**2018国家网络安全宣传周系列动漫③ 个人电脑安全篇**

电脑已经成为人们日常重要的工具之一，但电脑安全防护意识却在大众心目中并不完善，再之，信息安全系统的不完善，很容易成为黑客的攻击目标。

无论是企业，还是个人电脑安全防护，都与人们的很多信息和私有财产有着密不可分的关系，面对互联网的复杂形势，如何防护好电脑数据安全？以下这些漫画场景不妨仔细看看……

* 文件加密存储

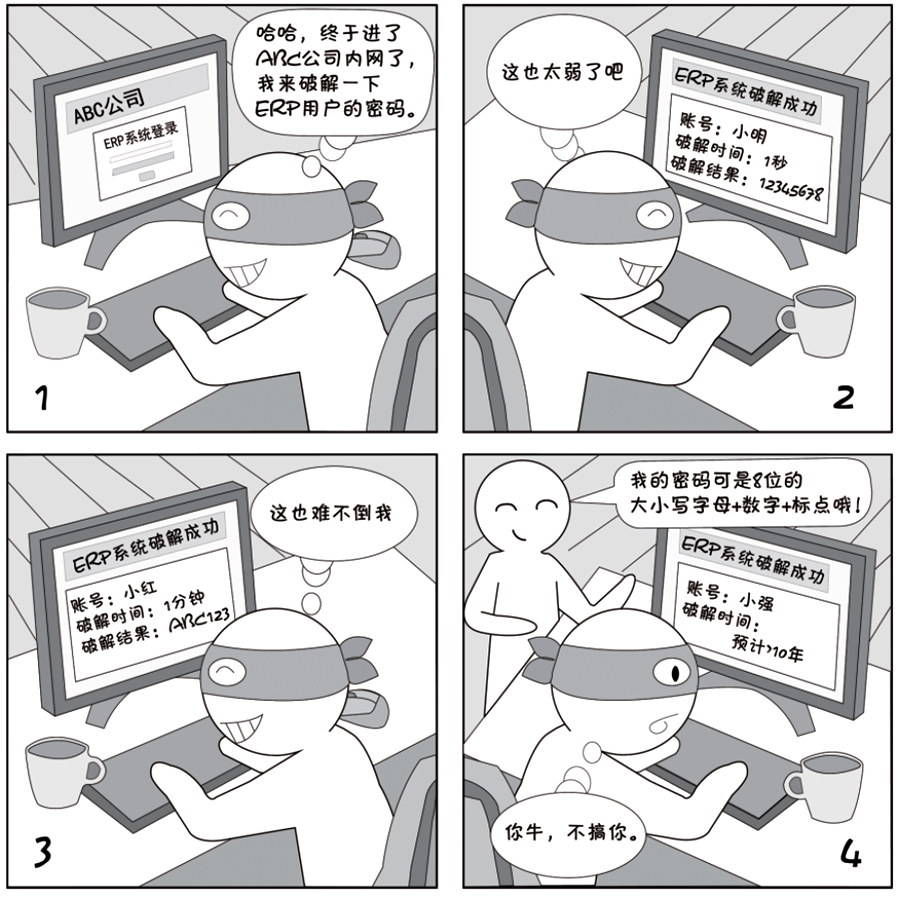


**【现象】**

文件直接放在硬盘上，电脑丢失后硬盘上文件就可以被直接读取，如果存到加密盘中，拿到硬盘后必须输入加密盘密码加密盘才能看到其中的文件，就有效避免了重要文件泄密。

**【建议】**

* 敏感文件建议存放在保密盘中，开机输入密码后加载加密盘
* 邮件中也会有很多敏感信息，Outlook或Foxmail的数据文件也建议放入加密盘
* 加密盘密码一定要设置复杂密码
* 加密盘可以使用微软的Billocker或Truecrypt
* 弱口令

