进行的任意互联网操作，甚至入侵接入设备，提取设备中的敏感信息，修改路由器登陆密码等，给用户造成密码输入错误或者路由器坏的假象。

同时，由于家庭网络一直将房主的设备列为可信任设施，一旦侵入这个网络，就可以对智能门铃、智能摄像头等智能设备进行恶意攻击。

安全小贴士：

1、一定要修改路由器管理初始账户，并增加密码强度；

2、限定路由器管理IP，开启相关登录限制措施，如路由器自带的"MAC过滤功能"；

3、随时关注并清理路由器上未知接入设备；

4、不要使用破解路由器密码的应用软件，防止在破解他人密码的同时，也泄露了自己的个人信息。

智能设备的安全使用

越来越多的市民为了"看家"方便，在家中装设智能摄像头，有的是看护年岁较大的父母，有的是看护年幼的孩子，有的是为了监测家里宠物的情况，还有的为了防盗。用户在获得方便的同时，隐私也可能在不知不觉中遭到泄露。

市民尹先生称，自己和妻子平时上班都比较忙，家里的老人年岁已高，为了方便照看，就在家中安装了智能摄像头，没曾想，自己和家人的隐私居然被曝光在某网站。

经调查，尹先生的生活录像被曝光的网站为不法网站，该网站可自由查看多家家庭实时摄像画面。

安全解读：

目前市场上的智能设备在使用过程中都会填写用户的个人信息（身份证号码、电话、邮箱等）、地理位置信息（家庭、公司地址）、个人账户信息等。以上所有信息由设备提供方统一监管，如存在员工监守自盗或平台自身安全防范措施有限等问题，都将被不法分子利用，轻则根据用户地理位置展开精准的买房、买车等各类推销，重则可能发生重大财产损失等。

安全小贴士：

1、通过正规途径购买设备；

2、随时关注所用品牌安全方面的消息，如果发现设备漏洞及时停止使用,等待厂家更新,并保证所使用APP是最新版本;

3、不安装第三方控制APP，尽量在系统提供的商店下载正规APP，碰到要输入身份证或照片的时候,提高警惕,确认安全后方可执行操作;

4、所使用的控制APP尽量关闭应用中的敏感权限，如读取通讯录、读取短信通话记录、允许定位等。

移动支付的安全使用

随着移动支付的盛行，为广大群众带来众多便利与快捷的同时，隐患也随之潜伏，随时随地可导致个人信息及财产受到威胁。其中，手机短信验证替代银行密码，在方便市民操作的同时，也留下了安全隐患。

市民李女士在跟朋友聚会的过程中，不幸挎包被盗，手机、身份证、银行卡都在包里。还没等她挂失，就发现银行卡被人通过支付宝盗刷了3700元。

李女士很纳闷，在没有密码的情况下，钱是怎么被盗走的?

安全解读：

微信支付、支付宝支付、Apple Pay等移动支付以绑定银行卡的快捷支付为基础，用户购买商品时，不需开通网银，只需提供银行卡卡号、户名、手机号码等信息，银行验证手机号码正确性后，第三方支付发送手机动态口令到用户手机号上，用户输入正确的手机动态口令，完成支付。不法分子从拿到受害人的手机和钱包，到绑定成功再到转账完毕，整个过程只需耗时3分钟。

安全小贴士：

1、手机、身份证和银行卡，尽量不要放在一起，避免同时丢失造成损失；

2、第三方平台的支付密码与银行卡的支付密码不要相同；

3、第一时间到公安机关和银行办理挂失，及时关闭无线支付业务；

4、手机和第三方支付平台设置不同的解锁密码，手机内不要存储身份证及银行卡信息；若丢失，及时补办手机号。

社交网络的正确使用

社交网络工具的广泛使用，使人们个人情感、生活和学识得到了更加充分的展示。然而，这些社交网络也潜伏着隐形的安全隐患。

杭州市民尤女士晚饭后带着6岁的外孙女茵茵到附近的广场跳舞，茵茵在广场上独自玩耍。一名约40岁的陌生女子问她是不是叫茵茵，随后还说出了许多与茵茵匹配的信息，并诱骗其一起去找妈妈。正在小姑娘犹豫的时候，尤女士的舞伴发现了端倪上前问询，陌生女子快速离开。

