预防电信诈骗校园安全教育讲座

亲爱的同学们老师们，大家好，我是止马营派出所的杨警官，很荣幸能够在今天这个中小学安全教育日给大家进行一次安全教育。我今天要讲的主题是如何预防电信诈骗。什么是电信诈骗呢?电信诈骗是指犯罪分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人给犯罪分子打款或转账的犯罪行为。说白了，就是犯罪分子通过各种电话或各种网络工具冒充各种角色编造各种理由骗你，骗的是什么，不是感情，是钱，骗子给你谈感情的时候，就是想骗你的钱。诈骗前面放上“电信”二字，也就说明了电信诈骗的最大特点，就是“你见不到骗你的人”，但他却伤你最深”。

同学们，虽然你们现在还在校园读书，但电信诈骗离在座的真的不远。同学们可能看到这样一条非常令人心酸的新闻:2016 年 8 月，一个即将踏入大学的女生徐玉玉，接到一通诈骗电话，将上大学的费用 9900 元寄给骗子。知道真相后，她伤心欲绝，最终抑郁身亡。现在大家几乎都有手机,有 QQ 和微信，都接到过垃圾短信和邮件，都在浏览网页的时候遇到过各种弹窗广告,刚才我说的这些都能用作电信诈骗的工具，在这个时代，你离不开网络，自然也就躲不开电信诈骗。所以我们每个人都要知道一些防范电信诈骗的常识和原则，了解一些电信诈骗的手段，让自己和自己的亲朋好友在遭遇电信诈骗时能马上识破。我现在给大家介绍几种电信诈骗的类型，一起分析下骗子都会用什么手段让我们相信，让我们被骗。

1.冒充公检法等国家机关诈骗

这是一个真实的案子，受害人高某向公安机关报案称:接到自称是工商银行的工作人员的电话，有一张在海办理的信用卡透支 1 万多，需要高某把这个钱补上。高某称这个卡她没有办理过，钱也不是其花的。这个邮政银行工作人员说让上海某街的公安分局帮她查一下怎么回事，之后就把电话转接到一个自称公安工作人员的人，自称公安工作人员的人说这个卡涉嫌贩毒案，犯罪嫌疑人已经交代往这张信用卡上转了 270 多万元，还有还很多人指证说受害人也是犯罪团伙，需要高某把其银行卡都提供给公安局配合，冻结其银行卡，查清楚后再解冻。之后，高某电话又转接到一个自称是检察院的工作人员的电话，这个自称是检察院工作人员的人要高某在晚上 6 点之前必须把这个冻结银行卡的过程操作完，不然就进行大规模批捕。随后，高某到了工商银行 ATM 机按照对方说的进行操作，在操作之后发现自己一张银行卡内 40000 多元现金不见了，另一张卡内也少了 5 万元钱。

这个案例中出现几个单位，银行、公安、检察院，还有一些专业术语， 什么涉嫌双毒、批捕、解冻，不了解这些人听到后基本都会蒙圈。我管这种诈骗叫做“我是一个演员”， 每名犯罪分子都有自己的角色和台词，台词会根据你的反应设置各种回答，总之就是让你被骗。大家记住一点， 司法机关查办案件要不就是直接找你本人，要不就是让你来司法机关，而且司法机关任何执法活动都是需要当事人签字的，是不可能通过电话或网络直接完成的。

遇到陌生人打来电话时，一定要冷静、沉稳、思考，特别是涉及钱款转账时，要立即停止，把好最后一道防范关口。还有就是司法机关的款项往来都是走对公账户，不可能叫你将钱汇入私人账户。如果有人打着公检法的名义，要求你将钱汇入私人账户，百分之百是诈骗。

2.中奖诈骗

“恭喜您获得xx公司十周年庆典抽奖活动一等奖”收到这种短信一定要提高警惕。不法分子以短信、网络、刮刮卡、电话等方式发送中奖信息，请对方领取大奖，不过预先缴纳手续费、快递费、公证费等各种费用。一旦市民将这些费用汇入指定的银行卡，对方就从此杳无音讯。此前，《我要上春晚》、“非常6+1”等不少知名节目都发表过声明，提醒大家莫要上当。辨别这类骗术很简单，如果你根本没有参加过这类节目的报名就说明肯定是骗局，而且真的中奖并不需要先缴纳费用。只要对方要你提供银行卡信息，就应该多长个心眼。

