

网络诈骗

【校园防骗指南】

在我们展望美好校园生活的时候，总有不法分子蠢蠢欲动，利用各种名义进行诈骗。面对即将到来的校园生活，管家侠教你练就火眼金睛，分分钟识破骗局！



演讲人：小熊猫



时间：2021.X.X



目录

CONTENT



1

诈骗电话

ADD YOUR ENGLISH TITLE

2

钓鱼网站

ADD YOUR ENGLISH TITLE

3

校园贷款

ADD YOUR ENGLISH TITLE





第一章

诈骗电话

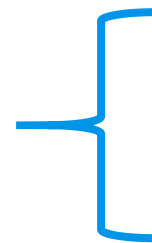
请在此处输入您的文字，请在此处输入您的文字



诈骗电话



诈骗电话要小心
警惕卡号和密码



- 套取现金
- 控制受害人

- 在非正规经销商处购买电话卡，可能会接到诈骗电话或垃圾短信。
- 有的以资助新同学学费、生活费为由有的自称是教育部或校方，以返还学费等为名骗取学生的银行卡卡号和密码，致使银行卡被盗刷



诈骗电话

各种诈骗招数

- 猜猜我是谁——感情套诱——假冒冒充——要钱诈骗——兼职诱饵——情色骗术——恐吓电话——新生入学——假助学金诱饵——恐吓+心理骗术——过于热情的“帮助”





诈骗电话

开学必备：要当心，正规渠道要当心

- 不法分子利用新生急于了解新学期信息，伪造“开学必备”文档例如“开学表格”、“开学需打印”等文件，放在论坛、网盘等地方诱使学生下载。
- 一旦这些文件运行，就会潜伏在电脑中，暗中窃取隐私信息、账号密码，更有甚者还会盗取用户银行财产，造成严重损失。民警提醒：在学校官网、教务处网站等正规渠道下载开学相关资料，不要轻信不知名的网站或个人上传到论坛、网盘等地方的文件。



第一章

钓鱼网站

请在此处输入您的文字，请在此处输入您的文字



钓鱼网站

贪小“便宜” 留心被“钓鱼”

在开学季期间，有些钓鱼网站将假链接附在邮件、或以弹窗等形式，通过“促销”，“购物卡”等话题吸引眼球，诱导用户访问仿冒的钓鱼欺诈网站，而且仿真度极高，一般用户很难辨别真伪

民

警

提

醒

在浏览网购网站，网商等购物信息时，注意核对信息链接，仔细确认网址信息，提高对钓鱼网站的警觉、避免上当。





钓鱼网站

- 钓鱼网站通常指伪装成银行及电子商务，窃取用户提交的银行帐号、密码等私密信息的网站，可用电脑管家进行查杀。
- “钓鱼”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的URL地址以及页面内容，或利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的HTML代码，以此来骗取用户银行或信用卡账号、密码等私人资料。





钓鱼网站

- 最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。这些个人信息对黑客们具有非常大的吸引力，因为这些信息使得他们可以假冒受害者进行欺诈性金融交易

- 从而获得经济利益。受害者经常遭受显著的经济损失或全部个人信息被窃取并用于犯罪的目的。的钓鱼网站有时，还会危害您的电脑，让您的电脑文件丢失，本电脑的文件转移到他的电脑上是一种最新骗术！



钓鱼网站

绿色软件藏木马，安全软件帮防护

在开学后，很多学生会下载专业相关软件，或辅导类应用帮助学习。不法分子将正常的软件或应用重新打包，加上恶意代码，以“绿色版”、“破解版”等名义进行发布。一旦大意，下载安装了此类程序，恶意代码会篡改浏览器首页、乱弹广告，更有甚者会安装后门木马，从而使电脑任不法分子摆布。民警提醒：在正规、官方的软件网站上下载软件。下载安装腾讯电脑管家，并保持时刻运行，全面保护您的电脑。

要在正规、官方的软件网站上下载！！！！





第一章

校园贷款

请在此处输入您的文字，请在此处输入您的文字



校园贷款



19名大学生陷校园贷骗局，涉及金额达70万

- 河南郑州某学院的一名在校大学生因无力偿还共计60万的各种网络贷款，最终跳楼自杀。近日，又曝出福建大四学生余某飞，自创青鸟创联的金融服务公司骗取同学身份信息，在8家网贷平台上贷款。目前已涉及19名学生，总金额70余万元。
- 之后，余某按时还款的承诺无法兑现，导致这些学生不断接到催款通知，他们的学习生活受到严重影响。



校园贷款

假冒公检法诈骗

- 犯罪分子假冒“警官”“检察官”“法官”等角色，谎称受害人涉嫌洗钱、贩毒等严重犯罪，诱导受害人将资金转入实为骗子持有的所谓“安全账户”，此类诈骗造成的损失金额最大。

提示

- 警方不会通过电话做笔录，逮捕证由警方在逮捕现场出示，不会通过传真发放，更不会在网上查到。公检法机关从未设立所谓的“安全账户”，更不会通过电话安排当事人转账汇款到“安全账户”





校园贷款



冒充熟人诈骗

- 犯罪分子通过非法渠道，获得受害人熟悉的亲友的手机号码、社交账号密码，并掌握受害人的社会关系，从而骗取受害人信任，进而编造“发生意外急需钱”“资金周转”“代缴话费”等理由，诱使受害人转账。
- 凡是亲友间涉及借款、汇款等问题
- 一定要通过拨打对方常用号码，或者视频聊天等方式核实对方身份后再作决定。