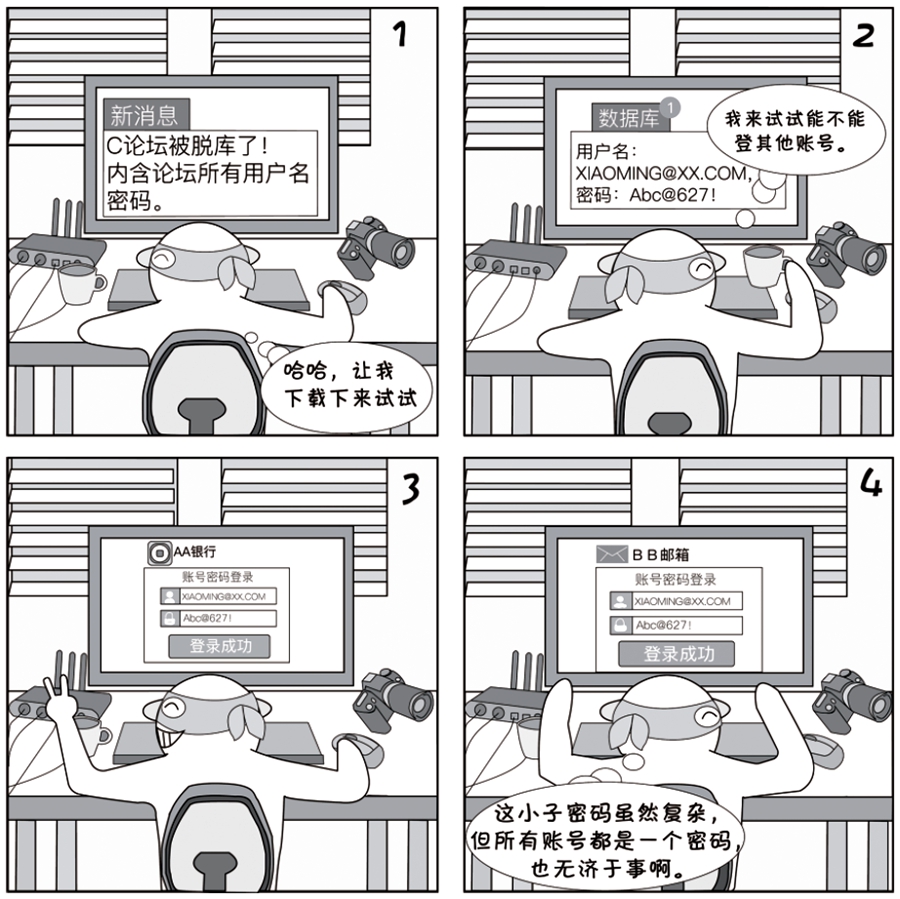


**【现象】**

密码越复杂，破解难度越高，且这个比例是成指数级的，假如说简单的6位数字密码秒破，而8位复杂密码的破解需要20年以上。

**【建议】**

* 包含大小写字母，数字和标点符号，位数在8位以上；
* 不能包含各字、生曰、手机号或车牌号；
* 定期修改各种密码，如三个月或半年；
* 密码分级

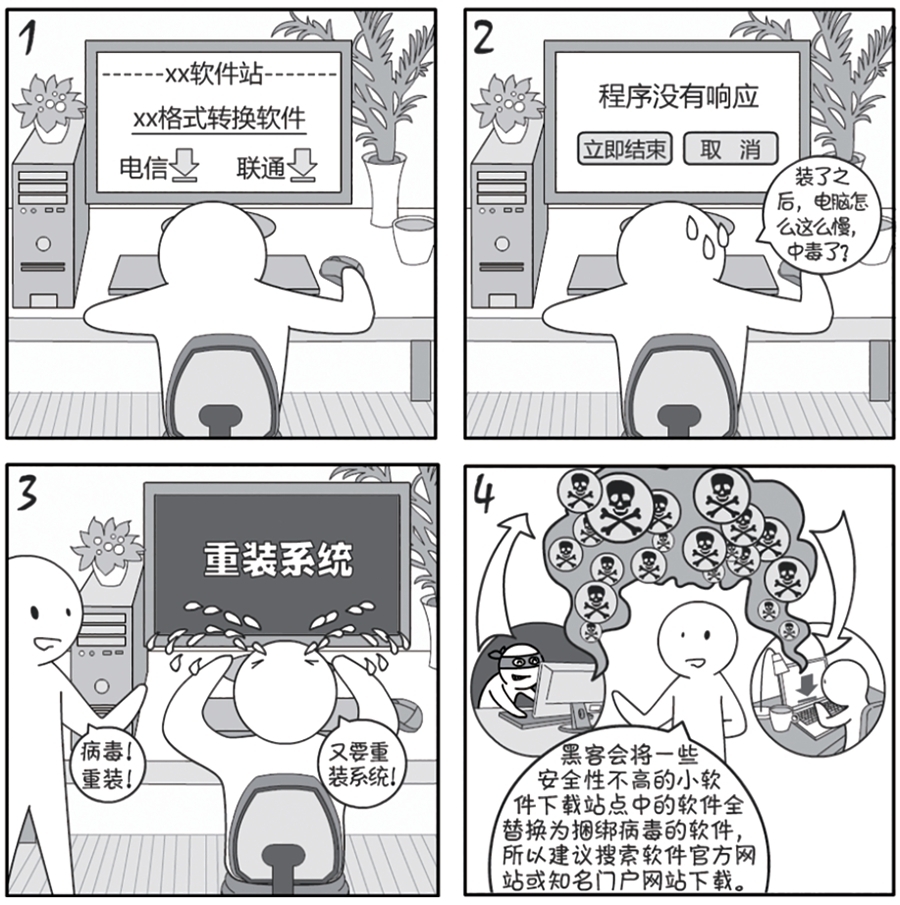


**【现象】**

很多人各个网站的用户名、密码相同，这样黑客用被泄露网站的密码登陆其他网站很有可能会成功。每个网站都设置不同的密码可能不现实，那就可以对密码分级管理。

