



计算机感染典型 病毒的现象

2024-12-20



目录 CONTENTS

CATALOGUE

01 计算机病毒概述

04 预防计算机病毒的方法

02 计算机感染病毒的现象

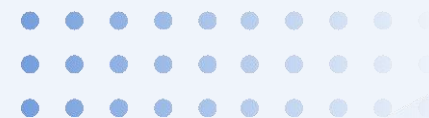
05 计算机病毒的防范策略

03 常见计算机病毒类型

06 计算机中毒后的应急处理

01

计算机病毒概述



计算机病毒的定义



计算机病毒是一种具有破坏性的程序，能够在计算机系统中自我复制和传播。

病毒通常通过依附在其他程序上，当这些程序被执行时，病毒就会被激活并开始破坏计算机系统。



计算机病毒的危害

破坏数据

病毒会破坏计算机中的数据，导致数据丢失或无法访问。

窃取信息

病毒能够窃取计算机中的敏感信息，如密码、个人信息等，导致隐私泄露。



破坏系统

病毒会破坏计算机系统的正常运行，导致系统崩溃或无法正常工作。

占用资源

病毒会占用计算机的资源，导致计算机运行缓慢或出现其他异常现象。



计算机病毒的传播途径

01

通过网络传播

病毒可以通过互联网或局域网进行传播，如通过电子邮件、下载文件等方式。

02

通过移动存储设备传播

病毒可以通过移动存储设备如U盘、移动硬盘等进行传播。

03

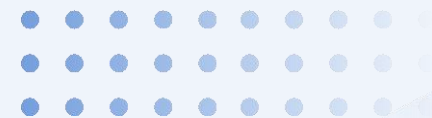
通过光盘传播

一些病毒可以通过光盘进行传播，如盗版光盘或未经授权的软件光盘。

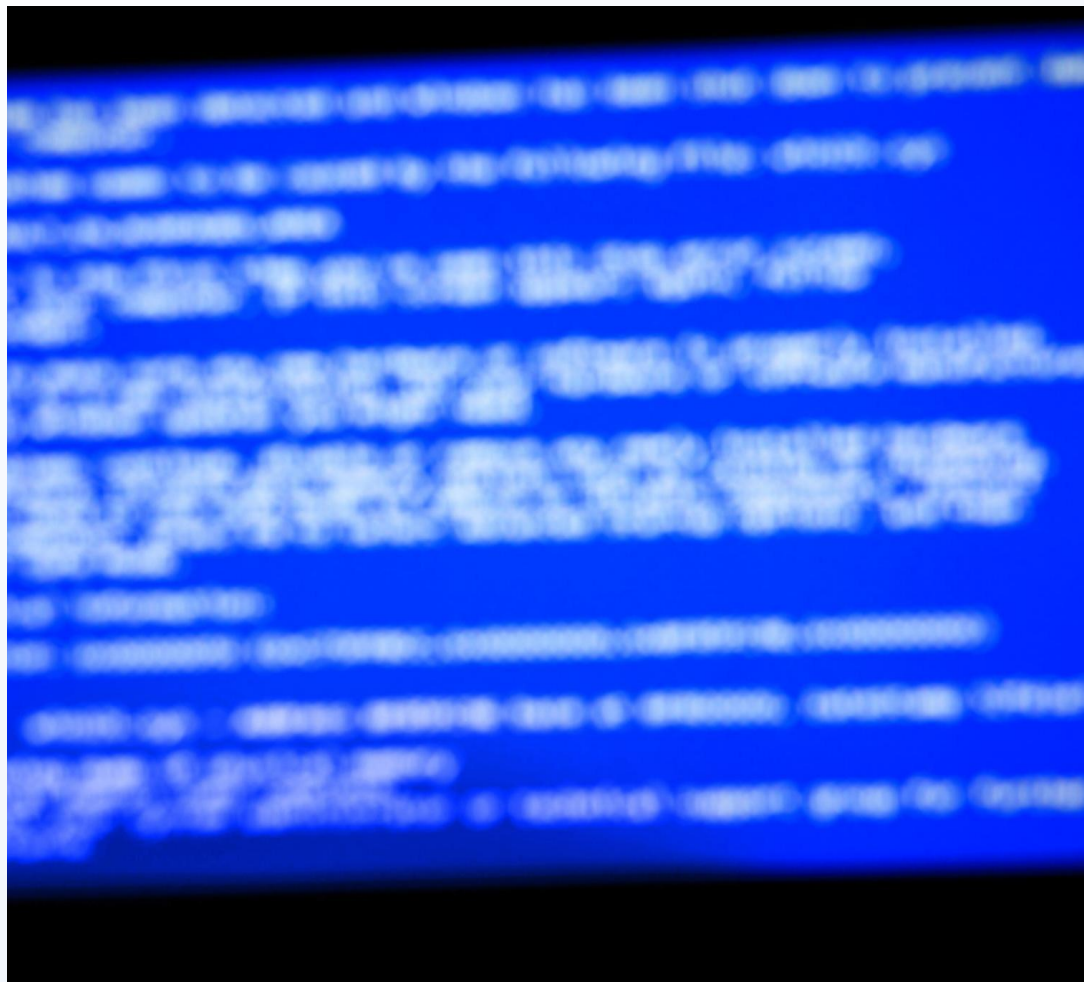


02

计算机感染病毒的现象



计算机运行异常



系统运行缓慢

计算机感染病毒后，病毒会占用系统资源，导致计算机运行速度明显变慢。

