# 模块八 信息安全技术

## ——单元8.2 信息安全技术

# 目录

CONTENTS


01 导入案例

02 技术分析

03 知识与技能

04 案例实现

05 拓展阅读

06 练习与提高

# 导入案例：消失的硬盘

小蔡是一位刚从某职业技术学院港口物流专业毕业的学生，毕业后在一家港务企业工作，主要负责车辆的调度工作。不到一年时间，小蔡的计算机里面已经积累了出库通知单、转仓单、车辆调运单、在港物资提运单、矿单等大量工作数据。某日，小蔡和往日一样，打开计算机，准备继续记录这些单据。当他打开D盘时，发现什么文件都没有了。小蔡觉得很纳闷，他在学校学过信息技术基础课程，也在计算机上安装了360安全卫士，因担心360安全卫士不起作用，还安装了腾讯电脑管家，尽管小蔡做了很多安全防护工作，计算机还是出问题了。

# 导入案例：消失的硬盘

请帮助小蔡进行分析，他的计算机有哪些安全威胁，如果是新计算机，需要采取哪些安全措施来维护终端设备安全。如果是正在运行的计算机，又该采取哪些补救措施来维护终端设备安全。

# 技术分析

文件丢失一般有三种可能，一是人为删除或误操作，二是硬盘损坏，三是病毒所致。小蔡用的是自己专用计算机，可以排除人为删除或误操作导致的文件丢失。计算机只有一块硬盘，能启动系统并正常进入桌面环境，可以排除硬盘损坏问题，因此，小蔡计算机D盘的文件丢失，病毒所致是大概率事件。

# 技术分析

小蔡在计算机上安装了360安全卫士、腾讯电脑管家，仍感染了病毒，这是为什么呢？

首先，360安全卫士和腾讯电脑管家都是安全防护产品，主要防止木马、恶意程序等方面的威胁，不是杀毒软件。

其次，他们是同类产品，都在抢占系统底层资源，存在着冲突，不但不能加固系统，反而会降低防护作用。

第三，来自终端安全的安全威胁不只是木马和恶意程序，还有其他方面的威胁。

# 知识与技能

一、防范来自密码的安全威胁

二、防范来自计算机病毒的安全威胁

三、防范来自恶意软件的安全威胁

四、防范来自黑客的安全威胁

# 一、防范来自密码的安全威胁

## （一）密码引起的安全风险

如果因为密码设置较弱或密码使用不当，一旦被别有用心的人获取，他就可以拥有和你一样的权限。例如，一旦黑客掌握了操作系统密码，他就有机会远程登录系统，此时整台终端设备就有完全被掌控的可能。

# 一、防范来自密码的安全威胁

## （二）计算机的常见密码

### BIOS密码

BIOS密码是为计算机使用安全设置的开机密码，一般分为管理者密码和用户密码。默认情况下，这两项密码都没有设置。如果设置了管理者密码，进入CMOS设置就必须输入密码。如果设置了用户密码，开机就必须输入密码。

### 操作系统密码

指登录到系统桌面所需要的密码。对Windows 10之类的桌面操作系统而言，此密码就是系统登录密码。

### 应用程序密码

指进入应用程序所需要的密码，如QQ、微信 。

### 应用系统密码

随着目前，大多数应用系统都是基于B/S（浏览器/服务器）架构的应用系统。应用系统密码指的是登录这些系统所需要的密码。如需要查课表去登录教务系统时所需要的密码。

### 数据加密密码

指给数据进行加密，所设置的访问密码，例如，可以为需要加密的盘符启用BitLocker并设置访问密码，将需要加密的文件压缩后加密，为Word、Excel、Powerpoint的文件设置打开密码或只读密 码。

# 一、防范来自密码的安全威胁

## （三）暴力破解

暴力破解是指通过枚举方式，一个一个尝试认证。不同的应用有不同的暴力破解工具，如有针对压缩文件的，有针对PDF加密文档的，有针对Office加密文档的。随着计算性能的猛增，暴力破解成功的几率越来越大。对只有10位以内，密码字符只包含数字的简单密码，普通计算机，不到1秒就可能破解。一般暴力破解工具都支持将英文单词及常见字符组合列入字典，在字典辅助下，暴力破解更加容易。

