

前言

近年来，科学技术的迅猛发展导致公众生活习惯发生着改变，人民群众在享受科学技术带来便利的同时，传统诈骗也借助科技手段不断衍化成新型的电信网络诈骗犯罪。该类侵财犯罪的智能性、隐蔽性逐步增强，给公众带来的经济损失更是无法估量。2017年之前，我国电信诈骗案件每年以20%至30%的速度快速增长，造成经济损失数百亿元。山西省的电信网络诈骗犯罪与全国的发展态势相同。

在电信诈骗案件受害群体中，高校学生占有比例较高。这是由于高校学生自身社会经验少、安全防范意识低，有一定的经济能力，使诈骗分子将矛头指向了在校学生。电信诈骗案件给大学生造成了巨大的财产损失和精神创伤，严重威胁了校园安全与和谐，损害了社会风气。比如发生在山东的“徐玉玉案”（因收到虚假助学金信息被误导致猝死）和广东的“蔡淑妍案”（因收到虚假中奖信息被误导致跳海自杀），防范和打击电信网络诈骗违法犯罪的工作任重道远。

2016年以来，公安部联合多部门在全国范围组织开展打击电信诈骗专项行动。2016年12月20日，公检法联合发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》，明确了诈骗罪“酌情从重处罚”的10种情形，包括“造成被害人或其近亲属自杀、死亡或者精神失常等严重后果”、“冒充司法机关等国家机关工作人员实施诈骗”等。各地公安机关成立相应的打击电信网络诈骗的专职机构，如太原市公安局的“反诈骗中心”，全面整合银行、电信等多部门形成打击合力，有效地遏制了电信网络诈骗案件高发态势。

太原市公安局直属分局肩负着省级高校的内部安全保卫工作，目前在校大学生 12 万余人。大学生是网络上的主力军，没有经历过社会的洗礼，多数不具备防范心理和警惕性，使这一群体成为电信诈骗的主要受害者。由于学生人数众多、基数庞大，所以在当前形势下，预防和打击电信诈骗，对净化和完善校园环境、维护高校安全稳定有着十分重要的意义。

2017 年省城高校诈骗案件稳中有降，但由于电信网络诈骗案件无犯罪现场，到账速度快，追赃难度大，犯罪分子多藏身境外，给高校师生带来巨大的经济损失，2017 全年诈骗案件经济损失共计 766968.17 元。

下面就针对校园电信诈骗案件的特点，将真实案例进行分类汇总，发布警情提示，希望广大师生要进一步增强安全防范意识，了解犯罪分子的作案伎俩，有效保护自身财产安全，不给犯罪分子可乘之机，以自己的实际行动共筑美好校园。

(本手册案例均为真实案例)



目 录

1. 自称公检法篇.....	1
2. 天上掉馅饼篇.....	4
3. 冒充熟人篇.....	7
4. 兼职招聘篇.....	11
5. 网络贷款篇.....	13
6. 购物欺诈篇.....	15
7. 助学补贴篇.....	19
8. 网络投资篇.....	20

自称公检法篇



1 自称“刑警”要监管你账户？

2017年6月13日，某大学学生宋某接到一个自称是太原邮政局的客服人员，对方称宋某在武汉市办理过一张信用卡透支16580元。后对方将宋某的电话转接给一个自称是武汉市公安局的警官让其配合调查，之后宋某在对方的指挥下，通过支付宝向所谓的“安全账户”（对方银行卡）内转了5700元人民币。



电信诈骗



民警提示

自称警方的涉案电话无需理会，特别是不要转账给并不存在的“安全账户”。若对方要你前往自动柜员机进行操作时，一定要注意不要因为诱导而按下转账键。

2 “公安局”说你洗钱、包裹藏毒？

2012年12月6日，张某在家中接到一个自称公安民警的男子的电话，对方称张某涉嫌一宗洗钱罪，“公安局”方面在嫌疑人身上发现有张某的身份证，需要清查张某的银行账户才能洗清嫌疑，要求张某将账户里的钱汇到“公安局”的账户核实情况。后张某在诈骗人员的引导下，在邮政银行给对方转去现金10000元，在工商银行给对方指定帐户转去现金160000元，共计被诈骗现金17万元。