经查证，陌生女子是通过尤女士女儿的社交网络了解到茵茵的长相、名字、日常活动场所等信息，于是发生了广场诱拐茵茵的一幕。

安全解读：

许多家长在社交网络"晒幸福"不经意间泄露了孩子的学校、相貌、家人等信息，这些都容易被不法分子利用，通过绑架、恐吓等方式向家长索要钱财，危害孩子的生命安全。信息发布时如果还带有炫富色彩，那就更可能被不怀好意的人"盯上"。

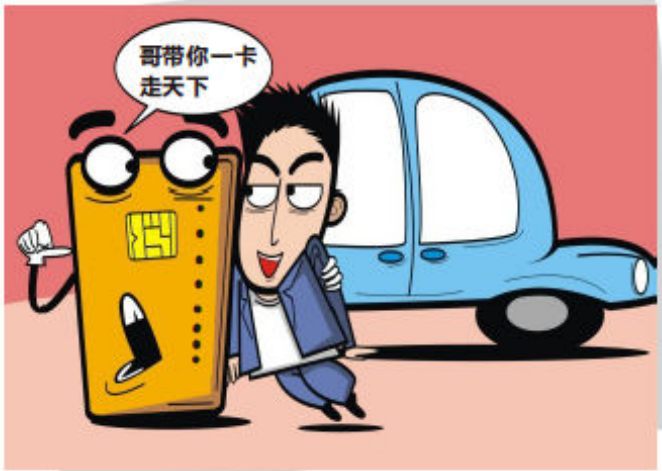
安全小贴士：

1、不要暴露平常外出的日程、行踪，不要晒贵重物品等；
2、不要随意发布火车票、飞机票、护照、车牌、孩子照片及姓名等信息；
3、在手机中关闭位置设置功能；
4、在社交软件设置中增加好友验证功能，关闭"附近的人"和"所在位置"等功能。

正确使用ETC

当今社会，几乎所有的商家都把"如何更加便捷的使用我们的产品"当作基本目标，因此便捷的出行、便捷的联系、便捷的支付等成为使用的热点。其中，便捷支付更是渗透到生活中各个角落。

日前，一段便携式POS机盗刷ETC的视频引发网友热议，不少网友开始担心ETC的安全性。视频显示，有人手持一台便携式POS机在一辆装有ETC的车前挡风玻璃处一碰，显示付款100元成功。随后，签购单显示，"交易金额未超300元，免密免签"。



安全解读：

专家进行了专门的测试，结果显示，如果车上插的是ETC专用卡，不用担心被POS机盗刷，因为只有高速公路的收费站才能扣款。该手段是不法分子利用了银联卡小额免密的功能，在特定场景下实施的不法行为。

其中，在使用小额免密免签服务时，持卡人只需要把具有"闪付"功能的金融IC卡，靠近POS机等受理终端的"闪付"感应区"挥卡"，就可以完成支付；另外，所有商户POS机的申领和小额免密免签业务开通都需要满足一系列条件，且双免交易一般要求机器和IC卡距离在3到4厘米以内才行，超过这个距离无法进行交易。

安全小贴士：

1、尽量使用ETC专用卡；
2、对于只有ETC用的卡片，关闭除ETC以外的其他功能；
3、可关闭所使用储蓄卡/信用卡等IC芯片卡的"小额免密支付"功能；
4、建议车里的ETC银行联名卡，在停车后最好拔下来；
5、若已有异常的免签免密交易发生，持卡人可以第一时间联系发卡银行申请补偿。