# 一、防范来自密码的安全威胁

## （四）密码策略

要确保密码安全，除了保证设备环境安全外，需要设置强密码才能防止暴力破解。符合以下条件的密码才算强密码。

（1）不少于8个字符。

（2）应该包含大写字母、小写字母、数字、符号等4种类型中的3种。

（3）不能包含用户名中连续3个或3个以上字符。

（4）不能使用字典中包含的单词或只在单词后加简单的后缀。

# 一、防范来自密码的安全威胁

## （四）密码策略

要确保密码安全，除了保证设备环境安全外，需要设置强密码才能防止暴力破解。符合以下条件的密码才算强密码。

（5）避免使用与自己相关的信息作为密码，如家属、亲朋好友的名字、生日、电话号码等。

（6）避免顺序字符组合，如abcdef、defdef、a1b2c3。

（7）避免使用键盘临近字符组合，如1qaz@WSX、qwerty。

（8）避免使用特殊含义及其变形组合，如password、P@ssw0rd、5201314、5@01314。

## 二、防范来自计算机病毒的安全威胁

### （一）计算机病毒的概念

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性、破坏性等特点。

计算机病毒传播的途径非常广泛，凡是能交换数据的环境都可能传播病毒。例如，U盘上的病毒有可能传入计算机，计算机上的病毒也有可能传入U盘。

# 二、防范来自计算机病毒的安全威胁

## （二）计算机病毒的危害

任何病毒只要侵入系统，都会对系统及应用程序产生程度不同的影响。轻则会降低计算机工作效率，占用系统资源，重则可导致数据丢失、系统崩溃。例如勒索病毒，它会对文件进行加密，用户想要解密这些文件，必须支付费用来拿到解密的私钥。

# 二、防范来自计算机病毒的安全威胁

## （三）计算机病毒的防治措施

### 1. 确保系统安全

系统安全是预防病毒的关键所在。病毒侵入计算机后，第一要务就是抢占系统资源并劫持系统。如果系统已经被病毒劫持，很难彻底根除。尽管市面不少杀毒软件称自己能查毒杀毒，作用其实是有限的。

# 二、防范来自计算机病毒的安全威胁

## （三）计算机病毒的防治措施

### 1. 确保系统安全

可以通过以下途径确保系统安全。

（1）新计算机需要安装系统时，应确保系统来源安全。

风险举例：大家都喜欢安装简单便捷的Ghost版系统，殊不知，多数Ghost版系统都已经植入了病毒或其他恶意程序。

# 二、防范来自计算机病毒的安全威胁

（三）计算机病毒的防治措施

1. 确保系统安全

可以通过以下途径确保系统安全。

（2）在未配置安全防护前应断开网络。

风险举例：假如计算机所在网络环境中，已有终端被病毒感染，在安装操作系统过程中，病毒可能已经通过网络侵入该计算机。

（3）在未配置安全防护前应拔出所有可移动设备。

风险举例：假如计算机上插着带毒的U盘，在计算机启动过程中，病毒可能已经侵入计算机。

# 二、防范来自计算机病毒的安全威胁

## （三）计算机病毒的防治措施

### 2. 安装或启用防病毒软件

在本单元的导入案例中，小蔡安装的360安全卫士或腾讯电脑管家都不是防病毒软件，不能起到查杀病毒及系统监控作用。可以使用Windows 10自带防病毒软件Windows Defender或安装第三方的防病毒软件，如360 杀毒、火绒等。无论采用哪款防病毒软件，都必须开启自动防护功能。

# 二、防范来自计算机病毒的安全威胁

（三）计算机病毒的防治措施

3. 防止病毒优先抢占系统资源

病毒想要入侵计算机，必须先抢占系统资源，在确保系统干净且有防病毒软件保护的情况下，病毒可以通过以下两个过程抢占系统资源。

（1）启动过程

入侵机制：如果启动计算机时插着带毒的U盘，计算机启动时，可能先从带毒U盘启动，然后防病毒软件再启动，已无法拦截病毒，病毒可能因此侵入计算机。

预防措施：将计算机启动顺序设置为当前磁盘优先或只允许当前磁盘启动。

# 二、防范来自计算机病毒的安全威胁

（三）计算机病毒的防治措施

3. 防止病毒优先抢占系统资源

（2）放入移动存储介质过程

入侵机制：根据Windows的自动播放机制，当插入新的设备时，会启动“自动播放”服务，自动搜索并安装所插入设备的驱动，根据需要自动打开设备内容。病毒正是利用此服务，利用此机制优先于防病毒软件抢占系统资源，从而达到入侵系统的目的。

