女子扫码打印照片 私密照外泄

昆明警方提醒：扫描利益诱惑型二维码要谨慎；8种行为或导致个人信息泄露

都市时报记者 周婷婷

只要扫描屏幕上的二维码，就可免费打印照片。近年来，这种街头新兴的照片打印机器，引起不少逛街市民驻足。但扫码关注商家并上传照片时，很可能会存在泄漏隐私的风险。近日，真实的案例就发生在河南省焦作市的孙女士身上，最终导致她的私密照外泄。

扫码要注意些什么，哪些途径会导致信息泄露，信息泄露会带来哪些的危害？本报邀请相关专家进行分析和提醒。

案例

女子扫码上传照片免费打印 大量私密照被挂上微信公号

前不久，河南焦作市的孙女士和好朋友逛街时，在一家商场里看到一台标有“免费打印照片”招牌的机器。她按照说明用微信扫了4个二维码，将照片上传后，免费打印了4张较为暴露的写真照。这些照片因衣着暴露没冲印，一直保存在她手机里。

让孙女士始料未及的是，没过几天，一位好友给她的微信发了个链接，链接中有她的大尺度照片。随后，她赶紧联系了链接上微信公众号的客服，表示“自己是照片主人，从来没有将照片授权给任何人，如果不删除，将起诉对方侵犯了自己的肖像权”。而对方回应照片是有人通过后台提供的，对于是否授权并不知情。

“本以为照片打印出来后，对商家取消关注就行了。”经过反复思量，孙女士怀疑是免费打印照片时，将照片上传到微信公众号里导致照片被泄露了。

近年来，随着微商兴起，类似扫描街头二维码导致个人信息外泄的案例屡见不鲜。昆明市公安局相关负责人分析，针对市民扫描二维码免费打印照片，极可能关注了做微商的个人微信号，一旦对方收集用户的照片及个人微信号，他们真正的目的，用户并不知情。若不小心扫描到病毒二维码，并不排除账号被盗的风险，极可能引发诈骗，带来的隐患不堪设想。

“二维码营销属于新生事物，传播具有隐蔽性，微信证据多以电子证据形式存在，不良商家达到窃取目的后往往会删除，导致受害者取证难，司法实践中对违法二维码链接行为的监管和惩处难度较大。”云南天外天律师事务所王强律师说，消费者扫码后发生隐私泄露，微信照片免费打印设备提供者和商家可能侵犯消费者的知情权、隐私权，消费者可依据消费者权益保护、广告管理、互联网管理规定等法律法规进行维权。

王强律师提醒：微信扫码前，要仔细查看二维码提供方的主体身份，核实来源是否正规，选择官方或正规途径发布的二维码。在陌生网页上不要随意输入个人信息，来历不明的程序不能随意安装。一旦出现扫码后账号被盗等情形，应立即挂失或修改绑定的银行卡密码，要及时向微信运营商投诉，申请密码找回，并及时报警。

警方提醒

A 街头安全扫码 谨记三要素

1、扫二维码前，先要确认二维码公布方的身份，选择扫取官方或正规途径发布的二维码，不扫来源不明的二维码。

2、不要轻易通过扫二维码访问网站并提交个人信息。

3、扫描利益诱惑型、拉粉求支持型、折扣返利型二维码前，需格外警惕。

B 手机4种功能 要慎用

1、“附近的人”：微信上“附近的人”功能，可定位你的位置。依次点击“设置—通用—功能—附近的人”，选择“清空并停用”。

2、“常去地点”：苹果手机系统中有“常去地点”功能，会显示你常去的位置。依次点击“设置—隐私—定位服务—系统服务—常去地点”，关闭即可。

3、“允许搜索”：在微信“隐私”中，关闭“通过QQ号搜索到我”和“可通过手机号搜索到我”。

4、“允许查看”：在微信“隐私”中关闭“允许陌生人查看110张照片”。

C 正确使用 手机软件

1、下载：尽量选择官方渠道，特别是支付宝、银行类APP。

2、流量使用：观察应用流量使用情况，对一些使用大流量且没有进行告知的应用程序，及时检查或删除。

3、授予权限：谨慎授予应用“发送短信”、“读取短信”、“查看通讯录”、“读取定位信息”等权限。

4、退出不彻底：大部分手机用户退出手机程序时，只是返回到手机桌面，并未真正退出应用程序，这会给一些后台运行的恶意程序以可乘之机。

★新闻延展

信息泄露的危害：经常被骚扰 甚至遭遇诈骗陷阱

“请问你近期准备买房吗？”“你打算给爱车购买哪些保险呢？”“恭喜×××，你中奖了，请点击下面链接进行领奖。”估计收到此类电话或是短信的市民都会纳闷，自己与对方并不认识，他们为何会获知自己的电话号码，甚至能准确说出自己的姓名、出生日期和家庭成员情况。这些骚扰或诈骗电话、短信“投放”越来越精准，说明个人信息安全正在遭受空前的威胁。