频繁重启或死机

病毒可能会破坏系统文件，导致计算机频繁重启或死机。

应用程序异常

病毒可能导致应用程序无法正常运行，出现错误提示或崩溃。



文件或数据异常



文件丢失或损坏

病毒可能会删除或损坏计算机中的文件，导致数据丢失或无法正常访问。



文件属性变化

病毒可能会更改文件的属性，如隐藏、只读等，使得文件无法正常使用。



数据篡改

病毒可能篡改计算机中的数据，导致数据不准确或无法正常使用。



弹出窗口或广告增多

弹出广告窗口

病毒可能会弹出广告窗口，干扰用户正常使用计算机。



浏览器主页被篡改

病毒可能会篡改浏览器主页，导致用户每次打开浏览器都跳转到其他页面。

恶意插件或工具栏

病毒可能会安装恶意插件或工具栏，窃取用户信息或干扰用户操作。



03

常见计算机病毒类型



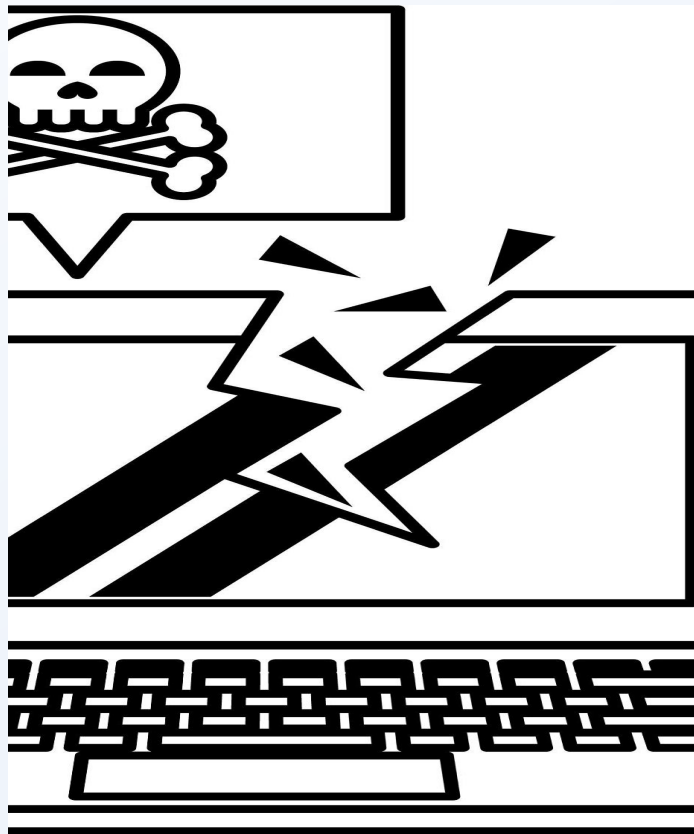
木马病毒

非法远程控制

木马病毒常被黑客用于远程控制计算机，窃取用户数据或执行恶意操作。

窃取信息

木马病毒可以窃取用户的个人信息，如密码、银行账户等，造成严重隐私泄露。



破坏系统

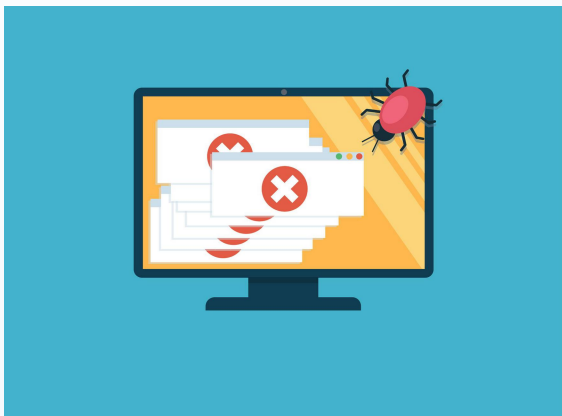
木马病毒可能破坏系统文件，导致计算机运行不稳定或崩溃。

耗费资源

木马病毒在后台运行，占用系统资源，导致计算机性能下降。



蠕虫病毒



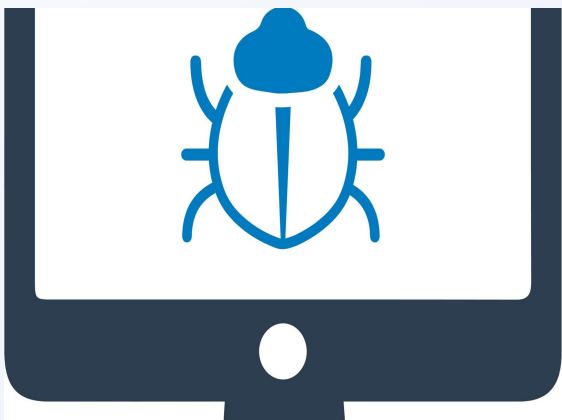
传播速度快

蠕虫病毒利用系统漏洞或网络共享进行传播，感染速度非常快。



破坏性强

蠕虫病毒可能删除文件、破坏系统或导致网络瘫痪，造成严重损失。



难以清除

