湖南食品药品职业学院信息中心

学校网络安全通报
（第一期）

校园网络已深度融入教学科研、办公生活，网络安全无小事，日常防护是关键。为持续筑牢校园网络安全防线，防范各类网络安全风险，保障师生个人信息、财产安全及校园网络秩序稳定，结合近期学校安全稳定风险隐患大排查大整治交叉大检查及校园网络安全动态，现将日常防护重点要求通报如下，望全体师生时刻警惕、严格遵守。

经核查，何X、华X、姚X等三名学生因存在不当上网行为，个人电脑被植入木马程序和病毒，多次攻击学校校园网；另有胡X、张X等两名学生存在翻墙浏览境外网站和登录境外游戏服务器等行为，此外还有2名教师也存在翻墙行为。

一、日常高频风险提醒

账号安全不松懈：云端教学平台、教务系统、校园网等账号需设置强密码（大小写 + 数字 + 符号），开启双重认证，定期更换，严禁转借他人；避免使用“姓名 + 学号”“123456”等弱口令，谨防账号被盗。

终端防护要到位：个人电脑、手机等设备需安装正版杀毒软件，及时更新系统补丁与病毒库；不点击陌生链接、不扫描不明二维码、不下载非官方APP，严防恶意程序窃取信息。

网络连接辨真伪：优先连接学校官方 Wi-Fi，不连接无密码的开放网络或名称仿冒官方的“伪 Wi-Fi”；不在公共网络环境下登录重要账号、进行支付操作或传输敏感数据。

合法用网守底线：严禁私自使用 VPN 等工具违规“翻墙”，不浏览、传

播违禁信息；不参与非法网络活动，不私自搭建无线 AP、私人云盘，避免触碰网络安全红线。

二、日常防护核心要求

（一）个人层面：做好“自我防护第一责任人”

养成“三不原则”：不泄露验证码、银行卡密码、身份证号等敏感信息；不轻易相信陌生信息，遇到疑问先向学院、部门或相关职能部门核实；不随意授权 APP 获取通讯录、相册、位置等权限，定期清理闲置 APP。

定期自查设备：每周扫描设备病毒、检查账号登录记录，发现异地登录、设备卡顿、异常弹窗等情况，立即修改密码、断网排查，并及时上报。

保护科研与学业数据：毕业设计、科研成果、课程资料等重要数据，做好本地备份与加密存储，不通过非官方渠道传输或存储，谨防数据泄露、丢失。

（二）单位层面：落实“日常管理常态化”

各部门、二级学院网络安全第一责任人需定期排查本单位办公终端、服务器、物联网设备（门禁、考勤机等），及时修改默认密码、清理废弃账号，建立设备安全台账。

加强内部提醒：通过班会、部门会议等形式定期传达网络安全知识，分享典型案例，提升师生安全意识；关注本单位师生网络行为，发现异常及时干预。

规范数据管理：梳理本单位敏感数据（如学生信息、科研数据、经费信息等），落实分级保护要求，避免数据随意存储、传输，防止泄露风险。

三、异常情况处置流程

若遭遇账号被盗、信息泄露、网络诈骗等情况，第一时间修改相关账号密码，关闭支付功能，保留聊天记录、转账凭证等证据，并立即向学校信息中心、学保部报告。

若发现设备被入侵、网络异常或疑似恶意攻击，立即断网隔离设备，避免风险扩散，同时联系学校信息中心技术人员协助处置。

网络安全防护重在日常、贵在坚持。请全体师生将网络安全意识融入日常工作、学习、生活的每一个环节，共同营造安全、健康、有序的校园网络环境。学校将持续开展网络安全检查与宣传教育，对违反网络安全管理规定的行为，将依规依纪处理；涉嫌违法犯罪的，移交司法机关。

特此通报。

信息中心（免章）

2026 年 5 月 26 日