

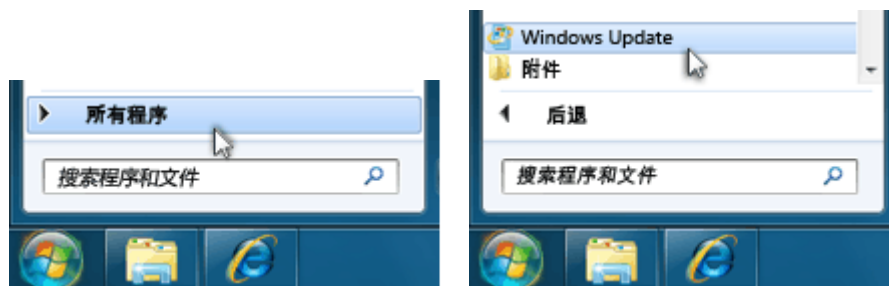
网络勒索病毒防范帮助手册

一、使用 Windows 系统自动更新功能更新补丁

使用 Windows 系统“开始”菜单检查更新：

Windows 更新包括在“控制面板”中。要检查更新，请执行下列操作：

➡单击“开始”按钮，单击“所有程序”，然后单击“Windows 更新”。



二、针对 MS17-010 漏洞的 Windows 系统安全补丁

微软已发布补丁 MS17-010 修复了该病毒攻击的 Windows 系统漏洞，请尽快安装，网址为：

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

提示：打开页面后按“Ctrl+F”，输入“MS17-010”，可迅速查询到相应补丁。



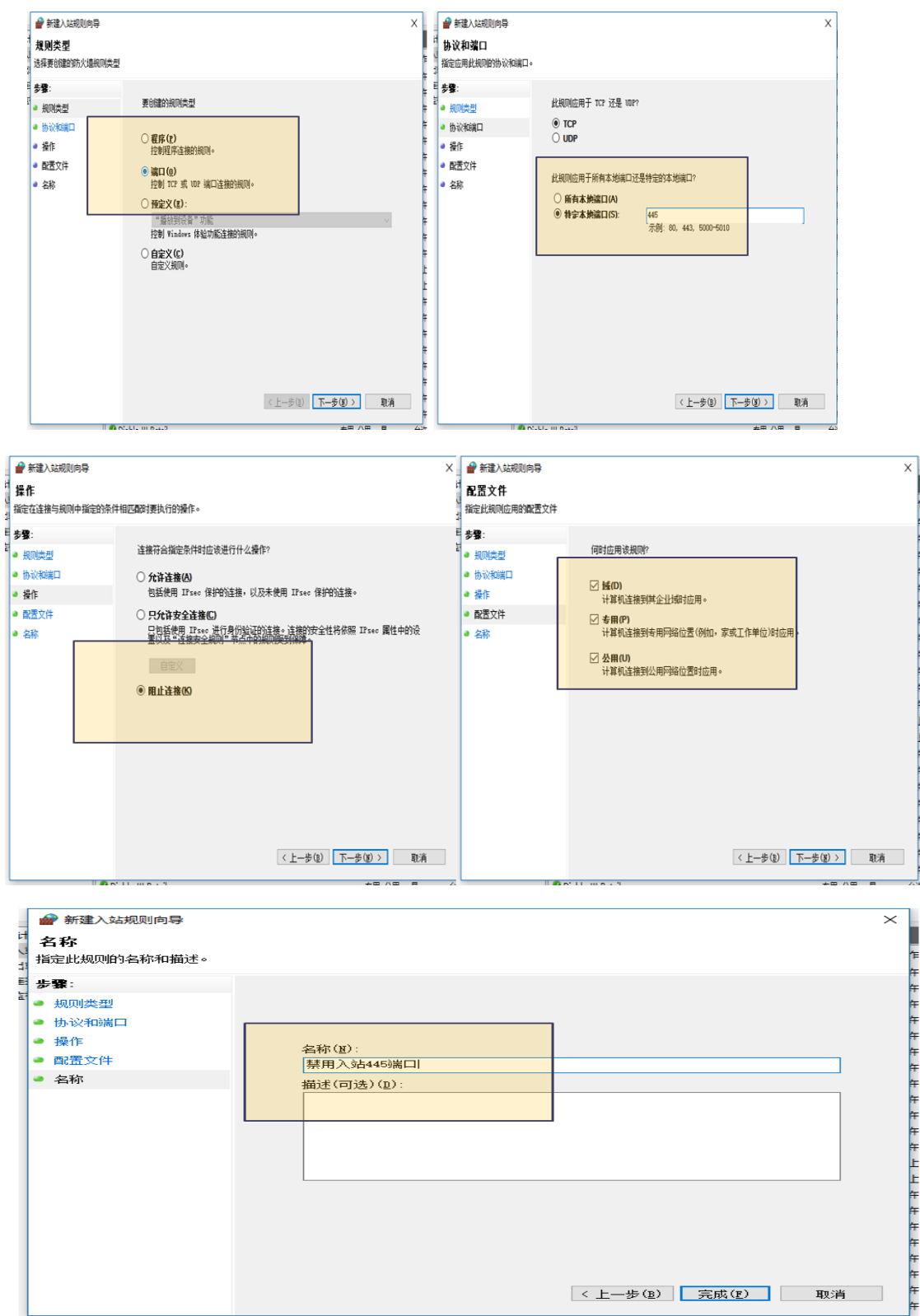
三、 个人电脑的系统防火墙设置（关闭个人电脑的相应端口）