预防措施：一是通过组策略关闭“自动播放”，二是禁用“自动播放”服务。

# 二、防范来自计算机病毒的安全威胁

## （三）计算机病毒的防治措施

### 4. 管理维护防病毒软件

不少终端设备在已有防病毒产品的情况下仍被病毒感染，主要原因是没有管理维护好防病毒产品。

（1）确保防病毒产品处于实时保护状态。

要经常检查防病毒软件是否处于实时保护状态，如果关闭了实时保护，需要立即开启，否则会给病毒入侵之机。尤其在重启计算机、安装软件等关键时刻之后，要立即检查防病毒产品的运行状态。

# 二、防范来自计算机病毒的安全威胁

（三）计算机病毒的防治措施

4. 管理维护防病毒软件

（2）坚持先查杀后使用原则。

无论是从互联网下载的文件还是从U盘等移动存储介质复制来的文件，或是通过聊天工具传送的文件，都应用防病毒软件查杀之后再使用。如果文件是压缩包，需要解压后再查杀。如果查出风险，不能为了使用需求关闭或退出防病毒软件。

# 二、防范来自计算机病毒的安全威胁

（三）计算机病毒的防治措施

4. 管理维护防病毒软件

（3）及时更新防病毒软件。

尽管防病毒软件都提供了自动更新功能，经常手动更新防病毒软件仍然必要。更新内容包括更新杀毒引擎和病毒定义文件。

# 三、防范来自恶意软件的安全威胁

## （一）恶意软件的定义

恶意软件是基于软件预期定义的，凡是对个人或单位存在恶意的，对计算机、服务器或网络造成损害的软件都可以称为恶意软件。因为不少恶意软件具有“强制安装”“难以卸载”“浏览器劫持”“广告弹出”“恶意收集用户信息”“恶意卸载”“恶意捆绑”“恶意安装”等特征，一般把恶意软件称为流氓软件。

# 三、防范来自恶意软件的安全威胁

## （一）恶意软件的定义

### 1. 蠕虫

蠕虫是一种自我复制能力极强的恶意软件，蠕虫的破坏性在于它具备不需要用户操作就能够进行自我复制并传播的特征。如SQL Slammer蠕虫，它利用了微软SQL数据库的一个漏洞，在其连接到网络之后，大约十分钟之后，网络上所有存在该漏洞的SQL数据库服务器都会出现缓冲区溢出的问题。

# 三、防范来自恶意软件的安全威胁

## （一）恶意软件的定义

### 2. 木马

木马是一种将自己伪装成合法应用程序的恶意软件，诱骗用户点击，木马一旦被用户激活就可能会控制用户计算机。如今，木马已成为黑客的首选工具，如Bots木马，黑客可以利用它在被感染计算机上任意妄为，包括偷窃数据、利用受感染机器继续攻击其他计算机等。

### 3. 勒索软件

勒索软件是一种通过加密用户重要数据达到劫持用户的恶意软件，多数勒索软件都是由木马演变而来。

# 三、防范来自恶意软件的安全威胁

## （一）恶意软件的定义

### 4. 间谍软件

间谍软件是一种秘密收集用户数据的恶意软件。不少间谍软件会记录用户键盘和鼠标行为，从而获取密码或其他重要数据。

### 5. 恶意广告

恶意广告是一种借助合法的广告页面（或软件）暗中嵌入或暗中发放信息的恶意软件。犯罪分子在广告页面嵌入恶意软件，等待用户点击。用户一旦点击则会自动安装、自动执行。

# 三、防范来自恶意软件的安全威胁

## （二）恶意软件的防范

**采取病毒防治措施**

有的恶意软件本身就是病毒，因此，要采取防范病毒一样的措施。

**安装安全防护产品**

很多恶意软件都不是病毒，它和正常软件一样，没有病毒码，防病毒软件可能检测不到它。此时可以安装安全防护产品。在同一个系统中，不要安装多个类似产品。

**及时修补漏洞**

恶意软件之所以能大行其道，漏洞是主因。无论是操作系统还是应用软件，都可能存在漏洞，这些漏洞一旦被发现，都可能被黑客利用并注入病毒或恶意软件。因此，要及时修补漏洞。

