计算机安全操作指引

（信息与设备管理处　2024 年 9 月发布）

一、计算机病毒防治

计算机病毒是目前计算机安全最大的威胁，能造成计算机系统运行缓慢、频繁重启或死机、程序无法启动、数据丢失或被盗、文件被勒索病毒加密、网络堵塞等各种危害。

病毒的分类主要有：引导区、文件、宏、脚本、蠕虫、木马病毒、勒索病毒等。

病毒的传播载体包括：网络电子文件、移动介质（如光盘、U 盘、移动硬盘等）。

病毒的传播途径有：可执行文件(exe/bat 等)、Office 文档（宏病毒）、电子邮件、非法网站、即时通信工具、网络共享等。

【预防方法】

以**预防**为主：

1.每台计算机都必须**安装杀毒软件**，并**每天定时更新、每周定期进行全盘扫描**。

2.不要轻易下载不明站点的软件或程序，如驱动人生、免费软件、破解软件、盗版软件、绿色软件等，**很多下载链接都是钓鱼网站**，非专业人士一般很难分辩。

3.不要浏览那些很诱惑人的小网站,或随便打开来路不明的 Email 中的链接、附件。

4.安装驱动、下载软件、下载文档等，尽量从官方网站提供的链接下载。

二、系统安全漏洞补丁更新

Windows 操作系统非常庞杂，难免存在许多程序漏洞，如果被病毒等恶意软件利用，容易导致计算机系统中毒，产生诸多安全风险与问题，需要更新“系统补丁”封堵漏洞。

【解决办法】

1.正版 Windows 系统可以通过设置,**开启自动更新,并至少每周安装一次更新补丁**。

2.通过杀毒软件、安全卫士自带的修复系统漏洞功能进行更新修复。

3.开启系统自带的 Windows 防火墙和 Windows Defender 防护程序。

三、计算机用户与弱口令问题

在计算机安全领域，口令（密码）是进入系统的第一道钥匙，如果钥匙太简单，就很容易被木马或黑客入侵，导致系统中毒，从而出现各种安全问题。

【解决办法】

1. 禁用系统自带的 guest 用户和其他非必要用户；

2. 修改超级用户的用户名（不要用 administrator 或 admin）

3. **设置强度较高的用户密码**（10 个字符以上，含大小写字母、字符和数字），**切忌设置空密码或弱口令**。

特别注意的是：部门公用电脑或服务器可能有24小时开机的需要，更容易成为黑客的目标而被木马病毒侵入，因此一定要设置强密码（至少每半年更换一次密码），并由专人管理，定时更新系统，定时杀毒，定时进行数据的脱机备份或在线异地备份。

四、硬盘数据安全

计算机中存储数据的部件主要为机械硬盘HDD或固态硬盘SSD，HDD使用寿命约为**五年**，SSD寿命更短，当硬盘开始出现如下异常时，应**及时备份数据并更换新硬盘**：(1)硬盘工作中经常出现怪异的不规则响声；(2)系统频繁死机、崩溃，文件出现乱码等；(3)对文件或文件夹进行操作时，速度非常缓慢。

【预防方法】

1.**硬盘至少5年更新一次，要重视数据的脱机备份**（比如定期拷贝到移动硬盘）。

2.硬盘的C盘易受病毒感染或自身故障导致数据丢失，重要文件**不要**存储在C盘。

3.建议部门配备NAS服务器或文档管理系统，对重要的数据文件进行归档和保存。

五、日常使用习惯

1.从校外或其他电脑用优盘拷贝文件到本机前，一定要**用杀毒软件对优盘进行扫描**，确保优盘和文件未中毒。

2.离开座位时，要按WIN徽标键+L键锁定电脑屏幕，防止他人使用你的电脑。

3.取消电脑中不必要的共享文件夹与远程桌面；

4.不随意浏览不明网站或未确认安全的网络链接，不打开陌生的电子邮件及附件。

5.下载软件一定要到官方网站下载，**不要通过百度搜索下载不明来源的软件**。

6.安装软件时，要一步一步按照流程操作，**看清安装提示**，对于非必要安装的选项不要选择安装，防止第三方恶意插件强制安装。

7.每天下班后切记要关闭电脑。