

中共安徽科技学院委员会网络安全与信息化办公室



网信〔2023〕28号

关于开展木马和僵尸网络安全专项治理工作的通知

各学院党委、机关党委、各党总支，各单位，各部门：

为了进一步贯彻落实党和国家关于网络安全工作的总体部署，有效遏制利用木马、僵尸网络发起大规模网络攻击的威胁，降低网络风险，维护网络空间安全稳定，结合我校实际，特通知如下：

一、工作目标

（一）全面排查

各单位要立即开展自查，

（二）重点整治

各单位要立即开展自查，重点整治利用木马、僵尸网络发起大规模网络攻击的威胁，降低网络风险，维护网络空间安全稳定。各单位要立即开展自查，重点整治利用木马、僵尸网络发起大规模网络攻击的威胁，降低网络风险，维护网络空间安全稳定。

二〇二三年四月二十三日，各单位网络安全与信息化办公室主任

按照网络安全防范工作提醒进行处置，开展网络防范的知识宣传教育引导。

3、10月30日-11月3日，开展学校网络安全应急演练和培训，通过漏洞挖掘或模拟，以学校某重要信息系统为重点进行应急演练。

4、网络与信息技术中心通过技术手段进行本园网站、邮箱、

网络安全应急预案及应急处置流程

网络安全应急预案及应急处置流程

三、网络安全应急处置流程

1. 应急响应：发生网络安全事件时，应立即启动应急预案，成立应急响应小组，由组长负责指挥协调，成员分工负责。应急响应小组应立即对事件进行初步判断，确定事件性质、影响范围和严重程度，并及时向上级领导和相关部门报告。

造成网络安全责任不清。

2. 计算机病毒防治软件应定期升级并安装最新病毒库，并及时安装系统补丁。（正版操作系统随病毒库更新，盗版操作系统无法更新，建议，使用正版操作系统）不是所有 Windows 操作系统均支持网络 Windows 更新版本。

4. 计算机应安装杀毒软件且升级病毒库，定期扫描系统病毒，对可疑文件，可安装“木马”查杀软件等，及时查杀。木马下载：<http://www.lama.com/>。

5. 关闭计算机设备上不必要的端口及服务，如 138、139、130、445、3389 等。

6. 计算机应设置磁盘密码及输入密码复杂度，并定期更换登录密码。

7. 提高网络安全防范意识，不打开来历不明的邮件附件、QQ 或微信文件，不到来历不明的网页，不随意点开来历不明链接，不下载安装来历不明的软件，不使用未经杀毒端口盘，谨防钓鱼等诈骗事件。

8. 发现计算机使用异常，如突然蓝屏卡顿、运行缓慢、上网异常等现象，应及时进行病毒查杀，对于检测出的异常数据无法确认是否为“挖矿”木马或病毒软件不能清除的情况，可联系网络与信息安全中心咨询。

发现钓鱼网站，举报至“举报”；发现任何可疑诈骗行为，

请及时联系网络与信息技术中心。联系人：李原，15005507202。

注：本页面指出政十长字壮在巫字书以笈担！似宜