# 四、防范来自黑客的安全威胁

## （一）黑客

黑客泛指擅长IT技术的计算机高手。站在网络安全角度，黑客是指善于发现计算机系统和网络缺陷和漏洞的人。

# 四、防范来自黑客的安全威胁

## （二）黑客的安全威胁

与病毒、恶意软件相比，黑客的安全威胁更大。黑客不仅可以利用病毒、恶意软件之类的工具来进行常规攻击，还可以利用计算机和网络原理，收集网络系统中的信息，探测目标网络系统的安全漏洞，建立模拟环境，进行模拟攻击，最后实施网络攻击。

# 四、防范来自黑客的安全威胁

## （三）防火墙

防火墙原指在寓所之间所砌的砖墙，一旦火灾发生，可以防止火势蔓延到别的寓所。在计算机领域，防火墙是指在网络之间插入的一个中介系统，用于阻断外部网络对本网络的威胁和入侵。

随着防火墙技术的不断发展，功能越来越强大，在防范恶意软件方面的作用越来越明显。防病毒软件是从代码角度监控和查杀病毒，防火墙则是从数据通信角度拦截恶意软件和黑客的非法访问。二者有效结合才能真正保证计算机系统安全。

防火墙作为一种中介系统，有硬件防火墙、软件防火墙、软硬结合的防火墙等存在形式。

# 四、防范来自黑客的安全威胁

## （四）防范黑客攻击

防范黑客攻击最有效的手段就是防火墙，一般操作系统都自带软件防火墙。为防范黑客攻击，应经常关注防火墙工作状态，确保防火墙时刻处于启用状态。同时根据需要设置防火墙规则，关闭所有不使用的端口。

# 案例实现

1. 清除硬盘安全风险

小蔡的计算机系统可能已被“病毒”劫持，尽管许多反病毒软件号称自己具备“带毒杀毒”功能，但仍有安全风险。要彻底清除现有硬盘的安全风险，有以下两种途径可供选择。

（1）拆卸现有的硬盘，将硬盘挂接到一台干净且安装反病毒软件的计算机上，然后对挂接的硬盘进行全盘扫描，清除硬盘中存在的安全风险。

# 案例实现

## 1. 清除硬盘安全风险

### （2）360急救盘方案。

1. 找一台干净的计算机。
2. 进入360官网下载360急救盘。
3. 运行下载的360急救盘，插入一块空白U盘，按照提示将360急救系统写入U盘。
4. 用制作好的360急救盘启动带有病毒的计算机。
5. 登录到系统桌面，打开360系统急救箱后，钩选“强力模式”和“全面扫描”，然后单击“开始急救”即可按最严的扫描规则扫描整台计算机，彻底清除硬盘中的安全风险。

# 案例实现

2. 卸载不必要软件

清除硬盘安全风险后，计算机暂时没有风险。此时可以重启计算机，然后卸载所有不需要的软件。小蔡计算机上同时有360安全卫士和腾讯电脑管家，可以保留其中一个。

# 案例实现

## 3. 关闭自动播放

1. 进入组策略管理控制台，分别在“计算机配置”和“用户配置”里面设置自动播放策略，尤其需要关闭所有驱动器的自动播放功能。

2. 进入服务管理控制台，禁用“为自动播放硬件事件提供通知”的服务“Shell Hardware Detection”。

## 4. 管理维护反病毒软件

1. 进入Windows安全中心，检查Windows自带的防病毒软件“Microsoft Defender”，确保“实时保护”和“篡改防护”处于开启状态。

2. 手动进行病毒和威胁防护更新。

# 案例实现

5. 管理维护防火墙

进入Windows安全中心，检查防火墙和网络保护是否打开。检查时需注意，Windows定义了域网络、专用网络和公用网络，要确保这三类网络的防火墙都是打开状态。

6. 修补漏洞

对Windows 10操作系统而言，可以通过维护系统模块来修补漏洞。

Windows默认设置是每日凌晨两点自动维护系统，维护过程中执行的任务包括软件更新、安全扫描和系统诊断等。

# 案例实现

7. 修改计算机启动顺序

开机后进入CMOS设置，修改计算机启动顺序，将本地硬盘设置为第1个启动设备。如果允许禁用其他启动设备，则禁用其他设备。

8. 设置开机密码

进入BIOS，设置开机密码。

# 案例实现

9. 管理维护本地用户

经常进入本地用户和组管理页面，进行以下管理维护操作。

1. 查看用户列表，只保留自己登录的用户账户，禁用其他用户账户。
2. 如果当前用户账户是“Administrator”（超级管理员），需要新建一个用户账户，并将新用户账户放进“Administrators”（超级管理员用户组）。然后禁用“Administrator”。
3. 将当前用户设置为强密码。

