大学生防盗防骗知识

安全防范是一种意识，也是一个人的生存技能，是人生的一门“必修课”。现将大学校园里常见的盗窃、网络诈骗、电信诈骗案件及防范措施列举如下，供大家参考。

一、 校园防盗

（一）校园盗窃案的行窃方式

盗窃分子在校园作案往往有以下特点：

1、疏于防范，乘虚而入

作案分子趁宿舍无人，房门抽屉未锁之机入室行窃。夏天，一些同学贪图凉快，夜晚睡觉不关房门或者最后一个离开宿舍的同学不锁门，小偷趁机入室行窃，或偷走钥匙，伺机作案。

2、混水摸鱼，就地取“财”

宿舍内发生意外情况或学院组织大型活动时，乘人不备，进行盗窃。

3、里应外合，勾结作案

利用学生对校内情况熟悉的特点作案。

4、趁其不备，顺手牵羊

作案分子趁主人不备将放在桌上、床上、走廊、阳台等处的钱物信手拈来而占为己有。

5、破坏门窗，入室行窃

作案人翻越没有牢固防范的窗户、围栏等入室行窃。

6、撬门扭锁，胆大妄为

作案分子使用各种工具撬开门锁而入室行窃。

（二）宿舍防盗措施

1、 妥善保管好现金、贵重物品，身上不带太多现金。

2、最后离开寝室的同学要反锁房门。 短时间离开也要锁门。

3、不能留宿他人。

4、对形迹可疑的陌生人要提高警惕。

5、注意保管好自己的钥匙。

二、 网络、电信诈骗及防范

1、利用伪基站群发短信，冒充移动客服，银行客服诈骗。

诱使受害人登陆虚假网站链接填写个人银行及身份信息后，盗刷银行卡的诈骗犯罪。

破解这一骗局最直接的办法就是不要点对方发来的链接，自己上移动公司官网查看。

2、免费赠品的诱惑

“恭喜你 中大奖”，“你可以获得电脑、手机等高价的商品”，但总是通知你先支付一笔不菲的“邮费”。结果是付款后，奖品就遥遥无期了。

3、信用卡信用不保

在电子邮件中保证免费办理信用卡，但是消费者提供了个人资料后，可能会因“信用”被冒用而背负巨债。

4、虚假信息诈骗

发送短信以高薪招聘、招工、刷信誉为幌子，然后要求向指定账户汇入保证金、培训、服装等费用进行诈骗。天上不会掉馅饼，如果要你先掏钱再赚钱，那么这种可定都是假的。

5、“猜猜我是谁”诈骗

以手机通话中故意让事主“猜猜我是谁”或者冒充是自己的朋友、同学、老师等套取信任，然后冒充熟人、好友谎称在外地出事或者嫖娼等被公安机关抓获，急需要用钱交纳罚款的方式诈骗事主钱财。

6、冒充好友诈骗

利用网络通讯“QQ”“微信”等即时文字、视频聊天工具，通过植入木马或者病毒事先盗取事主个人主页和视频片段，然后冒充事主本人向网络好友借钱的手段诈骗。

7、冒充淘宝、京东等购物平台商家或者客服，以退款名义诈骗犯罪。

破除这类骗局，最有效的方法是直接拨打购物网站的官方客

服电话咨询。客服电话一定要从官方网站获取，通过搜索引擎搜到的很可能还是骗子电话。

防范建议：

（1） 问他一些专业性的问题，不出三个问题就会露出马脚。

（2） 先做诚信调查，打电话到相关单位咨询。

（3） 发现上述情况，要及时报警。

8、约见网友诈骗

随着网络的发达，许多骗子开始在网络上实施诈骗行为，利用网友见面敲诈、勒索的案件时有发生。骗子通常以约见网友为名，将网友骗至事先选定的酒吧、饭店等地，点餐后找机会溜走，要网友支付高额费用，或敲诈、窃取钱财。

防范建议：

（1） 网络交友要慎重，不要轻易相信陌生人，不经过长时间的接触最好不要见面。

（2） 选择安全的上网环境，从而可以预防意外事件发生几率和保证财物安全，尤其提醒单身女性注意选择上网地点。

（3） 不要随意在网络上泄露个人资料，如：电话、住址等。

（4） 加强私密信息的保护，在将自己的私密信息告诉网友之前要慎重考虑。

（5） 如果确实要约会，约会时间不宜过晚，最好选择在白天在公共场所见面。以免给对方留有可乘之机。第一次网友见面最好与好友同去，以防万一。发现被骗要及时报警。

附一：网络诈骗典型案例

1、假冒 QQ 好友诈骗

案例：2013 年 3 月，无锡市民朱某在家中上网，其 QQ 接到在国外留学的女儿的 QQ 消息，称住处被盗，手机和银行卡均被盗，要求朱某向其同学卡上汇款，朱某事后向对方账号汇入 19 万余元，与女儿联系后发现被骗。

警方提示：1、遇到亲友在 QQ、微信等网络即时通讯工具上借钱，务必与亲友电话联系确认再转账汇款，防止上当受骗。2、养

成良好的上网习惯，防止 QQ 被盗。电脑要及时更新杀毒软件和系统升级补丁，不要接受、打开陌生人传送的文件，不要浏览色情等不良网站，防止电脑中病毒木马导致自己 QQ 被盗。3、广大网民尤其是国外留学人员要注意防止自己个人信息泄露，自己 QQ 号被盗要及时申诉取回，防止被诈骗分子利用。

2、网银升级诈骗

案例：2013 年 10 月，南京某高校学生王某收到短信，称其工行卡的电子密码器即将过期，让其登陆网址……进行升级。王某随即登陆该网站，根据提示输入自己的银行卡号、密码、电子口令等信息进行升级。10 月 15 日，王某发现卡中 2 千余元被人通过网银转账方式盗走。

