教你如何防治Access宏病毒的通用技巧 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/245/2021_2022__E6_95_99_E4_BD_A0_E5_A6_82_E4_c97_245689.htm 本文从技巧到解决方案来逐步介绍利用Access的安全特性及良好习惯防治Access宏病毒的技巧。 防病毒通用技巧 保持防病毒软件随时更新非常重要。新病毒每天出现，防病毒厂商也通过网络、BBS等载体不断推出最新的病毒资料库和软件，所以一个重视安全的用户，应当保证一个合适的频率不断更新自己的防病毒软件，不与不可靠的人或系统共享数据库，不从网络上下载或使用来历不明的Access数据库，是有效防治Access病毒的方法。 微软未来的解决方案 熟悉Word 97、office/9.shtml ’ target= ’_blank ’ class= ’ article ’ >Excel 97的用户都知道，在打开一个含有宏的文档或工作簿时，Word和Excel都会提示：“ 该文件中包含宏，是否运行宏 ”。这是因为在95版的软件中开始大量出现宏病毒，所以在97版中增加了这一报警功能。Access病毒以前一直没有出现过，Access 97中就没有提供这一功能，微软将在新版Access中提供这一功能。 使用Access安全特性预防病毒 数据库安全有两个选项：数据库密码保护、用户级安全性。 1．数据库密码保护： 可给数据库加上密码，步骤如下：（1）以独占方式打开数据库。（2）在“ 工具 ”选单中选择“ 安全 ”，然后选择“ 设置数据库密码 ”。（3）输入并校验密码。 此后，要打开数据库，必须输入正确的密码。而病毒要想感染一个加了密码保护的数据库，Access的安全特性就会提示用户输入密码，警觉的用户此时就会察觉这是异常操作，在口令输入对话框中选择“ 取消 ”就不会打开数

据库，从而防止了病毒感染。 2．用户级安全性：使用用户级安全性可给不同组的用户赋予不同的权限。操作方法如下：（1）使用“ 工作组管理员 ”程序创建并连接一个工作组文件。该程序一般位于\Program Files\Microsoft Office目录中，快捷方式名为“ MS Access Workgroup Administrator ”。 （2）新建一个用户，把该用户加到管理员组中。 （3）从管理员组中移去管理员账号。 （4）给新建的管理员组中的用户分配密码，强制他登录时必须使用密码。 （5）重启Access，以这个新管理员用户身份登录。 （6）运行“ 用户级安全性向导 ”，新建一个数据库，并把所有的对象都拷贝到新数据库中。 现在，你就拥有了一个具有安全防护的数据库。可以通过安全对话框向其中增加用户和组，分配适当的权限。此后，如果从网络上下载了可能含毒的数据库，可以使用默认工作组文件打开这个数据库，即使真的有毒，含毒数据库中的病毒也没有足够的权限感染加了安全防护的数据库。 100Test下载频道开通，各类考试题目直接下载。详细请访问www.100test.com