早在2012年，盘龙警方破获云南省首例非法获取公民个人信息案，上千万条个人信息被泄露。令人唏嘘的是，盘龙公安分局网络安全保卫大队有一半民警的家庭信息都被犯罪分子掌握，包括住房、家庭、车辆、身份证号码以及车位信息样样有。犯罪团伙通过网络、QQ空间、邮件等出售各个小区业主的信息，并定期更新信息，或者是直接通过电话售卖。

这些信息被犯罪团伙转手倒卖，会对信息当事人带来哪些影响呢？侦办民警分析，稍好一点可能会向当事人打来各种推销电话，但不排除有些人用来从事通信诈骗，骗子都能说清楚受害人及家人的身份信息，一旦引起受害人恐慌，他们的骗术就离成功不远了。还可能引发冒名办卡透支欠款、账户钱款不翼而飞、个人名誉无端受损等困扰。

8种行为 会导致个人信息泄露

公民的信息是如何被泄露的？昆明市公安局相关负责人表示，公民的身份信息可能是不法人员买来的，也可能是通过技术终端窃取的。不法分子通过物管公司、房产中介购买，团伙之间也会将不同渠道获取的信息进行交换，形成利益共享，或是通过网络收集下载。而真正的高科技就是通过技术终端窃取，若网站受到黑客攻击，只要用户留下登录信息，不法分子就可通过技术手段关联出与支付宝、银行卡相关的密码。

要真正避免个人隐私泄露，引发不必要的麻烦和财产损失，仅靠相关部门的打击是远远不够的，关键在于防范。市民要注意些什么呢？有哪些行为是常常被忽视的？昆明警方进行了总结。

社交媒体晒生活 危险系数：★★★★★

通过微博、QQ空间、贴吧等和熟人互动时，有时会不自觉说出或标注对方姓名、职务、工作单位等真实信息。晒美照、晒孩子、晒机票、晒位置，是时下最热的生活方式之一。有些家长在朋友圈晒的孩子照片包含孩子姓名、就读学校、所住小区；晒火车票、登机牌，却忘了将姓名、身份证号、二维码等进行模糊处理。

各类单据随手扔 危险系数：★★★★☆

快递单、车票、登机牌、购物小票、办理手机卡的业务单，其实都是个人信息泄露的源头。随手乱扔，很可能造成个人隐私泄露，甚至导致个人财产的损失。

免费WiFi要慎用 危险系数：★★★★

公共场所WiFi安全防护功能比较薄弱，黑客只需凭借一些简单设备，就可盗取WiFi上任何用户名和密码，甚至网银和支付账号、密码等各类信息，可能在毫不知情的情况下，就被盗走了。

出售旧手机 危险系数：★★★☆

尽管卖手机前已将旧手机恢复到“出厂默认设置”，甚至格式化，但通过技术手段，专业人员还是可以把短信、通讯录、软件甚至浏览记录等全部恢复，就连支付账号、信用卡信息也可能被还原。

密码太简单 危险系数：★★★

在密码时代，很多人习惯一码通用。这个行为存在严重隐患，不法分子盗取或破解了你的某个账户之后，就会在你的其他账户进行尝试登录，专业术语叫“撞库”。一旦得手，损失增大。

把电话留给中介机构 危险系数：★★★

如今，各类教育机构、中介机构、房地产公司、装修公司、保险公司，办理业务时都会留下身份证复印件、个人姓名、联系方式等信息，稍不留意这些信息会被人非法倒卖。办理业务时，市民的身份证复印件要备注用途。

参与网络调查 危险系数：★★★

上网时经常会碰到各种填写调查问卷、玩测试小游戏、购物抽奖，或申请免费邮寄资料、申请会员卡等活动，一般要求填写详细联系方式和家庭住址等个人信息。

网络求职 危险系数：★★★

通过网上投简历找工作，简历中的个人信息一应俱全。