附件一：防范网络勒索病毒的安全措施建议

根据多个安全组织反馈，此次网络勒索病毒是利用 Windows 系统 SMB 漏洞（MS17-010）进行感染和通过 445 网络端口进行传播；感染勒索病毒后，电脑中重要文件（如 Word、Excel、JPG）将被病毒加密，并显示类似图 1 所示的弹出窗口，由于**加密强度高**、**解密难度大**且**付费恢复可能性极小**，将对个人重要信息造成严重损害。

图 1 感染网络勒索病毒后弹出窗口示例

微软公司在今年 3 月份发布的 MS17-010 补丁，已修复该网络勒索病毒所利用的 SMB 漏洞。此次网络勒索病毒利用的 SMB 漏洞影响以下未自动更新的操作系统：

Windows XP / Windows 2000 / Windows 2003/Windows Vista / Windows Server 2008 / Windows Server 2008 R2/Windows 7 / Windows 8 / Windows 10/Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016

在做好校园网络层面各项安全防护措施的基础上，建

议师生加强安全防护措施，降低被网络勒索病毒感染风险，避免因病毒感染造成不可挽回的损失。

Windows 个人主机和服务器的防护措施建议如下：

1）启用并打开“Windows 防火墙”，进入“高级设置”在入站规则里禁用“文件和打印机共享”相关规则；关闭 445、135、137、138、139 端口，关闭网络文件共享。

2)通过 Windows 系统补丁自动升级、微软公司 Windows 官方渠道（MS17-010 漏洞相关补丁升级包参见：https://technet.microsoft.com/zh-cn/library/security/MS17-010)、主要安全厂商安全客户端等，将 Windows 主机系统更新升级到最新状态。

如仍在使用 Windows XP、Windows 2003 等微软公司已停止支持的操作系统的用户，请参考如下微软公告进行补丁更新：

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

3）保持良好的网络使用习惯：

- 不随意打开不明来源的 Office 文档、可执行文件（特别是电子邮件附件文档）；
- 使用 Chrome、Firefox、360 安全等安全防护功能较好的浏览器；不打开来源不明的网络链接；
- 不下载、不安装来源不明的主机应用和移动应用。

特别的，建议对于有大量重要文档信息的个人主机和

服务器，经常性进行重要**文件备份**，并将备份介质**离线保存**（也就是将备份的硬盘断开与主机的 USB 等连接来存放）；停止使用 Windows XP、Windows 2003 等微软公司已不再提供安全更新的操作系统，及时升级操作系统补丁到最新。