# 拓展阅读

1. 数据备份

大型单位一般都有信息管理系统，用于线上办公，其系统和数据都有可靠的备份措施。这里只介绍个人计算机的数据备份措施。目前多数用户都和小蔡一样，没有养成数据备份的习惯，或采用的数据存储方式不科学。

（1）移动硬盘或U盘备份数据（不推荐）

人们习惯使用移动硬盘或U盘备份数据，事实上，移动硬盘或U盘损坏几率可能比本地硬盘还大。如果随时携带、使用移动硬盘或U盘，数据安全风险更高。

# 拓展阅读

1. 数据备份

（2）使用光盘备份

使用光盘备份数据，具有数据不被篡改的优点，如果保护得当可以长期存放。其缺陷之一是每张光盘容量有限，因此，用光盘备份前，需要根据光盘容量组织文件。用光盘备份另一个缺陷就是存放不当，容易丢失和变形。

# 拓展阅读

1. 数据备份

（3）使用云存储备份

可以在百度网盘、腾讯微云等地申请云存储空间，这些云存储空间提供商无论在网络安全还是在物理存储安全方面，都能让你的数据存储安全得到保证，因此，将数据存放到云存储是不错的选择。其缺陷是免费云存储在空间和速度上都有限 制。

# 拓展阅读

1. 数据备份

（4）使用NAS（network attached storage，网络附属存储）存储备份

小企业或家庭可以单独购买NAS存储备份数据，其缺陷是只能在企业内部或家庭内部访问。

# 拓展阅读

2. 数据恢复

如果数据有备份，可以直接用备份数据来恢复损坏或丢失的数据。如果像本单元导入案例中的小蔡一样，事前没有进行数据备份，则需要使用第三方数据恢复工具恢复，常用的数据恢复工具包括DiskGenius、EasyRecovery、R-Studio、Ease US Data Recovery、Disk Drill等。

# 拓展阅读

3. 数据加密

在日常应用中，如果不使用第三方加密工具，仍有办法对重要数据进行加密。

（1）用BitLoker加密整个分区

Windows自带的BitLocker是一款驱动器加密工具。每次启动操作系统后，首次访问必须输入密码才能访问用BitLocker加密的分区。如果使用BitLocker加密，以后计算机出现丢失或被盗，则不用担心数据泄漏。

# 拓展阅读

3. 数据加密

（2）压缩加密

BitLocker不能单独对指定文件夹或文件加密，如果计算机上已安装通用的压缩解压缩软件“WinRAR”，可以将欲加密的文档压缩成压缩包，然后对压缩包设置解压密码。

（3）Office文档加密

Microsoft Office是一套办公套件，Word、Excel和PowerPoint是该办公套件中最常用的三款软件。用Microsoft Office打开的文档都可以设置文档打开密码和文件修改密码。

# 拓展阅读

3. 数据加密

（4）PDF加密

PDF是一种电子文件格式，具有可移植性，无论是Windows、Unix、Linux、Mac OS或安卓操作系统，都支持PDF文档。流行的PDF编辑工具是Adobe Acrobat、Foxit Phantom，这两款工具都可以对PDF文档进行加密。

注：目前比较流行的做法是将Word文档另存为PDF，可以在另存过程中设置PDF文档密码。

# 练习与提高

1. 今年，小明考上了大学，家里从电脑城给他买了一台笔记本。笔记本随机安装的不是Windows操作系统，电脑城的店员给他装的是Ghost版Windows 10，还告诉他，常用的Office、QQ、微信等软件都有了。学习完本单元后，小明不放心了，想对自己的计算机做一个全面的信息安全维护，如果你是小明，该如何进行维护？

2. 小琼的计算机已安装360杀毒和360安全卫士，自上周闺蜜用U盘给她拷贝了一段舞蹈学习视频后，她的计算机变慢了不少，还总报错。请你帮小琼找出计算机变慢、报错的原因，从安全角度帮她优化系统。

# 练习与提高

3. 小兵学的是跨境电商专业，本学期要学习Photoshop课程，他要从老师那里复制软件、素材和学习视频，U盘剩余空间不够，当时他比较着急，就把U盘格式化了，格式化后才想起里面有好多珍贵照片。请你帮小兵找回这些照片。