广东技术师范学院

宣传册

个人信息安全防护

网络信息中心

2018.09

广东技术师范学院

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，信用卡明明在自己手里，钱却被人取走；手机号码只告诉了认识的人，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；还有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？”已成为每个人关注的问题。

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，用浅显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，将期望让每一位读者都能轻松地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。

伪基站和钓鱼Wi-Fi的防范

安全解读：

"伪基站"即假基站，不法分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，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的可能之外，若通话时信号突然中断，很可能是被伪基站强制"吸走”，导致信号中断。

另外，用户喜爱在公共场合使用免费Wi-Fi，常常被不法分子利用，以低廉的成本架设钓鱼Wi-Fi。受害者访问钓鱼Wi-Fi时，所有的数据信息都可能会被钓鱼Wi-Fi记录下来，从而盗取受害者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。

安全小贴士：

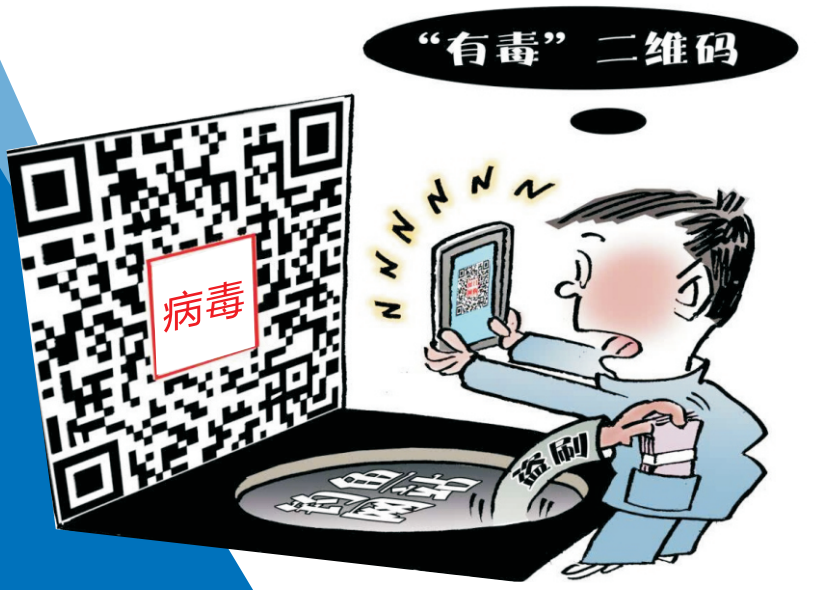
1、关闭手机自动连接Wi-Fi的功能，不轻易连接未知Wi-Fi；

2、未知Wi-Fi信号下，不要输入涉及个人信息的账号及密码；

3、不打开不明短信链接，如遇手机信息突然中断,需提高警惕；

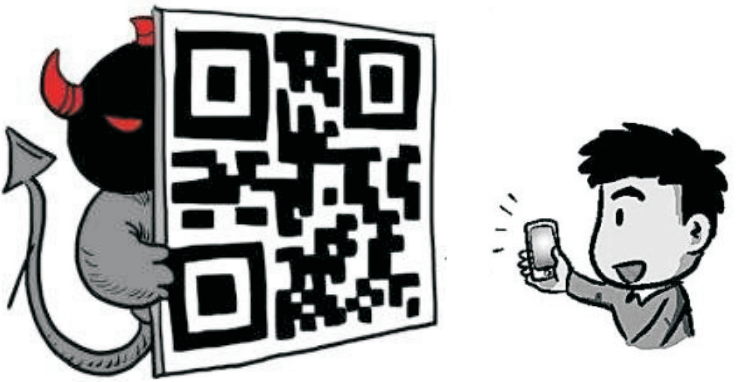
4、在手机上被要求输入银行、支付宝等账号及密码时要格外小心，尽量不要在非官方APP或网页上进行操作。

校园二维码的正确使用



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受害人的身份证号、银行账号、手机号码等重要信息，并截取正在使用的某平台发来的验证码、确认码等，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，随便扫描未知其安全性的二维码；

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。

邮件的正确使用

安全解读：

大部分入侵事件的入口和出口都是电子邮件。不法分子利用电子邮件打开安全防线的突破口，而电子邮件内容的泄露可能导致个人重要信息泄露。而在网络里，电子邮件是永存的，这使得邮件面临巨大的安全隐患。

