**附件1**

**“挖矿”木马排查处置方法和防范指南**

一、计算机设备安装、使用的Windows操作系统建议升级到最新版本，且安装对应安全补丁及漏洞补丁。（正版化操作系统请到校园软件正版化服务平台下载，http://ms.zknu.edu.cn/）。

二、计算机设备必须安装杀毒软件且升级最新病毒库，对本机系统定期全盘病毒查杀，开启系统自身防火墙功能。

三、多台计算机设备不要使用相同的账号和口令，登录口令满足复杂性要求并定期更换登录口令。

四、避免使用远程控制软件，非必要不通过远程手段进行运维。

五、针对教学、科研、管理等重要数据务必做好相应备份措施，避免重要数据丢失。

六、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，不浏览不明的网页，不随意点开不明链接，不下载安装不明的软件。

七、可使用“挖矿”病毒巡检工具，进行系统扫描，“挖矿”工具下载地址：<https://edr.sangfor.com.cn/#/introduction/mining_virus>。