中国公民防开户（开盒）指南

开盒，也叫开户，就是把躲在账号后面的真人挖出来，然后公开。

这本书讲两件事：怎么不让人把你的信息拼成一份完整档案，以及已经被拼出来之后怎么办。

写给普通人看。只讲怎么防、怎么维权，不讲怎么查别人。

在线看：<https://frameira.github.io/NovaYu/> ，手机直接打开。

下载：PDF 版 ，离线看、打印出来给家里人看都方便。

没时间看：先看十分钟版。**已经出事了**：直接看应急卡，一页纸，可以直接转发。

正文里带方括号的标注是来源类型：［官方］［法律］［标准］［平台］［案例］［经验］。说明见 6.8 来源与延伸阅读。

序言

在中国互联网的历史长河里，往往伴随着黑客攻击、数据泄露、开盒。它有很多名字：开户、人肉搜索。

当一个陌生人拿着你的身份信息恶意散布，用电话和短信骚扰你，我相信任何一个正常人都会感到害怕与无助。互联网上确实有一部分心理变态，拿随意开盒开户取乐，把自己的恶趣味建立在别人的担惊受怕之上。

电视剧里有句台词："10 分钟内，我要这个人的全部信息。"所谓背调、尽调，有些也是建立在开户开盒之上。但现实里极少有一次查全的——多数是几条线索慢慢拼，耗时几小时到几周，中间还经常拼错。

本仓库由网络安全专家余鑫隆创建，旨在减少中国互联网的开盒、开户乱象，让大家可以尽可能的保护自己的隐私。

这份指南只能帮你挡掉大概八成的开盒手法。到目前为止，没有任何手段可以让人完全不被开盒。

好消息是局面在收紧：国家在收紧公安的查询权限，平台也在收紧查询权限，大部分数据已经做了脱敏。

作者：余鑫隆，英文名 NovaYu，05 后，16 岁起担任某单位网络安全顾问，中国最年轻的网络安全专家之一，曾获《北京日报》报道，专注 Web 与区块链网络安全，孙宇晨门徒。

联系邮箱：iamnovayu@gmail.com

这份指南只针对中国大陆居民。香港特别行政区、澳门特别行政区、台湾省不在本书范围内。

目录

先看这两页

- 十分钟版：没时间看完整本的，看这一页
- 应急卡：被开盒了先做这 9 件事，一页纸，可以直接转发

第一部分 认识开盒

- 1.1 什么是开盒（开户）
- 1.2 开盒的组成方式
- 1.3 一条信息怎么拼成一份完整档案
- 1.4 这些数据最后流到谁手里
- 1.5 谁在开盒
- 1.6 什么行为会招来开盒

第二部分 你暴露了什么

- 2.1 先列一张自己的单子
- 2.2 手机号是钥匙
- 2.3 身份证别乱给
- 2.4 社交账号的开关
- 2.5 快递和地址最实在
- 2.6 出行、住宿、消费
- 2.7 公开数据里的你
- 2.8 照片会说话，先认识 EXIF
- 2.9 截图也会说话
- 2.10 家人是最软的一环
- 2.11 有人直接来问你

第三部分 自查：把自己查一遍

- 3.1 三条规矩

- 3.2 查你名下有几张手机卡
- 3.3 试一遍平台的找回密码页，看它露多少
- 3.4 查你的信息在不在泄露数据里
- 3.5 查你的公开足迹
- 3.6 查照片里的 EXIF
- 3.7 查老账号
- 3.8 查你的身份证号能不能被算出来
- 3.9 自查记录表

第四部分 加固：把口子一个个堵上

- 4.1 手机号分层
- 4.2 关掉两个开关
- 4.3 昵称和头像别全网一样
- 4.4 密码和找回方式
- 4.5 别把身份证信息凑齐
- 4.6 地址
- 4.7 照片
- 4.8 家人
- 4.9 设备
- 4.10 这几类人要更小心

第五部分 被开盒了怎么办

- 5.1 头一个小时做什么
- 5.2 接下来的 30 天
- 5.3 证据怎么留
- 5.4 平台举报
- 5.5 报警
- 5.6 走法律途径
- 5.7 骚扰电话和短信
- 5.8 家里人被打电话

- 5.9 心理和生活
- 5.10 以后怎么办

第六部分 附录

- 6.1 官方渠道
- 6.2 一页速查
- 6.3 应急卡（可以打印）
- 6.4 术语表
- 6.5 法律条文
- 6.6 常见问题
- 6.7 更新日志与贡献
- 6.8 来源与延伸阅读

第七部分 未成年人和家长

- 7.1 孩子的信息从哪里漏出去
- 7.2 给孩子配手机之前，先做这几件事
- 7.3 孩子自己要记住的四句话
- 7.4 孩子被同学开盒了怎么办
- 7.5 家长最容易犯的三个错
- 7.6 给家长的检查清单
- 7.7 法律上，未成年人有特别保护

免责声明

本书**仅用于个人隐私防护与合法维权**。

- 本书不提供、不链接任何查询他人信息的工具、渠道或方法
- 书中所有自查方法，都要求**只查你自己，或已获本人明确授权的人**
- 未经授权查询、买卖、传播他人个人信息，在中国可能构成**侵犯公民个人信息罪**等刑事犯罪
- 本书内容不构成法律意见，具体个案请咨询执业律师

完整条款见 DISCLAIMER.md。

授权

本书采用 CC BY-NC-SA 4.0 许可：可自由转载、改编，需署名、非商业用途、以相同方式共享。

贡献

欢迎提交 Issue 或 PR 指错、补充平台设置截图、更新失效的官方入口。**请勿在 Issue 中讨论任何获取他人信息的方法**，违者直接删除。

改完 Markdown 之后，跑这一条命令：

```bash bash tools/build.sh ```

它会重建网页版和 PDF，然后自检所有链接和锚点。推送之后 CI 也会跑同样的检查。
```

十分钟版

没时间看完整本，就看这一页。

一、开盒是什么（1 分钟）

有人拿着你的手机号或者社交账号，把你散在各处的信息翻出来，拼成一份档案：姓名、身份证号、地址、家人、行踪。

拼的办法主要是把公开信息对上号。手机号是所有账号的钥匙。

二、现在就能做的 7 件事（6 分钟）

1. 关掉所有平台的"通过手机号找到我""通讯录匹配"
2. 关掉相机的定位，发照片别勾"原图"
3. 快递地址写到驿站，收件名字用化名
4. 一个账号一个密码，微信、QQ、邮箱、银行开二次验证
5. 社交资料里的真实生日、性别、籍贯删掉
6. 装国家反诈中心 App，跟家里人约一个暗号
7. 去"一证通查"，看你名下有几个手机号

三、为什么这几件事管用（2 分钟）

前三后2。 平台的找回密码页会露出你手机号的前 3 位和后 2 位。关掉搜索权限，别人就补不全中间那几位。

身份证号能被缩到很小的范围。 知道你户籍地的区县、出生年月日和性别，顺序码就只剩一小段可能。所以这三样别同时公开。

老账号是后门。 你注销的手机号会被卖给别人。没解绑的账号，下一个拿到这个号的人能用验证码进去。

四、出事了（1 分钟）

顺序别乱：先止损，再取证，最后才对外说话。

直接看应急卡。

五、想看完整版

七部分：认识开盒、你暴露了什么、自查、加固、应急、附录、未成年人和家长。

从目录进。

← 返回目录

被开盒了，先做这 9 件事

一页纸，可以直接转发给需要的人。

头一个小时，按顺序做

1. **改密码。** 先邮箱，再微信、QQ，再银行。邮箱能重置其他所有账号，先保住它
2. **踢设备。** 把账号里不认识的登录设备全部下线
3. **关权限。** 关掉"通过手机号找到我""通讯录匹配"
4. **查邮箱。** 看有没有被设置自动转发规则，看有没有陌生登录
5. **打运营商客服。** 问三件事：有没有被开通短信转移、呼叫转移，名下有没有多出副卡
6. **查钱。** 免密支付、快捷支付、代扣，不认识的全关
7. **截图取证。** 账号名 + ID + 时间 + 内容 + 链接，五个都要
8. **通知家里人。** 约好的那个暗号，这时候用
9. **别对骂。** 你回的话也会被截图

然后

- 平台举报，选"泄露隐私""人肉搜索"
- 报警。带身份证、打印的证据、书面经过、损失证明
- 跟警察说清三件事：我的哪些信息被公开了、造成了什么后果、我怀疑信息是从哪里来的
- **要一份受案回执**

接下来一周

- 第 1 到 3 天：把账号、权限、地址的口子全堵上，别去看那些帖子
- 第 3 到 7 天：跟进平台举报和报警，开始记流水账（时间、谁、做了什么）
- 第 2 周：骚扰一直不停，或者对方已经知道你家在哪，就换号

详细节奏见第五部分的 5.2。

这几个号码

号码	用途
96110	反诈专线，打给你一定要接
12321	垃圾短信、骚扰电话举报
12377	网信办举报。人肉搜索、平台不处理
12389	公安举报投诉。报案不受理、不给回执
12356	心理援助热线。睡不着、恐慌，打这个

