浙江省教育厅

浙教办函〔2017〕27号

浙江省教育厅办公室关于印发部分高校师生受通讯网络诈骗案例的函

各高等学校，各市、县（市 、区）教育局：

随着通讯网络的快速发展，通讯网络诈骗违法犯罪案件呈现出快速增长的态势。高校师生是通讯网络诈骗案件的主要受害群体之一，为加强对高校师生预防通讯网络诈骗知识的宣传教育，省教育厅会同公安部门对涉校通讯网络诈骗案件进行了梳理，对学校师生受害最多的六类通讯网络诈骗典型案件进行了分析，并针对性地提出了防范建议。现将典型案例分析印发给你们，请加强宣传教育，强化工作措施，杜绝通讯网络诈骗案件在校园的发生。

一、全面开展防诈骗宣传教育工作，提高师生防骗意识和能力。要从知识与技能入手，着力提高学生防范通讯网络诈骗的能力。要注重通过案例开展警示教育，对一些典型案例进行深入剖析，使广大师生掌握各类诈骗的特点和防范要点，增强识别和分辨能力。高校已陆续开学，各校要在学生返校开学后，集中开展

一次校园安全教育，发动辅导员、班主任、学生骨干开展多形式的防范通讯网络诈骗的宣传教育活动，尤其是通过电话、短信、网络等进行的非接触型诈骗活动。要注重通过案例开展警示教育，对一些典型案例进行深入剖析，使广大学生掌握各类诈骗的特点和防范要点，增强识别和分辨能力。提醒师生遇到要求转账、提款等涉财型诉求时，既不贪图不义之财，又不轻易被对方编造的谎言所吓唬。必要时学校要主动为师生提供咨询服务，切实提高师生的防骗意识和防骗技能，把涉及师生诈骗案件高发的势头降下来。

二、进一步强化动态信息的掌握，建立健全预警应对处置机制。要进一步建立健全师生信息员队伍，落实责任，加强培训，增强对各类通讯网络违法犯罪行为的识别力和敏感度。加强对学生的日常关注，对学生接收到的异常短信、电话、邮件、链接等帮助进行辨别，对学生异常的转账、支付、消费等行为争取早发现，早劝阻，早报告，尽力避免发生被诈骗案件。辅导员要密切关注学生异常消费行为和异常支付行为，把握通讯网络诈骗的类型与特点，提高甄别和防范能力。对校园网络贷款行为也要进行风险警示教育，及时引导，对新出现的新型诈骗手法要及时预警并加强关注，同时对案例进行分析总结并上报。此外，各高校要加强校园 110 指挥中心建设，对师生无法辨别真伪的求助事项及时提供帮助。加强校园内银行网点、ATM 机等设备的监控管理，一旦发现异常行为的，第一时间派出校卫队员进行应急处置。

三、进一步加强沟通协作，建立健全沟通协调机制。由于通讯网络诈骗专业性强、发展变化速度快、形式多样，涉及的部门又较多，需要各部门协同处置，齐抓共管。要进一步建立健全沟通协调机制，加强信息的沟通交流，针对出现的新情况新问题，研究制订综合性的整治措施，形成工作合力。各高校要加强与公安、银监、网信等职能部门的联系，在他们的指导下，提升主动防范通讯网络新型违法犯罪活动的能力，确保广大师生生命财产安全。

附件：高校师生被通讯网络诈骗典型案例分析

浙江省教育厅办公室

2017 年 2 月 16 日

抄送：杭州外国语学校。

附件

高校师生被通讯网络诈骗
典型案例分析

为了让更多高校师生了解当前的诈骗手法，提高防范鉴别能力，近期，省教育厅会同公安部门将高校师生受害最多的六类通讯网络诈骗典型案例进行了摘编，并针对性地提出了防范提醒。希望广大师生能从案件中吸取教训，引以为鉴，并广泛宣传，杜绝通讯网络诈骗对自己及周边人员造成侵害。

一、冒充“公检法”诈骗

2016 年 12 月 6 日 13 时，事主朱某（女，61 岁，大学退休教师）接到了一自称杭州市公安局陈立警官的电话，对方告知朱某涉嫌北京市公安局办理的一起洗黑钱案件，并给了“北京公安”电话 010-5846****，让其马上联系。朱某接到电话后慌了神，急于证明自己不可能涉及洗钱，便立即拨打了骗子给的号码。一个自称北京市公安局专案组的赵警官接了电话，询问了朱某及案件相关情况后，又将电话转接到了“支队长陈某”处，陈某声称要调查朱某的财产状况，并称办案时间紧张，需朱某新办网银并立即转账。当日下午 15 时，朱某按骗子的要求新办了网银。同时，骗子称由于案件保密需要，要求朱某去酒店开房单独接受调查。在宾馆房间内，朱某点击对方发来的网址，登陆假冒检察院网站，看到了贴有自己照片的假通缉令，就愈加信以为真。在该网站填

写了身份证、银行卡账号、密码等信息，并将新办理的 U 盾插入电脑，之后，朱某发现自己银行卡内的 42 万元已被盗转，方才发现被骗。

警方提醒：公检法办案会面对面向当事人出示证件或法律手续并讲明情况，不会电话询问当事人、不会在电话里做笔录，更不会要求通过网银转款到指定账户，公检法执法办案中没有所谓的“安全账户”。

