

固原市实验小学信息中心

针对近期计算机病毒高发有效防范的通知

各位老师:

近期各类计算机病毒活动频繁,校园网络安全面临严峻挑战。为保障您的教学资料安全和学校网络稳定运行,请务必高度重视并立即落实以下防范措施:

一、提高警惕,严防入口(最重要!)

1. 谨慎处理电子邮件:

不轻易点击链接或打开附件:即使是看似来自同事、学校或熟悉机构的邮件,也要高度警惕。仔细核对发件人邮箱地址是否真实(注意拼写错误或奇怪域名)。特别警惕:

带有紧急、重要通知、账单、快递、会议邀请等字眼的邮件。

要求你输入用户名密码、个人信息或进行“安全验证”的邮件。

附件是.exe、.scr、.zip、.rar、.docm、.xlsm、.js、.vbs等可执行文件或宏文件。

启用邮件过滤和反垃圾邮件功能:确保你使用的邮件客户端开启这些功能。

对可疑邮件直接删除或报告：不确定时，宁可删除或联系学信息中心确认。

2. 安全使用 U 盘/移动硬盘：

来历不明的 U 盘绝对不用：不要随意使用捡到、他人赠送或来源不明的移动存储设备。

插入前先杀毒：即使是自己的 U 盘，在插入学校电脑前，务必先用杀毒软件进行全盘扫描。重要！

禁用 U 盘自动播放：在系统设置中关闭自动播放功能，防止插入即自动运行病毒。

3. 警惕网络钓鱼网站和恶意下载：

不点击不明链接：无论是在邮件、社交媒体、即时通讯工具（如微信、QQ）还是网页弹窗中，对不明链接保持戒心。

只从官方/可信来源下载软件：下载教学软件、驱动、资料等，务必通过官方网站、学校提供的正版软件库或可信的应用商店。绝对不要从不知名的小网站、论坛或 P2P 网络下载。

注意网址拼写：访问重要网站（如什么系统、网银）时，手动输入网址或使用可靠书签，注意域名拼写是否正确（如 micorssoft.com 是钓鱼网站）。

二、加固系统，降低风险

1. 及时更新操作系统和软件：

开启自动更新：确保电脑的操作系统（Windows, macOS）、

办公软件(Office, WPS)、浏览器(Chrome, Edge, Firefox)、PDF 阅读器 (Adobe Acrobat Reader)、Flash Player (如果必须用) 等都保持最新状态。安全补丁是堵住漏洞的关键。

定期检查更新: 即使设置了自动更新, 也应定期手动检查一下。

2. 安装并更新可靠的杀毒软件/安全软件:

确保已安装: 学校统一部署的杀毒软件必须安装并保持运行。

保持病毒库更新: 确保杀毒软件的病毒库/特征库设置为自动更新。

定期全盘扫描: 至少每周进行一次全盘病毒扫描(可设置在空闲时间自动进行)。

开启实时防护: 确保软件的实时文件监控、网页防护、邮件防护等功能都处于开启状态。

3. 启用系统防火墙:

确保操作系统自带的防火墙处于开启状态。这是阻止外部恶意连接的基础屏障。

4. 使用强密码并定期更换:

复杂且唯一: 为电脑登录账户、邮箱、宁夏教育云平台、云盘等设置强密码(包含大小写字母、数字、特殊符号, 长度至少 12 位)。不同平台使用不同密码!

定期更换: 尤其重要账户的密码应定期(如每 3-6 个月)

更换。

不共享密码：个人账户密码不要告知他人。

考虑密码管理器：如果密码太多记不住，可以考虑使用可靠的密码管理器。

5. 关闭不必要的服务和端口：普通教师用户一般不需要手动操作，但需知晓学校信息中心会进行此类安全加固。

三、良好习惯，数据无忧

1. 定期备份重要数据：

3-2-1 原则：重要教学资料（课件、试卷、成绩、科研成果等）必须定期备份！遵循“3-2-1”原则：

至少 3 份副本。

使用 2 种不同的存储介质（例如：电脑硬盘 + 移动硬盘/U 盘 + 网络存储/云盘）。

其中 1 份备份存放在异地（例如家里、可靠的云存储）。

自动化备份：利用操作系统或专业软件的自动备份功能。

备份后验证：定期检查备份文件是否可用。

2. 使用标准用户权限：

日常工作时，不要使用具有管理员权限的账户登录电脑。使用标准用户权限账户，这样即使中毒，病毒的破坏力也会受到限制。需要安装软件或进行系统更改时，再临时使用管理员账户。

3. 安全使用云存储：

利用可靠的公有云(如 OneDrive, Google Drive, iCloud 等, 注意选择信誉好的)备份和同步文件。

确保云账户使用强密码并开启双重认证。

注意云盘共享链接的权限设置(避免设置为“公开”或“有链接即可访问”)。

4. 离开时锁定电脑:

短时间离开座位时, 养成习惯按 “Win + L” (Windows) 或 “Ctrl + Cmd + Q” (Mac) 锁定屏幕, 防止他人未经授权操作你的电脑。

四、遇到可疑情况怎么办?

1. 立即断网:

如果电脑出现异常(如运行极慢、频繁弹窗、文件被加密、杀毒软件报毒或失效等), 第一时间断开网络连接(拔掉网线或禁用 Wi-Fi)。这能阻止病毒进一步传播或与黑客服务器通信。

2. 停止操作:

不要继续使用电脑进行操作, 特别是不要尝试登录网银或输入密码。

3. 立即报告信息中心:

立即联系学校的信息中心, 详细描述你观察到的现象和采取的措施(如已断网)。切勿自行尝试“修复”或运行来历不明的“杀毒工具”。

4. 不支付赎金:

如果不幸感染勒索病毒（文件被加密索要赎金），绝对不要支付赎金。支付了不一定能解密，且会助长犯罪，立即报告信息中心。

特别强调:

教学资料是核心资产：课件、试卷、研究成果等往往凝聚了大量心血，定期备份是重中之重！

以身作则，教育学生：教师在防范病毒时表现出的谨慎和良好习惯，本身就是对学生最好的网络安全教育。

不安装非教学必要软件：避免在办公电脑上安装游戏、盗版软件、来源不明的工具软件等，这些往往是病毒温床。

请各位教师务必提高网络安全意识，将以上措施融入日常工作中，共同维护学校网络环境的清洁和安全。保护好个人电脑和数据安全，就是保障教育教学工作的正常开展！

固原市实验小学信息中心

2025年6月18日
