

泄露的个人信息 成了骗子的“导航仪”



新华社发

一个电话、一条短信，一辈子的“保命钱”瞬间就被骗个精光。类似的电信诈骗时时在上演。从根源上说，骗子屡屡得手，在于个人信息的泄露。学生家长、金融用户、新手妈妈、买房卖房者等各种隐私，不断变成骗子的“导航仪”。

信息有多廉价？ 百万人次信息以“分”为单价贱卖

个人信息售卖产业链之成熟，正不断刷新我们的认知。分行业“定点投放”：学生、股民、金融理财客户、产妇、家长应有尽有，不同群体售价不同。

记者随意在QQ群里加了一个名为“营销数据商”的电话表明想购买的来意后，他立刻发来了一个湖北省利川市第五中学的100个学生信息列表，其中包括姓名、出生年月日、身份证号、家庭住址、父母亲姓名及电话。

面对记者购买时的犹豫，信息中介说，“农村的钱少，大城市不容易被骗，你买三线城市的吧。800元可以买到一万条学生及家长信息，也可以用其他数据来换，例如3万母婴信息换1万条学生信息等。”

“以P2P为例，非法获取、使用消费者个人信息的行为十分普遍。”上海市工商局一位执法人员介绍，2015年监

管部门对一家财富管理公司上海分公司的调查发现，纸质资料涉及的个人信息共有38000余人次，电子数据保存的个人信息名单有120M(兆)，涉及了100万余人次。

据了解，一些经营理财业务的公司为拓展市场、发展客户，通过购买、交换等方式大量收集消费者个人信息。在收集和使用个人信息后，大多未进行妥善保管和处理，甚至二次售卖。

诈骗有多“精准”？ 产业链上下游往往附着多个专业团伙

在安徽警方与柬埔寨警方合作破获的一起跨国诈骗案中，警方在犯罪窝点查到一本“诈骗剧本”。诈骗团伙事先编写好“剧本”，设计好诈骗时的对白和语音内容。诈骗人员会冒充不同地区不同单位的工作人员，所提供的单位名、电话号码等保证与当地信息吻合。

上海市公安局刑侦总队二支队副支队长韦健介绍，

每一起通讯信息诈骗中，产业链上下游往往附着至少五个专业团伙：专司策划骗术、拨打电话的直接诈骗团伙；盗卖个人信息团伙；收集办理非实名电话卡、银行卡卖给诈骗分子的团伙；在互联网上搭建诈骗网络平台并与传统通讯网对接及提供任意改号、群呼服务和线路维护的技术支撑团伙；专门负责替若干个诈骗窝点转取赃款

的洗钱团伙。

现在170和171的虚拟运营商号段，让诈骗也变得更加简单。记者在上海火车站附近一家电话卡营业厅，购买了一张171开头电话卡，不需要任何证件。“这个是虚拟运营商的，和普通的手机号码一样使用，也能注册支付宝。你用这个转账，支付宝也找不到你。”店家说。

损失有多严重？ 一年“盗”走网民900多亿元

中国互联网协会《中国网民权益保护调查报告2016》显示，近一年，国内6.88亿网民因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算达915亿元。

网络非法获取公民个人信息日益猖獗，形成了“源头—中间商—非法使用人

员”的黑色产业。机关单位、服务机构以及个体企业相关人员参与的泄露活动更加隐蔽，而通过技术手段实施攻击、撞库或利用钓鱼网站、木马、免费WIFI、恶意APP等技术手段窃取成为重要的泄露方式。

犯罪团伙拥有大量电话

卡和银行卡，说明运营商实名制没有完全落实，很可能存在一些员工非法寻租、参与犯罪。银行也存在发卡泛滥，实名制未落实、银行网络在境外转账分解资金缺乏限制等现象，这些是导致诈骗案猖狂肆虐的根源所在。

据新华社电

警方为您梳理 常见电信诈骗手法和防范对策

□记者 马涛 通讯员 卢淑仪

随着我市反虚假信息欺诈中心的运行，今年以来，我市电信诈骗案件连续呈下降趋势。但紧绷之弦不可松，电信诈骗的“套路”到底有哪些？究竟该如何防范？昨天，记者采访了市公安局刑侦支队民警刘益，为您一一解读。