二、冒充客服诈骗

2016 年 10 月 29 日 17 时，事主吴某（女，20 岁，知名院校学生）接到一自称“韩都衣舍”客服的男子电话，称公司为答谢客户，赠送其一张贵宾卡，可在消费时享受折扣，但需通过“支付宝”交纳 200 元年费。吴某称不需要该贵宾卡，于是对方称注销贵宾卡需持有存款 10000 以上的本人银行卡至就近 ATM 机，通过输入验证码的方式销卡。而后，对方让事主在 ATM 机上用英文界面操作，输入所谓贵宾卡卡号（实际为骗子的账户），验证码 9999（实际为转账金额），后事主发现账户被转 9999 元。

警方提醒：正规企业客服联系会员，基本都通过站内信的形式发送。如有人通过打电话或网络聊天自称客服的，请提高警惕！通话中可详询对方工号和相关事宜，挂断电话后反打网站官方客服电话求证。如果涉及先交钱或是预交保证金的，需反复核实，确保自身权益，谨防网上类似骗局。一旦要求使用 ATM 机英文界面进行操作的，肯定是诈骗无疑。

三、冒充领导、导师诈骗

2016 年 9 月 24 日 18 时，事主戚某（女，21 岁，在杭大学生）在寝室内接到一陌生男子电话。该男子始终未表明身份，任由戚某猜测。戚某根据该男子声音特质将其误判为杨老师，对方顺水推舟，默认了“杨老师”身份，并在电话中让戚某第二天去趟办公室。次日 8 时 40 分，戚某接到该男子电话，称有领导在，不方便见面，并以送领导红包为由向事主借款 16000 元。戚某用支付宝分两次向对方提供的账户汇款 16000 元，之后戚某无法联系到该男子，遂发现被骗。

警方提醒：接到“领导、导师”的电话，切莫惊慌。在对方未表明身份的情况下，不要胡乱猜测。可直接挂断电话，搞清楚对方真实电话后致电求证或当面求证。

四、网络兼职、刷单诈骗

2016 年 11 月 10 日，事主郭某（女，20 岁，在校大学生）在网上寻找兼职工作时，发现一公司招募网络刷单（虚假交易，帮助提升网店信誉）人员，承诺退还保证金、交易本金，并给予高额佣金。郭某用 QQ 与对方取得联系，并按对方发来的申报表要求，详细填写了个人信息及银行卡号，同时通过支付宝缴纳了 1000 元保证金。对方先给出了简单的网购刷单任务，郭某完成后，得到了 20 元佣金及被返还的本金。郭某觉得赚钱非常轻松，渐渐放松了警惕。随后，对方连续给出了大量刷单任务，郭某共支付刷单所需的本金 14000 元。接着，对方以系统故障为由，未

返还本金及佣金。郭某多次催促未果，最终连报名保证金，共计被骗 15000 元。

警方提醒：找工作选择正规网站，填写个人资料时要注意保护个人隐私信息。任何单位向个人求职者收取报名费、风险金、保证金等名义费用的，都属非法。同时，网络刷单本身即属于违规行为，不受网站保护，切莫为了蝇头小利被犯罪分子钻了空子。

五、网购退款诈骗

2016 年 11 月 12 日，事主李某（女，21 岁，在校大学生）在校内接到自称淘宝某店家客服人员张某电话，称李某“双 11”购买的一件衣服因系统问题导致交易失败，需要退款，并称当前系统故障未修复，可通过特定退款链接实现快速退款。事主李某加了客服张某 QQ 后，对方发来一网站链接，李某点击后出现所谓的购物退款网页，并显示可直接将款退到银行卡，于是李某填写了个人及银行账户详细信息（卡号、背面后三位 CVV 码）及手机收到的验证码，之后发现账户内 1000 元存款被别人在某购物网站网络消费。

警方提醒：正规购物网站的退款一般会将钱打入“支付宝”、“财付通”等特定的第三方支付平台或该网站支付账户内，正规客服人员不会直接询问客户个人及银行账户等详细信息，更不会要求互加好友，指导客户点击通过聊天工具发来的不明链接。同时，网络购物要注意不能脱离网站担保的交易流程，否则极易上当受骗。

六、网络交友诈骗

2016 年 7 月，事主吴某某（男，20 岁，在校大学生）通过网游结识网友“小金”（自称女大学生），并数次从“小金”处代购韩国商品。8 月下旬，吴某某准备去韩国旅游，“小金”谎称可通过韩国的朋友廉价预定当地星级酒店。于是吴某某先后通过支付宝及网银向“小金”转款 3000 元。几日后，网友“小金”便无法联系，吴某某这才发现被骗。

警方提醒：网络交友需谨慎，不知名、不了解的，一律不要谈钱。

通过近年来的案件分析，警方总结出防通讯网络诈骗的 8 个突出特点，凡是符合这 8 种情形的，一定是诈骗。即“八个凡是”：凡是自称公检法要求汇款的；凡是要求汇款到“安全账户”的；凡是通知中奖、领奖要先交钱的；凡是通知“家属”出事要先汇款的；凡是在电话中索要银行卡信息及验证码的；凡是要求开通网银、U 盾、电子解码器接受检查的；凡是自称领导要求汇款的；凡是以任何非当面形式要求接受通缉令、逮捕令、传讯令、资产清查令的。