答：2012年12月6日上午9时许，我家里的固定电话接到了一个电话，因为没有来电显示，不知道这个电话号码。对方是一个男子声音，他说是太原市公安局的民警，说太原市有一个叫“王军”的犯罪嫌疑人，现羁押在郑州市公安局，涉嫌洗钱罪，警方从犯罪嫌疑人身上搜出来我的身份证，现在警方怀疑我涉嫌该案件，让我赶紧去郑州市公安局报警，并给了我一个电话：0371-66222023，这次通话持续了大概十二、三分钟。我用我的手机给这个电话打过去，是一个男子接的电话，对方自称叫陈海，警号是067241。我问他有没有一个叫涉嫌洗钱罪的犯罪嫌疑人叫王军。他说是的，现在王军被郑州市公安局羁押。他告诉我说王军向我的建行卡上汇了216万人民币，给了我21.6万的好处费。我说我并没有收到一分钱，他说你需要洗清罪名。他问我有多少存款，我说有20万元存款，其中19万存在工商银行，1万存在邮政储蓄。我问他该怎么办，他说他给我接到局长办公室的电话。过了不一会儿，电话里就有一个男子的声音，对方自称“小杨”，他对我说今年10月5日的时候，犯罪嫌疑人王军给我的账号汇钱。如果不能洗清罪名就成为犯罪嫌疑人了，让我把存款取出来汇给他，警方要清查一下。他还问我有没有他的号码；我说我没有来电显



遇到冒充公检法类诈骗，请注意：不要轻易泄露个人信息，更不要轻易汇款，及时拨打相关部门电话核实对方身份，或是直接拨打110报警。

3 电话已欠高额话费？

2015年11月23日，某大学学生丁某接到一个自称是中国电信客服人员的电话，对方告知其电信网络业务欠费2685元，丁某称其从未办理电信网络业务。对方告知丁某其身份证信息可能被人冒用，并将电话转接至“天津市公安局西青区分局”，随后被自称公安人员的“陈海涛”以丁某名下的建设银行卡从事贩毒洗钱违法犯罪行为为由，骗走其



6400元。



不存在所谓的“安全账户”。公安民警、检察院法院工作人员也不会通过电话办案或网络办案。民警一般通过电话联系，在正规办案场所或当事人处处理警情。

天上掉馅饼篇



4 “幸运观众”先交押金？

2015年3月16日，某大学学生姚某在宿舍打开手机后发现收到陌生号码发来的一条短信，称其中奖获现金16万和一台苹果笔记本电脑，并提示其登陆tb859.com查询。姚某按对方提示登陆网页进行操作，并与网页上标注的客服电话400298606联系，在对方哄骗下分三次给对方提供的工商银行帐户转账共38000元人民币，事后意识到被骗。



手机号码已被浙江卫视《中国好声音》节目活动抽选为场外幸运观众，我将获得惊喜奖金9.8万元创业基金以及苹果公司赞助提供的苹果MacBookPro笔记本一台，并让我用电脑登陆活动网站www.zjtvsh.com查看领取，我的验证码是2988。我当时非常高兴，就在宿舍上网查看了网址，然后输入了验证码，填写了一份幸运观众的调查表，也就是我自己的基本情况。填写完以后，网页上跳出一个对话框，上面提供了一个专门针对我的客服电话，号码是089888110330。然后我就拨通了089888110330，客服是个男性，自称姓陈，先恭喜我中了二等奖，然后告知我按规定必须先转账2800元的保证金，让



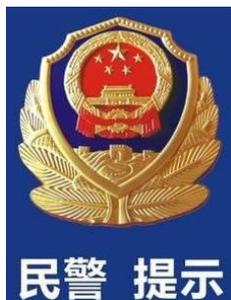
请理性对待中奖信息，致电官方客服询问是否真有抽奖，切勿随意填写个人信息，更不要转账给任意个人。不要心存侥幸，不存在飞来横财。