记住三句话

- 能一口报出你姓名、航班、订单的电话，不是熟人，是拿着你数据的人
- 谁要验证码都不给，包括自称客服、公安、银行的
- 有人说"给钱就能删帖"，那是二次诈骗

完整处理流程见第五部分。全书从目录进。

第一部分 认识开盒

1.1 什么是开盒（开户）

有人拿着你的手机号，去社交软件上翻你在平台留的信息，翻出你的实名、地址、家人。

这就叫开盒。

它还有两个名字：开户、人肉。开户是躲关键词审核的谐音写法，跟银行开户没关系。

开盒分三步：先拿到信息，再把这些信息对上号，最后发到网上或者打电话骚扰你。

第一步你防不住。信息在平台、在运营商、在快递公司手里，你管不了。

你能防的是第二步：别让这些线索对上号。

被翻出来的东西，无非这几类：

- 姓名和身份证号
- 手机号、邮箱、微信号
- 户籍地址、住址、收件地址
- 配偶、父母、子女、同事
- 开房、出行、快递、消费、就医记录
- 各个平台的账号，和你在上面说过的话
- 人脸、手持身份证照、密码和验证码

最后这条要说一句：手机号能换，密码能改，人脸换不回来。

以后谁让你手持身份证拍照，先想三秒。

这些信息不是一次泄露凑齐的。是你自己发一点，平台存一点，运营商登记一点，线下办业务再留一点。

单看每一处都不多。对上号，就是一份完整档案。

所以防的重点就一句话：别让几条线索能对上。别指望哪个网站永远不出事。

动手的成本很低，几百块、几分钟。你的代价是换号、搬家、被骚扰几个月，家里人还可能被骗钱。

这就是为什么值得花两个小时，提前把口子收一收。

这里要分清两种数据，来路不同，危险程度也不同。

一种是社工库里的老库。公开流传的，多是好几年前拖走的，集中在 2016 年前后。

另一种是行业里正在流动的新料。你现在用的电话、住址、订单，多半来自学校、航司、快递这些环节的内部泄露，是新的。

老库的问题是过时：旧号你早不用了，它基本就对不上你了。

但旧号还在你名下，或者还绑着你的老账号，它就还是一把钥匙。

别因为"流传的都是老库"就放松。

你现在正在用的电话、住址、订单，属于新料，它不过时。新料是现在进行时，只能靠少给、分开放来防（看第四部分）。

先去查一遍：哪些老账号，绑的是你早就不用的号。

1.2 开盒的组成方式

一共三种。

一、社工库

就是超级 App 的数据库被黑客拖走（业内叫脱库），集中放到一起，加个索引用来查。

社工库里公开流传的，基本都是老库，好几年前拖走的。[经验]

网上常说 QQ 8 亿、微信 10 亿、微博 5 亿、支付宝 10 亿，加起来上百亿条。这些数字是黑产自己说的，重复、注水，信不过，你听个量级就行。

能确定的只有一件事：QQ 的数据很老。查一下你的老 QQ，绑的是不是早就没用的号。

微信这边以前有过通过流量分析关联手机号的漏洞，腾讯已经补了。我只说结论，不说怎么做。

记住一句：补了不等于永远安全。

二、信息贩卖

主要是学校、航司、快递行业的人往外卖。

这一类已经有不少判例，快递行业尤其多。案例和判决结果列在 6.8。[案例]

这些是新数据，你正在用的姓名、电话、地址、订单，还能成套对上。比社工库危险。

三、内鬼查询

有查询权限的人违规查你。公安、社保、银行都出过事。

这块我不讲怎么做，只说结果：这是刑事犯罪，《刑法》第二百五十三条之一，侵犯公民个人信息罪。

还有一种更麻烦的：有些单位的对外查询接口本身有漏洞，能被成批调用。

这不是某个人偷看，是一个口子被人打开了。

这种你个人防不住，只能靠上面去修。但如果你发现自己的信息是从这类地方流出来的，报案时一定要说。

如果对方报出的信息只有某个系统里才有，报案时一定写进去，这类案子查法不一样。

三种来源，一个解法：别让单独一条信息就能指到你。

1.3 一条信息怎么拼成一份完整档案

很多人问，我什么都没做，怎么就被查到了？

因为信息是散的，总有些东西能把这些散的信息串起来：

- 手机号，几乎所有平台都要，最危险
- 邮箱，注册和找回密码都用它
- 同一个昵称、同一个头像，很多人全网都用一套
- 同一个密码，一个站泄露，别的站就跟着被撞
- 同一台手机登录过的账号，也会被关联

串起来靠的是对得上。一条只是猜，两条能印证，三条基本就确认了。确认了，才开始挂人、打你电话。

举个例子。对方手里只有一个手机号。

他搜到一个二手帖子，帖子里留了微信。

微信昵称跟另一个平台一样。

那个平台上发过录取通知书。

通知书上有学校和姓名。

四步，全是公开信息，没动任何库。

所以防的重点不是删哪一条，是别让它们能串起来。

1.4 这些数据最后流到谁手里

搞清流向，你才明白为什么有些电话能精准到你自己都吓一跳。

第一手，是拿到数据的人。

有查询权限的岗位人员、脱库的人、批量采集面单的人。他们一般不直接骗你，他们卖数据。

第二手，是料商和中介。

把数据归类、清洗、打包，按类目卖：机票数据、快递数据、车主数据、股民数据、宝妈数据。

类目越细，价格越高。因为越细的数据，越好骗。

第三手，是买家。

- 电诈团伙，最常见
- 营销公司，打推销电话
- 催收和私人调查，拿来找人
- 还有一小部分，就是开盒骚扰你的人

为什么会流到境外。

这些数据会被打包卖到境外，在境外的通讯软件群组里分销。

境外园区里有专门的"数据组"，把数据分给话务组，话务组照着剧本打电话。

难追，是因为服务器在外面、人在外面、钱也在外面。

为什么他们知道你的航班。

机票退改签诈骗就是这么来的。姓名、证件号、航班号、起飞时间，都在那份数据里。[经验]

接到"航班取消，给你退改签"的电话，直接挂掉，自己去航司官方 App 或者打官方客服核实。

为什么他们知道你的快递。

快递面单被批量采集，或者电商订单数据被卖出去。常见剧本是"你的快递丢了，给你理赔"。[经验]

接到这种电话，挂掉，去购物平台里自己看物流。

记住一个判断标准。

能一口报出你姓名、航班、订单、住址的电话，不是熟人，是拿着你数据的人。

你能做的：

- 96110 打来的电话要接，装国家反诈中心 App
- 手机里把陌生号码静音
- 快递地址用驿站——少一张面单，就少一条数据
- 出境的数据你拦不住，但你能让自己那条又旧又不全

1.5 谁在开盒

按动机分，大概这么几类。

为了取乐的人。

闲着没事，拿别人的信息当玩具。多半混在特定的群里，互相"交作业"。

这类人没有明确目标。你被选中，可能只是因为你的 ID 好记、头像好看，或者你回了他一句。

为了报复的人。

你在网上跟他吵过、给过他差评、退过他的货、游戏里赢过他，或者你跟他分手了。

这类人只盯着你。他可能已经知道你是谁，也可能正在拼。后果通常是电话、短信、寄东西。

为了钱的人。

- 卖数据的：不针对个人，按类目批量卖
- 敲诈的：先查你，再拿你的信息找你要钱
- 诈骗的：手里有你的数据，打电话演戏

饭圈和网络暴力。

粉丝群体互撕，"人肉对家"是被默许甚至被鼓励的。

这类人最多、动作最快，而且会去骚扰你的单位、学校和家人。

熟人。

这是最容易被忽略的一类：同事、前同事、前任、同学、邻居、亲戚。

他们本来就知道你很多事，开盒对他们来说只是把你的信息发出去。

很多开盒案的起点，是熟人。

最后一种：不该查却查了的人。

有查询权限的岗位人员。见 1.2 第三条。

一句话总结：**你不需要做错什么，只要被人注意到。**

1.6 什么行为会招来开盒

下面列的是触发点。不是说做了就一定被开盒，是说这些场景下风险明显升高。

一、网上对骂。

任何平台的对骂都可能升级。对方吵不过你，就会去查你。

最危险的一句话是"你有本事来找我"。

骂完就拉黑。别给对方情绪，也别给对方线索。

二、差评、退款、投诉。

给商家差评、要求退款、投诉骑手、举报卖家。

你有理，但对方手里有你的姓名、电话、地址。

有话走平台流程。别加微信私聊，别接受"给你钱，你撤诉"。

三、二手交易。

买家和卖家都能看到对方的一部分信息。纠纷一起，地址就成了武器。

用驿站地址，不发快递单截图，不加微信。

四、游戏和社交平台。

游戏里被骂、被举报、抢装备、开挂冲突。

游戏 ID 常常跟其他平台重名，这是最短的一条线。

游戏号用单独的昵称和头像。

五、饭圈、超话、小组。

粉丝互撕是人肉的重灾区。你的关注列表、超话等级、发过的照片，都是线索。

追星的号跟生活号分开，别放自拍和定位。

六、直播和内容创作。

打赏纠纷、粉丝脱粉回踩、同行竞争。具体怎么防，看 4.10。

七、情感纠纷。

分手、离婚、追求被拒。对方手里可能有你的照片、聊天记录、家庭情况。

这类最难防，也最该提前处理：**分手的时候，把账号密码、共享位置、家人联系方式，全部切断。**

八、求职和招聘。

简历上有你的全名、电话、学校、经历。有人专门收集简历卖钱。

简历用专门的号，别写家庭住址，别上传手持身份证照。

九、在群里跟人吵架。

群里的备注、群名片、历史发言，都能被截图。

最典型的一句：**群昵称写成"真名 + 公司"，等于自己签名。**

总结一句：

开盒的起点往往不是你的信息泄露了，而是有人**盯上你了**。

信息可以提前收，情绪当场收不住。

← 返回目录

第二部分 你暴露了什么

想防住，先得知道自己漏在哪。

这一部分不讲怎么防，只讲你身上有哪些口子。

2.1 先列一张自己的单子

拿张纸，或者开个本地文件，把这些写下来：

- 你有几个手机号，哪个是主号，分别绑了哪些平台
- 姓名、身份证号、户籍地
- 常用邮箱，还有几个备用邮箱
- 微信、QQ、微博、抖音、小红书、贴吧、知乎、B 站的账号
- 收件地址、常用的外卖地址、打车常用地址
- 银行卡预留的手机号
- 常联系的家人、同事
- 你在网上发过的照片、视频、截图

