2016年8月27日 星期六
值班主任：黄娟 主编：王红卫 美编：红胄
海南日报


徐玉玉生前照片。

核心提示

随着大学开学临近，临沂市接连发生至少3起电信诈骗学生案件，3名学生银行卡内资金被骗，其中两名学生猝死，疑与被骗有关，引发社会关注。

记者今天从山东省临沂市公安部门获悉，其中关注度最高的“临沂市罗庄区徐玉玉电信诈骗案”26日已经成功告破。另一起“临沭宋振宁被骗案”也已锁定2名犯罪嫌疑人，案件侦破工作取得重大进展。

大学生连遭电信诈骗，其中两名学生猝死

山东临沂徐玉玉被诈骗案告破

另一起“临沭宋振宁被骗案”侦破取得重大进展，目前已锁定2名犯罪嫌疑人

综合新华社电 8月19日，山东省临沂市罗庄区高都街道中坦村18岁女子徐玉玉接到了一通诈骗电话，即将进入南京邮电大学英语系就读的她被骗走9900元学费。在和父亲报警回家的路上，家境十分贫寒的徐玉玉突然心脏骤停，经医院抢救无效死亡。

同期，在临沂市河东区，另有一名女学生被骗走6800元学费。

8月23日凌晨，临沂市临沭县即将进入大二学习的山东理工大学学生宋振宁也在遭遇电信诈骗后心脏骤停，不幸离世。

记者从国家公安部获悉，徐玉玉被骗案件发生后，公安部高度重视，立即组织山东、福建、江西、广东等地公安机关开展侦查。26日，临沂市徐玉玉电信诈骗案成功告破。

与此同时，记者从当地警方了解到，山东临沭宋振宁被骗案侦破工作也已取得重大进展，目前已锁定2名犯罪嫌疑人，抓捕及相关工作正在进行中。

记者从临沂市委宣传部了解到，被骗女学生徐玉玉接到的诈骗电话是171号段，河东区被骗女学生接到的诈骗电话显示是021开头的固定电话，被骗男学生宋振宁接到的也是固定电话，都用改号软件改过。

4名犯罪嫌疑人落网

据新华社电 经查明，徐玉玉电信诈骗案为犯罪嫌疑人陈文辉、郑金锋、陈福地、熊超、郑贤聪、黄进春等人所为。26日，专案组分赴福建、安徽、江西、贵州、广东多地，经连续紧张奋战，截至8月26日晚，主要犯罪嫌疑人熊超、黄进春、郑金锋、陈福地4人被抓获。

熊超，男，汉族，1997年10月28日出生，户籍地址：重庆市丰都县三合街道啄木嘴村2组53号，身份证号码：500230199710286110。

黄进春，男，汉族，1981年08月10日出生，户籍地址：福建省泉州市安溪县湖头镇下坑村下坑43号，身份证号码：350524198108101597。

郑金锋，男，汉族，1987年11月05日出生，户籍地址：福建省永春县达埔镇乌石村1192号，身份证号码：350525198711053530。

陈福地，男，汉族，1987年09月27日出生，户籍地址：福建省安溪县白濑乡下镇村待御潭31号，身份证号码：350524198709278611。

公安部A级通缉在逃人员

26日，公安部发布A级通缉令，公开通缉熊超（已落网）、陈文辉、郑贤聪3名犯罪嫌疑人。目前山东警方正在有关地区协同支持下，全力追捕其他2名在逃人员。

陈文辉，男，汉族，1994年12月10日出生，户籍地址：福建省安溪县白濑乡下镇村待御潭66号，身份证号码：350524199412108616。

郑贤聪，男，汉族，1990年01月25日出生，户籍地址：福建省永春县达埔镇达山村837号，身份证号码：350525199001253559。

请举报

公安部：

请各地公安机关接此通缉令后，立即部署查缉工作，发现犯罪嫌疑人即予拘留，并速告公安部刑侦局。

公安部将对发现线索的举报人、协助缉捕有功的单位或个人，**每抓获一名犯罪嫌疑人**将给予人民币**五万元奖励**

（以上图片均来自公安部网站）

电信诈骗成为“打不死的小强”

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，近一年的时间，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。

类似的电信诈骗时时在身边上演。学生家长、金融用户、买房卖房者等各种隐私，不断变成诈骗的“导航仪”。电信诈骗犯罪呈现“虚拟化、智能化、集团化、国际化”特点。专家指出，“问题号段”频出，运营商疏于监管难辞其咎。

诈骗有多“精准”？

从最初的中奖、房租汇款，到网银升级、邮包藏毒，再到冒充公检法等公职人员、伪造网上通缉令、助学金领取，通讯信息诈骗类型已扩展到数十种，更从过去的“撒网式”诈骗，变成了“精准化”锁定。这种靶向性更强的行骗手段，成功概率更高。

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。社交平台被“充分应用”：建数十个QQ群不断推送广告，最终指向同一个数据商。

在安徽警方2013年9月与柬埔寨警方合作破获的一起跨国电信诈骗案中，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。行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。

这只是诈骗团伙“产业化”“企业化”的一个缩影。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的一家电话卡营业厅，就购买到了一张171开头的电话卡，随买随打，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。

信息有多廉价？

很难想象学生的不设防，会成为骗子叫卖的宣传语。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。”而对于信息来源却讳莫如深，“有专门的渠道，告诉你了，我还能吃啥？”

