请注意：这样使用光盘就会泄密！

原创：郝耀鸿保密观7 月 4 日

光盘作为一种容量大、易携带、性价比较高的存储介质，已成为保密工作者的得力助手，但如果不谨慎使用，依然有较高的泄密风险，您了解吗？

丢失泄密

有的单位为了防止移动硬盘、U 盘等携带病毒感染计算机系统造成泄密，规定只能用光盘充当涉密计算机、内网计算机与外界进行数据传输和交换的载体，光盘也因体积小、重量轻、使用方便等受到了大家的欢迎。

但与此同时，不少人却忽视了它小巧、易丢失的特性。再加上很多光盘及其中的信息都未经过加密处理，一旦丢失，无异于拱手送密。

光盘病毒

光盘虽然不会像 U 盘那样被病毒传染，但在刻录过程中也存在风险，尤其是盗版光盘，厂家技术力量薄弱，疏于管理，会将携带病毒的文件刻录到光盘中，从而感染读取光盘的计算机主机，并通过网络扩散，造成严重危害。

例如，1998 年 6 月爆发的 CIH 病毒，就是以盗版光盘游戏“古墓奇兵”为媒介，严重破坏计算机硬件结构。据统计，CIH 病毒共造成全球 6000 万台电脑瘫痪，经济损失高达 5 亿美元。

摆渡木马

“摆渡”原指在河两岸来回运送人员、物资的行为，而在这里，光盘则成为木马窃取内网或涉密计算机信息 ,输送到外网的一种媒介。

用户通过互联网下载软件时，可能会被木马恶意捆绑，一并刻录到光盘中。当光盘在内网或涉密计算机上运行时，木马就会自动下载到本地，伪装成重要系统文件或潜伏在后台，收集涉密或敏感信息。当再次有刻录行为发生时，这些信息便随被刻录的文件一同存储到新的光盘中，如果新的光盘被插入连接互联网的计算机，木马就会伺机将窃取的信息传输给窃密者。

可见，在安全保密领域，光盘并不能完全“免疫”，我们必须提高警惕，规范使用操作。

使用管理要严格

光盘要统一规范采购，明确使用范围，注明涉密光盘和非涉密光盘。在使用过程中，必须严守保密规定、严格刻录审核，有效管控使用过的光盘，安全存储、及时销毁，防止国家秘密或敏感信息泄露。

杀毒检查常态化

在光盘刻录前，必须对文件或程序例行杀毒查验；光盘插入计算机读取信息前，也要先查杀病毒，再安装使用；每次使用时，还须遵守“一次一用”原则，做好记录。

清除木马有窍门

由于光盘内容不可改写，杀毒软件发现木马病毒后，有可能只报警而无法查杀。遇到这种情况，可将带有病毒的文件或程序拷贝到中间机上，用杀毒软件清除干净，再重新刻盘后在内网或涉密机上读取

操作。

数据加密上保险

在光盘使用时可引入加密策略，包括基于光盘本身的硬件加密和针对光盘内容的软件加密。前者速度快、效果好，但成本较高；后者成本低、使用便捷，不少第三方刻录软件就能提供加密功能，这两种方式可在工作中酌情使用。

小贴士

光盘的日常保养

取放：要抓住两侧、轻拿轻放，防止沾染灰尘、划伤盘面。

存放：最好放入封套或盘盒内，临时放置要光面朝上，以免划伤；光盘要置于通风干燥处，注意不要过热，如阳光暴晒，以防盘面变形，数据无法读取。

清洁：光盘表面出现霉点或污渍，切忌用酒精、汽油等有机溶剂擦拭，可以用清水冲洗，然后用软布擦干（不要沿纹路旋转擦拭，以免损坏盘面），也可用专用清洁剂清洁。

工作环境：光盘信息轨道间距很小，光驱尽量不要在不稳定的环境下（震动、冲击、摇晃等）工作，否则会出现卡顿、跳跃等，严重影响激光头读取数据。