5 视频交友网“免费”无底洞



2016年5月3日，某大学学生张某在网上看到一个美女视频交友广告，点击链接发现是个隐蔽的色情付费裸聊网站。系统显示只有十秒的免费体验时间，必须充值成为VIP

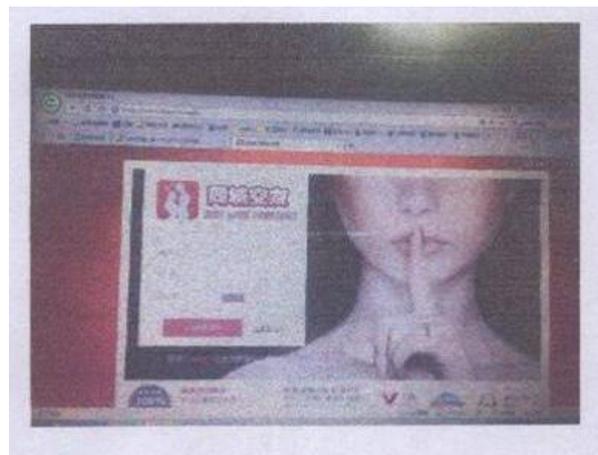
会员才能继续进入聊天室。观看一段时间后只有缴费升级到超级VIP才能继续观看。张某意识到不对要求退款，客服表示还需要购买“礼物”才能退款。整个过程中，张某通过支付宝转账的方式转给对方，其中10元2笔、298元1笔、600元1笔、1000元2笔、1888元2笔、2000元4笔和3000元52笔。共计被骗现金170694元。



要充值缴费的各种色情网站、视频聊天大多是诈骗，甚至隐藏木马病毒盗窃注册者的个人和银行信息，一定不要“自投罗网”。

6 婚恋交友一线牵？

2017年11月2日，某大学学生白某登录手机QQ，在其中的“兴趣部落”中看见一女子照片，白某加其为好友。11月3日下午，白某通过聊天得知：该女子名叫“杨晓雨”，网名“雨雨”，19岁，河南省人，现在当地打工。在2017年11月3日至11月4日期间，“杨晓雨”以“吃饭、碰车、来太原见面购买飞机票、手机欠费、购买衣服和住宿”等多种理由，先后向白某借钱4354元钱人民币，白某事后发现被骗。



网上交友需谨慎，遇到需要给对方礼物、红包时，要提高警惕，避免转账或是借钱给结识不深的人，遇到发布虚假信息者可向网站举报发布者。

冒充熟人篇



7 冒充亲友托你转个账



2016年6月8日中午，某大学学生张某在学校宿舍玩手机时，其嫂子徐某的QQ主动跟其聊天，让张某通过支付宝帮其代付购买衣服的钱，张某信以为真先后4次同意了对方发来的代付请求，通过支付宝先后支付人民币1122元、3978元、4794元和8670元人民币，随后张某察觉不对，通过电话向其嫂子核实后发现被骗，被骗18564元钱。



民警提示

通过聊天工具提及资金时需谨慎，接到亲友借钱、汇款、救急等消息，一定要先打电话跟对方确认真有其事后再汇款。发现自己的聊天工具被盗后，应尽快找到密码，并告知亲友谨防被骗。

8 我是你领导 来我办公室

2016年1月，省城多所高校领导调整工作，某大学领导韩某接到诈骗电话（山西太原号码），对方以新任校党委书记的口气约其到办公室谈话。次日诈骗人员表示正在开会，不方便见面，要求韩某汇款6万元“应急”使用。韩某一时失察，误信对方，被骗6万元。