**【建议】**

* 不同网站/应用的账号设置不同的密码是最安全的
* 也可以按账号重要程度进行分级，不同级账号设置不同密码，同一级账号设置相同或相似密码
* 爆发拖库事件时第一时间修改自己的相应级别的账号密码
* 软件下载

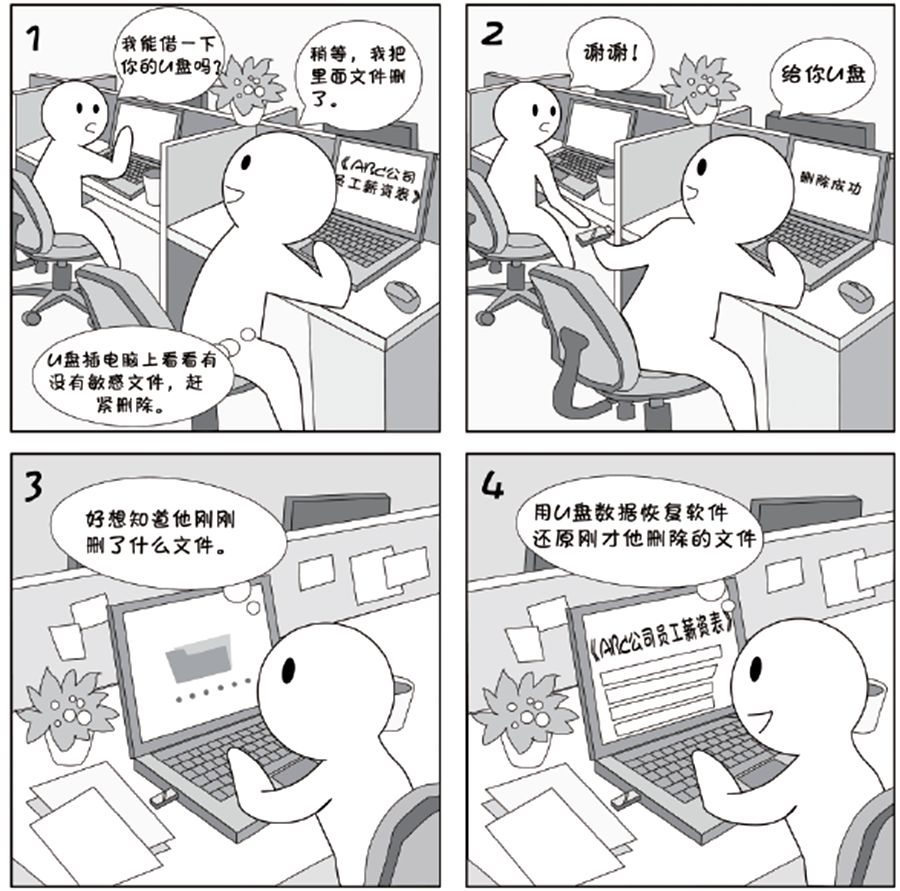


**【想象】**

黑客会入侵一些安全性不高的小软件下载站点，将其中的软件全部替换为捆绑病毒的软件，这些软件安装使用和原版一模一样，但后台就默默运行着病毒木马，各种主流杀软无法检测到。

