安医大金融知识进校园

开学季到来 了 ，骗子们也带着“诈骗套餐”走进 了校园，以下是**几种常见的骗术：**

一、打着学校名义的短信

开学季 ，你可能会收到各种 以学校 7 名义发送 的短信，内容如“查看分班情 况”、“查看课程表”、“缴纳学杂费”、“办理入学手续”等，并附带不明链接，不少同学看到是学校发送 的就不假思索地打开了，遭受了损失后才发现是骗子发来的诈骗短信。

防骗提醒：利用伪基站发送钓鱼短信是骗子们的常用套路，还是那句话，不明链接接千万别点，更不要填写个人账户信息 和短信验证码。在各种短信狂轰乱炸的时代，要注意对信息的真实性加以判断哦！

二、山寨学“大学新生群”

面对即将到来的大学生活 ，加入“新生群 吐行信息交流成为不少新 生的首选。一些骗子建 了所谓的“大学新生群”来吸引新生加入，实则是为了 在群里发兼职广告赚取提成甚至是 或以学长、学姐名义骗取钱财。

防骗提醒：有人邀请你加入大学生群聊的时候，要注意分辨真伪，尤其是涉及到钱款的时候。最好是只加入通过学校、辅导员或者是学校的团委、学生处等推荐的群聊。

三、找上门的“老师”

“小王，我是你的老师，我现在遇 到点困难，急需用钱，能麻烦你把钱 打到这个账号吗？”一些学生因未步入 社会，辨别能力不高 ，骗子利用这一 点，冒充高校老师，以遇到困难为借 口，要求学生给自己汇款。

防骗提醒：老师向学生借钱的可能性少之又 少。遇到这种找上门的“老师”或辅导员，首先应向求助老师拨打电话进行核实真假 ，切不可在未经亲 自核实的情况下给对方转款。

四、主动联系的“助学金”

骗子在开学各种助学奖补申请发放 的高峰期，骗子锁定一些家境 困难的考生作为目标 ，冒充成教育局工作人员，谎称考生可领取助学补贴，但需先交纳一定费用。随后诱导考生或家长去 ATM 机操作，将资金转到骗子掌握的银行账户。

防骗提醒：学校的资助项目一般不会要求学生 预先交纳任何费用。一旦接到此类电话，应提高警惕 ，先与老师、学校核实是否有这类消息及流程，以证实真伪，更不要泄露自己的相关信息。

五、不怀好意的校园货

骗子以办理校园货需要先缴纳保险金为由，诱骗学生多次向其转账汇款；又或者让一些想要购买高档手机的大学生，提供自己的个人信息在网货平台进行贷款，承诺所有贷款不用大学生偿还，事后还会给大学生一定金额的现金作为好处费。然而一但贷款成功，骗子会将手机变现 ，卷款消失，造成被骗学生无故背债。

防骗提醒：天上不会掉馅饼 ！不轻信开学季网上、短信、小广告等发布的贷款信 息；不随意泄露个人信息；切忌使用虚假“不良校园货”平台。

六、高回报的“兼职工作”

兼职详骗己成为一种典型常见的网络诈骗类型 。骗子抓住一些学生想找份兼职工作的心理，骗子传播虚假广告招聘兼职以工作轻松、高新刚回报为谓情，骗取学生所谓的押金或保证金等。

防骗提醒：看到高回报的兼职工作要提高警 憾。般应通过学校正规的中介平 台，或者有资历的大公司，寻找适合 自己的工作。

大学生必知的安全指南：

1、终极防骗提醒：任何来路不明的转账、汇款要求，请直接拒绝！并立即报警！

2、对付四大套路终极大招：上述电信诈骗，万骗不离其宗，所有铺垫最终都为“让你转账”面对骗子的套路要做到：不贪、不信、不怕、不转账！

3、随时牢记三个不会：公安局、检察院和法 院绝则不会使用打电话的方式开展案件侦查工作，通知你涉嫌犯罪、洗黑钱、贩毒等，也不会通过网络或传真给你下达“法院传票”等法律手续；司法机关等执法部门 绝耐不会打电话要求群众转 账汇款；司法机关绝则不会设 立所谓的 “国家安全账户”。

在大数据时代，尽快织成一张保护个人信息的安全网，才能让信息泄露不再是人们心头的一块硬伤！

• 电信诈骗花样多多，这也许 都曾发生在你、我身边！要 想真正减少诈骗，就得从源 头入手，此我们自身做起...
• 与其纠结魔高一丈，还是道 高一尺，不如借前车之覆为后车之鉴，提高自身防范意识，全面“免疫”！