核实对方身份，及时与领导联系询问，切勿对号入座或转账。接到领导重大工作指示，特别是涉及款项等经济事务，一定要慎重，最好的办法就是当面核实或通过可靠联系方式确认。

9 车祸？手术？急用钱

2012年11月27日9时许，太原居民冯某接到一陌生电话，谎称是他儿子在从大同到太原的路上发生车祸，要求汇款，然后



其在工商银行向对方银行账号汇款2万元整。11时许，对方又打电话要求汇款3万元，随后冯某给他儿子打电话核实情况，发现被骗。



被告知家人遇到车祸、手术等紧急情况，应立即与家人朋友进行核实，确实联系不上，也应找人商量，切忌轻易转账汇款。

10 被绑架？要赎金？

2016年8月19日下午16时许，某大学一名学生家长接到电话称其女儿张某被绑架，要求给对方账户打入40万元。

民警通过认真查看视频监控资料，查找“被绑架人”活动轨迹，发现其于8月19日下午15时许，一人独自来到某宾馆开了一间钟点房，于17时许离开宾馆。同时根据受害人手机定位系统沿途追踪，最终于晚上21时许在该宾馆找到张某。

张某表示8月19日接到自称公安局人员的电话，对方称张某涉嫌犯罪，需要配合对方接受调查，详细询问张某家庭成员信息后要求其独自一人去某宾馆开一间房，为避免泄密将手机呼叫转移到“骗子”手机上，并在手机上换一张卡保持通话，还让张某在太原市大范围地活动一圈。



民警 提示

遇到蹊跷的电话，最好是通过多种渠道设法核实情况，不要轻信陌生人，接到此类电话立即报警，以便警方及时打击犯罪。

兼职招聘篇



11 打字招聘 轻松高薪？

2017年11月13日，某大学学生周某寻找网上兼职，被诈骗人员以招打字员为名，要求周某缴纳培训费、管理费、验证费等费用共计1518元，周某随后意识到被骗。



城上找到一个做打字员的兼职工作。对方客服要求我叫一部分钱（300元）做保证金，培训费500元钱。部门管理费审核费499元，验证费219元。我通过微信红包的方式共交费1518元钱。随后我感觉不对要退钱，对方拒绝后我报警。



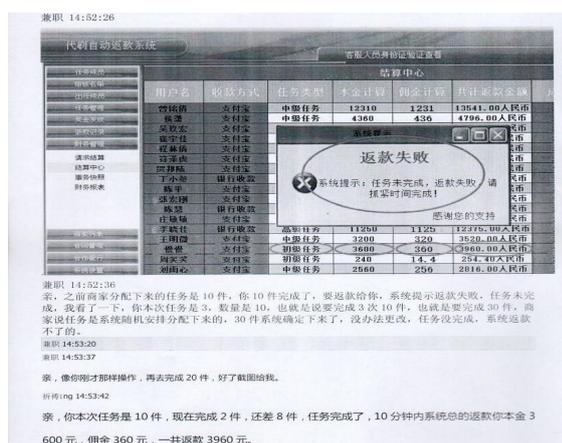
民警提示

在网上找兼职时，要核对对方公司的信息，轻松高薪的工作多是犯罪分子丢出的烟雾弹，正规工作是不需要在上岗前缴纳押金、保证金、诚信金的，网络上签订的电子合同没有任何法律效力。

12 刷钻刷信誉 淘宝兼职?



2017年11月5日,某大学学生李某在宿舍用手机上网加了一个刷单的QQ好友,对方先发了一个226元淘宝购物链接,让李某拍下后不要付款,并发了一个收款二维码,李某扫描后给对方付款226元,对方给李某返还本金和佣金共238元,接着对方分别给李某发了770元、1499元、1300元、4800元、4800元的淘宝购物链接,李某按照上面的方法拍单并扫描二维码支付,完成后对方以



各种理由不给退还本金,还让继续刷单,李某发现被骗,共计13169元。



仔细甄别网站的真实性,查看网站制作是否精良,如发现内容比较空洞需谨慎考虑。刷信誉及刷钻本就属于违规行为,应避免参与此类工作。

网络贷款篇



13 “网上贷款” 押金连环骗

2018年1月7日上午，梁某使用手机上网申请贷款，在“北京平安普惠投资担保有限公司”网页填写资料后，添加对方客服QQ之后，对方以需缴纳手续费、提高银行账户信用评级、激活账户等为由，哄骗报案人使用本人微信软件、在单位及某大学校园内，先后三次向对方银行账户转账，共计9000元人民币，后无法联系，也未收到贷款。