3.冒充微信、QQ好友诈骗：

某公安机关接到居民任某报案，称:接到冒充她叔叔的微信，因为微信头像和名字都与她叔叔的一样，她以为是她叔叔，对方在微信上同受害人说她往受害人的卡上打6050元钱，让受害人将600元钱给她朋友打过去,50元钱用作手续费，让受害人将其卡号发给她。受害人就将自己的农行卡拍照通过微信发发过去了，随后对方将建行网上银行的截图给受害人发过来，说钱给转过来了，因为是跨行的不能马上到账，并让受害人先垫付给她的朋友转过去，并将收款人的户名和账号发给受害人，受害人打完钱后联系其叔叔发现微信被拉黑，打电话跟其叔叔核实后才知道被骗了。

这种诈骗手段要避免其实很简单的，这个大家就记住一点，亲朋好友的声音和面容你会弄错吗？遇到亲戚朋友借钱的事情，就要亲眼去见、亲耳去听。在互联网时代，你不知道网络对面和你聊天的是一个人还是一只狗，只有眼睛见了，耳朵听了，才知道答案。

4.利用含木马链接的短信、二维码等诈骗犯罪分子发送的短信中暗藏木马　病毒的网站链接，且点击就可能盗取手机内的网银密码等信息，最终导致网银内的资金被盗。同时，中毒的手机还有可能自动向通讯录中存储的号码再次扩散病毒短信，导致亲友“中招”。为达到目的，这些骗子的手段也是花样翻新，同时还很会抓热点，比如爸爸去哪儿、中国好声音、我是歌手，均以“被抽选为幸运观众”为由，诱使用户点击植入木马病毒的链接。

司法实践中还发现，一　些不法分子通过邮件、短信、电话等方式，以系统升级或身份认证工具过期激活等为由，要求客户到指定的网页修改网银密码或进行身份验证。需要注意的是银行不会通过邮件、短信、电话等方式，以系统升级或身份认证工具过期激活等为由，要求客户到指定的网页修改网银密码或进行身份验证。客户在登录银行网站时，最好直接输入银行门户网站地址，避免通过搜索链接进入冒牌网站。

还有相信在座的很多同学都会经常使用微信扫一扫功能，在此要提醒大家不要去随意扫来历不明的二维码。司法实践发现，有不法分子先将二维码植入木马病毒，再以降价、奖励为诱饵，诱使用户扫描，一旦扫描安装，木马就会进入手机系统，盗取银行账号、密码等个人隐私信息，再以短信验证的的方式篡改对方密码，将对方账户的资金转走。

5.网络购物诈骗

网购已成为越来越多人的首选购物方式。不法分子也看中其中的机会。比如有消费者就接到过自称淘宝客服的电话，说因为拍下的货品缺货，需要退款，要求购买者提供银行卡号、动态密码等信息。事实上，退款根本不需要直接知道银行卡号，退到支付宝账号就好了，即便直接退还银行下，系统也会默认操作，不需要另行提供，更别说告知动态密码了。

想必同学们一定看见或者收到过类似刷单的信息，“一天150-300元，一任

务一结算，用手机就能赚钱”听起来很诱人的背后是骗子的套路。或许你能白剽个一单两单，也就是几十块钱，等你放松了警惕，骗子就会发来大额链接，你支付了对方就到手了。不要想着天上掉馅饼，被这种刷单骗局给骗了。

