针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 备份什么以及何时备份
- 如何备份
- 恢复
- 关键点

备份与恢复

概览

或早或晚，你都很有可能遇到些问题，丢失你的个人文件、文档或照片。比如误删、硬件故障、丢失笔记本电脑或者电脑中毒。像这样的很多时候，备份是你重建自己数字生活的唯一途径。本期，我们将解释什么是备份、如何备份你的数据，并为你量身定制一套策略。

客座编辑

Heather Mahalik是业界闻名的取证专家，她专注于智能手机取证。她还是《手机取证实战（Practical Mobile Forensics）》的共同作者和《学习安卓取证（Learning Android Forensics）》的技术编辑，并在SANS Institute共同教授“FOR585 高级智能手机取证（Advanced Smartphone Forensics）”和“FOR518 Mac系统取证（Macintosh Forensics）”课程。你可以在Smarterforesnics.com上了解她的动向并且关注她的Twitter（@heathermahalik）。

备份什么以及何时备份

备份就是把你的信息在另一个地方副本。当你丢失重要数据的时候，你就能从你的备份恢复它。问题是大多数人都不备份，这其实并不好，毕竟备份简单易行而且又花不了多少钱。在确定备份什么内容时有两种策略：（1）对你重要的特定数据；（2）任何数据，包含你的整个操作系统。第一种策略能提升你的备份效率，并且节省硬盘空间，但第二种更简单且更全面。如果你不确定要备份什么，那么我们建议你备份所有数据。

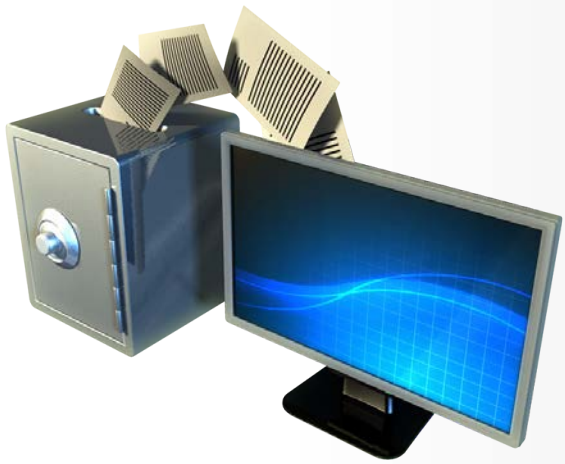
你要做的下一个决定就是多久备份一次。通常你可以选择每小时、每天、每周等等。对于家用而言，诸如Apple的“时间机器”、微软的Windows备份与恢复等个人备份程序让你能创建一个高枕无忧的自动备份计划，它们会在一天中你用电脑或不在电脑旁的时间静默备份你的数据。还有些解决方案提供“持续保护”功能，新建或被修改的文件在关闭时将立即被备份。我们建议你至少每天备份一次。追根溯源，你要问自己：“我能接受多少信息损失，如果我要从备份恢复的话？”

如何备份

有两种方式备份数据，一种是通过物理介质，另一种是通过云存储。物理介质指的是诸如DVD、U盘、移动硬盘等硬件。无论你选择哪种介质，你都绝不应该将文件备份放在同一设备上。物理介质的问题在于，如果储存位置发生

备份与恢复

灾难性事件（如火灾或盗窃），那么你不仅将丢失你的电脑，同时还会丢失你的备份。因此，你应该计划将你的几个备份放在远离现场的安全地点。如果你将它们放在别处的话，记得还要给它们贴上标签，注明备份的内容和时间。要提高安全性的话，你还可以加密你的备份。



自动化的可靠备份通常是你数据保护的最后一道防线。

云解决方案则不同，通过云服务，你的文件将被存储在互联网上的某个地方。根据你想备份的数据量的大小，这项服务可能还会收费。你只需在电脑上安装一个程序，它会自动为你备份文件。这类解决方案的优点在于，因为你的备份存储在云端，如果你的住宅发生灾难性事件，你的备份仍然是安全的。除此以外，你几乎能从任何地方访问你的备份或是备份中的单独几个文件，出门在外也行。缺点是云端备份（以及恢复）可能会更慢，特别是你有大量数据需要备份的时候。如果你不确定那种备份手段（物理介质或云）更适合你，记住你总能两种方式都做。

最后，不要忘了你的移动设备。移动设备的优点在于大多数数据——如邮件、日历事件、联系人——已经储存在了云端。然而，你可能还有些数据不在云上，比如APP配置、近期照片、系统偏好设置。通过备份移动设备，你不仅保留了这些信息，而且能更轻而易举地重建设备，比如你手机更新换代买了新的。iPhone、iPad能自动备份至Apple的iCloud上，安卓或其它移动设备则要看制造商和服务提供商了。在某些情况下，你可能需要购买特定的APP来备份。

恢复

备份完了数据，你只赢了这场战争的一半；你还要确保你能从备份恢复。每月检查一下，看备份是否正常，尝试恢复一个文件看内容对不对就行。此外，在重大升级（例如换新电脑或者新移动设备）、重大修复（例如更换硬盘）前务必进行全系统备份，并且检验备份可用。

备份与恢复

关键点

- 尽可能自动化备份并时常检查备份文。
- 从备份中恢复整个系统后，确保你在使用系统前打上了最新的补丁，安装了最新的更新。
- 过期的备份可能会成为一种负担，应该将其销毁，以避免它们被未经授权的用户访问。
- 如果你是用一款云解决方案，调研一下条款和提供商的声誉，确保它们能满足你的要求。例如，它们是否加密存储你的数据，谁能访问你的备份，是否支持两步验证等强验证方式。

公共电脑

不要使用酒店大厅、图书馆或网吧里的公共电脑，你完全不知道在你之前有多少人用过它们，他们可能或无意或有意地让其感染了病毒。无论何时，都尽量使用你能控制和信任的设备用于线上活动。如果你必须要使用公共电脑，那么不要使用需要你登录或输入密码的任何服务。

了解更多

订阅OUCH！安全意识月刊，访问OUCH！过往存档，了解更多关于SANS安全意识解决方案的信息，请访问：http://www.securingthehuman.org

相关资源

《密文》：	http://www.securingthehuman.org/ouch/2015#april2015
《两步校验》：	http://www.securingthehuman.org/ouch/2013#august2013
《安全使用云服务》：	http://www.securingthehuman.org/ouch/2014#september2014
《加密》：	http://www.securingthehuman.org/ouch/2014#august2014
今日贴士:	http://www.sans.org/tip_of_the_day.php

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：成自豪