警方提示：1、不要轻信手机收到的“网银升级”短信，应打电话至银行客服咨询，或去银行柜台处理。2、登陆网上银行时，一定要仔细核实是否正确的银行网站域名（银行卡上一般都有正确的银行网站域名），防止登陆到骗子设立的钓鱼网站。

3、中奖类网络诈骗

案例：2013 年 7 月，南京某高校学生崔某手机收到内容为“恭喜您被《中国好声音栏目组》抽中场外幸运观众，请登录网址……领奖”，崔某按照短信提示登录网站并与客服联系后，先后 3 次将所谓“保证金”、“税金”共计 1 万余元打入骗子账号，随后发现被骗。

警方提示：对于手机、电子邮箱、QQ、旺旺等通讯工具收到的中奖信息切不可轻信，特别是以缴纳“税金”、“保证金”等理由要求预先汇款的要求更要提高警惕，犯罪分子正是利用“天上掉馅饼”的侥幸心理设置重重圈套，实施诈骗。

4、网络购物诈骗

案例：2013 年 9 月，镇江某高校学生谈某在网上购买平板电脑，谈某通过支付宝付款后接到一陌生电话称其付款未成功，要求获取其银行卡和动态密码，谈某告知对方后，卡内 2 万余元被转走。警方提示：网上购物时，一是不要轻信明显低于市场价的购物网站； 二是货到付款时一定要仔细验证货物在付款，防止受骗；三是网购

时不要直接从银行给对方汇款，尽量使用支付宝、财付通等第三方支付平台进行担保支付；四是在登陆淘宝、拍拍等网购平台时一定要注意核实网站的域名是否正确，不要点击商家从 QQ、旺旺等即时通讯工具上发送的支付链接，以防是钓鱼网页链接；五是不要告知陌生人银行卡号和动态密码。

5、虚假购票网站诈骗

案例：2013 年 5 月，苏州某高校学生傅某报案称通过网络搜索到一个特价机票网站，在网上购买机票，与网站客服电话联系后，按其要求向对方账户汇款 3 万余元后发现被骗。

警方提示：不法分子在互联网上制作虚假订票网站，通过不法手段使得网站在搜索引擎中排名靠前，这些虚假网站上一般还有 24 小时客服电话，以超低价格吸引受害人拨打电话联系购票。一旦受害人拨打电话，骗子以种种理由要求受害人向指定账户付款，从而达到诈骗目的。警方提醒广大网民，网上购票时请注意核对网站域名真假。切勿贪图便宜，被诈骗分子建立的低价打折机票网站所骗。**6、网上兼职刷信誉诈骗**

案例：2013 年 4 月，镇江某高校学生赵某在浏览求职网站时，看到招聘“兼职刷信誉“信息（通过帮别人刷网店信誉获得佣金），于是通过 QQ 与网站客服联系。客服让赵某到正规网站购买 100 元面值的充值卡，并将充值卡密码发送过来，成功后会将本金和佣金共计 103.5 元返还到赵某银行卡上。首次交易客服即给赵某返还了成本和佣金，随后赵某多次共购买 5 万余元的充值卡，并将密码发送给对方，对方以种种理由推脱不予返还，赵某发现被骗后随即报警。

警方提示：骗子正是利用受害人“工作简单轻松，收入丰厚”的心态，设置网上兼职爱刷信誉的诈骗陷阱。面对网络兼职，网民一定要绷紧神经，对于需要提前支付所谓订金押金等涉及钱财的交易，更要提高警惕。

附二：电信诈骗典型案例

1、冒充公检法诱骗恐吓类

他喜欢冒充公安局、检察院、法院工作人员，以银行卡欠费、涉嫌洗黑钱或者账号被犯罪团伙利用为名，打电话或发短信诱骗、恐吓你将资金转汇至所谓的“安全账户”，再通过网上银行将资金迅速转移，从而实施诈骗。

2、假扮亲友熟人紧急求助类

他喜欢冒充你的单位领导、老师、战友和同学等特定身份，打电话、发短信和你联系，以“自己在外地发生车祸需花钱救人”、“嫖娼被抓需缴纳罚款”、“子女在外遭遇绑架需交钱赎人”等为名，骗取你的信任，“请求”你通过银行转账汇款，从而实施诈骗。**3、发布贷款等虚假消息骗取费用类**

他会以“提供无担保、低吸贷款”为诱饵，发布虚假信息，并留下联系电话号码。一旦你回复电话，他就会说要贷款需先交部分利息；待你将钱款汇入其指定账户以后，他还会要求你缴纳“还款保证金”等费用，骗取钱财。

4、刷卡异常诱骗转账类

他会用手机群发短信，称你在商场刷卡消费若干，若有疑问建议你咨询所谓“银联中心”，并留下电话号码。你一旦回复电话，他又会说你的银行卡可能被刷盗，然后提供所谓的“XX 市公安局”报警电话。你拨打他提供的电话号码“报警”后，“XX 市公安局民警”会以“保护当事人账户”为由，要求你到 ATM 机上把银行卡上的存款转至他指定的“安全账户”上，从而轻易转走你的钱财。

5、恐吓诈骗类

他常常冒充黑社会或自称“彪子”、“强哥”，让你回忆是否在某年某月某地得罪某个人，这个人要“卸”你的胳膊和大腿，或伤害你的家人，让你心神不宁。随后，他会声称，要不然你就拿多少万元来破财免灾，让你几天内汇款到账户。

以上内容请同学们认真阅读，提高防范意识，谨防受骗上当。