





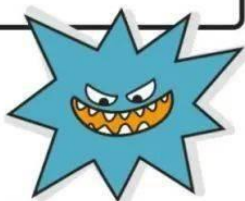
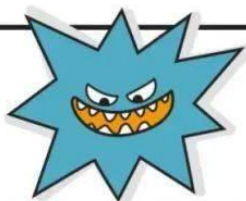
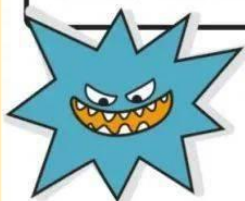
# 做好个人信息保护



## 定义

**个人敏感信息** 是指一旦遭到泄露、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。

**个人验证信息** 是有关一个人的任何数据，这些数据能帮助识别这个人，如姓名、指纹或其他生物特征资料、电子邮件地址、电话号码或社会安全号码。



### 1. 信息泄露事件频频发生

- 快递信息泄露事件频发
- 个人简历信息遭内鬼贩卖
- 客户预留信息遭违规泄露



### 2. 个人信息过度收集不止

- App要求用户提供与服务不相关的隐私信息
- App在用户不知情情况下后台读取用户通讯录、通话记录、GPS位置信息
- 部分App因侵害个人信息权益被下架



### 3. 个人信息非法买卖成网络黑产关键环节

- 利用职务便利非法获取并出售公民个人信息从中牟利
- 街头扫码成个人信息收集陷阱，转手打包获利
- “暗网”倒卖成千上万条个人信息



### 4. 个人信息滥用助长恶意违法行为

- 垃圾短信、骚扰电话、垃圾邮件源源不断
- 冒名办卡透支欠款，造成经济损失
- 冒名挂失补卡并重置密码，账户钱款不翼而飞



▲ 树立权威，言语震慑

**你摊上大事儿了！**

不要告诉你的家人！  
否则他们会受牵连。



转账

▲ 要求转账，榨干事主

要求事主转账，变卖有价证券、抵押房产，借高利贷等方式给对方继续汇款，直到倾家荡产为止。



▲ 心理暗示，深度洗脑

假冒的“检察官”“公证人员”轮流登场，欺骗受害人登录假网站查看假通缉令。

## 防范要点



凡是打着类似民族资产解冻旗号进行敛财的、让你交钱的，不管钱多钱少，都是诈骗。

凡是自称党中央、国务院领导干部，通过电话、微信、电子邮件、QQ等方式进行所谓的“委托”“授权”“任命”的，都是诈骗。

凡是声称缴纳数十元、上百元会费就能获利数万元、数十万元甚至数百万元的各类App、项目，都是诈骗。

凡是“客服”要求必须通过发来的二维码、链接下载贷款APP的，一定是诈骗；未收到贷款之前，坚决不缴纳任何费用。

凡是网络兼职刷单的，要求先垫付资金的，一律都是诈骗。

网络交友一定要注意核实对方的真实身份，不要透露自己的隐私信息；不要轻信陌生人发来的“盈利图”，不加入全是陌生人的“投资群”，不轻信“营业执照”，不做“国际盘”。

不要向陌生个人账户汇款转账，向平台注资时要多方验证是否合法正规。

一旦遭遇诈骗，保存好汇款或转账时的凭证并立即报警。

任尔东西南北风 捂住钱包不放松







# 谨防电信网络诈骗



## 定义

电信网络诈骗犯罪，是指以非法占有为目的，利用电话、短信、互联网等电信网络技术手段，虚构事实，设置骗局，实施远程、非接触式诈骗，骗取公私财物的犯罪行为。

## 典型诈骗套路



### 杀猪盘类诈骗

甜言蜜语假惺惺，骗情骗财害人精



#### “技术组”

购买公民个人信息，  
搭建诈骗网站



#### “供料组”找猪

广撒网，物色诈骗对象

话术！  
搞起来！



#### “话务组”养猪

按话术陪聊建立恋爱  
关系



#### “技术组”杀猪

“生意周转需要钱”  
“生病医治需要钱”  
“遇到好项目，拉你赚大钱”



#### “洗钱组”洗钱跑路



### 冒充公检法诈骗

平生未作亏心事，不怕“李鬼”来敲门



#### ▲ 骗取信任，保持沟通

“你的银行卡涉嫌洗钱”  
“你名下的手机卡发送大量骚扰信息”  
“你涉嫌骗取保险”  
“你邮寄的包裹是假疫苗，面临刑罚”  
.....  
“请尽快联系办案‘民警’”

