

全体师生高度重视，严格防范新型网络诈骗

---转载自北京青年报社“政知见”

近日，一种新型网络诈骗频发——诈骗分子针对助学金、奖学金和各类补贴发放的校园场景精准施骗，造成部分学生财产损失。北京房山警方 11 月 30 日发布紧急防范提示，请全体在校师生高度重视、严格防范。

警方明确告知：正规补贴发放绝不会通过私人链接、非官方平台要求填写银行卡密码、验证码等敏感信息，学校官方通知也会通过正规渠道统一发布。遇此类异常要求，直接判定为诈骗。

警方介绍，针对在校师生的骗局中，诈骗分子先通过邮件在被害人不知情的情况下，诱导被害人下载病毒文件，从而通过木马病毒非法盗取相关工作人员的电脑操作权限。

之后，诈骗分子再借助校园内部通讯群组（如钉钉工作群、校内微信群）、校内邮箱等渠道，伪装成“助学金”“奖学金”“科研补贴”“人才补贴”“生活补贴”等热门名义，批量发送虚假网址链接。

最后，受骗师生点击链接，在伪造的虚假页面中填写姓名、身份证号、银行卡号、密码、验证码等关键个人信息后，诈骗分子会直接盗刷银行卡，或利用获取的信息实施后续诈骗，给师生造成财产损失。

警方表示，此类骗局中，诈骗分子惯于伪装成学校财务处、人事处、信息化中心、科研院、后勤部等校内职能部门，或冒用同事、领导、老师、同学的账号发送信息，发件人身份存疑时务必多方核实。对通过校

园 OA 系统、校园邮箱、工作群、班级群等校内渠道传播的未知链接保持高度警惕，无论链接标题多么诱人，均不得盲目点击。

首先，坚守“三不铁律”。不点击陌生未知链接、不向非官方渠道填写身份及银行卡敏感信息、不轻信陌生账号或非正规渠道发布的补贴类通知。

其次，严格执行核实流程。收到任何形式的补贴类信息后，务必通过学校官方公布的联系电话、线下办公地点当面确认、对接校内相关部门等方式，核实信息真伪，确认无误前绝不操作。

第三，筑牢账户安全防线。坚决杜绝从非官方应用商店、不明链接下载 APP 或插件，防止设备被植入木马病毒，导致账号被盗；校内系统账号、邮箱密码及网银密码需定期更换，避免使用生日、学号、手机号等易被破解的弱密码，降低账号被盗风险。

警方还提出一些防诈骗细节和建议。为了有效防止诈骗，请师生在不操作内部通讯群组时退出登录；休息、下班时关闭计算机；装有内部通讯群组 APP 的计算机安装杀毒软件并及时更新病毒库；遇有跨部门、跨单位添加好友的情况，在填写个人信息前要先线下核实情况。如收到“发放补贴”“助奖学金”邮件、群通知或私信，切勿贸然点击链接，绝不向任何陌生页面提交个人银行账户相关信息。第一时间通过官方渠道核实信息真伪，避免落入诈骗陷阱。