写在纸上，或者存在自己电脑里。

别放网盘，别发到微信收藏，别存进邮箱草稿箱。

这份单子本身就是一份档案，只不过写的人是你自己。

2.2 手机号是钥匙

手机号是使用率最高的身份标识。注册要它，找回密码要它，收验证码要它。

拿到你的手机号，等于拿到一把能试遍你所有账号的钥匙。[经验]

号码本身就是信息。

- 前几位是号段。看号段能知道你用的是哪家运营商，也能看出是不是虚拟运营商（170、171 这类）
- 号段还登记了放号地。网上查"手机号归属地"，查的就是运营商公布的号段表，只能查到号段登记在哪儿，而且携号转网之后，连运营商都可能变

- 后面几位是分给你的用户号码，里面不写城市

这里要纠正一个很常见的说法：**手机号的中间几位不是城市编码，读不出你在哪。**

座机才有区号，010、021 那种，那个才是直接写在号码里的城市编码。

所以光看一个手机号，对方能知道的是：大致哪家运营商、哪个号段、号段登记的归属地。[官方]

归属地不等于你人在哪。

名下有几个号，你可能自己都不知道。

以前办过的卡、给家人办的副卡、公司发的卡，可能都还挂在你名下。

"一证通查"能查出来（怎么查看 3.2）。

只要有一个号不是你在用，当天就去注销。

实名制下，这个号登记在你名下。出了事，第一个被找上的是你，你得先花力气去证明那不是你干的。

不是"责任一定是你的"，是"**麻烦一定先是你的**"。

二次放号。

你注销的号，运营商会放出来重新卖。

下一个买到它的人，能用短信验证码进你那些没解绑的老账号。

反过来，你现在用的号，也可能是别人用过的。[官方] 运营商号码回收再放号机制

去运营商 App 里搜"二次号码焕新"，能把前任机主绑过的互联网账号批量解绑。各家叫法不同，以你当地运营商为准。[官方] 运营商提供的号码焕新服务

换号要做的解绑清单。

换号不是去营业厅办一下就完事。下面这些都要改：

- 钱：所有银行卡的预留手机号、支付宝、微信支付、证券
- 社交：微信、QQ、微博、抖音、小红书
- 政务：社保、公积金、医保、交管 12123
- 出行：12306、航旅纵横、打车、共享单车
- 生活：外卖、电商、快递、物业、各种会员卡
- 工作：企业微信、钉钉、公司邮箱

旧号别急着注销。留一两个月专门收验证码，确认没有遗漏了再销。

手机号还留在这些地方。

快递面单、外卖单、门店会员登记、招聘简历、学校公示、业主群、二手交易、停车扫码。

这些地方的信息都是纸面的、公开的、没人管的。

2.3 身份证别乱给

身份证号 18 位。前 6 位是户籍地的行政区划代码，中间 8 位是你的生日，最后 1 位是按前面 17 位算出来的校验位（为什么这三样别同时公开，看 3.8）。

这两段本身就是信息：暴露你哪年出生、户籍在哪个区县。

这些场合必须给：

办银行卡、办手机卡、住酒店、买火车票机票、寄快递、医院挂号、办护照通行证、入职。

这些场合不需要给：

办理发店会员卡、健身房、试听课程、超市积分、停车登记、抽奖活动、网上下个资料、进小区访客登记。

遇到后面这些，你有权利不给。要么说没带，要么说只留名字和电话。

手持身份证照，尽量别拍。

这类照片是身份冒用的第一手材料。网贷、注册空壳公司、批量注册账号，用的就是这么一张图。

非要拍，拿张纸写清楚"仅供某某平台实名认证使用，他用无效"，跟身份证一起拍进去。

复印件也要处理。

用蓝笔在空白处写"仅供办理某某业务使用，他用无效"。字要压住一部分身份证的影像，但别遮住姓名和号码。最后写上日期。

这一行字，是防别人拿你的复印件去别处用的。

2.4 社交账号的开关

平台默认帮你开着的功能，比你想象的多。

微信

- 添加我的方式：微信号、手机号、QQ 号、群聊、二维码、名片
- 允许陌生人查看十条朋友圈
- 朋友圈可见范围：改成三天或者半年
- 附近的人：不用就关，用过之后清除位置

- 向我推荐通讯录朋友

QQ

- 允许通过手机号、QQ 号搜索到我
- 空间的访问权限、动态的可见范围
- 登录设备管理，不认识的设备踢掉

微博

- 手机号搜索、真实姓名展示
- 发博默认带定位
- 关注列表、粉丝列表是否公开
- 资料里的生日、学校、公司

抖音

- 向我推荐通讯录好友
- 同城展示、作品带位置
- 谁可以评论、谁可以 @ 我
- 抖音号别做成跟微信号、手机号一样

小红书

- 手机号搜索、通讯录推荐
- 笔记带位置
- 绑定信息的对外展示

贴吧、知乎、B 站

- 历史发言是公开的，很多年前说的话也能被翻出来
- 关注列表、收藏夹有时也是公开的
- 这些平台的老号，往往绑的是你已经不用的旧手机号

有三件事每个平台都有，挨着关一遍就行：手机号能不能被搜到、要不要匹配通讯录、位置展不展示。

具体每一项在哪个菜单下，各平台版本不同，以你手机上的实际界面为准。[平台]

2.5 快递和地址最实在

快递面单上有你的名字、电话、地址，有的还有你买了什么。

现在很多平台默认用隐私面单：电话打码、名字只留姓。但不是所有快递、所有驿站都这样。[平台] 各平台规则不同，以下做法不依赖平台

驿站签收的那张单子，往往什么都没处理。

今天就能做的几件事：

- 地址写到小区或者驿站，不写门牌号，不写楼层
- 收件名字用化名
- 拆完的快递单，把名字、电话、地址那几行涂掉或者撕碎
- 退货地址填驿站，别填家里
- 外卖备注别写"放门口鞋柜""门没锁"这类话——那等于告诉别人你家的结构和你在不在家

2.6 出行、住宿、消费

- 火车票、机票都是实名，行程单上有全名和证件号
- 酒店入住要登记身份证，很多还要留手机号
- 打车、共享单车的行程记录里，有你家和公司的位置
- 外卖、电商的地址簿里，存着你所有用过的地址

登机牌、车票、房卡别拍照发出来。

上面的二维码扫一下，能扫出姓名、证件号后几位、行程。

行程也别实时发。今天发"在三亚"，等于告诉所有人你家现在没人。

2.7 公开数据里的你

这一节最容易被忽略，也最容易查到。下面这些不用查库、不用花钱，搜就能搜到。

企业信息

开过公司、做过个体户、当过股东或法人，你的名字、公司注册地址、注册电话，在公开的企业信息平台上都能查到。

企业年报里留的联系电话，很多就是老板本人的手机号。

裁判文书和执行信息

打过官司、被强制执行过，文书是公开的，里面有姓名、出生年月，有的还带住址。

招投标和中标公示

投标要留联系人、电话。中标结果会公示，附件里经常带着项目成员的姓名和手机号。

招聘网站的简历

很多平台的简历默认对企业、猎头可见，手机号能直接下载。

学校和单位的公示名单

奖学金、录取名单、评优名单、值班表，经常是 Excel 直接传到官网，里面全名、学号，有的连身份证号都有。

单位通讯录

有些单位的内部通讯录 PDF 会流到网上，或者被传到文库类网站。

GitHub 和代码仓库

提交记录里的邮箱是公开的。很多人用的就是私人邮箱，甚至是真名邮箱。

域名 WHOIS

注册域名时填的姓名、邮箱、电话。现在多数有隐私保护，但历史记录会被第三方存档，一样查得到。

学术论文、专利、软著

作者信息里有单位和邮箱。

商家平台

大众点评、美团上的商家电话，很多就是老板本人的号。

做法很简单：**拿你自己的名字去搜一遍。**

加上城市、加上公司、加上学校，一条一条点开看。

你会知道别人能搜到什么。

2.8 照片会说话，先认识 EXIF

照片的原始文件里带着一段隐藏信息，叫 EXIF。[标准] Exif 标准，JEITA CP-3451

EXIF 里可能有这些字段：

- 拍摄时间，精确到秒
- 设备型号，甚至镜头型号

- **GPS 坐标**，也就是拍摄地的经纬度
- 图像方向、处理软件

先纠正一个误解：不是每张照片都能查到 GPS。

有没有、还剩下多少，取决于四件事：

拍摄设备、系统设置、文件怎么处理、发到哪个平台。

- 相机 App 没拿到定位权限，压根就没有 GPS 这一条
- 有些 App 拍完直接上传，原始文件根本没落到你手里
- 平台转码、压缩、加滤镜，大部分字段会被丢掉
- 截图、二次编辑、重新导出，一般只剩很少甚至没有