蠕虫病毒在系统中往往有自我复制和传播的能力，难以完全清除。



潜伏期长

蠕虫病毒可能长期潜伏在系统中，不易被发现，随时可能爆发。



勒索病毒



加密文件

勒索病毒会加密用户的重要文件，使其无法正常使用。

勒索赎金

加密文件后，勒索病毒会显示勒索信息，要求用户支付赎金以解密文件。

破坏系统

如果拒绝支付赎金，勒索病毒可能会破坏系统或删除文件，造成严重后果。

难以解密

勒索病毒使用的加密技术往往比较高级，一般用户难以自行解密。

03

预防计算机病毒的方法



安装杀毒软件

01

杀毒软件的作用

杀毒软件可以检测和清除计算机中的病毒，防止病毒对计算机系统进行破坏。

02

杀毒软件的选择

选择正版、专业的杀毒软件，并定期更新病毒库，以确保对最新病毒的防范能力。

03

杀毒软件的实时防护

开启杀毒软件的实时防护功能，可以及时发现并处理计算机中的病毒。



不打开未知来源的文件



● 未知文件的风险

不要随意打开来自未知来源的文件，特别是通过邮件、聊天工具等途径传送的文件，以免感染病毒。

● 文件来源的确认

在打开文件之前，要确认文件的来源是否可靠，并查看文件的扩展名是否安全。

● 文件的安全处理

如果确需打开未知文件，建议先使用杀毒软件进行扫描，确认安全后再打开。



定期进行系统升级



系统升级的意义

系统升级可以修复系统漏洞，提高系统的安全性，防止病毒利用漏洞进行攻击。



系统升级的时机

定期进行系统升级，及时安装最新的安全补丁和更新程序，确保系统的安全性。



系统升级的方法

可以通过系统设置或专业升级工具进行系统升级，升级前建议备份重要数据以防丢失。



04

计算机病毒的防范策略



建立正确的安全意识

强调网络安全的重要性

