关于做好春季开学防范电信网络诈骗工作既推广“国家反诈中心”官方政务号的通知

当前，以电信网络诈骗为代表的新型网络违法犯罪持续高发，严重侵犯人民群众财产权利和人身权利，因此，为深入贯彻落实习近平总书记重要指示和全国打击治理电信网络新型违法犯罪工作电视电话会议精神，国家反诈中心依托互联网新媒体平台大力开展反诈防骗宣传，从而提高人民群众防骗意识和能力，营造全民反诈的浓厚氛围。国家反诈中心在人民日报客户端、微信视频号、新浪微博、抖音（ID: gjfzzx96110）、快手（ID: gjfzzx96110）等五个新媒体平台上同步开通“国家反诈中心”官方政务号，政务号采取民警宣讲、警民互动、网络情景剧、公益宣传片、抓捕实录等多种形式，常态化更新宣传内容，及时发布防骗预警，为广大师生提供了一个新的识骗、防骗、拒骗信息渠道，在此，敬请广大师生踊跃关注。

结合“国家反诈中心”官方政务号开通这一契机，针对春季开学网络电信诈骗进入高发期，诈骗案件花样翻新、隐蔽性更强的特点，为保障广大师生的人身、财产安全，保卫处将常见的电信诈骗手法进行汇总如下，以期提高全体师生防范电信诈骗的警惕性，减少案件的发生以及财产损失:

一、冒充熟人进行诈骗

利用盗取的QQ、微信、手机等，冒充受害人的亲友，谎称急需用钱。

防范提示：对于亲友未当面要求汇款的，一定要进行核实。

二、网络兼职刷单诈骗

不法犯罪分子利用招聘网站、兼职类QQ、微信群等途径发布虚假兼职(给电商平台商铺刷单以提升信誉度）信 息，以高额回报为诱饵,等刷单成功后,再以缴纳保证金、系统网络问题等种种借口,要求受害人多次汇款的网络诈骗。

防范提示：坚决抵制网络刷单违法行为；对于网上的招聘信息，要多方鉴别；不要在网上支付保证金或相信对方开出的各种汇款条件。

三、网上购物退款诈骗

不法分子冒充购物网站客服，声称因断货、质量问题或支付未成功要给予退款或重新支付，并通过 QQ 等发送退款链接,受害人打开链接后,根据提示输入身份信息、银行卡、手机号、验证码,犯罪分子通过远程操作,在输入验证码后，该银行卡内的钱即被转走。

防范提示：网上购物时不使用第三方社交账号联系，更不能随便在不明链接中输入个人身份、银行卡信息、验证码等。

四、游戏充值诈骗

不法分子打着“超低价”“充值优惠”的旗号，对虚假诈骗链接进行包装，随后通过群聊、游戏聊天系统等途径发布，待有玩家点击填写后盗取资金。

防范提示：不要轻易点击非官方发布的链接，更不要轻易将账号密码等信息告诉他人或在陌生网站上填写。

五、注销校园贷诈骗

“注销网贷账号”骗局持续高发，不法分子冒充“银行以及网贷平台客服”来电，以“根据国家相关政策，要求当事人配合注销在大学期间曾注册的网络贷款平台账号”，或“当事人的身份信息被盗用注册了网贷账号，影响个人征信需要配合注销”等为由，引诱当事人下载 APP 贷款平台转账到指定账号实施诈骗。

防范提示：凡自称借贷平台客服，以“不注销网贷将会影响征信”为由要求转账汇款的都是骗局。查询个人信用信息要通过当地人民银行征信部门或中国人民银行征信中心信息服务平台等官方渠道，如有疑问应拨打征信中心官方客服电话进行咨询。

六、售卖防疫物品诈骗

不法分子利用学生及家长欲购买口罩供开学使用，通过微信、QQ 等渠道发布虚假商品信息，最后拒不发货就此消失实施诈骗；甚至冒充其子女的 QQ、微信添加其亲朋好友，谎称学校安排统一订购在校期间的口罩，要求将钱款转至学校

指定账户。

防范提示：一定要通过正规渠道购买口罩、酒精等防护用品，不要相信陌生人口中所谓的“特殊渠道供货”、“国外代购”等信息，及时关注官方发布的防疫信息内容。

七、冒充各种角色发送特殊内容链接的短信诈骗

不法分子冒充老师，发送成绩单链接；冒充同学，发送聚会相册链接等。短信中的链接一旦点开，会有木马病毒被置入手机，从而导致个人信息泄露甚至绑定手机的银行卡内钱财被转走。

防范提示：对于陌生号码发来的链接，要提高警惕，切勿轻易点开。

八、冒充“公检法”机关工作人员打电话诈骗

受害人接到自称是某公安局电话，被告知其因涉嫌毒品走私、信用卡套现、赃款贷款不还等理由让其将资金打到安全账号，受害人因害怕便按其指示转账，从而被骗。

防范提示：接到自称是公检法等政府工作人员的电话并要求转账的，可拨打 110 进行咨询，切勿轻信并转账。

九、冒充 10086、95515 等客服电话诈骗

犯罪分子利用伪基站冒充 10086、95515 等客服，发短信告知受害人其网银或电子密码器升级、有积分兑换等，诱骗受害人登录短信上的钓鱼网站以获取银行账号和密码。

防范提示：在收到含有陌生网址或链接的短信时，不要

轻易登录或点击，可以就短信中的内容向银行或者公安机关进行求证，以防上当受骗。

十、退改签诈骗

不法分子以“航班、列车因控制疫情被取消，办理退改签可获赔偿”为借口，或以“受疫情影响，快递滞留补偿”等为由，诱导受害人点击虚假网址，要求提供验证码等信息，进而盗取受害人银行卡中资金。

防范提示：一定要到正规官网进行网上购票，当需要退订或改签时，一定要与官方客服进行核实确认。

最后，保卫处提醒广大师生做好以下几点，防患未然：

一、加强保密意识，防止个人及家庭信息外泄；

二、遇到可疑情况要多与亲戚、朋友商议，并及时拨打公安机关、金融等部门的官方客服电话进行查证核实；

三、不轻信陌生信息，不点击陌生链接，未经核实不转账、不汇款；

四、遇到紧急情况或被骗及时拨打 110 报警。

保卫处

2021 年 3 月 10 日