同一张照片，走不同的路，结果完全不同。

一部开着定位的手机拍的照片，往下走：

走的路径	EXIF 还剩什么
相机里的原始文件	全套：时间、机型、GPS、拍摄参数
发微信，勾了"原图"	基本保留，GPS 常常还在
发微信，不勾原图	被压缩，GPS 一般会被去掉
发微博、抖音、小红书	平台会重新压缩转码，多数字段会丢，但**不保证**，别当保险
截图	基本没有。截图有自己的信息，但不含拍摄地点
二次编辑：裁切、加滤镜、重新导出	看用什么工具。有的清干净，有的把原始信息一起写回去
邮件附件、网盘、论坛传原文件	全套保留，一点不少

所以真正危险的是两种东西：原图、原文件。

压缩过的、截图出来的、转过几手的，风险明显低——但"低"不等于"没有"，自己验一遍最稳。

EXIF 之外，照片本身也在说话。

- 窗外的楼、地标、山形，能定位到城市甚至小区
- 门牌号、单元号、电梯里的楼层显示
- 工牌、门禁卡、快递单、外卖单

- 车牌、车型
- 孩子的校服、书包上的姓名牌
- 固定的机位和视角，几张照片一比，能看出你家在几层、朝哪边
- 瞳孔、眼镜、手机屏幕的反光，能把拍照的人或者屏幕内容还原出来

视频也一样。背景音里的方言、门铃声、地铁报站、邻居说话，都能用来定位。

2.9 截图也会说话

这是最容易被忽略的一类。

一张随手发的截图，可能带着：

- 手机状态栏：运营商、信号、电量、时间、定位图标
- 聊天列表、群名称、联系人的备注
- 输入法联想出来的词
- 平台自带的水印，上面有你的账号 ID
- 截图里别人发的信息——你替他泄露了

发截图之前，把状态栏裁掉，把聊天列表挡住，把水印裁掉。

2.10 家人是最软的一环

你的信息泄露，被骗的往往是他们。

- 你的紧急联系人、通讯录同步，暴露了你和谁有关系
- 家长群里的备注"某某妈妈"，等于把你的真名和孩子绑在了一起
- 亲友的社交账号、关注列表、合照，能反推出你们的关系
- 婚礼、家庭聚会的照片里，全是关联线索

有人冒充你给家里人打电话，说"我出事了，快打钱"。

现在还有用 AI 模仿声音、模仿脸打视频的。

这一招到现在还有人上当。

小结

这一部分不是让你把信息全删掉，是让你知道自己漏在哪。

下一部分教你怎么自己查一遍。

2.11 有人直接来问你

前面讲的都是信息"被动"流出去。这一节讲"主动"被套走。

先记住一条总原则：

没有任何正规机构，会在电话、短信、私聊里向你索要完整的身份证号、银行卡号、验证码，或者手持身份证照。

- 银行不会问你的密码和验证码
- 公安不会打电话让你转账，也不会让你下载 App"配合调查"
- 平台客服不会要你的登录密码
- 快递公司不会用私人号加你微信，要你的身份证照片

七套常见话术。

一、"核对信息"。

"我这边核对一下您的收货地址，请问是 XX 路 XX 号吗？"

前半句他是故意说错的，等你纠正。你一纠正，地址就到手了。

应对：不纠正，不补充。问他是哪个平台、工单号多少，然后自己去官方 App 看。

二、"理赔、退款"。

"您的快递丢了，我们给您理赔，需要您提供身份证号和银行卡号。"

应对：挂掉，自己去购物平台看物流。平台不会让快递员私下找你理赔。

三、"入职背调"。

"入职前需要您提供身份证正反面，还有手持身份证照。"

应对：正规背调不需要手持照。先确认对方公司是不是真的，非拍不可就加水印纸（见 2.3）。

四、"老同学、老朋友"。

"你还记得我吗？我们以前……你现在在哪上班？"

应对：别报单位，别报城市。让他先说自己是谁。

五、"改价、验货"。

二手交易里的："你发个订单截图给我""你把商品信息发我，我改价"。

截图里有你的订单号、姓名、电话、地址。

应对：只走平台站内消息，不发任何截图。

六、"我帮你查查是谁"。

"网上有人开你盒，我帮你查。"

这是专门骗正在恐慌的人的。你一配合，就轮到你被套了。

应对：不理会，直接走 5.4 和 5.5。

七、"免费测一测"。

帮你看"你的信息泄露了多少""输入手机号查一下"。

这是来收料的。见 3.4。

怎么判断对方是不是真的。

- 挂掉，用官方渠道打回去。号码在卡背面，客服在 App 里
- 不听他念的信息，只看你自己查到的信息
- 任何"不要挂电话""不要告诉家里人""抓紧时间"的要求，本身就是诈骗标志
- 96110 打来的电话要接，但别人自称是 96110 不算

如果已经被套了。

别慌，也别觉得丢人。这是专业话术，很多人中过。

1. 记下时间、对方号码、说了什么
2. 改掉相关账号的密码
3. 拉黑，别再联系
4. 如果给了身份证号或者银行卡号，按 5.1 走一遍
5. 保留记录，有必要就报警

一句话：

你在电话里说的每一句话，都可能被记下来当线索。

少说，比什么都管用。

← 返回目录

第三部分 自查：把自己查一遍

想防住，先自己当一次靶子。

3.1 三条规矩

- 只查你自己，或者明确同意让你查的人
- 查到的东西别下载、别保存、别转发
- 查出来的口子，当场就改，别拖到明天

3.2 查你名下有几张手机卡

这件事分两个服务，别混成一个：

一、电话卡的"一证通查"

工信部推出的，查你名下在三大运营商各办了几张电话卡、一共几张。

二、互联网账号的"一证通查"

后来加的一版，能查你名下注册了哪些互联网账号。

要注意：**它查的是一份固定名单里的平台**——阿里、腾讯、字节、美团、京东这些旗下的常见应用，不是全网。

名单会更新，以官方页面为准。所以这套查不到的小网站，不代表你没注册过。

两个服务在同一个入口，支付宝或者微信里搜"一证通查"，进去会让你选查哪一项。[官方]

顺便把运营商 App 里的"副卡管理""亲情号""名下号码"也翻一遍。

查出来有不认识的号，当天去营业厅注销，并且要一份书面说明。

那不是你的号，但出了事第一个被找上的是你。

3.3 试一遍平台的找回密码页，看它露多少

做法很简单：打开你常用平台的登录页，点"找回密码"，输入你自己的手机号。

你会看到三种情况：

- 有的平台直接显示：你的手机号是 138****12 这样，只看得到前 3 位和后 2 位
- 有的显示你绑定的邮箱，邮箱也可能被打码
- 有的直接告诉你："该手机号未注册"

具体显示什么，各平台不一样，以你手机上实际看到的为准。[经验]

前 3 位加后 2 位，这个片段很危险。

中间那几位是可以一个一个试的。有人在通讯录匹配这类功能上做比对，就能把号补全。

补全之后，手机号就是所有账号的钥匙。

"该手机号未注册"这句话本身也是信息。

对方拿一个手机号，把常见平台挨个试一遍注册或者找回，就能列出一张清单：这个号注册过哪些平台。

这叫账号枚举。手机号是钥匙，这张清单就是钥匙能开哪些门。[经验]

所以你现在要做的：

- 把常用平台挨个点一遍"找回密码"，记下哪些会露出你的号码
- 记下哪些平台能被搜到、能被匹配
- 然后去关掉"通过手机号找到我"（怎么关看 4.2）

一句话提醒：这套动作只能在你自己号上做。

3.4 查你的信息在不在泄露数据里

先说一条红线。

别在任何来路不明的"开盒查询""查自己有没有被泄露"的网站上输入手机号和身份证号。

十个里有九个是来收料的。你输一次，等于亲手把自己的信息交出去一次。

能用的办法：

- 邮箱：Have I Been Pwned，这是国外的，按邮箱查有没有出现在已知泄露里。只用邮箱，别用手机号
- 看邮箱里有没有平台的"检测到异常登录""请尽快修改密码"通知
- 进常用平台的"安全中心"，看登录设备列表和风险提示
- 检查邮箱有没有被设置自动转发规则——账号被入侵后，这是最常见的后手

说实话的部分：**手机号在国内没有可信的公开泄露查询渠道。**

所以别指望"查一下没事就放心了"。查不到，不代表没泄露。

3.5 查你的公开足迹

拿搜索引擎，搜这几样：

- `"你的真名"`，加引号是精确匹配
- 真名 + 城市
- 真名 + 公司名 / 学校名
- 你的手机号，完整的和片段都试
- 你常用的昵称、邮箱、游戏 ID
- `site:github.com 你的邮箱`，限定在某个站里搜
- `filetype:xls 你的真名`，专门找公示类的表格文件

