网络安全为人民　网络安全靠人民

国庆来临之际，祝伟大祖国繁荣昌盛！

祝全校师生节日快乐！

警惕网络钓鱼安全事件

近期网络钓鱼木马活跃度不断提高， 常利用微信、钓鱼网页等方式以虚假的“发票”、“财税”、“人员名单”等诱导性文件在微信群聊中相互传播。用户下载运行该文件后，病毒会被激活并释放多个恶意文件，添加计划任务，远程控制受害者的终端等，对用户构成较大的安全威胁。

而这些文件无论是标题还是其伪造的内容都极具欺骗性，因此也导致不少用户中招。

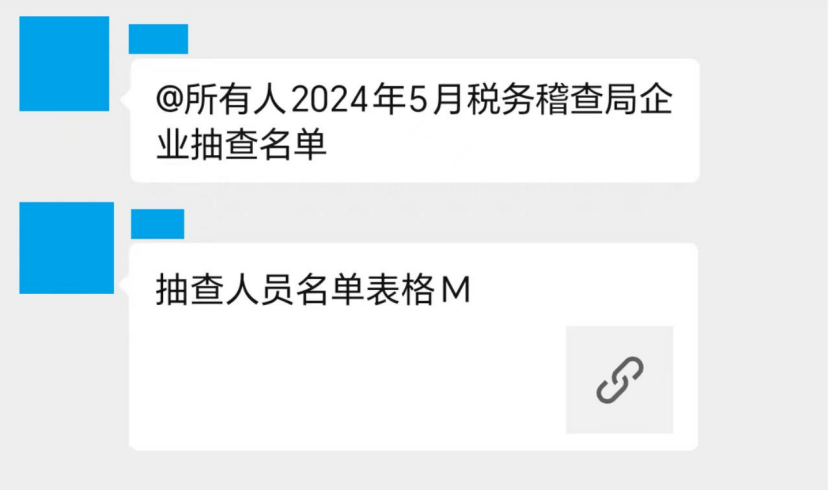
被远控后，攻击者会创建群，拉受害者的好友进群，然后踢出受害者，再进行后续的诈骗活动

以“银狐木马”举例，下面这个钓鱼网页便是伪装成税务稽查通知，诱骗用户下载其附件并运行。该钓鱼网页具有很大的迷惑性，用户稍不留神便会中招。

银狐木马典型钓鱼页面

一旦完成对受害者设备的感染便会开启免杀对抗机制，对安全软件实现免杀。而银狐木马则利用了一些正规的企业管理软件来实现在系统中的长期驻留。

此外，此类软件也具备“自我保护”能力来防止被停用或卸载，所以一般用户即使发现异常也难以清除。最终，受害用户便会在不知不觉的情况下被黑客长期控制。黑客以受害用户的设备作为跳板，进一步扩散病毒木马，甚至发起新一轮的诈骗。



通过被控电脑微信群发钓鱼链接

通过受控者聊天工具诱导好友运行木马或进行诈骗

目前我校信息中心已对校内教职工网络采取了相应的安全措施，禁止了部分远控工具及定期封锁校内出现的木马远控域名和 ip。但网络攻击手段层出不穷，目前无法对校内众多终端进行统一管理各位在日常上网中要提

高网络安全意识，**对于发现微信被异常控制，出现自动建群发送消息等问题的及时断网报修进行处理。**

安全建议：

1、陌生人发送的恶意文件不要随意打开，打开前建议使用杀毒软件进行扫描；

2、下载工具去正规的下载站进行下载，日常注意访问的网站域名是否正确；

3、安装杀毒软件进行防御和杀毒，并定期更新病毒库和主动查杀；

4、对于安全软件报毒的程序，不要轻易添加信任或退出安全软件；

信息中心

信息化管理办公室

2024 年 9 月 27 日