提示:本文档以 Win10 操作系统为例说明以供师生参考,但因个人电脑的系统版本存在细节差异,师生参照本文操作时应酌情调整操作,如遇疑问请联系信息技术研究院（网络中心）具体咨询。

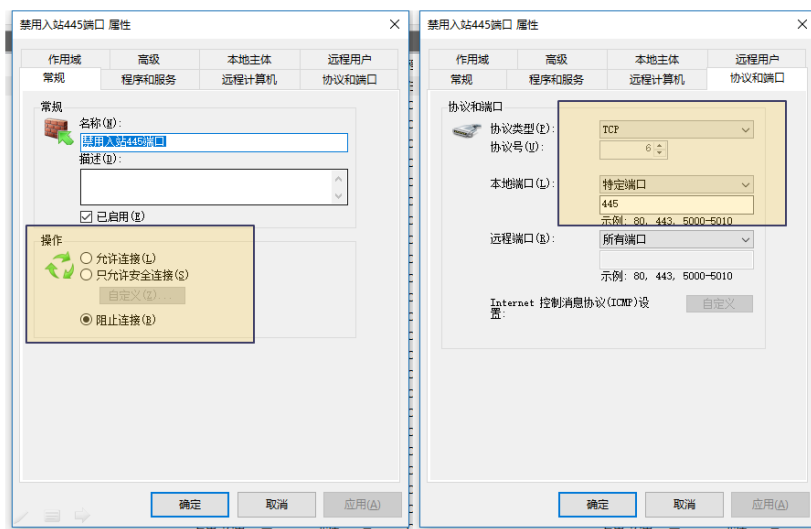
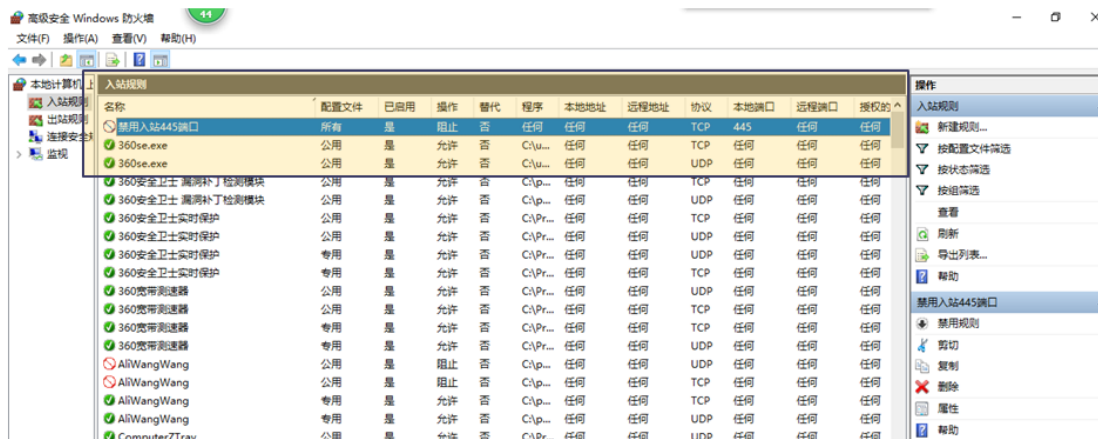
现在,开始关闭你电脑的 445、135、137、138、139 端口。按照以下步骤操作（以 445 端口操作为例,请按透明橙色标注框体的设置内容具体操作）:

在开始之前,请将电脑断网!

在电脑上查找系统自带的防火墙(路径在“控制面板”中)并设置为启用。



2、 核实关闭 445 端口访问的规则已经正确添加并且生效。



3、 还须关闭 135、137、138、139 端口，操作与上述关闭 445 相同。

综上所述，阻断网络的 TCP 445 、135、137、139、445 端口连接请求只是临时措施，尽快完成各类用户 Windows 系统软件的升级或修复漏洞才是防范该病毒的根本措施。

信息技术研究院
2017 年 5 月 15 日