安全小贴士：

1、经常登录的邮件客户端，如计算机、手机、平板电脑等应当安装有防火墙、杀毒软件等防护工具，并及时更新病毒库和操作系统安全补丁；

2、邮箱可根据不同用途设置多个账号，重要账号密码可定期更换；

3、谨慎打开来历不明的邮件，勿随意点击邮件中的链接或附件；

4、不要在不确定其安全性的Wi-Fi环境下，登录使用重要邮箱。

移动支付的安全使用

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、如盗刷事件已发生，应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。若手机丢失，及时补办手机号，重新绑定相关信息。

社交网络的正确使用

安全解读：

许多用户在社交网络“晒幸福”，不经意间就泄露了与自己相关的外貌、住址以及家人等信息。不法分子利用这些信息，通过绑架、恐吓等方式向家人索要钱财，危害自身及家人的生命安全。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”，导致重大人身财产损失。

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、家人照片及姓名等信息；

3、关闭手机中的自动定位功能，需要时再打开使用；

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。

网盘、云盘的正确使用

安全解读：

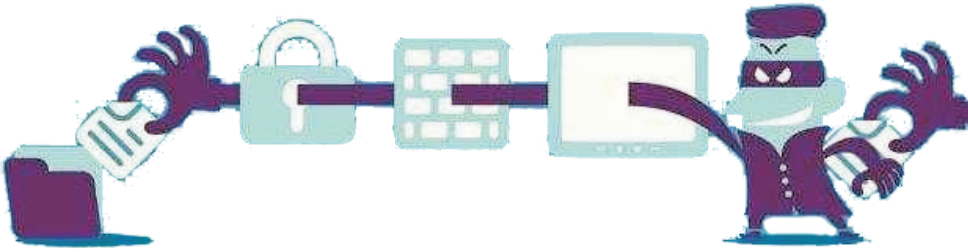
专家测试后表示，许多网盘在进行数据上传和下载的过程中，客户端和服务器传输的数据是没有经过加密的明文，攻击者（黑客）可以直接截取数据包。同时，黑客还能够利用窃取到的用户历史访问数据，适当修改文件名和路径，对用户的所有数据进行读取和删除操作，给网盘使用者带来重大损失。

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，应及时进行云端信息删除处理。



手机APP的安全使用

安全解读：

一些手机APP掌握了庞大的客户信息，一旦泄露，用户不仅可能遭遇广告骚扰，也可能受到诈骗，造成重大财产损失。某些手机APP甚至本身在后台会执行“吸费”程序，以谋取暴利。

安全小贴士：

1、选择正规下载渠道和更新渠道，不要点击未明确来源的链接或二维码随意下载；

2、慎重安装“破解版”APP，以避免有恶意代码植入的APP；

3、适当设置“应用权限”，不可所有权限都设置“允许”；

4、对不同用途的APP进行分类，设置不同的密码。

智能设备的安全使用

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、电话）、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，轻则会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、不装陌生APP，尽量在系统提供的商店下载正规APP，在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；

2、分类管理APP，设置不同的账号、密码；

3、不要随意登录或扫描不确定其安全性的免费Wi-Fi和二维码；

4、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。

个人信息的正确使用

安全解读：

许多服务提供商会自行整理归档用户的个人信息。如果内部存在投机人员，这些信息将会被贩卖给其他盈利机构。信息一旦泄露，轻则不断遭受各种推销电话的困扰，重则造成个人财产损失，甚至危害个人生命安全。

