**大学生 别再“中招”！**

**教你如何反诈防骗！**

**如何开启境外来电拦截功能**

当前，电信网络诈骗案件持续高发，我校部分学生频繁接到境外人员冒充公检法机关、疫情流调人员的诈骗电话。为从根源上铲除电信网络诈骗滋生土壤，切实保障学生财产安全，小编总结了开启拦截功能、关闭三大运营商境外来电具体操作方法：

**1中国移动用户**

通过短信发送“KTFSR”到10086免费开通。再关注微信公众号“中国移动高频骚扰电话防护”，开启国际号段拦截功能。

**2中国联通用户**

关注微信公众号“中国联通微厅”。点击办理、选择智慧沃服务，找到页面内的防骚扰拦截，点击免费订购。订购完成后，关注微信公众号“智慧沃服务”，在号段拦截功能内开启国际电话拦截功能。

**3中国电信用户**

关注微信公众号“天翼防骚扰”。点击业务设置，选择智能拦截设置，开启国际长途电话、诈骗电话拦截功能。

据公安部网站消息，当前，学生群体已经成为全民反诈新格局中不可忽视的“角落”。

**让学生群体屡屡“中招”的诈骗类型**

网络贷款、刷单返利、“杀猪盘”、冒充电商物流客服、冒充熟人或领导、冒充“公检法”、虚假投资理财、虚假购物、注销“校园贷”、网络游戏虚假交易等电信网络诈骗类型中均有学生被骗的案例出现，学生群体成为遭受诈骗的“重灾区”。针对在校生遭遇电信网络诈骗案例频出的现象，警方总结了学生群体受骗的五类高发类型，提醒广大学生加强防范。

**01类型一：刷单返利诈骗**

案件回放：

5月18日，云南省昆明市嵩明县公安局反诈骗中心民警接到咨询电话，来电者是在校大学生刘同学。经了解得知，近期，刘同学加入了一个大学生兼职群，群主组织学生们通过兼职刷单来赚取“零花钱”。刚开始刷的几单均顺利完成任务并获取了小额佣金，尝到甜头后，刘同学对此刷单平台深信不疑，并准备“大干一场”。由于囊中羞涩无法承受“大单”的任务费用，刘同学只得去找父母借钱，母亲听到她的描述后，告诉她可能是诈骗。不相信事实的刘同学在母亲的再三要求下，拨打了当地反诈中心的电话咨询。

民警了解此情况后，立刻意识到这是一起典型的网络刷单诈骗，马上制止了刘同学在刷单平台上的操作行为，并对其进行了反诈骗宣传教育。最后，成功帮助刘同学挽回损失1.6万余元。

**手段揭秘：**

骗子发布网购刷单兼职信息，承诺在交易后立即返还购物费并额外提成。刷第一单时，骗子会小额返利。刷单交易额变大后，骗子就会以各种理由拒不返款。

**02类型二：冒充电商物流 客服诈骗**

案件回放：

8月5日，家住浙江省台州市的高中生张同学在微信上加了一个好友，对方自称是物流客服，因将张同学买的连衣裙在派件的过程中丢失了，愿意三倍赔款给张同学。对方借口要走公司转账流程，让张同学下载App，按照指示开通借贷功能，将借贷到的3000多元钱转到对方提供的一个账号内。对方继续要求她借款，张同学感觉到不对劲儿就“刹住车”，共被骗3050元。

**手段揭秘：**

骗子冒充电商、物流客服人员打来电话，能够准确说出你的购物信息和个人信息，骗取信任。接着，他们就以网购平台系统升级造成订单丢失、商品存在质量问题需召回等原因，说可以退款，诱骗你下载网贷App或登录钓鱼网站，骗取或盗取资金。

**03类型三：注销“校园贷” 诈骗**

案件回放：

7月12日，刚从高校毕业不久的小张接到自称是“国家校园贷客服”的来电，称“应国家要求”，其在校期间申请的助学贷款的还款利率已上调，要求小张补足未偿还的利息，若逾期未偿还就会“影响个人征信”。

由于小张确实在学校办理过助学贷款，而且还处于还款阶段，对方来电又能准确报出她的个人信息，小张便信以为真。随后，小张按“客服”要求，下载了某屏幕共享软件，对方称需要“查看小张支付宝的芝麻信用分”，以便了解其还款能力。接着，对方又让小张将“借呗”里的借款额度“走个流水”，以验证其资金账户，验证完成后会将钱款原路返还给小张。