图片也要搜：把你的头像、自拍拿去百度识图、Google 图片，看看被转到哪里去了。

老账号也别放过：贴吧、豆瓣、知乎的历史发言，很多人早忘了自己说过什么。

网盘也能出事：在百度网盘之类的搜索里搜自己的名字加公司，有些人的文件是公开分享的。

查出来之后：

- 能删的删掉
- 删不掉的找平台申诉
- 找客服没用的，看 5.4

3.6 查照片里的 EXIF

先分清你手里是哪一种图，不然白查：

- 相机拍的原始文件：信息最全，要查就查这种
- 从微信、微博保存下来的：多半已经被压过，字段所剩无几
- 截图：基本不含拍摄信息

所以别拿别人发你的图去查，那说明不了他有没有暴露位置。反过来也一样，**别以为自己发出去的图一定带 GPS**——到底带没带，自己验一遍最准。

手机上看：相册里点开一张照片，"详情"或者"信息"里，能看到拍摄时间和地点。

电脑上看：Windows 右键照片 → 属性 → 详细信息；macOS 用"预览"打开，然后显示检查器，或者右键"显示简介"。

注意一件事：**别把照片上传到网上的"在线 EXIF 查询"网站。** 那等于把照片直接交给对方。

去掉 EXIF 的办法：

- 导出的时候选"不包含位置信息"
- 用图片工具重新保存一遍，或者压缩一下
- 直接截图，截图一般不带原始 EXIF
- 微信发的时候不勾"原图"

现在就去翻一翻，你以前发过多少张原图。

3.7 查老账号

翻邮箱。 搜这几个词：欢迎注册、验证、激活、订单、订阅、退订。

搜出来的，就是一份你注册过的网站清单。

翻短信。 搜"验证码""登录"，能看到你最近在哪些平台活动。

翻密码管理器。 手机自带的钥匙串、浏览器保存的密码，里面存着你早就忘了的站点。

翻授权。 微信和 QQ 里都有"授权管理"，能看到你用微信登录过哪些第三方 App。

这份清单通常最惊人——几十个你根本不记得的应用，都拿着你的微信信息。

处理办法一样：还在用的改密码，不用的去注销。

3.8 查你的身份证号能不能被算出来

身份证号 18 位，分四段：[标准] GB 11643《公民身份号码》

- 前 6 位：户籍地的行政区划代码，精确到区县
- 中间 8 位：出生年月日
- 后面 3 位：顺序码
- 最后 1 位：校验位

顺序码的意思是：同一个地区、同一天出生的人，按顺序编号。

而且奇数分给男性，偶数分给女性。

校验位不是随机的，是按前面 17 位用固定算法算出来的，全国统一。

所以结论要说得准一点。

别人同时知道了你的户籍地（精确到区县）、出生年月日和性别，范围就会被缩得很小。

同一个区县、同一天出生的人，顺序码本来就只有一千个，按性别再分一半。校验位不用猜，是算出来的。

但也别把它想成"随手一算就有"：

- 不是每个号都发出去过，真实存在的只是其中一部分
- 要把号试出来，得拿去逐个核验，会留下痕迹
- 现在多数正经业务，除了姓名和身份证号，还要人脸或者短信验证

所以准确的说法是：**这三样同时泄露，你的身份证号就不再是秘密了。**

这值得防，但不必恐慌。

套话的人要问的就是这三件事：你是哪里人？哪年生的？资料上写的是男还是女？

现在自查，这三样你是不是同时公开过：

- 社交账号资料里填了真实生日和性别
- 简历里写了籍贯
- 群昵称、群备注里带着地名加真名
- 学校、单位的公示里有你的户籍地
- 寄快递时寄件人信息写全了

再说一句：光有身份证号，很多业务也办不了，一般还要人脸或者短信验证。

但姓名加身份证号就是"二要素"，能过一部分风控比较弱的核验。

所以别觉得"反正还要人脸，无所谓"。

3.9 自查记录表

挨着做完，把结果填在后面：

- 名下手机号 ____ 个，主号是 ____，不认识的号 ____
- 会露出手机号片段的平台：____
- 邮箱 ____，在泄露库里查过没有：____
- 已经开了二次验证的账号：____
- 已经关掉手机号搜索的平台：____
- 生日是否公开：____ 籍贯是否公开：____ 手持身份证照给过谁：____

- 常用收件地址，现在是门牌还是驿站：_____
- 和家里人的暗号，约了没有：_____

填完的这张表，跟 2.1 那张单子放一起。

别放网盘。

小结

自查的目的不是让你害怕，是让你知道从哪下手。

下一部分，把这些口子一个一个堵上。

← 返回目录

第四部分 加固：把口子一个个堵上

前两部分说的是你的信息漏在哪。这一部分说怎么堵。

4.1 手机号分层

按用途分成三层：

主号：只给银行、政务、公司、家人。永远不发到网上，不注册任何论坛、游戏、二手交易。

生活号：外卖、快递、电商、门店会员。可以给商家，但不给陌生人。

网络号：论坛、贴吧、乱七八糟的注册。泄露了直接扔。

实际怎么弄：办一张副卡，或者单开一张便宜的低价卡当网络号。

一个号只干一件事。这样就算泄露，损失也是可控的。

旧号的处理顺序是：先挨着解绑，再留一两个月收验证码，最后才去注销。

4.2 关掉两个开关

这一条是全书最要紧的操作。

针对 3.3 说的那个问题，两个开关必须关：

1. **允许通过手机号找到我 / 搜索到我**
2. **向我推荐通讯录好友 / 允许通讯录匹配**

关完之后，别人就算拿到了你号码的一头一尾，也没法在平台上把中间几位确认出来。

挨个平台关一遍：

- **微信**：设置 → 朋友权限 → 添加我的方式（微信号、手机号、QQ 号、群聊、二维码、名片）；再把"允许陌生人查看十条朋友圈"关掉
- **QQ**：设置 → 隐私 → 加我为好友的方式；再接动态权限、登录设备管理
- **支付宝**：设置 → 隐私 → 常用隐私设置 → 关闭"可通过手机号搜索到我"，关闭"向好友公开我的真实姓名"
- **淘宝、闲鱼、拼多多**：隐私设置里的手机号搜索、通讯录推荐、真实姓名展示
- **微博**：隐私设置 → 手机号可搜索、关注列表可见

- **抖音**：设置 → 隐私设置 → 通讯录推荐、同城展示、作品可见范围
- **小红书**：设置 → 隐私 → 不把我推荐给通讯录好友、手机号搜索

关完要自测。

找个朋友，拿你的手机号去搜你。搜不到，才算关好了。

有些平台的"手机号搜索"关不掉。那就把资料和动态对外收起来，让别人搜到也没东西看。

关一个平台不算完。花一个下午，一次关干净。

4.3 昵称和头像别全网一样

同一个昵称、同一个头像，就是把几个账号串起来的那根绳子。

昵称怎么起：

- 主号可以用真名，这是给熟人看的
- 网络号用随机字母数字组合，别用姓名拼音
- 别用生日、手机号尾号、QQ 号、学号
- 别在所有平台都写同样的简介，比如都写"某某大学 程序员"

头像要注意：

头像能被以图搜图反查。拿同一张头像在全网用，等于自己把账号串起来了。

私人号和网络号用不同的头像。网络号用不相关的图，或者生成的图。

4.4 密码和找回方式

一个账号一个密码。记不住就用密码管理器。

密码长度比复杂度重要，12 位以上的随机串。

二次验证的优先级，从强到弱：

1. App 生成的动态码（TOTP 这类）
2. 硬件密钥
3. 短信验证码

短信验证码最弱，因为它能被冒名补卡截走。

所以去运营商设置一下：补卡需要服务密码。服务密码别告诉任何人。

找回方式是最容易被忽略的一环。

- 恢复邮箱的安全级别，要和主账号一样高
- 密码找回的安全问题（母亲姓名、出生地、第一所学校）别填真的，这些都能被查到
- 定期清理登录设备列表，不认识的踢掉

验证码谁也不给。 自称客服、公安、银行、快递的，要验证码的都是骗子。

邮箱单独说一句：开登录二次验证，并且定期检查有没有被设置自动转发规则。

4.5 别把身份证信息凑齐

回头看你 3.8 的结果。

户籍地、出生年月日、性别，这三样别让人同时拿到。

具体怎么做：

- 社交账号的生日填假的，或者不填
- 资料页的性别，能不填就不填
- 简历、群备注、老乡群、家长群里，别说自己是哪里人
- 手持身份证照，能不拍就不拍
- 非拍不可，拿张纸写"仅供某某用途使用"，跟证件一起拍进去
- 复印件用蓝笔写用途、压边、写日期（见 2.3）

如果发现被冒名注册了公司、网贷、账号：

- 去市场监管部门申请撤销登记
- 去平台申诉，要求注销
- 全程保留记录，这些是你后面报案和维权的材料

4.6 地址

- 写到小区或者驿站，不写门牌号，不写楼层
- 收件名字用化名
- 快递单撕碎再扔，或者把名字、电话、地址那几行涂掉
- 退货地址填驿站
- 外卖备注别写"放门口鞋柜""门没锁"