# 网络安全法律体系构建与发展



## 1 《网络安全法》是我国网络安全领域的基础性法律

《中华人民共和国网络安全法》由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，自2017年6月1日起施行。

## 2 《电子商务法》是电子商务领域的一部基础性法律

《中华人民共和国电子商务法》，2018年8月31日第十三届全国人民代表大会常务委员会第五次会议通过，自2019年1月1日起施行。

## 3 《儿童个人信息网络保护规定》是国内第一部专门规范儿童个人信息网络保护的规定

2019年8月22日，《儿童个人信息网络保护规定》经国家互联网信息办公室室务会议审议通过，予以公布，自2019年10月1日起施行。

## 4 《数据安全法》是数据领域的基础性法律

《中华人民共和国数据安全法》，2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过，自2021年9月1日起施行。

## 5 《个人信息保护法》是我国首部针对个人信息保护的专门性立法

2021年8月20日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，自2021年11月1日起施行。

## 防护要点



|         |                                                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 网站注册和使用 | 要关注网站信息泄露事件方面的新闻，及时修改相关密码                                                                                                                                 |
| 手机、电脑使用 | 要安装安全软件，定期升级更新操作系统<br>要从官方软件市场下载和安装App<br>要认真辨别公共Wi-Fi真实性，不要通过公共Wi-Fi办理转账汇款等敏感业务<br>要防范通过伪基站短信等途径访问钓鱼网站<br>不要在虚假贷款App或网站上提交姓名、身份证照片、个人资产证明、银行账户、地址等个人隐私信息 |
| 个人信息保管  | 要保管好身份证信息；提供复印件时，一定要写明“仅供某某单位做某某用，他用无效”<br>不要随意丢弃与个人信息相关的物品，在处理快递单时先抹掉个人信息再丢弃<br>不要随意参加小调查、小接力、抽奖或免费赠送、街头问卷、电话问卷、非正规办卡等活动，不要随意透露填写个人信息                    |
| 个人信息分享  | 不要在朋友圈、社交网站等发布个人敏感信息                                                                                                                                      |
| 投诉举报    | 个人信息一旦被泄露，可以向互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报                                                                                                            |

信息分享要谨慎

敏感信息别外泄



# 保护你的密码

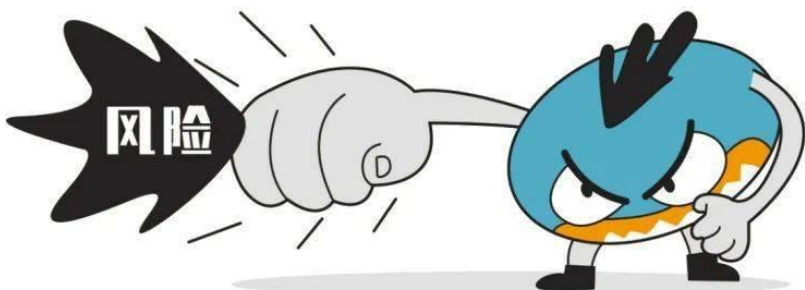


## 定义



**拖库：**指网站遭到入侵后，黑客窃取其数据库。

**撞库：**指黑客获得一批A网站的账号口令（俗称密码）后，批量尝试登录其他网站，得到一系列可以登录的用户账户。



黑客侵入有价值的网络站点

把用户资料（注册用户的用户名和密码）  
全！部！盗！走！

## 拖库



账号一大堆，密码都要强。记忆很疲劳，干脆设一样。以为能省事，黑客喜欲狂！



## 避免弱口令



- 登录名的任何一部分
- 字典中的任何单词
- 曾经用过的口令的任何一部分
- 字母或数字的重复序列
- 键盘上相邻的键，如qwerty
- 个人信息相关，如驾照、电话、地址等

## 设置强口令



- 至少8个字符
- 包含至少大写和小写字母 (e.g. A-Z, a-z)
- 包含至少一个数字 (e.g. 0-9)
- 包含至少一个特殊字符 (e.g. ~!@#\$\$%^&\*()\_-=)
- 不同网站设置不同的用户名、口令
- 利用歇后语等技巧设置和记忆口令