安全小贴士：

1、填写个人信息之前，先明确信息的用途；

2、不随意填写身份证号、家庭住址、联系电话等重要信息；

3、如需提供身份证复印件，一定要在复印件上的关键位置标明“仅作……用途，他用无效”等字样；

4、丢弃任何记录个人信息的物品前，注意清理个人信息后再丢。

废弃电子产品的安全处理

安全解读：

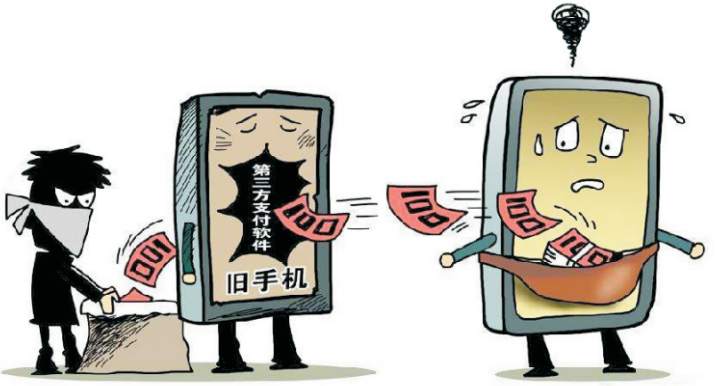
删除电子产品中的数据只是对被删除信息做了一个标记，手机上的数据删除后只要储存路径没有被覆盖，都能通过软件恢复。即便使用手机自带的“恢复出厂设置”功能，也无法彻底删除全部数据。

安全小贴士：

1、电子产品废弃处理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其中个人信息；

3、解除产品中应用软件所关联的服务。



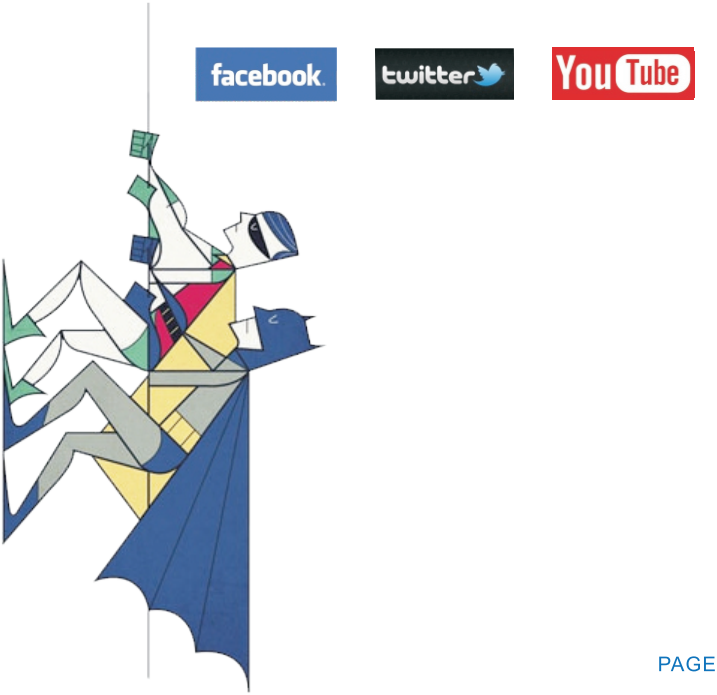
翻墙软件和翻墙行为的正确对待

安全解读：

翻墙软件提供商通常都是提供一个客户端桌面软件供我们使用，因为不了解软件是否安全，贸然使用极大可能会导致用户个人隐私被泄露，甚至一些银行账号信息的泄露。部分用户也会通过这种方式参与网络赌博，或者浏览色情网站，极大的危害了用户个人信息安全的同时触碰法律底线，每年都有很大一部分人因为翻墙软件而被盗取了各种账号密码。

安全小贴士：

使用合规合法的软件浏览网页，不采取任何翻墙行动，不使用任何翻墙软件。



防病毒、防病毒、防病毒

安全解读：

如果出现了以下的一些现象，则可以判断很可能是中毒了：

1、计算机系统经常无故死机；
2、计算机系统的运行速度明显减慢；
3、系统出现异常的重新启动的现象；
4、磁盘坏簇莫名其妙地增多；
5、操作系统无故频繁地报警或虚假报警；
6、丢失文件或文件被破坏；
7、系统中的文件时间、日期、大小发生了变化；
8、磁盘出现特殊标签或系统无法正常引导磁盘；
9、磁盘空间迅速减少；
10、计算机屏幕上出现异常显示；
11、部分文档自动加密码；
12、以前能正常运行的应用程序现在运行时经常发生死机或者出现非法错误；
13、自动发送电子邮件等。

安全小贴士：

1、建立病毒检测系统，能够在第一时间内检测到网络异常和病毒攻击；
2、建立应急响应系统，将风险降到最低；
3、建立灾难备份系统，对于数据库和数据系统，必须采用定期备份，多机备份措施，防止意外灾难下的数据丢失。

广东技术师范学院 信息中心

38256601 www.gpnu.edu.cn

地址：广州市天河区中山大道西293号

邮编：510665 传真：020-38257901