- 定期清理外卖、打车、电商里的常用地址，尤其是搬家以后
- 别晒新家的装修、门牌、小区大门、门锁

4.7 照片

- 关掉相机的定位功能
- 发之前去掉 EXIF（方法见 3.6）
- 别发原图
- 记住哪条路最危险：**原图 > 压缩过的图 > 截图**。发之前先想一下自己发的是哪一种
- 裁一下背景
- **打码用实心色块**：马赛克和模糊不是绝对安全。小面积、小字的模糊，有时能靠工具复原，公开的那类还原案例多数也是这种。稳妥做法是用不透明的色块直接盖住，盖严实，别留边
- 车票、登机牌、快递单：盖住二维码、条码、姓名、证件号
- 孩子的照片少发正脸，别带校徽、姓名牌，别写学校和班级
- 截图：裁状态栏、挡聊天列表、去水印

4.8 家人

跟爸妈约一个暗号。别用生日、名字这类能猜的，用一件只有你们知道的事。

告诉他们三句话：

- 不转账
- 不点链接、不扫码
- 先挂电话，再打你原来的号码确认

还要告诉他们：现在 AI 能模仿声音，也能换脸打视频，声音和脸像都不能信。

接到 96110 的电话一定要接，那是反诈专线。

有空帮他们把手机里的"手机号搜索""通讯录推荐"也关掉。

家里老人的收件地址，尽量也用驿站。

4.9 设备

- **锁屏**：6 位以上，别用生日，别用图案

- **查找设备**：iPhone 的"查找"、安卓的"查找手机"，确保是开着的
- **权限最小化**：通讯录、位置（改成"仅使用期间"）、相册、麦克风，用不上的全关
- **输入法**：关掉云同步、剪贴板同步、云联想。你打过的字，可能被上传
- **公共 Wi-Fi 和公共充电桩**：别用来支付，别接来路不明的 USB
- **旧手机**：退出所有账号 → 关掉查找设备 → 恢复出厂 → 再塞满无关文件，再恢复一次
- **旧号卡**：注销前先解绑，销号后要回执

4.10 这几类人要更小心

未成年人

- 账号由家长代管，不填真名、学校和班级
- 关掉同城、附近的人、通讯录推荐
- 不发校服、校徽、校车、放学路上的照片

主播、自媒体

- 单独的号、单独的设备
- 不露真实姓名，不露小区，不露常去的那家店
- 行程延迟发布，别实时发
- 背景固定，但要有窗帘，别让窗外入镜
- 打赏和转账信息别公开展示

公职人员、正在打官司的人

- 单位公示里的联系电话，换成办公电话
- 别用私人号当业务号
- 把所有能证明生活轨迹的内容先收起来

老板、个体户

- 企业年报里的联系电话，换成专门的号
- 注册地址能用园区地址或者代账地址，就别用家庭住址

今天就能做完的五件事

1. 关掉所有平台的"通过手机号找到我"和"通讯录匹配"

2. 查一遍名下有几个手机号
3. 把不用的老账号注销，旧号解绑
4. 快递地址改成驿站，名字改成化名
5. 跟家里人约一个暗号

← 返回目录

第五部分 被开盒了怎么办

先稳住。这种事有处理流程，一步一步来。

5.1 头一个小时做什么

顺序别乱：先止损，再取证，最后才对外说话。

1. 改密码，按这个顺序

先改邮箱，再改微信、QQ，然后改银行。

因为邮箱能重置其他所有账号，它是最该先保住的。

2. 踢设备

把账号里不认识的登录设备全部下线。

微信、QQ、微博、抖音的设置里都有"登录设备管理"。

3. 关掉手机号搜索和通讯录匹配

防止对方顺着你继续扩线（见 4.2）。

4. 查邮箱

看有没有被设置自动转发规则，看登录记录里有没有陌生 IP。

5. 打运营商客服

问三件事：有没有被开通短信转移、呼叫转移，名下有没有多出副卡。

短信转移是最阴的一招——你的验证码被转到别人手机上，你改了密码也白改。

6. 查钱

银行、支付宝、微信支付里的免密支付、快捷支付、代扣，全部看一遍，不认识的全关。

7. 截图取证

趁对方还没删，把证据留下来（怎么留看 5.3）。

8. 通知家人

特别是父母，先给他们打个预防针，防止有人冒充你骗钱。

9. 别去对骂

你回一句骂人的话，也可能被截图当证据。

5.2 接下来的 30 天

头一个小时做完了，不等于结束了。这类事有个节奏，大概分三段。

第 1 到 3 天：把口子全堵上

- 挨着检查所有重要账号：登录设备、绑定的手机和邮箱、微信和 QQ 里授权过的第三方应用
- 换掉那些跟泄露信息有关的密码，比如用生日、手机号、名字拼音做的密码
- 关掉所有平台的"通过手机号找到我""通讯录匹配"（见 4.2）
- 快递和外卖地址清一遍，改成驿站
- 给家里人打个电话，把暗号说清楚
- 这几天别去看那些帖子。越看越焦虑，而且每次点开都在提醒对方"我在意"

第 3 到 7 天：走流程

- 平台上举报过的，跟进结果。没处理就再报一次，同时报 12377
- 报警的，跟进案件进展。新出现的骚扰记录，补交给警察
- 骚扰电话和短信：开运营商拦截，12321 举报，把记录攒着
- 开始记流水账：什么时间、谁、做了什么。这份记录后面报案和打官司都要用

第 2 周：判断要不要换号

换号是个大决定，看情况：

- 骚扰集中在电话和短信上，一直不停 → 换号
- 对方已经掌握你的住址、单位，还在升级 → 换号，同时考虑搬家
- 只是网上骂几句，没有线下骚扰 → 别急着换，先把账号权限收干净

换号之前先列解绑清单（见 2.2）。**换了号不解绑，等于白换。**

第 3 到 4 周：收尾和恢复

- 确认该删的删了，该处理的处理了
- 把这次的经过写下来：从哪漏的、哪一步做错了、下次怎么避免
- 睡不好、不敢出门、反复刷手机看有没有新帖子，超过两周就去看医生，或者打 12356
- 该恢复的生活就恢复。躲着不是办法

一件要长期记住的事

数据一旦出去，就收不回来了。你能做的是让它变旧、变乱、对不上。

所以别指望"处理干净就没事了"。养成习惯：每半年把第三部分的自查做一遍。

5.3 证据怎么留

截图要有四个要素：

- 对方的账号名和 ID，不能只截内容
- 时间
- 发布位置：群名、帖子链接、主页地址
- 内容本身

截的时候，从对方主页开始截一张，再截内容，两张一起才说明得了是谁发的。

重要的内容做录屏。

录屏要从打开 App 开始，一路点到那条内容，中间别剪。

保留原始载体。

手机别刷机，别恢复出厂，别删聊天记录。原始设备本身就是证据。

做存证。

- 公证处公证，最稳，也最贵
- 可信时间戳
- 部分法院认可的电子存证平台

自己写一份时间线。

什么时间、谁、在哪个平台、发了什么、造成了什么后果。按时间顺序写，写清楚。

被电话骚扰。

通话录音一般可以作为证据，把号码和时间都记下来。

被诈骗。

立刻打 110，同时打银行客服，争取止付。

5.4 平台举报

每个平台都有举报入口，选"泄露隐私""人肉搜索""人身攻击"这一类。

举报的时候写清楚：

- 哪个账号
- 哪条内容
- 泄露了你的什么信息
- 要求删除

举报完把回执截图留着。

平台不处理的话：

- 向 12377 举报平台
- 找律师发律师函

这里有个规则要记住：**你正式通知平台之后，平台如果不处理，导致损失扩大的，平台要担这个责任。**

所以每一次通知都要留痕。

5.5 报警

去哪报：

网络犯罪发生地、你的居住地、户籍地，都可以试。直接打 110，或者去派出所。

带什么：

- 身份证
- 证据材料，打印出来
- 一份书面的经过，按时间顺序写
- 造成损失的证明：转账记录、医院诊断、单位证明

怎么说：

三件事说清楚。

一是我的哪些信息被公开了。

二是造成了什么后果。

三是**我怀疑信息是从哪来的**。

第三点特别重要。如果对方报出的信息精准到只有某个系统里才有，一定要说出来。内部人员违规查询、单位接口被成批调用，案件方向完全不一样。

把后果量化。

"我被打了 300 个骚扰电话""我被骗了 8000 块""我因此住院了""我因此丢了工作"。

这些话不是卖惨，它们直接对应立案标准。

立案标准：

下面这组数字，出自《最高人民法院、最高人民检察院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》（法释〔2017〕10 号）。[法律]

非法获取、出售或者提供公民个人信息，达到其中任意一条，就属于"情节严重"：

- 行踪轨迹信息、通信内容、征信信息、财产信息：50 条以上
- 住宿信息、通信记录、健康生理信息、交易信息：500 条以上
- 其他公民个人信息：5000 条以上

