

个人信息防泄漏小妙招

个人信息泄露在这个网络信息时代可以说是很平常的事情。上至耄耋老人，下至襁褓小儿，任何人的信息都可能被有心人获取。但并非所有的个人信息都构成隐私，只有个人信息中的私密信息，才构成个人隐私。

个人信息的范围和定义具体见以下法律规定：

- 《个人信息保护法》第四条：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。
- 《民法典》第一千零三十四条：自然人的个人信息受法律保护。个人信息是指：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的各种信息包括自然人的姓名、出生日期、身份证件号码、住址、生物识别信息、电话号码、电子邮箱、健康信息、行踪信息等。

在信息高度电子化的时代，保护自己的隐私是每个人的必备技能。万事网联特别分享以下提示，希望能帮助大家更好地保护个人隐私：

1. 不要在公共电脑上使用个人信息登陆网页。如果需要在网上留下电话号码或者银行卡号，可以在数字间用“-”或者“ ”间隔，降低被搜索到的概率。

2. 不要向陌生人透露自己的隐私信息，例如：银行卡号、CVC、有效期、住址、电话、邮箱等。

3. 如非必须，不要在卧室安装摄像头；电脑摄像头在不需要使用，也建议关闭或用胶布等物品遮挡。

4. 身份证复印件上应写明用途。在提供身份证复印件时，建议在含有身份信息区域注明“本复印件仅供××用于××用途，他用无效”，并写明日期。

5. 不在公开社交平台泄露家人、朋友的敏感信息。在发布自己或亲友照片时，记得关闭相机里的定位功能，这样别有用心者无法提取 EXIF 信息定位拍摄地点。

6. 机票、车票、快递单等使用后及时销毁，尽量使用自提柜收取快递，防止具体地址和个人信息等被恶意盗取利用。

7. 个人电脑不需要安装任何杀毒软件，目前 Windows10/11 系统可以使用自带的安全防护软件。某些流氓软件，会伪装成杀毒软件窃取信息。

8. 在网购或交易时不使用公共场所的 WiFi，否则交易数据和密码容易被截取泄露。

9. 不贪小便宜，不随意参与转发/扫码送礼物活动、不点陌生短信链接，不随意填写问卷调查。这些都是钓鱼攻击的典型套路。

10. 通过 QQ/微信提出转账的，需要电话确认身份。银行密码和账号分别用不同的方式告知对方。

11. 定期检查个人信息是否被利用。在搜索引擎输入个人信息，例如：姓名、邮箱、手机号等，如发现信息暴露，尽快从源头删除，或联系搜索引擎、监管部门投诉处理。

12. 注册网站、APP 时不要填写过多信息。防止信息泄露被窃取使用。

13. 社交平台添加好友时务必进行验证，定时清理好友列表，删除陌生人，同时建议限制非必要的浏览权限，以防止他人利用信息。

14. 不使用非正规厂商生产的路由器。一些路由器生产厂商可能会定向监听用户来往某个网站的数据，获取用户在特定平台的账号控制权。此外在安装路由器时，尽可能使用复杂密码提高网络安全性。

15. 简历只提供必要信息。部分公司在面试时会要求应聘者填写所谓的“个人信息表”。为避免信息安全隐患，一般情况下不要在简历中填写过于详细、具体的个人信息，尤其是家庭住址、身份证号等。

那么，如何知道自己的信息是否被泄露呢？以下是 6 种常用的检查方法：

1. **查微信支付账户。**微信可以绑定多个支付账户，打开自己的微信，点击“我—服务—消费者保护—钱包—帮助中心—实名问题”，接着点击“查询名下账户—前往查询”。这里需要输入姓名和身份证号，最后的“验证”环节还需要刷脸验证。完成以上所有步骤之后，就能看到自己名下绑定了多少微信支付账户了。如果出现了未知支付账户，或者不想绑定的支付账户，直接点击“清除”按钮即可冻结该账户，被冻结的账户无法继续使用支付功能。

2. **查支付宝账户。**打开支付宝，在最上方的搜索框搜索“我的客服”，在“我的客服”界面输入“查看名下账号”就能看见自己

名下有多少支付宝账户。对于有问题或者不需要的账户，可点击“注销”处理。

3. **查名下手机卡。**打开微信，搜索“国务院客户端”小程序，选择“便民服务”中的“电话卡一证通查”，输入个人信息（身份证，电话号码）查询。结果将通过工信部反诈中心短信通知。但这里的查询结果只会告知办理了哪个运营商的几张电话卡。如与实际不符，需要进一步联系对应运营商的客服，或者直接到营业厅咨询。

4. **自己是否“被放贷”。**通过“中国人民银行征信中心”（官网地址：<http://www.pbccrc.org.cn/>）能了解到自己名下所有的贷款信息，包括信用卡以及担保贷款情况。在官网首页，点击进入“互联网个人信用信息服务平台”，查询后，如果发现异常，立刻联系银行，或直接报警。

5. **自己是否“被就职”。**如果“被就职”正规公司，别人可能正在用你的名号冒领一份收入；如果“被就职”非正规公司，公司出了问题，那么你可能会在不知情的状况下惹上麻烦。在手机上下载“个人所得税”APP，点击“我的一任职受雇”就能看到自己目前任职的公司信息。如果出现了非所在公司信息，点击公司名并选择“申诉”进行下一步操作吧！

6. **自己是否“被法人”。**除了“被兼职”，“被法人”也是常见的一种情况。企业法人需要承担风险，甚至面临诉讼，需要引起重视。用微信搜索“电子营业执照”小程序，在弹出的提示框选择“我再看看”后点击“其它应用”，选择“投资任职情况查询”，这样就能

查到你是否是“法人”了。如果“被法人”了，迅速 110 走起吧！

如果个人信息已经被泄露，应该如何应对呢？

1. 及时止损。发现个人信息泄漏后，第一时间更换账号。信息泄露之后如果不换账号，登陆的各种信息就会源源不断地流出。因此，一旦发现了泄露的源头，就要立刻终止使用账号，切断泄漏源。如涉及的“个人隐私”属于网络数据，应及时更改相关数据；如果是骚扰电话多、垃圾短信多，可选择换个手机号，或用黑名单功能处理。

2. 一旦信息泄露，或者联系工具账号丢失，第一时间通知亲友，告知他们提高警惕以免上当受骗。因为个人信息泄漏后，不仅涉及账号盗用，还可能被利用于欺骗他人。

3. 及时取证。对于侵犯“个人隐私”的情形，我们可以通过电话录音、截屏甚至找公证机关进行公证的方式留证，方便后续维权；如果是网络平台侵权，可找到网站运营主体或者 APP 运营者进行投诉，要求其及时处理，并对投诉情况予以取证。同时可向互联网行业监管机构，如网信办投诉。

4. 如果不是网络侵权，而是通过其他方式泄露隐私，比如通过张贴告示等，可以联系派出所或社区街道人员协同处理；如果已经严重影响了正常生活，出现被骗、遭跟踪等情况，可以选择报警。

5. 无论是网络侵权还是非网络侵权，都可以通过消费者保护协会热线（12315）、市长热线（12345）等进行投诉。

6. 通过社交平台曝光相关行为，给涉事主体以压力，但曝光的同时，注意保护他人隐私，勿让自己也变成了隐私侵犯者。