校园贷款

利用伪基站发送木马链接实施诈骗

- 犯罪分子使用“伪基站”，冒用银行、运营商等客服电话号码发送短信给受害人，以账户积分兑换奖品等为由诱导受害人点击短信中的木马链接。用户一旦点击，犯罪分子就能在后台获取用户的银行账户信息和密码，进而盗取其账户资金。
- 当收到“银行卡密码升级”“积分兑换”“中奖”等含有链接的短信时，要通过银行、运营商的官方网站或客服电话进行核实，不要轻易点击短信中的链接。





校园贷款



利用“先垫付”兼职诈骗

- 犯罪分子许诺在各种网络平台刷得消费记录后，将返还本金并支付佣金。受害人在完成前几单任务后都会很快收到回报，而当做更多的任务时，骗子就会切断与受害人的联系，就此消失。求职者不要轻信网络上“高佣金”“先垫付”等兼职工作，不要轻信没有留固定电话和办公地址的招聘广告。
- 犯罪分子通过非法手段获得考生信息，并有针对性地发送短信或邮件，声称“提供考题”“改分”“办假证”等，引诱考生汇款。漏题、改分、改档案、伪造资格证等行为本身就是非法的，请坚持用自己的实力说话。



校园贷款

1. 用“免抵押、低利息”为诱饵诱导学生贷款，并要求缴纳贷款手续费、管理费、保证金等费用；
2. 声称能通过培训提高综合技能，夸大培训效果，签订培训合同，诱导学生贷款支付学费；
3. 与兼职诈骗结合，要求学生贷款购买手机等产品做“销售代理”。这些贷款的利息和滞纳金很高，学生如不能如期还款，将迅速背上难以承受的债务压力。

校园贷诈骗

- 学生在申请借款或分期购物时，要衡量自己是否具备还款能力。对于关乎自身信息、财产安全的事，要多方求证，不要轻易相信他人的一面之词轻易透露个人信息，甚至将身份证借与他人使用。发现危险，及时报警。校园贷诈骗的形式主要有三种：



校园贷款

编造“资产解冻”诈骗

- 犯罪分子先编造一个民族资产秘密流落海外的故事，然后声称受国家委托对这些海外资产进行解冻，号召受害人缴纳手续费或资料费，称成功后每人可以拿到高额善款补助。
- 除了“民族资产解冻”，犯罪分子还会编造所谓“养老”“扶贫”等噱头来吸引投资实施诈骗。此类诈骗的受害人多为中老年人，他们远离社会舆论，缺乏辨别诈骗的能力，年轻人要多关爱长辈，及时传达安全防范知识。此外，留意父母长辈的网络支付使用情况，保障财产安全，及时止损。





校园贷款



投资返利诈骗

- 此类骗局通常标榜具有海外背景，从事的行业能赚取巨额利润，投资者将会获得高额投资回报。投资初期，犯罪分子会按时返利，让投资者尝到甜头，继续追加投资后，将会血本无归。
- 投资理财前要对所投资的项目进行了解多咨询评估，做到深思熟虑谨慎对待。特别要警惕网络上各类标榜“低投入、高收益、无风险”的投资理财项目，切勿盲目追求高息回报谨防被骗。



校园贷款

保健品购物诈骗

- 犯罪团伙假扮医疗机构的顾问、专家、教授等，以为老年人“问诊”为名夸大病情，再以会员登记、免费体验、国家补贴、中奖等噱头诱骗客户购买各类保健品。
- 而这些“保健品”基本上都粗制滥造，成本低廉却以高价出售。经常给家中老人说一些老人被诈骗的例子，让他们不要相信保健品推销，一旦发现受骗要立即报警。





校园贷款



引诱裸聊敲诈勒索

- 犯罪分子非法获得被害人信息后，通过社交软件建立联系，步步引诱受害人进行“裸聊”，从而获取受害人不雅照片、视频，以此敲诈受害人。
- 应远离网络不良行为，不向陌生人透露身份和家庭等敏感信息。

版权声明

感谢您下载平台上提供的PPT作品，为了您和熊猫办公以及原创作者的利益，请勿复制、传播、销售，否则将承担法律责任！熊猫办公将对作品进行维权，按照传播下载次数进行十倍的索取赔偿！

1. 在熊猫办公出售的PPT模板是免版税类（RF：Royalty-Free）正版受《中华人民共和国著作权法》和《世界版权公约》的保护，作品的所有权、版权和著作权归熊猫办公所有，您下载的是PPT模板素材的使用权。
2. 不得将熊猫办公的PPT模板、PPT素材，本身用于再出售，或者出租、出借、转让、分销、发布或者作为礼物供他人使用，不得转授权、出卖、转让本协议或者本协议中的权利。

更多精品PPT模板：<http://www.tukuppt.com/ppt/>

[点击进入](#)

网络诈骗

【校园防骗指南】

在我们展望美好校园生活的时候，总有不法分子蠢蠢欲动，利用各种名义进行诈骗。面对即将到来的校园生活，管家侠教你练就火眼金睛，分分钟识破骗局！



演讲人：小熊猫



时间：2021.X.X

