关于加强计算机终端网络安全防护工作的通知

各单位、校园网用户:

根据学校网络安全监测平台信息，发现部分单位师生用户的计算机终端存在感染恶意软件（木马）情况，可能被利用窃取用户账号密码等个人信息，导致数据泄露或个人财产损失，或者计算机终端被远程控制执行恶意活动，对学校网络安全造成危害。

为进一步加强学校网络安全管理，防范计算机病毒、木马等恶意软件的感染和传播,保障学校网络信息安全,现就有关事项通知如下:

一、落实安全防护措施

各单位应加强对计算机终端的管理，落实以下安全防护措施:

1.安装运行杀毒软件(**如火绒安全软件、360 杀毒、360 安全卫士、Windows Defender 等**）。计算机终端必须安装杀毒软件并确保实时运行，及时升级病毒库，定期进行全盘杀毒；接入移动存储设备、下载文件时，应先进行病毒扫描。

2.及时更新操作系统和应用软件。使用正版操作系统，打开操作系统自动更新功能，及时给操作系统打补丁；要从官方网站下载正版软件，避免使用捆绑有第三方恶意程序的盗版软件，及时给应用软件打补丁，以修复安全漏洞，防止病毒的入侵。

3.计算机终端设置强密码。计算机终端不设密码或使用弱密码的用户应尽快设置或修改密码，且使用强密码，避免弱密码被攻击者利用进行暴力破解及病毒扩散。

4.防范钓鱼邮件。强化网络安全意识，谨慎核对和确认发件人信息，不要打开来历不明的邮件，不要点击邮件中的不明链接和附件，

不要轻易填写账户密码等个人信息。防止钓鱼邮件利用邮件中的链接或者附件，在计算机设备上植入木马病毒或窃取个人信息。

二、妥善处置受感染终端

各单位应做好网络安全应急处置工作，如果发现计算机终端感染恶意软件，及时采取以下处置措施:

1.立即采取断网等措施隔离受感染的计算机，防止病毒进一步传播、数据被窃取和计算机遭到远程控制。

2.使用杀毒软件对受感染的计算机进行全盘病毒扫描,查杀病毒。

3.检查受损情况，修改系统密码，防止攻击者利用受损账户密码进一步入侵，窃取数据。

3.备份重要数据,必要时重新安装操作系统,彻底清除病毒木马，防止类似情况再次发生。

4.如果引发网络安全事件，应及时报告信息管理中心，并按照指导进行后续处理。

各单位应严格落实网络安全责任制，对本单位计算机终端使用情况进行网络安全排查，及时整改网络安全风险隐患，防止计算机终端感染病毒引发网络安全事件。学校将加强对校园网内计算机终端的安全监测，发现计算机终端感染恶意软件情况将及时通报相关单位。

信息管理中心

2025 年 6 月 25 日