加强安全意识培训，提高员工对网络安全的重视程度。

养成良好的上网习惯

不打开可疑邮件、不下载未知来源的软件或文件。

定期备份重要数据

以防病毒感染导致数据丢失或损坏。



学习计算机病毒相关知识

● 了解病毒的定义和类型

明确病毒是一种能够破坏计算机系统和数据的恶意程序。

● 掌握病毒的传播途径

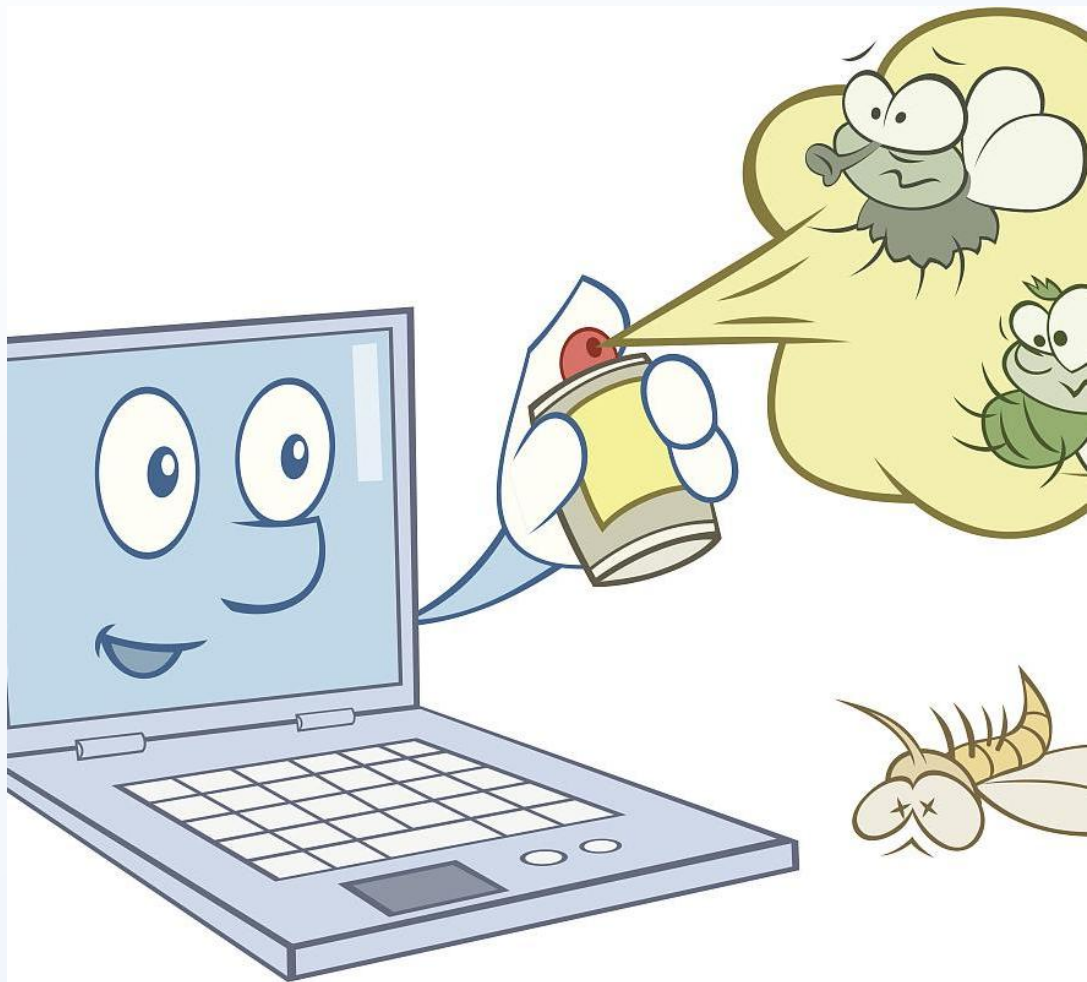
了解病毒通过哪些途径传播，如网络、移动存储设备、电子邮件等。

● 识别病毒感染的症状

学会识别计算机感染病毒后的异常症状，如系统运行缓慢、文件丢失等。



制定防病毒计划



安装杀毒软件

选择一款可靠的杀毒软件，并定期更新病毒库。

定期扫描系统

对计算机系统进行全面扫描，及时发现并清除潜在病毒。

启用防火墙

设置防火墙规则，阻止外部攻击和恶意软件的入侵。



05

计算机中毒后的应急处理



立即断网并杀毒



断开网络连接

立即断开与网络的连接，防止病毒进一步传播。



启用杀毒软件

启动计算机上安装的杀毒软件，对全盘进行扫描和清除病毒。



更新病毒库

确保杀毒软件病毒库为最新版本，以便能够识别和清除最新病毒。



备份重要数据

备份文件

将重要文件复制到移动存储设备或网络存储空间，以防数据丢失。



备份系统

创建系统备份，以便在需要时恢复系统到中毒前的状态。

验证备份

确保备份数据能够正常打开和使用，避免因备份损坏而导致数据无法恢复。



寻求专业帮助

联系技术支持

如果自己无法解决病毒问题，可以联系计算机技术支持或专业杀毒软件厂商寻求帮助。

寻求专家建议

对于复杂的病毒问题，可以向计算机安全专家或反病毒机构寻求帮助，获取专业建议和支持。

