個人信息安全保護

宣傳手册

天津城建大学信息化中心制

前 言

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。隐私泄露层出不穷，“我的信息安全吗？”已经成为每个人关注的问题。

本宣传册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，期望让每一位师生都能轻松地获知个人信息安全保护的基本知识。

目 录

关于《网络安全法》

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？

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；

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：

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；

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。

关于《网络安全法》

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。

个人信息使用与传输

安全解读：

许多商家会整理归档获得的个人信息，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。此外，微信、QQ、邮箱等越来越成为工作中信息传输的媒介，信息一旦泄露，轻则不断遭受各种推销电话的骚扰，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. 减少使用微信、QQ、商用邮箱等传输涉及重要信息的文件，传输文件时采用加密传输的方式；
4. 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“仅做……用途，他用无效”等字样。

密码的正确使用

安全解读：

网上办理业务成为越来越大众化的选择，无数系统和软件的使用需要各式各样的账号和密码。为了方便，大家常常会把常用系统和软件设置为自动登录。若相关设备丢失，这些账号密码极容易被泄露，从而损害大家的信息和财产安全。

安全小贴士：

1. 设置密码时，使用字母、数字及特殊符号叠加的高强度密码；
2. 各系统和软件不设置相同密码；
3. 慎用自动登录；
4. 养成定期更换密码的习惯。

社交网络的正确使用

安全解读：

许多人习惯在社交网络“晒日常”，不经意间泄露了自己的住址、相貌、单位等信息，这些都容易被不法分子利用，盗用相关信息进行违法犯罪行为。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。

软件正版化

安全解读：

正版软件需花钱购买，而网上有许多可自由下载的免费软件资源，所以大家都习惯于从网上下载盗版软件安装使用。盗版软件易受病毒攻击，盗版的老版本操作系统已停止服务，无法升级，漏洞无相应的修复补丁，威胁信息安全。

安全小贴士：

1. 加强软件版权保护，是鼓励软件创新、优化市场环境、实施创新驱动发展战略、加快创新型国家建设的必然要求；
2. 用户使用盗版软件面临着承担一定的行政责任、民事责任甚至刑事责任的法律风险；
3. 软件正版化事关国家和单位的信息安全。

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了受害人的身份证号、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。

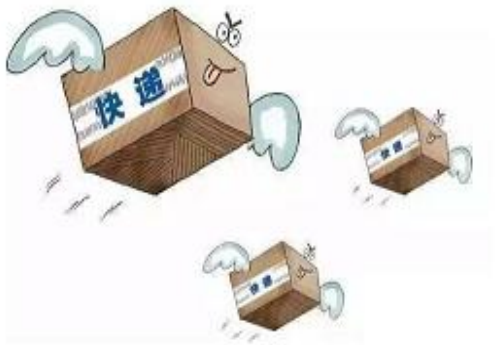
快递单的正确处理

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。



淘汰手机的安全处理

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。

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

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。

钓鱼 Wi-Fi 的防

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。

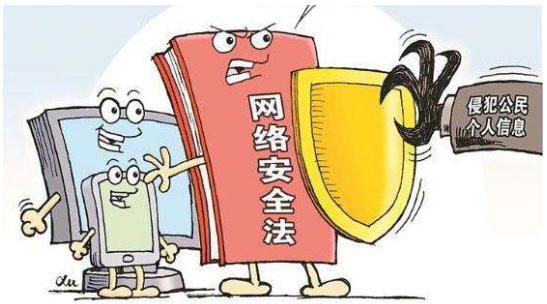
安全小贴士：

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。

校园网账号的安全防范

安全解读：

请提高警惕，保护自身信息安全和隐私，不给黑客攻击和网络诈骗以可乘之机。对不确定的链接不要轻易点击打开，同时加强校园网密码强度，妥善保管个人上网账号和密码，不要将账号借与他人，在公共设备使用个人账号认证登录完成相关业务后，请及时退出。



安全小贴士：

1. 坚决杜绝弱口令（例如：123456、111111、666666 等），并定期更换密码。

2. 遵循“上网信息不涉密，涉密信息不上网”的原则，坚决不通过互联网涉密业务，存储、处理、转发国家涉密信息或重要敏感信息。

3. 对不再使用的校园网账户，请即时提交注销申请。

4. 手机里有密码钥匙的同学，请卸载密码钥匙，安装密码钥匙就等于把 WIFI 密码公之于众。

5. 一旦发现感染病毒，请立即断网，防止病毒扩散蔓延，并及时进行全盘杀毒。