18种常见诈骗手段

(一)“电话欠费”诈骗。这种方式最为普遍。犯罪嫌疑人以电信部门名义群发信息或直接拨打电话，称事主开户的固定电话欠费，事主否认有此情况后，犯罪嫌疑人建议事主报警，然后冒充公检法等政府部门，以银行账户涉嫌诈骗或洗钱等为借口，要求事主把账户内存款转到所谓的“安全账户”实施诈骗。

(二)银行卡消费、银行转账短信息诈骗。犯罪分子会给你发送一个银行卡消费、转账或透支等内容短信，当你电话“垂询”时，几名犯罪分子则分别扮演“银行工作人员”、“警察”、“银联管理中心”层层设下圈套，只要确定你卡上有资金，他们并会忠告你把钱转到“安全账户”

内，骗走你的钱财。
(三)“猜猜我是谁”诈骗。
(四)退税诈骗。
(五)虚构绑架诈骗。
(六)虚构“紧急情况”诈骗。
(七)网络荐股、帮忙买股诈骗。
(八)盗用QQ借款诈骗。
(九)贷款信息诈骗。
(十)中奖信息诈骗。
(十一)汇款诈骗。
(十二)“冒充领导”诈骗。
(十三)无偿提供低息贷款诈骗。
(十四)“骗取话费”诈骗。
(十五)冒充黑社会敲诈实施诈骗。
(十六)“高薪招聘”诈骗。
(十七)以销售廉价违法物品为诱饵诈骗。
(十八)电话交友诈骗。

防骗做到“三不一要”

宁波市公安局刑侦支队民警刘益说，防范电信诈骗最根本的还是要提高自身防范意识。

银行账户、支付账户、普通网站会员账号需要区别使用账号名和密码，每3个月修改一次密码，密码组合尽量采用大写字母、小写字母、数字等组合；不随意登录不明wifi，不打开不明短信中的链接，不下载不明软件，电脑中安装安全软件，及时查杀木马病毒软件，拦截钓鱼链接；遇到自称变更手机号码的情况，应该直接拨打手机中存储的电话，或通过联系通讯录好友和其亲友进行甄别确认。

公安机关提醒广大群众：防止上当受骗，在工作生活中，要做到“三不一要”：

不轻信：不轻信来历不明的电话和手机短信，不管不法分子使用什么甜言蜜语、花言巧语，都不要轻易相信，要及时走开，挂掉电话。不回复手机短信，不给不法分子进一步设圈套的机会；

不透露：无论什么情况，都不向陌生人透露自己及家人身份信息、存款、银行卡等情况。如有疑问，可拨打110求助咨询，或向亲戚、朋友、同事核实。警方特别提醒说，

对通过电话、短信要求进行涉及资金的操作，务必保持警惕，如有疑问可拨打110进行咨询；收到熟人发来的转账、代付款等信息后，需要电话当面确认是否属实；收到银行、运营商等商业机构发来的短信，如有链接不要轻易点击，不要轻易安装链接中的软件。接到电话，可以采用回拨官方客服的方式进行确认；警惕冒充公检法等机构的短信、电话，若收到，可以咨询亲友意见或到相关机构进行核实。

不转账：学习了解银行卡常识，保证自己银行卡内资金安全，决不向陌生人汇款、转账。老年人和妇女要格外引起注意，还有一些财会人员和经常有资金往来的人群等，在汇钱、转账前，要再三核实对方账号。

要及时报案：万一上当受骗或听到亲戚朋友被骗，请立即向公安机关报案，可直接拨打110，并提供骗子的账号和联系电话等详细情况，以便公安机关开展侦查破案。

这“三不一要”总结起来，就是：陌生电话勿轻信，对方身份要核清，家中隐私勿泄露，涉及钱财需小心，遇到事情勿惊慌，及时拨打110，诈骗信息勿删除。