个人信息泄露是网络通讯诈骗最大帮凶

八个渠道成信息泄露重灾区

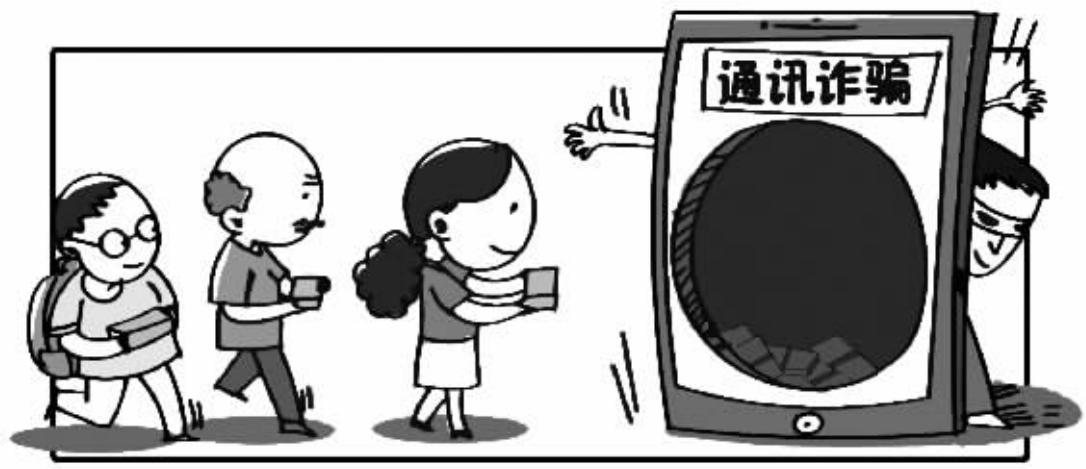
主要集中在手机应用程序、简历、网络调查、社交媒体、身份证复印件、旧手机、公共WiFi和各类单据等方面

山东临沂3名大学生遭遇通讯诈骗，不仅钱财被骗走，其中2名学生还不幸死亡。连日来，此类事件不断发酵，关于通讯诈骗的话题再次掀起舆论风波。

通讯诈骗无孔不入，几成社会顽疾。难道真的如“牛皮癣”一样，防不住，治不了吗？

据了解，随着我市反虚假信息欺诈中心的运行，今年以来，我市通讯诈骗案件连续呈下降趋势。但紧绷之弦不可松，通讯诈骗的“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，为您解读。

记者 马涛



漫画 章丽珍

诈骗背后是个人隐私泄露

今年7月27日10时，市民张女士接到一个开头为189、尾号为110的陌生手机号码的电话。对方自称是宁波市公安局民警，称张女士涉嫌一起3岁儿童拐卖案，案件由上海公安机关调查，说着就把电话转到上海一位“民警”那里。

接通“上海民警”的电话，对方就要核实张女士身份，一番查询下来，说张女士除了涉嫌儿童拐卖案以外，还涉嫌一起210万元的信用卡诈骗案，吓得张女士当场就说不出话来。

随后，对方就让张女士转一部分钱到一张卡上，转账途径可以登录“中国最高人民检察院”网址查询，同时附上网页具体地址。张女士根据要求操作转出51553.42元。

转完账，对方就音讯全无，张女士才发现被骗了。

刘益分析说，此类通讯诈骗中，不法分子之所以能够“精准出击”，根源在于受害人个人信息被泄露。那么，个人信息泄露问题究竟出在哪？刘益称个人信息泄露主要集中在以下8个方面：手机应用程序、简历、网络调查、社交媒体、身份证复印件、旧手机、公共WiFi和各类单据。

对此，他建议：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，PC和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。

防治网络通讯诈骗请做到“三不一要”

刘益说，防范通讯诈骗案件，最根本的还是要提高群众自身防范意识，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花言巧语，都不要轻易相信，不给不法分子进一步设圈套的机会；

不透露：无论什么情况，都不向对方透露自己及家人的身份信息、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。

不转账：决不向陌生人汇款、转账，中老年人和妇女要格外引起注意，还有一些公司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，不要让不法分子得逞。

要及时报案：万一上当受骗或亲戚朋友被骗，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。

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。

个人信息泄露有多严重？

一年“盗”走网民900多亿元

网络时代，伴随公民个人信息泄露而来的恶果令人瞠目。中国互联网协会《中国网民权益保护调查报告2016》显示，近一年间，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，涉及身份信息、电话号码、家庭地址，扩展到网络账号和密码、银行账号和密码、购物记录、出行记录，且形成了“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。

今年4月以来，公安部部署开展了打击整治网络侵犯公民个人信息犯罪专项行动，截至7月全国公安机关已累计查破刑事案件750余起，抓获犯罪嫌疑人1900余名，缴获信息230余亿条，清理违法有害信息35.2万余条，关停网站、栏目610余个。

上海市公安局刑侦总队二支队副支队长薛勇表示，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，这些是导致通讯诈骗案猖狂肆虐的根源所在。

业内人士认为，应在法律层面加大惩处力度、完善相关司法解释。目前我国并没有专门的个人信息保护法，现有法律中的相关规定过于宽泛、模糊。现在通讯诈骗利用网络作案较多，应出台司法解释完善电子证据的认定标准，对有关“帮助信息网络犯罪活动罪”等，应加强法律适用、加大追责力度。 据新华社

■相关链接

常见通讯诈骗手段

冒充公检法诈骗 犯罪嫌疑人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。

银行卡消费、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，分别扮演银行工作人员、警察等层层设下圈套，要求受害人把钱转到“安全账户”内，骗走钱财。

退税诈骗 犯罪分子冒充税务、财政、车管所工作人员打电话称，国家已经下调购房契税、购车附加税税率要退还税金，让你提供银行卡号直接通过ATM机转账退还税款。

虚构“紧急情况”实施诈骗 犯罪分子会冒充医院医护人员、学校教职工等人员，打电话谎称你的亲属（如在异地上学的孩子），遭遇车祸、突发疾病等“紧急情况”，要求您紧急汇款。

网络荐股、帮忙购买股票诈骗 嫌疑人以帮助选股票付酬劳、收益分成或帮受害人购买股票为由骗取受害人汇款。

盗用QQ借款诈骗 犯罪分子通过黑客手段，盗用某人QQ后，分别给其QQ好友，发送请求借款信息，进行诈骗。有的甚至在事先就有意和QQ使用人进行视频聊天，获取了使用人的视频信息，在实施诈骗时有意播放事先录制的使用人视频，以获取信任。

贷款信息诈骗 犯罪嫌疑人群发提供低息甚至无息贷款信息。当事主联系时，犯罪嫌疑人要求其向指定账户汇入“验资款”“手续费”“好处费”，以诈骗钱财；或索要事主银行账户，再层层设套，窃取事主银行账户密码，通过网上银行将存款迅速转走。

中奖信息诈骗 犯罪嫌疑人群发大量彩票中奖、电话号码中奖、QQ号码中奖等信息，要求中奖人打“兑奖热线”电话，以先交纳“个人所得税”“公证费”“转账手续费”等为借口，诈骗钱财。

汇款诈骗 犯罪分子大量群发“我的银行卡消磁了，请把款转至我同事账户，账户××××”等类似信息，恰巧你要汇款时，就有可能上当受骗。

冒充领导诈骗 不法分子假冒领导、秘书或部门工作人员等身份打电话给基层单位负责人，以推销书籍、纪念币、划拨款项、配车、帮助解决经费困难等为由，让受骗单位先支付订购款、配套费、手续费等到指定银行账号，实施诈骗活动。