这组数字不是全部标准，司法解释也会更新。用的时候以最新版本为准。

所以要一份**受案回执**。这是你后面追进展的凭证。

不给的话，可以打 12389 投诉，或者向检察院申请立案监督。

5.6 走法律途径

民事

案由是隐私权纠纷、个人信息保护纠纷。

可以告发帖的人，也可以告平台（平台接到通知后不处理的）。

人格权侵害禁令

不用等判决，可以申请先让内容下线。情况紧急的时候很有用。

赔偿

包括财产损失、精神损害抚慰金，还有你为维权花的合理费用：律师费、公证费。

在哪告

杭州、北京、广州有互联网法院，可以全程线上。

找一个懂互联网的律师，这类案子不难，难在找出对方是谁。

5.7 骚扰电话和短信

这是被开盒之后最常见的报复手段，也是最能耗人的一种。

短信轰炸

短时间内收到几百条验证码，各个平台的都有。

这说明有人拿你的手机号在批量注册账号。

怎么办：

- 别回，别点，别理
- 立刻把各平台的"通过手机号找到我"关掉（见 4.2）
- 开手机自带的垃圾短信和骚扰拦截。**别自己手动把"验证码"设成黑名单关键词**——那样你自己登录也会收不到验证码，反而把路堵死
- 轰炸特别猛的时候，可以临时开"仅通讯录可送达"，或者先换个号对外联系
- 再严重就联系运营商开通短信防护

电话轰炸（呼死你）

一分钟好几个电话，接起来没人说话，或者响一声就挂。

- 运营商 App 里都有高频骚扰电话拦截服务，免费，开通
- **被高强度骚扰的时候**，再把陌生号码全部静音。平时别这么设——快递、医院、学校、银行、工作电话、运营商，很多都是陌生号，全静音会把正事一起挡掉
- 别接、别骂、别回拨

恶意下单、货到付款

有人用你的地址和电话疯狂下单。

- 联系平台客服说明情况，让平台标记异常订单
- 货直接拒收
- 货到付款的一律不签收、不垫付

冒名挂失、冒名补卡

这是最危险的一类，目标是你的钱。

- 银行卡被冒名挂失：立刻打银行客服核实，冻结账户
- 手机卡被冒名补办：立刻打运营商客服挂失，去营业厅换卡，同时查有没有被开通短信转移

- 全程留记录，这些是报案材料

实在扛不住就转移

- 开运营商副号，把对外联系换到副号上
- 必要时直接换号，换号的完整解绑清单看 2.2

换号是最后手段，但有时候是最省心的手段。

5.8 家里人被打电话

提前约好的那个暗号，就是这时候用的。

跟家人说清楚三句话：

- 不转账
- 不点链接、不扫码
- 先挂电话，再打你原来的号码确认

再说清楚一件事：现在 AI 能模仿你的声音，也能换脸跟你视频。

声音像、脸像，都不算证明。

96110 的电话一定要接。

5.9 心理和生活

被开盒之后害怕、睡不着、总觉得有人盯着你，这些都是正常反应。

这不是你的错。你只是遇上了一件别人用来取乐的事。

别一个人扛。跟家里人说，或者打心理援助热线。

12356 是国家卫健委设置的全国统一心理援助热线，2025 年 5 月 1 日起全国统一使用，各地原来的心理热线都并入了这个号。

实在不行就换号、搬家。社交账号先改成私密，缓过来再说。

还有一件事：**别反复去搜自己，别一直盯着那些帖子看。** 越看越焦虑，而且每次搜索都在提醒对方"我在意"。

5.10 以后怎么办

- 把第三部分的自查，每年做一次

- 关注有没有新的账号被关联出来
- 单位、学校的公示，能不写全名和电话就不写
- 把这次的经过写成一份清单，下次就不会手忙脚乱

← 返回目录

第六部分 附录

6.1 官方渠道

一证通查（电话卡）

工信部的服务。查你名下在三大运营商各办了几张电话卡。[官方]

一证通查（互联网账号）

同一个入口下的另一项服务。查你名下注册了哪些互联网账号。

它只覆盖一份固定名单里的平台，不是全网。名单以官方页面为准。[官方]

搜索"一证通查"，认准工信部反诈专班。

国家反诈中心 App

公安部出的，来电预警、诈骗举报、身份核实。

96110

反诈专线。打给你的电话一定要接，那是有人在提醒你可能正在被骗。

12321

网络不良与垃圾信息举报。管骚扰电话、垃圾短信、不良网站。

12377

网信办违法和不良信息举报中心。管网络上的违法信息，包括人肉搜索。

12389

公安机关举报投诉电话。报案不受理、不给出具回执的时候可以打。

12356

国家卫健委设置的全国统一心理援助热线，2025 年 5 月 1 日起全国统一使用，各地原有心理热线都并入了这个号。被开盒之后失眠、恐慌、不敢出门，可以打这个。

各平台安全中心

微信、QQ、支付宝、抖音里都有。处理账号被盗、被冒充、被恶意注册。

6.2 一页速查

今天关掉这几个开关：

- [ ] 允许通过手机号找到我
- [ ] 允许通过微信号、QQ 号找到我
- [ ] 向我推荐通讯录好友
- [ ] 允许陌生人看我的朋友圈和动态
- [ ] 在附近的人、同城页里展示我
- [ ] 相机的定位
- [ ] 发照片时勾选"原图"

今天做完这几件事：

- [ ] 地址改成驿站或者小区门口
- [ ] 收件名字改成化名
- [ ] 查一遍名下有几个手机号
- [ ] 一个账号一个密码，重要的开二次验证
- [ ] 跟家里人约一个暗号

三个开关的自测办法：

找个朋友，拿你的手机号搜你，搜不到就算关好了。

6.3 应急卡（可以打印）

被开盒后的头一个小时：

1. 改密码，先邮箱，再微信和 QQ，再银行
2. 踢掉不认识的登录设备
3. 关掉手机号搜索和通讯录匹配
4. 查邮箱有没有被设置自动转发
5. 打运营商客服，问有没有短信转移和副卡
6. 关掉不认识的免密支付
7. 截图取证：账号名 + ID + 时间 + 内容 + 链接
8. 通知家里人

9. 不对骂

报案要带：

身份证、打印好的证据、书面经过、损失证明、时间线。

一句话跟警察说清：

我的哪些信息被公开了，造成了什么后果，我怀疑信息是从哪里来的。

要一份受案回执。

6.4 术语表

开盒 / 开户

把匿名账号背后的真人身份挖出来并公开。"开户"是谐音写法，跟银行开户无关。

社工库

社会工程学数据库。泄露的数据汇集到一起，建索引供查询。

脱库

数据库被整体导出。

撞库

拿一个网站泄露的账号密码，去别的网站试。

二要素

姓名加身份证号。

三要素

姓名、身份证号、手机号。

前三后2

平台在找回密码页露出的手机号片段：前 3 位加后 2 位。

账号枚举

拿一个手机号挨个平台试注册或找回，反推出这个号注册过哪些平台。

二次放号

你买到的手机号以前有人用过。前任机主没解绑的账号，可能被验证码打开。

号码焕新

运营商提供的服务。能把前任机主绑过的互联网账号批量解绑。

内鬼查询

有查询权限的人违规查别人。

EXIF

照片里的隐藏信息。可能包含拍摄时间、设备型号、GPS 坐标等。注意是"可能"——有没有这些字段，取决于拍摄设备、系统设置、文件怎么处理和发到哪个平台（见 2.8）。

AI 拟声、AI 换脸

用 AI 模仿你家人的声音或者脸来行骗。暗号就是防这个的。

6.5 法律条文

《刑法》第二百五十三条之一

侵犯公民个人信息罪。非法获取、出售、提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑。

《刑法》第二百八十五条、第二百八十六条

非法获取计算机信息系统数据罪、破坏计算机信息系统罪。攻击系统、越权调用接口取数据，走的是这两条。

《民法典》第一千零三十二条到第一千零三十九条

隐私权和个人信息保护。明确自然人的私人生活安宁、私密空间、私密信息受保护。

《个人信息保护法》

处理个人信息要取得同意，要最小必要。泄露要报告、要补救。

《反电信网络诈骗法》

电话卡、银行卡的实名管理，以及反诈的处置措施。

《治安管理处罚法》

写恐吓信、发送骚扰信息、散布他人隐私，可以拘留罚款。

两高《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》（法释〔2017〕10 号）

定"情节严重""情节特别严重"的数量标准。行踪轨迹信息、通信内容、征信信息、财产信息 50 条以上；住宿信息、通信记录、健康生理信息、交易信息 500 条以上；其他公民个人信息 5000 条以上。

具体条文以最新版本为准，打官司请咨询律师。

6.6 常见问题

我不是名人，会有人开我吗？

会。饭圈、游戏、二手交易、情感纠纷、直播打赏，都可能招来开盒。成本很低，这才是麻烦的地方。

我改了密码是不是就没事了？

不是。密码只是其中一环。对方手里如果有你的手机号和身份证号，光改密码不管用。要按第四部分把面收一遍，重点查短信转移和自动转发规则。

注销账号有用吗？

有用，但要连绑定一起处理。只注销账号不解绑手机号，等于没做。

网上那些"开盒查询""查老赖"的网站能用吗？

不能。它是来收你的信息的。你用一次，等于把自己的资料送出去一份。

对方说给钱就能删帖，怎么办？

不要给。这是二次诈骗。留好证据，走 5.4 和 5.5。

手机号换了就安全了吗？

换了要记得去各个平台改绑定。旧号不解绑，还是一把钥匙。

平台举报了没人管怎么办？

继续举报，同时向 12377 举报平台。保留每一次通知的记录，后面平台要担责。

我的信息好像是从某个单位流出来的，怎么判断？

看精准度。如果对方报出的信息只有某个系统里才有——比如内部的业务编号、只有后台能看到的备注——那基本可以确定。报案时把这一点写进笔录。

未成年人被开盒怎么办？

家长出面处理。未成年人信息受法律特别保护，报案时说明对方涉及的是未成年人信息，处理会更严。

怎样才能不被查到？

做不到百分之百。能做到的是：让查你的人成本变高，让查到的东西过时、对不上、不完整。

6.7 更新日志与贡献

欢迎提 Issue 或 PR，指出错误、补充平台设置截图、更新失效的官方入口。

请不要在 Issue 里讨论任何获取他人信息的方法。

6.8 来源与延伸阅读

这本书里的说法，大部分来自公开的法律条文、国家标准和官方公告。把出处集中列一下，方便你自己去核。

怎么读正文里的标注

正文有些句子后面带方括号，一共六类：

- `[官方]` 政府部门、运营商公开的文件或服务说明
- `[法律]` 法律、司法解释原文。都能在国家法律法规数据库核对
- `[标准]` 国家标准、行业标准
- `[平台]` 平台自己的帮助文档或设置页
- `[案例]` 法院、检察院、公安机关公开的案件
- `[经验]` 没有公开出处，是实践中的观察。会随版本、地区、时间变化