“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。

随着电信诈骗手段不断升级翻新，案件数量堪称“井喷”。2015年，仅上海就破获电信诈骗案件4209起，同比上升64.8%。

打击有多艰难？

网络交易、分工明确、跨国行骗，使得近10年来，公安机关抓获的此类犯罪嫌疑人大多是处于链条末端的“取款人”，摧毁一个完整的通讯信息诈骗犯罪跨国境团伙很难，不少策划者仍身在境外。

“由于电信诈骗属于‘非接触式’犯罪，环环相扣，很难留下诈骗的确凿痕迹，为警方办案带来困难。”韦健介绍，而且由于电信诈骗不受地域和空间限制，使得发现、跟踪和抓捕有很大难度，破案成本非常高。

上海政法学院教授汤啸天介绍，因为追赃定赃难，使得电信诈骗量刑过轻，对犯罪分子的威慑力不够。 **（据新华社8月26日电）**

新闻纵深

大学生为何成电信诈骗受害“重灾区”？

记者调查发现，大学生群体近年来已成电信诈骗受害“重灾区”，要避免“徐玉玉式悲剧”再现，必须多管齐下，综合施策。

A 高校学生成为新的受骗群体之一

在今年大学新生入学之际，山东地区大学新生遭遇电信诈骗并非孤例。临沂另一位女学生与徐玉玉同一天被骗走准备交学费的6800元。

翻开案卷，近年来各地大学生遭遇类似的电信诈骗案件屡见不鲜，高校学生成为新的受骗群体之一。

去年10月，长沙某高校大四学生小陈欲将一款网络游戏装备出售，登录某交易网站进行交易。不久，小陈就收到了来自“网站客服”的电话。对方在电话中称“游戏装备已被卖出，如提现需交足等额押金”。

沟通过程中，“客服”想方设法骗取了小陈信任，不断要求他开通“保障金服务”、支付“提现费用”。信以为真的小陈通过支付宝三次转账1万余元，之后拨打对方电话显示关机，才意识到上当受骗。

长沙市公安局内保支队调查发现，大学生是电信诈骗受害高发人群，极易遭受以网上兼职、低价网购、中奖通知、低价订票等名义实施的诈骗。

全国多地警方统计显示，大学生群体已成为电信诈骗受害“重灾区”。去年6月，北京市公安局对外通报，2015年前4个月，北京高校日均发生电信诈骗案件2.9起。

重庆渝北警方通过梳理辖区近3年电信诈骗案发现，20岁以下受害人占比12.85%，这个年龄段群体多以学生为主，容易受到虚假网络购物和游戏装备网站引诱。20－29岁占比43.73%，这个年龄段群体多以大学生和刚参加工作的年轻人为主，是网络购物的主力军，被骗手段以网络诈骗和电话诈骗居多。

B 不法分子为何频频盯上大学生？

一些办案者和教育工作者指出，个人信息泄露、容易受到诱惑、社会经验不足和防骗教育缺失，是大学生频频被不法分子盯上的关键原因。

——个人信息泄露。在徐玉玉案中，不法分子打来电话，称有一笔2600元的助学金要发放给她。因前一天曾接到教育部门发放助学金的通知，因此她并未辨别电话真伪。这表明，徐玉玉的个人信息可能已遭泄露。

——容易受到引诱。湖南省刑侦总队重案支队副支队长郭建华说，“高薪兼职”和“中奖通知”是大学生上当最多的两类电信诈骗。不法分子利用部分大学生急于赚钱或积累工作经验的心理，一步步引诱大学生“上钩”。

——社会经验不足和防骗教育缺失。北京大成（济南）律师事务所律师梁珊认为，青年学生涉世不深，社会阅历较浅，安全防范意识相对薄弱，加之又是互联网和手机的重度用户，容易暴露在诈骗高发的环境之中。

C 综合施策守住大学生“钱袋子”安全

近年来，电信诈骗愈演愈烈，涉及面之广、受害者之众、受损金额之大，触目惊心。专家指出，打击电信诈骗，除了要加大打击力度之外，针对特定受害人群的防骗措施也必须跟上。

——多部门联动齐抓共治。广东中山市公安局刑警支队副支队长古伟民提出，光靠公安机关一家难以有效防范和打击电信诈骗犯罪，必须堵塞银行、电信部门监管漏洞，形成多部门齐抓共管、源头治理格局。

——高校积极开展防骗警示教育。郭建华建议，高校可联合办案机关，开展多种形式的防骗警示教育，向大学生讲解避免个人信息泄露的方法，以及一些发案率较高的电信诈骗类型、特征及避免上当受骗的技巧。

——建立快速止付和账户冻结机制。一些办案者指出，打击治理电信诈骗是项系统工程，尽管国家近年来加大了打击力度，但短期内还难以根治。在受害者遭遇诈骗时，若能快速止付或冻结账户，可以最大程度挽回损失，避免引发悲剧。

本月16日，湖南省打击治理电信网络新型违法犯罪中心揭牌运行，公安、银行、银联公司和通信运营商等部门工作人员合署办公，具备快速止付、冻结账号、封堵诈骗电话等功能。

“在受害者遭遇诈骗后，只要及时拨通反诈中心报警电话，就有可能追回损失。”反诈中心一位民警说。

（据新华社长沙8月26日电）