个人信息保护手册

# 个人信息基本概念

Q**:**什么是个人信息？

**A:**以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

《GBT 35273-2017 信息安全技术个人信息安全规范》

Q**:**什么是个人敏感信息？

**A:**一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

《GBT 35273-2017 信息安全技术个人信息安全规范》


# 个人信息安全相关法律法规

Q:关于个人信息安全有哪些法律规定?

**A:**根据**《中华人民共和国网络安全法》**规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

另外，个人信息安全规范(GB/T 35273-2017)标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。针对个人信息面临的安全问题，规范个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。

此外，2015年《刑法修正案九》开始施行，将刑法第二百五十三条之一修改为【侵犯公民个人信息罪】。



Q:什么是侵犯公民个人信息罪?

**A:**根据《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》中的内容，对违反国家有关规定，向他人出售或者提供公民个人信息的；将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的；窃取或者以其他方法非法获取公民个人信息的，都属于侵犯公民个人信息罪。

Q：提供个人信息“情节严重”标准是什么？

**A：**非法获取、出售或者提供公民个人信息时，以下情况算作情节严重：

　　（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；

　　（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

　　（三）根据敏感程度不同，最低非法获取、出售或者提供个人信息五十条以上的；

　　（四）违法所得五千元以上的；

　　（五）将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到二千五百元以上的；

　　（六）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；

　 （七）利用非法购买、收受的公民个人信息获利五万元以上的；

　　（八）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的；

　　（九）其他情节严重的情形。

《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》



Q：那什么算“情节特别严重”？

**A：**非法获取、出售或者提供公民个人信息时，以下情况算作情节特别严重：

　　（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

　　（二）造成重大经济损失或者恶劣社会影响的；

　　（三）数量或者数额达到情节严重规定标准十倍以上的；

（四）其他情节特别严重的情形。

《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》



Q:有没有可供参考借鉴的个人信息保护方式和方法？

**A:**为有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会和公安部第三研究所等单位相关专家，研究起草了**《互联网个人信息安全保护指南》**，供互联网服务单位在个人信息保护工作中参考借鉴。

Q:法律如何保护个人信息？

**A:《中华人民共和国个人信息保护法（草案）》**是一部保护个人信息的法律条款，现尚在制订中。涉及个人信息处理的基本原则、与政府信息公开条例的关系、对政府机关与其他个人信息处理者的不同规制方式及其效果、协调个人信息保护与促进信息自由流动的关系、个人信息保护法在特定行业的适用问题、关于敏感个人信息问题、法律的执行机构、行业自律机制、信息主体权利、跨境信息交流问题、刑事责任问题。对个人及行业有着很大的作用。


# 个人信息保护案例

1. 个人信息保密不当造成损失案例

 案例一：2018年1月张某某先后接到手机自称“丽江移动客户经理陈明”、“北京市东城区公安局宋权警官以及周杨队长”三人的电话，谎称张某某用个人身份在北京申请了另一个手机号码注册的微信号用来诈骗他人，后“陈明”、“周杨”称其涉嫌洗黑钱案件，骗取报警人的中信银行卡卡号、密码以及登录密码，随后要求其把所有信用卡以及支付宝蚂蚁信用的额度共计113871.47元转入到中信银行卡中，再把银行卡里的钱全部转入嫌疑人指定的安全账户中，期间被嫌疑人先从中信银行卡中转走50000元到其他的账户又诱骗受害人将钱转入到安全账户中，被骗114999元。

 案例二：2018年10月16日8点多，罗某某接到一位自称为北京市公安局周姓民警的电话，称其身份证在文进（音）处登记了一张银行卡，现文进（音）被抓，供述该银行卡转了200万给罗某某，要求罗某某打20万元给他保管证明其清白，当天下午罗某某分两次按照对方提供的卡号转了96000元，10月17日上午又分两次按照对方提供的卡号转了100000元，10月18日上午通过微信按对方提供的卡号转了4000元，前后总共被诈骗20万元。

1. 侵犯公民个人信息罪案例

被告人杜立明、冯丹、李晓光、汪甜蜜等11人分别原系河北某快递公司快递员、仓管员、市场专员和负责人。2015年以来11名被告人为谋取非法利益，利用微信、QQ等软件平台，出售、提供、非法获取包含快递单号、面单（即包含快递单号、地址、电话号码的图片）中公民的个人信息，情节严重（其中被告人杜立明情节特别严重）。

 案发后，湖北省荆州市沙市区人民法院于2018年1月22日开庭进行审理并作出（2017）鄂1002刑初375号刑事判决，认定各被告构成侵犯公民个人信息罪，判处各被告1年到3年不等的有期徒刑，共判处罚金近50万元人民币。之后部分被告人不服提前上诉，二审法院荆州市中级人民法院经过审理，于2018年4月24日作出（2018）鄂10刑终84号裁定，认为原判认定事实清楚，适用法律正确，审判程序合法，裁定驳回上诉，维持原判。



# 个人信息安全保护技巧

**钓鱼WIFI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WiFi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WiFi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。



　　**安全小贴士**

　　1、 关闭手机自动连接WiFi的功能；

　　2、 在公共场所，不要连接未知的WiFi；

　　3、 不要将自己家的WiFi密码共享，定期修改密码；

4、 在未知的WiFi信号下不要输入QQ、微信、游戏、银行、支付宝等密码。

**通讯诈骗的防范**

　　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非常难过，两天后遗憾离世。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。

**移动支付的正确使用**

　　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**

　　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。

**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，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。