**Petya勒索病毒注意事项和防范措施**

为协助全校师生共同防范Petya勒索病毒，信息中心现将注意事项和防范措施通告如下：

1. 安全操作提示
	1. 及时升级计算机操作系统到最新版本，并安装官方提供的最新补丁包；
	2. 安装升级防火墙和杀毒软件，确保病毒库更新，并及时扫描和查杀；
	3. 不打开来历不明的附件，尤其是rtf、doc等格式；
	4. 不访问不安全网站及不明链接；
	5. 及时做好文件备份，确保重要文件安全；
	6. 如果计算机已经感染了该病毒，请立即断开网络，并立即联系信息中心。

二、漏洞修复补丁MS17-010的安装方法

1、微软官方漏洞修复补丁

微软已发布了修复该病毒攻击的Windows系统漏洞补丁MS17-010。下载地址： [http://technet.microsoft.com/zh-cn/library/security/MS17-010](https://technet.microsoft.com/zh-cn/library/security/MS17-010)

2、第三方工具查杀和检测

对于不熟悉微软官方补丁修复方法的师生，可使用360“NSA武器库免疫工具”等第三方安全工具检测系统是否存在漏洞，并关闭受到漏洞影响的端口。

免疫工具下载地址<http://dl.360safe.com/nsa/nsatool.exe>

三、计算机系统安全设置

1、个人电脑：设置系统防火墙，并关闭TCP 135端口。

2、服务器：停止服务器的WMI服务。在服务器的开始-运行栏中输入SERVICES.MSC，找到页面中的WMI，双击后停止WMI服务。亦可在控制面板中点击管理工具，在管理工具中双击“服务”选项，然后完成WMI服务关闭操作。

信息中心

2017年6月30日