**【建议】**

* 建议搜索该软件的官方网站，到官方网站下载
* 下载后用MD5工具查看下载软件的MD5值，并同官方网站公布的MD5值做对比，如果不一样则肯定被修改过
* 文件删除



**【现象】**

删除电脑或U盘中的文件时，如果仅点删除按钮或快速格式化，真实并未真正从硬盘或U盘中删除，利用数据恢复软件可轻松恢复出来，清空回收站同样可以恢复。

**【建议】**

* 单个文件彻底删除可利用杀毒软件自带的文件粉碎功能，一般在文件上点鼠标右键可以看到
* 电脑出售或移交其他人使用，删除敏感文件后，同样需要对硬盘脱密，使用脱密工具反复擦写5次以上
* 数据备份

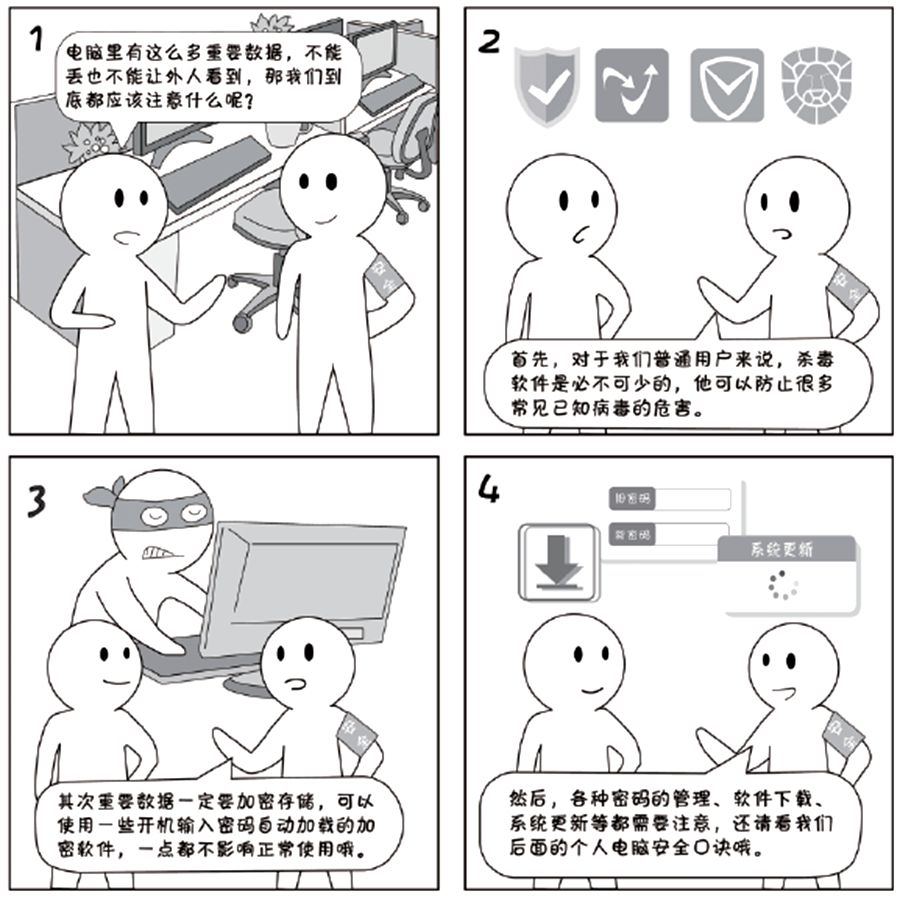


**【现象】**

有很多原因可能导致硬盘上的文件丢失或不可用，比如硬盘日久老化故障，电脑掉电硬盘故障，电脑中病毒将文件都加密，甚至电脑丢失等，所以，日常需要注意重要数据的备份。

**【建议】**

* 个人电脑上的重要数据要定期备份到备份服务器或移动硬盘
* 备份时，注意数据要加密，建议使用加密盘，备份整个加密盘原始文件
* 个人电脑安全总结



**<安全口诀>**

敏感文件要加密，邮件文件莫忘记

软件请到官网下，MD5要对比

文件删除要彻底，硬盘移交须脱密

密码设置要复杂，分级忘记又好记

系统补丁及时打，不怕黑客常惦记

数据备份要定期，备份文件须加密