

# OUCH!

## 本期导读

- 概览
- 选择一个云服务提供商
- 保护你的数据

## 安全使用云服务

### 概览

“云”是无论个人还是组织都在快速采用的强大技术。对不同的人来说，“云”有不同的含义，但总体而言，“云”指的是使用互联网服务提供商来为你存储和管理数据。云的优势不仅在于你能轻松在世界任何地方的多个设备上访问和同步你的数据，还在于你能将你的信息与任何你想共享的人共享。我们将这些服务称为“云”的原因就是，很多时候你并不知道你的数据物理上存储在哪儿。云计算的例子包括在Google Docs上创建文档，通过Dropbox分享文件，在亚马逊的云上创建服务器以及在苹果的iCloud上储存音乐或图片。这些在线服务可能让你更加多产更加有效率，然而，与之俱来的还有一些独特的风险。本期，我们将讲解如何安全地使用云。

### 客座编辑

James和Kelli Tarala (@isaudit / @kellitarala) 是Enclave Security的首席顾问，并且开设过多个SANS培训课程，其中就包括“SANS Audit 566: 实现和审查21个关键安全控制”和“MGT 415: 风险评估实用入门教程”。

### 选择一个云服务提供商

云不好也不坏，它仅仅是一个工作中或家里面做事的工具。然而，你在使用这些服务的时候，你就将你的隐私数据交给了陌生人，并且你指望他们能将其保护好并且保持其可用性。因此，你得确信你的选择是明智的。对于你的工作电脑或与工作相关的信息，问问你的上司，看看你是否被允许使用云服务。如果是，请务必确认一下你能使用哪些云服务以及使用过程中有什么条款。如果你在考虑将云服务用于个人，请掂量掂量下面这几条：

1. **支持**：获得帮助容易么？问题被解答的几率大么？有没有一个能与服务提供商联系的电话或者电邮地址？有没有其它的支持选项，例如公共论坛或者网站上的FAQ？
2. **易用性**：服务使用起来容易么？服务越复杂，你就越有可能犯错误，越有可能暴露或者丢失你

## 安全使用云服务

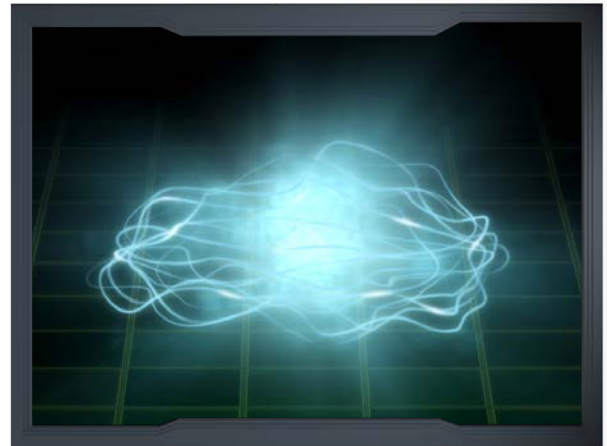
的信息。使用一个提供你觉得容易理解、配置和使用的云服务的提供商。

3. **安全性：**数据如何从你的电脑传输到云？连接有加密吗？你的数据是如何存储在云上的？它们被加密了吗？如果是，谁能解密？
4. **服务条款：**花点时间读读服务条款（与预期相左的是，他们往往很容易阅读）。确认一下谁能访问你的数据以及你有哪些合法的权利。

### 保护你的数据

在你选择了云服务之后，紧接着就是要确保你正确地使用它们。你访问和分享数据的方式往往比其它因素对你的文件安全影响更大。你能采取一些措施，其中主要包括：

1. **验证：**使用强而独一无二的密文来保护你的云账号。如果你的云服务提供商支持两步验证，我们强烈建议你启用此项功能。
2. **分享文件或目录：**有了云，分享变得非常简单，有些时候过于简单了。最坏的情况就是，你可能不小心将你的文件甚至是整个目录都共享给了整个互联网。保护自己的最佳方法就是默认不要分享任何文件给任何人，然后只允许需要知道对应信息的特定的人（或特定的组）访问特定的文件或目录。当某人不再需要访问你的文件的时候，移除他们的权限。你的云服务提供商应该提供一个简单的方法让你来跟踪拥有权限访问你文件和目录的人。
3. **通过链接来共享文件或目录：**一些云服务的一个共同特性就是让你能创建一个指向你文件或目录的链接。这个功能让你能简简单单通过提供一个链接就能把文件分享给你想分享的人。然而，这个方式没有多少安全性可言，任何知道这个链接的人都能访问你的个人文件或目录。如果你把这个链接发送给一个人，那个人可能将之又分享给其他人，还有可能这个链接出现在搜



云能使你的信息更容易被访问，使你更高产，但是在储存和分享信息的方式上，你要格外留意。

## 安全使用云服务

索引上。如果你通过链接来分享数据，不需要的时候就及时删掉它，或者如果可能的话，用密码来保护它。

4. **设置**：理解你的云服务提供商支持的安全设置。例如，如果你和他人分享一个目录，这个人不能再把你的数据在你不知情的情况下再分享给另外一个人呢？
5. **反病毒**：确保你的电脑及你用来分享数据的任何电脑上都安装了最新版的反病毒软件。如果你分享的一个文件受到了病毒感染，其它访问该文件的电脑都可能受到感染。
6. **备份**：即使你的云服务提供商为你备份数据，你还是应该考虑自己来定期备份。这不仅能保护你的数据免遭云服务商破产、关停或由于某种原因服务无法访问的影响，还能使得大规模的数据恢复更加容易，因为你只需要从本地恢复即可，而不需要从云端拉取数据。另外，确认一下你的云服务提供商每隔多久备份一次你的数据，是否允许你将你的文件恢复至之前的版本以及保存你的备份多长时间。

## 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

- 强密码：<http://www.securingthehuman.org/ouch/2013#may2013>
- 密码管理器：<http://www.securingthehuman.org/ouch/2013#october2013>
- 备份：<http://www.securingthehuman.org/ouch/2013#september2013>
- 安全术语：<http://www.securingthehuman.org/resources/security-terms>

OUCH! 由SANS Securing The Human出版，根据“[知识共享许可协议4.0 \(署名-非商业使用-禁止演绎\)](#)”发行。你可以在不对其进行修改的前提下，自由传播这份新闻简报或在你的安全意识课程中使用它。了解翻译或更多信息，请联系：[ouch@securingthehuman.org](mailto:ouch@securingthehuman.org)。

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



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org)