一条原则：**能给出出处的就标出处，给不出的就老实标 `[经验]`，不假装有来源。**

查东西用这几个官方入口

- 国家法律法规数据库：<https://flk.npc.gov.cn/> —— 中国所有法律的官方原文。查条文、查最新修订，用这一个就够
- 工业和信息化部：<https://www.miit.gov.cn/> —— 电话卡实名、"一证通查"的组织方
- 公安部：<https://www.mps.gov.cn/> —— 国家反诈中心、96110
- 12321 网络不良与垃圾信息举报受理中心：<https://www.12321.cn/>
- 12377 网信办违法和不良信息举报中心：<https://www.12377.cn/>

书里引到的法律和文件

- 《中华人民共和国个人信息保护法》：<http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html>（全文）
- 《中华人民共和国民法典》人格权编：第一千零三十二条到第一千零三十九条
- 《中华人民共和国刑法》：第二百五十三条之一（侵犯公民个人信息罪）、第二百八十五条、第二百八十六条

- 《最高人民法院、最高人民检察院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》：法释〔2017〕10 号。第五部分引用的数量标准出自这里
- 《中华人民共和国反电信网络诈骗法》
- 《中华人民共和国未成年人保护法》：网络保护专章，以及个人信息保护的相关规定
- 《中华人民共和国治安管理处罚法》：关于骚扰、恐吓、散布他人隐私的规定
- 国家卫生健康委《关于应用"12356"全国统一心理援助热线电话号码的通知》：国卫医政函〔2024〕259 号，<https://www.gov.cn/zhengce/zhengceku/202412/content_6994470.htm>（原文）
- 身份证号的 18 位结构与校验位：国家标准 GB 11643《公民身份号码》
- 照片里的元数据 EXIF：JEITA CP-3451 标准

公开案例

快递行业卖信息，是国内判得最多的一类。下面两起是公开报道过的：

- 广东深圳宝安，两名快件处理员利用分拣集包的便利，出售快递面单信息 **2.1 万余条**，法院以侵犯公民个人信息罪分别判处有期徒刑，并处罚金。

[案例] 中国法院网：<https://www.chinacourt.cn/article/detail/2026/08/id/9437103.shtml>

- 江苏常州钟楼，快递公司员工庄某、朱某出售客户信息，经检察院提起公诉，法院判处**有期徒刑十个月**，各并处罚金。

[案例] 京报网：<https://news.bjd.com.cn/2026/04/26/11711949.shtml>

这两起说明两件事：

- **一条快递信息在市场上只值几毛钱，卖到上万条就是刑事案子**
- 判决结果不只是刑期，还有罚金；作案用的手机这类工具会被没收

想要更多案例和案号，去**中国裁判文书网**，按"侵犯公民个人信息罪"加"快递""通讯""房产"这些关键词检索。新闻报道一般不写案号，判决书里才有。

三点说明

- 法律会修订，条文序号和数量标准都可能变。引用之前，**以国家法律法规数据库里的现行版本为准**
- "一证通查"的入口会变，认准工信部反诈专班，别用来路不明的第三方网站
- 本书不保证上面这些外部链接长期有效。链接失效时，用机构名字直接搜，或者去国家法律法规数据库找

← 返回目录

第七部分 未成年人和家长

未成年人被开盒的比例不低，而且有两个特点：**信息本来就少，一旦被开，伤害特别大**；**遇到事通常不敢跟家里说**。

这一部分写给两拨人：孩子自己，和替孩子操心的家长。

7.1 孩子的信息从哪里漏出去

- 学校、班级的公示名单：全名、班级、学号，有的还有身份证号
- 家长自己发在朋友圈和群里的照片：校服、校徽、校门、奖状上的全名
- 家长群备注："某某妈妈"，把家长和孩子的名字绑在一起
- 学校和培训机构的报名表，会被转手
- 孩子自己用的 App：游戏、社交、短视频，注册时填的资料
- 学校发的在线表格，链接可能被转发到外面

7.2 给孩子配手机之前，先做这几件事

- 账号用家长的手机号注册，别用孩子自己的号
- 关掉：通过手机号找到我、通讯录推荐、附近的人、同城展示、位置共享
- 只装必要的 App，每个 App 都关掉通讯录和相册权限
- 相机的定位关掉
- 头像不用真人照，昵称不带真名和生日
- 学校、班级、校服、校门，一律不发

7.3 孩子自己要记住的四句话

1. 网上不要写真名、学校、班级、住址
2. 有人问这些，不要答，回来告诉家长
3. 跟人吵架了就停，不要互相骂
4. 出了事第一时间告诉家长

最后一条要反复说。

孩子最常做的事，是害怕被骂，于是自己删掉聊天记录、自己处理。结果是证据没了，对方更嚣张。

7.4 孩子被同学开盒了怎么办

先判断到了哪一步。

- 只是同学翻到了 QQ 空间的老内容：先找班主任，同时联系对方家长
- 已经发到群里、发到网上：平台举报、学校、报警，三条线一起走
- 伴随辱骂、威胁、造黄谣：直接报警，不要在学校内部消化

三件事同时做。

一、找学校。

班主任、德育处、校长。要求学校出面制止，并且留下书面记录。学校对校园欺凌有处理责任。

二、找平台。

举报理由选"泄露隐私""涉及未成年人"。平台对涉及未成年人的信息处理更快。

三、报警。

带证据去派出所。涉及未成年人的案件，处理力度更大。

注意：

- 不要让孩子自己去跟对方理论
- 不要在班级群里公开对骂，那只会扩大传播
- 保留所有证据，包括孩子被骂的聊天记录
- 如果孩子出现厌学、失眠、自伤，立刻看心理医生，或者打 12356

7.5 家长最容易犯的三个错

一、自己先把孩子的信息发出去了。

生日、学校、班级、奖状、准考证、录取通知书，这些都是敏感信息。

发之前问自己一句：这条信息，陌生人看了能做什么？

二、出事后第一反应是骂孩子。

孩子被开盒，多半不是因为做错了什么。第一句话如果是指责，第二句话你就听不到了。

三、删证据。

看到孩子手机里的骚扰信息，很多家长第一反应是删掉、拉黑。

先截图，再拉黑。

7.6 给家长的检查清单

- [ ] 朋友圈里孩子的照片，有没有带学校、校服、校门、奖状全名
- [ ] 家长群、班级群的备注，是不是"某某妈妈 + 真名"
- [ ] 孩子的设备有没有关掉位置和通讯录权限
- [ ] 孩子的账号绑的是谁的手机号
- [ ] 学校发的在线表格，链接有没有被转发到外面
- [ ] 跟孩子说过"出事了先告诉家里"吗

7.7 法律上，未成年人有特别保护

- 《未成年人保护法》对未成年人的个人信息有专门规定
- 《个人信息保护法》把不满十四周岁未成年人的个人信息列为**敏感个人信息**，处理要取得监护人同意
- 涉及未成年人的网络欺凌、隐私泄露，平台和学校都有处理义务

报案和举报的时候，明确说一句"涉及未成年人"，处理层级会不一样。

← 返回目录

免责声明

本仓库内容**仅用于个人隐私防护与合法维权**。

允许

- 学习、自查自己的信息暴露情况
- 帮助**已获本人明确授权**的人做同样的自查
- 转载、改编本仓库内容（需遵循 LICENSE：署名、非商业、相同方式共享）

禁止

- 使用本仓库内容去查询、获取、买卖、传播**他人**的个人信息
- 将本仓库内容用于骚扰、威胁、勒索、诈骗或任何形式的报复
- 以"安全研究""背景调查"为名，行开盒之实

法律提示

未经授权查询、买卖、提供他人个人信息，在中国可能触犯：

- 《刑法》第二百五十三条之一 **侵犯公民个人信息罪**
- 《刑法》第二百八十五条、第二百八十六条 非法获取/破坏计算机信息系统数据罪
- 《个人信息保护法》《民法典》人格权编 相关民事责任
- 《治安管理处罚法》关于骚扰、恐吓、散布他人隐私的规定

其他

- 本仓库不提供、不链接任何查询他人信息的工具、渠道或方法
- 本仓库内容**不构成法律意见**，具体个案请咨询执业律师
- 作者不对任何人误用本仓库内容所产生的后果负责