6.“响一声”电话诈骗

不知道同学们有没有这种遭遇，就是电话来了，只响一声对方就挂断，还是一个陌生的号码，然后你回过去，对方会问你要不要购买某种商品，或者要不要参与某种投资。告诉大家，这是一一种“撒网式电信诈骗”。这类电话多采用特殊群拨设备或者软件进行拨打，对指定号码段进行自动拨号，一旦接受出电号码后立即挂断。如果一个个电话打过去解释会增加成本，采用特殊设备群拨不仅仅节约了成本而且方便快捷，这种情况下一旦有人回复了电话证明其可能成为潜在客户或者诈骗对象，简单来说就是广撒网锁定目标对象。

个人信息泄露是垃圾短信、骚扰电话乃至电信诈骗泛滥的罪魁祸首。我们平时应做好个人信息保护工作，防止个人信息泄露或被第三方利用。例如，不要随意丢弃快递单据，火车票，飞机票，　各种办理业务的凭证。手机上安装拦截骚扰电话的安全软件类似于手机管家等。

在这里我还要给大家补充说明一点，旧手机号停机前一定要将绑定的重要账户解绑。曾经有这样一个案件，某天杭州一派出所接到报警，事主俞先生称自己银行卡里面的钱被黄某刷走，民警调查后才知道黄某发现新买的手机号之前被人使用过的，还实名认证过注册过支付宝。禁不住贪念的诱惑，黄某尝试着用短信验证的方式改好密码的支付宝在借贷平台上贷到了 1 万多元。之后，黄某又陆续将支付宝拥绑的建行卡里面的几千元钱转到了自己的支付宝。因此，换手机号时一定要注意，跟旧手机号绑定的各个账户都需要检查、核对、解绑，尤其是涉及到支付宝、网上银行等资金账户，还有邮箱等涉及个人隐私的账户千万大意不得。

电信诈骗手段不断翻新，让人防不胜防。但所有的骗术都万变不离其宗，那就是最后会要求客户把自己的钱转移到骗子的账户里。骗子都是在利用我们对利益或者亲情的不冷静，致使我们盲目相信他们的话。结合刚才给大家介绍的电信诈骗的几种类型，我给同学们总结四点预防电信诈骗的建议，供大家参考：

首先，不向来历不明的人透露自己及家人的身份信息、存款、银行卡等情况；不要轻信陌生短信和电话中要求汇款的任何理由。如收到陌生短信或电话，不要惊慌无措和轻信上当，最好不予理睬，更不要为“消灾”将钱款汇入犯罪分子指定的账户。

其次，如果家人通过网络交流时提出汇款需求，必须确认对方身份。大量诈骗案件源于网络账号的丢失，在通过网络与家人沟通时，建议通过细节或者特定的约定方必要的确认。比如，通过其他的通讯方式联系家人本人确认汇款信息与汇款真实性，不要轻信任何非家人本人提出的汇款需求。如对汇款业务心存怀疑不能确认，应与银行工作人员及时沟通，银行工作人员经验丰富，可以有效帮助客户解决各类特殊情况。

最后，不要轻易相信网络、短信等提供的信息。不要因贪小利而受违法短信的诱惑。不要轻信虚假信息，要用头脑来甄别。不要在慌乱中作出决断，心态要保持平静。如果自己不确定是否是诈骗信息，可到就近公安机关询问情况，谨慎对待。

关于电信诈骗，除了要知道怎么预防，还要知道被骗后怎么做，再我们知道自己被骗后就是俩字“时间”，你要抓紧时间冻结你骗子的银行账户通过拨打该诈骗账号所属银行的客服电话，根据语音提示输入该诈骗账号，然后重复错输五

次密码，第二种是进入网上银行页面，输入该诈骗账号，重复输错五次密码，第三，也可以就近到嫌疑卡归属银行的AIM机，输入诈骗账号并进行无卡存款操作，在操作过程中输错密码三次，可将该卡智时冻结24小时。现在银行为防范客户遭遇电信诈骗也制定了相应措施，比如通过自动存取款机向他人转账，24小时后才会到账，在到账前可以到银行申请撤销转账。另外，再拨打96110反诈中心进行停止支付操作。

在采取完上述措施后，要保留好所有证据:录音、聊天记录、转账记录，第一时间向有关公安机关报案，不要因为害怕丢脸而贻误了最好的时机。