## 撞库



### 小窍门【从一句话开始，做替换和变换】

- 德尔塔太强了，打疫苗预防它：Deltatql,dymYFta
- 七八颗星天外，两三点雨山前：78k\*tw,23.Yu3qian

口令如牙刷  
常换莫分享！





# 关注手机安全风险



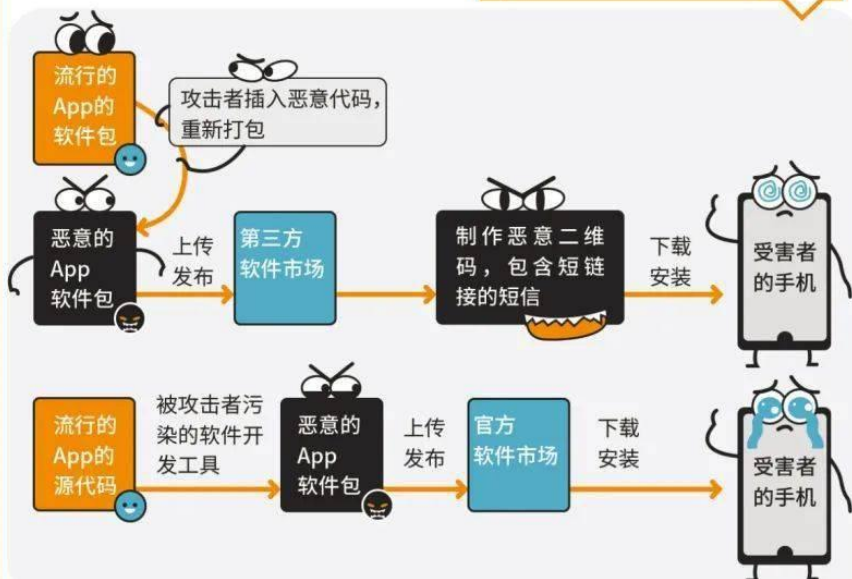
智能手机指具有移动操作系统，可通过安装应用软件、游戏等程序来扩充功能，并可以通过移动通讯网络来实现无线网络接入的手机类型的总称。



智能手机在手机系统、应用软件和云平台等方面，存在安全风险。其信息安全问题不容忽视。

## 1 手机木马软件

## 典型安全威胁



## 2 山寨Wi-Fi热点



黑客冒充店铺等场所名称，提供假冒的热点信息，贸然连接存在信息泄露风险。

## 3 废弃手机泄露隐私

废旧手机的信息表面上看似删除了，而实际内容可能仍然在存储卡上，通过技术手段往往可以恢复出短信、通信录、账号、信用卡号、浏览记录等信息。



## 典型危害

### 1 隐私窃取

获取短信、邮件以及通话记录等内容；获取地理位置、手机号码等信息；获取本机已安装软件、账号、密码等信息

### 2 恶意转账、吸费

自动订阅移动增值业务、利用手机支付功能消费、直接扣除用户资费、自动订购各类收费业务

### 3 资费消耗

自动发送短信、邮件；自动连接网络，产生网络流量

### 4 远程控制

遥控摄像头、远程访问手机内容，在用户毫不知情的情况下在其手机上安装未经许可的软件等

## 防范建议

- 1 要警惕使用手机时出现的异常状况，如电话账单中出现一些莫名其妙的收费、非正常短信和网络活动、或是在手机锁屏的情况下出现的一些应用活动。
- 2 要从安全来源网站、应用商店下载应用程序，不明来源的软件尽量不要装，评价不好的软件谨慎装；要安装一个手机安全软件，及时更新操作系统和App；不要点击来源不明的二维码、短信中的短链接，提示安装.apk时最好果断拒绝！
- 3 谨慎通过App授权请求，经常检查授权请求是否与实际功能匹配，及时关闭不匹配、有风险的授权。
- 4 要谨慎辨别公共Wi-Fi热点的真实性，连接公共Wi-Fi热点时，不进行网络购物、网上银行转账等操作，避免登录帐户和输入个人敏感信息；平时关闭Wi-Fi自动连接，不接受陌生蓝牙、红外等无线连接请求。
- 5 要将废旧手机与各种账号解绑，恢复到出厂设置或者格式化，再反复存入大文件覆盖存储空间；参加“路边摊”以旧换新活动的风险要高于卖给正规商家。
- 6 激活远程定位和擦除功能。一旦手机丢失，致电运营商挂失手机号、致电银行冻结手机网银、解绑支付宝，解除微信绑定。

手机羽翼已丰满 莫让手机成“危机”！