公安部“反电信网络诈骗宣传”活动正式启 动

防范电信诈骗是全社会共同的责任，2016 年 6 月由公安部刑侦局与腾讯公司联合举办“反电信网络诈骗宣传月”活动，发出“全民防骗、要你出手”的号召–就是要通过揭示诈骗手法，以更加“吸引眼球”的方式提高社会关注度，全国高校陆续开学... 防诈骗成为不少学校为新生准备切实提高公众反诈骗意识的开学第一课。

如何给自己的信息穿上保护衣？

1、防止网络钓鱼和木马：不点击不明链接；不扫描不明二维码；不随意连接公共场合不明 WiFi；不随意安装来路不明的软件；到正规网站购物；开启设备防护功能，定期查杀病毒
2、防止撞库攻击：设置较高强度密码；不同网站设置不同密码
3、不在网络说太多：不在社交网站公布个人信息；不在社交网络发布个人出行信息；不随便参加注册信息获赠品的网络活动或调查
4、形成信息保护意识：丢弃快递单、账单或交通票据前先清除个人信息部分；使用公共网络时，不留下使用痕迹保护好身份证等有个人信息的证件

在移动网络时代，随着信息存储与抓取技术的进步，人们的购物、出行、消费记录等“痕迹”被完整保留在网络上，这就容易被别有用心的人利用而导致隐私泄露...

1、被小看身份证复印件：复印件不用的或作废的要处理好，不能随意丢弃，复印件上要标明用途。
2、撕碎、涂黑+保管：快递收货单等无用的单据可以直接碎掉，或将姓名，电话，地址等个人信息涂黑再丢弃，有用的单最妥善保存切勿乱乱放!
3、使用公共电腑公共网络要谨慎：在不安全的公共网络环境里不处理个人数感
信息，不使用 U 盘等存被交互个人信息。

日常生活多留意以防信息被盗取：你的日常行为会不经意“出卖”自己，这些个人信息一旦被泄露，可能就会被诈骗分子盯上并造成严重损失...

1、聊天晒照要谨慎：在公共社交平台上现尽可能避免透露或标注真实身份信息，朋友圈，微博晒照片，一定要谨慎

2、少注册多改密码: 不在不正规或不可靠的网站，APP 上注册真实姓名等信息,定期修改常用软件的密码。

3、不该填的不填：一般情况下，填写简历、登记、调查等要先

核实对方或网站的身份和资质，只提供必要的信息不要过于洋细填写本人具体信息。

信息安全无小事，用户必须增强信息保护意识：四大常用网站密码要“单设”

1、支付账号、社交账号、常用邮箱、网络购物这些重要网站--要单独设置密码

2、每隔三个月就要对密码进行一次修改，防止黑客撞库，造成多个网站个人信息连环失窃

工银融 e 联——让电信诈骗统统退散！

对诈骗短信说“不”。用工银融 e 联接收余额变动提醒，安全、免费、真实、可靠

工行利用大数据成功截堵 16 亿电信诈骗

用户只需通过手机下载并登录工行的“融 e 联”APP，即可在“发现”栏目中找到“融安 e 信”，并免费使用该软件，在办理转账汇款前对收款账号进行安全性查询.....

客户通过工行汇款，如收款账号与外部欺诈风险信息系统内电信诈骗风险账号匹配，自动预警提示

遭遇电信诈骗后，你该怎么做？

2016 年 3 月 3 日起，公安部依托“电信诈骗案件侦办平台”，实现对全国电信诈骗涉案账户的快速接警、止付、拦截通道，可最大限度的减少和挽回了群众损失.....

请牢记：

当发现遭受电信诈骗后，请保存好汇款或转账时的凭证并立即拨打 110 报警，或到当地公安机关刑警队、派出所报案，说清被骗经过，准确提供转出现金的账号和骗子的账号，公安部侦刑局实行破案账户快速接警止付，最大限度挽回损失。

微信公众号“反欺诈部落”寓教于乐

“今日说案”

发布“今日工银说案”系列内容：

1. 诈骗团伙运作模式简介
2. 各类常见诈骗手法介绍
3. 我行安全产品介绍
4. 良好的电子银行使用习惯
5. 如何进行风险防范
6. 事后应对措施
7. “骗子日常”

案例解析
生动易懂
寓教于乐
“防骗考试”
安全问题小测试
互动娱乐性
拓宽教育渠道
“欢迎勾搭”
虚拟小编形象
个性化烙印
增加亲和力
提高互动性

现在诈骗电话升级换代速度极快，如果我们不及时补补课、升级防骗知识，了解诈骗的最新手段，难保下一个受骗的就不是自己！打击电信诈骗是个漫长的过程，铲除毒瘤不是一朝一夕，因不法分子在只争朝夕，正在暗精套路与技能，作为一个普通老百姓，保护好个人信息一定要从你、从我做起！--让我们携起手来，共同防范电信诈骗！