关于最近爆发的勒索病毒，请大家在使用个人电脑时做好预防工作，具体方法如下：

1. 核对操作系统版本

若Windows7及以上操作版本系统，建议尽快安装微软官网布补丁MS17-010，该补丁修复了“永恒之蓝”攻击的系统漏洞。

\*补丁下载地址：

<https://technet.microsoft.com/zh-cn/library/security/MS17-010>

同时检查系统更新，将各种系统版本更新至最新。

若是XP等微软已不再提供安全更新的机器，可以安装反勒索防护软件。例如360“NSA武器库免疫工具” 下载地址：

<http://dl.360safe.com/nsa/nsatool.exe>；

注：此软件属于第三方软件。

2. 关闭445、135、137、138、139端口，关闭网络共享

关闭方法参考如下，供参考：

家庭普通版系统（无组策略）： <https://jingyan.baidu.com/article/0aa22375bf88b288cc0d6490.html>

专业版系统（有策略）: <http://blog.csdn.net/wangjialiang/article/details/7241875>

3. 强化网络安全意识

不明链接不要点击，不明文件不要下载，不明邮件不要打开；

4. 数据备份

定期将电脑中的重要文件备份资料到移动硬盘、U盘，备份完后脱机保存该存储介质；

5. 系统升级

建议仍在使用Windows XP， Windows 2003操作系统的用户尽快升级到 Window 7/Windows 10，或 Windows Server 2008/Windows Server 2012/Windows Server 2016操作系统并更新至最新版本。