于是，小张向对方账户转账1.7万元。转账后，“客服”马上断线失联，小张才发现自己被骗并报警。

**手段揭秘：**

骗子冒充网贷平台工作人员，称你之前开通过校园贷、助学贷等，需要消除校园贷不良记录，或不注销会影响个人征信，诱骗你在正规网贷网站或互联网金融App贷款后，骗取钱财。

**04类型四：网络游戏产品 虚假交易诈骗**

案件回放：

某高校学生何同学将自己的游戏账号挂在网上出售，一位网名叫“怀念”的人与何同学取得联系，表示要购买何同学的账号。对方要求何同学通过某游戏交易平台进行交易。何同学感觉那个网站比较正规便同意了。随后，对方给何同学发来一张“支付成功”的截图。可当何同学提现时，却显示账号被冻结。何同学随即联系平台客服，客服以绑定银行卡号有误、提现金额不合规、提现操作违规等借口，要求何同学转账8500元至指定账户，才能完成解冻并将余额提现。何同学转账之后，平台客服就失去了联系并屏蔽了何同学，联系何同学购买游戏账号的网友也已将何同学拉黑。这时，何同学意识到不对劲，才发现该游戏交易平台是伪造的虚假平台，随即报警求助。

**手段揭秘：**

骗子在社交平台推广充值游戏币、游戏点卡优惠出售或优惠购买的广告，诱导受害人先付款，制作各种虚假的游戏界面和充值界面截图，发送截图给受害人获取信任，对其实施诈骗。

骗子在网上发布买卖游戏装备、游戏账号的广告信息，诱导你在虚假游戏交易平台进行交易，通过钓鱼网站窃取你的账号和密码，让你以“注册费、押金、解冻费”等名义支付各种费用，并盗取账号。

骗子以出售游戏外挂、游戏代练、解除游戏账号冻结、解除游戏防沉迷限制等为由，诱骗受害人汇款实施诈骗。

游戏消费要量力而行，不要轻信“低价充值”和“高价收购”，不要在非官方网站上进行游戏账号交易。

**05类型五：冒充熟人诈骗**

案件回放：

某高校学生小张突然收到好友通过QQ发来的信息：“遇到点急事，能不能帮帮忙，借我800元钱。”小张心想朋友一定是遇到难事了，不然不会这么着急地向他借钱，随即转账了800元。半小时后，“好友”说自己出了车祸，人正在医院抢救，需要1000元救命钱。小张再次不假思索地给“好友”转了钱。“好友”收到钱后连声道谢，并承诺第二天就会还钱。可到了次日，发现对方已将自己拉黑了。小张觉得不对头，立即拨通好友电话询问此事，才发现，原来前一天好友的QQ被人盗了，那个借钱的人是个“冒牌货”。

**手段揭秘：**

骗子利用QQ或者微信冒充亲人、同学、朋友与你联系，称遇到紧急情况要借钱，一定通过电话或视频通话等方式向当事人核实。

**五大对策，教你如何反诈防骗！**

大数据、人工智能、网络直播等移动通信和互联网新技术的更新迭代是电信网络诈骗犯罪案件高发的客观背景，但除此之外还有许多其他原因。

结合审判实践，我们总结出电信网络诈骗犯罪案件高发的原因，主要有六个方面：

**1.**大量个人信息遭泄露、甚至被买卖，成为犯罪分子筛选潜在行骗对象的重要手段；

**2.**部分地方的工商登记机关、银行机构对申请注册公司、开立银行账户行为把关不严；

**3**.行政监管、行政处罚缺位，导致部分一般违法行为发展为犯罪；

**4**.互联网技术的发达同时导致电信网络诈骗行为查处、打击困难；

**5**.犯罪分子依靠技术手段，具有较强的反侦查能力；

**6**.被害人因自身贪念、心理承受能力差、识别能力差等弱点，易陷入犯罪分子精心设计好的圈套。

结合以上犯罪特点和原因，反诈民警总结出以下防范电信网络诈骗犯罪的对策及建议，一起来看看这份“反诈宝典”吧！

**1、妥善保管个人信息**

个人信息泄露、贩卖等现象突出已成为诈骗犯罪黑色产业链的重要组成部分。由于许多电信网络诈骗方式都以获取被害人隐私信息为先决条件和必经步骤，因此，广大人民群众把好个人信息保护的第一道关口，从源头杜绝隐私外泄对于避免财产损失至关重要。