不要轻信无需抵押的贷款，特别是网上贷款公司。办理贷款可咨询银行，如有可疑可拨打110报警。

14 校园贷？债务缠身！

2017年4月12日，某大学学生周某听校友孔某讲，通过“名校贷”平台贷款15000元（根据平台规定，实际到款12000元）后交给其11000元，其有“上家”韩某能帮助其消除贷款记录。周某于4月14日按照孔某的指导，从“名校贷”平台贷款15000元（实际到款12000元），将其中11000元通过支付宝交给孔某后，周某再次登录“名校贷”平台发现不能查询到其贷款记录，周某信以为真。2017年4月18日至6月2日介绍同学郑某等6人在“名校贷”平台贷款，6人将所贷72000元中的69400元转给受害人，周某将其中56100元通过支付宝转给韩某，自己得到好处费13300元。2017年7月15日起，郑某等人



陆续收到“名校贷”平台催款电话和短信，周某再联系韩某后，对方至今不予还款，察觉被骗报警。周某、郑某等7人共损失67100元人民币。



不良校园贷往往存在费率不明、贷款门槛低、审核不严、不文明的催收手段、风险难控、易将风险转嫁给家庭、校园代理人无资质等风险问题，应加以识别，树立正确消费观和金钱观。

购物欺诈篇



15 订单“退款”让你点链接

2017年4月10日，某大学学生高某在校园接到一个自称是“打假办”的客服电话，对方称高某之前在淘宝购买的彩妆有害物超标，需要退款，并让高某在其支付宝查收退款。后对方让高某开通支付宝借呗借款平台，分2次骗取受害人共8822元人民币。



民警 提示

网购需谨慎，不要轻信自称客服的陌生号码，切勿私下交易退款；谨防泄漏个人银行卡信息；绑定手机的银行动态验证码一定不能告诉别人。

16 低价购物“藏”陷阱

2017年5月中旬，某大学张某在手机QQ软件看到一个好友空间里发的销售iphone手机的信息，6月5日14时许，张某给对方发信息说想购买一部iPhone7和一部iphone7Plus手机，对



对方称2部手机需要2046元人民币，张某将2046元打到对方银行卡后，对方又以手机是从香港发货，需要支付海关费等费用为由，要张某付款。最终共计被骗15846元。



在网购时，一定要巩固自己的心里防线，不要轻信来历不明的信息，切莫因贪小便宜而受到不法分子的诱惑，无论什么情况下都不能向陌生人透露自己的身份信息、银行卡资料。

17 机票取消请“改签”

2016年1月20日17时许，某大学学生屈某收到一条航班取消需要办理改签、退票的短信。屈某按照短信的客服电话与对方联系，客服说要收取25元的改签费



用，并赔付300元的保险金，需要手机银行和ATM机操作，屈某按照对方指示开通手机银行，将手机银行开通的验证码告诉对方，使自己的手机号与对方的银行卡绑定，并按照对方的提示在校园工商银行ATM机使用手机银行转账功能给自己的手机号所绑账户转账10345元，银行卡内的资金全部转入对方的帐户。



民警提示

联系官方客服查询自己的订票信息是否异常，如已正常出票，则无需理会诈骗信息。一旦涉及银行卡、身份证等敏感字眼，更要多加注意，切勿泄露信息。

18 设为批发商？骗你没商量

2015年11月16日上午，某大学学生刘某在淘宝网上买了一件毛衣，当晚22时30分，一名陌生女子自称客服给刘某手机打电话称：淘宝订单有误，给刘某的价格为批发



商价格，无法发货，需要给其退款，让刘某加指定QQ号码。刘某按照对方在QQ上提供的网址登陆，并按照提示填写了工商银行卡号、身份证号、网银密码后提交，对方让其输入几次验证码失败后，又让其用支付宝扫描发过来的二维码，扫描完成后，对方称会把钱退给刘某，就挂断电话。刘某网银绑定的手机两次分别收到被转走5000元和500元的短信提示，被骗5500元。



民警提示

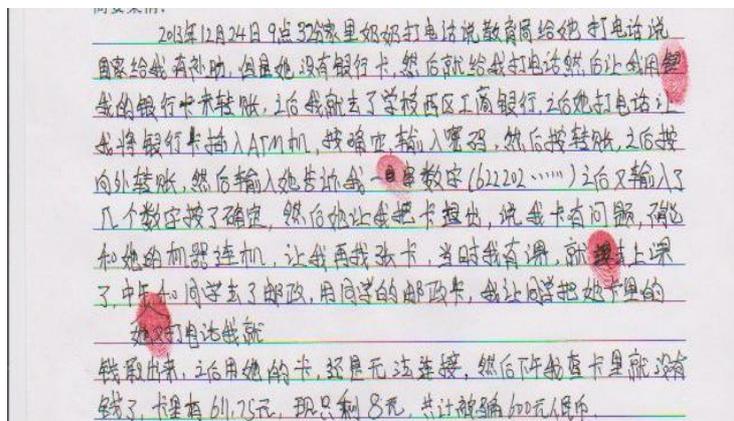
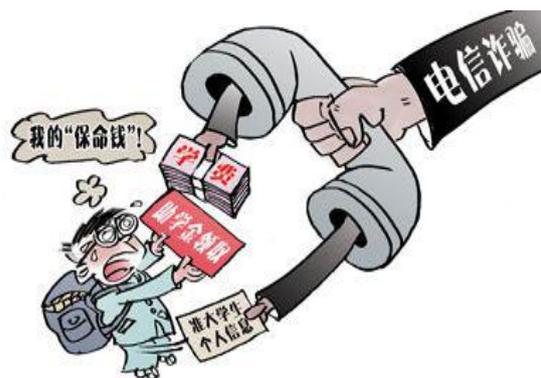
仔细甄别自称是客服的电话号码，购物时提高防范意识，不随意按他人要求操作汇款。购物出现问题时，第一时间联系官方客服咨询，通过正规途径办理。

助学补贴篇



19 借助学金骗生活费

2013年12月24日10许，某大学学生郭某在宿舍接到其奶奶在原籍打来电话讲，“国家给教育补贴，因没有银行卡让郭某接受转账”。郭某与对方联系，按照对方的提示在校内的工商银行ATM机上操作，对方将郭某银行卡中的600元人民币划走，被骗600元人民币。



民警提示

资助工作必须经学校、教育、财政部门严格审核，由学校通知并统一登记发放。如有疑问可拨打教育局或学校相关部门进行咨询和核实。

网络投资篇



20 “网上投资”高回报？

2017年3月23日，段某在微信公众号“思融财富平台”进行了会员注册，注册送18元现金，签到2次得1元，段某扫描平台支付宝二维码充值181元，账户内显示有200元可以提取，3月



29日，段某扫描平台支付宝二维码充值4000元，加上原来账户内的200元，共4200元进行投资，3月30日，段某又扫描平台支付宝二维码充值1100元进行投资，3月31日下午13时，4200元的投资到期，段某进行提现，提现不成功，4月1日1100元的投资到期，段某提现不成功，之后发现被骗，共计被骗5281元。



谨慎投资网络理财产品。如果缺乏相应投资理财能力，便无法核实对方公司资质和理财产品运营情况。只关注投资回报，对自身过度自信，就会被犯罪分子得逞。

防范电信诈骗十二句口诀

家庭情况要保密，涉及钱财需小心；

短信诈骗花样多，不予理睬准没错；

邮包违禁不要慌，欠费停机要骗你；

电信欠费要核实，来电信息需辨清；

公安法院来电紧，回拨号码查仔细；

亲属出事别轻信，骗取钱财是目的；

飞来大奖莫惊喜，让你掏钱洞无底；

天上不会掉馅饼，涉钱信息勿轻信；

陌生号码不急回，大额汇款要当心；

询问信息要警惕，卡号密码需保密；

陌生电话勿轻信，以害人又害己；

一旦难分假和真，110 咨询最放心。