**应对方法**

**①要保护好个人身份信息。**在非必要情况下，不向陌生人提供身份证号码、工作单位、家庭住址、职务等重要信息。不将身份证照片或号码保存在手机中。

**②要保管好个人账户信息。**在相关网站输入账号、手机号码、查询支付密码等重要信息前要谨慎核实域名真实性，不点击可疑链接，不连接来历不明的无线网络，不扫描非正规渠道获取的二维码，谨防钓鱼陷阱。

**2、绝不出租出售“两卡”**

千万不要认为没有直接参与诈骗行为就不算犯罪。在明知他人利用信息网络实施诈骗行为的情况下，仍出售银行卡、手机卡，为他人提供便利，就涉嫌构成违法犯罪，情节严重将被追究刑事责任。

**应对方法**

广大群众要保持警惕，不轻信他人，不贪图小利，绝不出售、转让、出租、分租、出借或者购买银行卡、支付账户（微信、支付宝等），以免给不法分子提供“作案工具”。否则，5年内将会被暂停银行账户非柜面业务、支付账户所有业务，还会在个人征信上留下污点，影响贷款办理等业务。

若发现出售、出租、出借电话卡、银行卡等犯罪行为，要及时向公安机关举报。

**3、加强账户安全管理**

一些电信网络诈骗案件反映出部分群众银行账户管理存在明显漏洞，因此，提高银行账户安全性，给自己的账户上好“锁”，是风险防范的关键一环。

**应对方法**

**①**为银行卡、网上银行、手机银行设置复杂程度较高的密码；

**②**不在其他任何网站上设置与网上银行、手机银行等相同的用户名和密码；

**③**不向任何人透露或转发短信验证码及其他形式的动态密码。

此外，为防范电信网络诈骗，人民银行、银监会等金融监管机构近期印发了一系列文件，要求同一个人在同一家银行只能开立一个Ⅰ类户，开立多个Ⅰ类户的，需进行清理；暂停涉案账户开户人名下所有账户的业务，经公安机关认定的用于开展电信网络新型违法犯罪的涉案账户，要中止业务往来等。

上述规定从银行支付端设置防线，群众应积极配合银行执行相关规定，保障自身财产安全权益免受侵害。

**4、提高金融安全意识**

被害人金融知识不足或风险意识薄弱是多数电信网络诈骗最终得逞的直接原因，因此，提高对金融产品和服务的认知能力及自我保护能力，是群众防骗避损的核心应对之策。

特别是近年来电信网络诈骗的被害人群更加广泛，逐渐从老年人、受教育程度较低群体向中青年、高学历、高收入人士蔓延，加强金融知识学习已成为每一位群众的必修课。

**应对方法**

**①**群众应密切关注媒体报道和网络曝光的诈骗案件，了解近期出现的作案手法，并提醒家人亲友提高警惕。

**②**对电信运营商通过短信推送的安全提示信息，以及公安机关通过网站、公众号不定期发布的风险防范要点，应认真研读并牢记。

另外，银行利用各渠道开展的金融知识宣教活动系统性、针对性强，对资金安全保护大有裨益，群众应当予以关注。

**5、培养良好支付习惯**

电信网络诈骗尽管无孔不入且真假难辨，但只要群众时刻保持警惕，养成良好支付习惯，把控住对外转账汇款的最后一道关口，仍可有效避免资金损失。

**应对方法**

**①**接到熟人通过短信、微信、微博、QQ、邮件、语音等形式发送的转账请求，或询问银行卡、网银密码等重要信息时，要通过电话核实确认；

**②**陌生人或长期失联的“熟人”要求汇款时，须保持谨慎多方求证，遇到可疑情况及时向公安机关、银行、电信运营商等机构咨询；

**③**如确需向对方转账，应尽量选择次日到账方式并于事后再次核实，如有异常及时申请撤销；

**④**具有移动支付习惯的消费者应选择安全性较高的支付产品，并下载安装正版应用软件；

**⑤**避免在与移动支付软件绑定的银行卡中存放过多资金以便分散和锁定风险。

来源： 辽宁工业大学 国家反诈中心