

OUCH!

给大家的安全意识通讯月刊

电子遗产

概述

你是否想过这样一个令人不自在的问题：在我们死亡或丧失行为能力之后，我们的数字踪迹会怎么样？许多人已经设立了或知道我们应该设立一份遗嘱和清单，告诉我们所爱的人在我们去世后需要知道的事。但是我们的数字资料和线上账号怎么办呢？我们是否应该考虑设置某种数字遗嘱？我们是否应该创建一个“数字继承”方案？

想一想你的数字踪迹。银行和退休账户、住房贷款、家庭照片和视频、智能家居账号、电子邮箱、社交媒体，这些只是构成我们数字足迹的众多例子中的一部分。如果你或者至亲去世，家人和所爱之人可能需要及时获取这些账号或数据。另外，随着时间的流逝，遗留的历史数据和线上账号可能更容易受到黑客的攻击，这样一来便将家人和朋友置于风险之中。

创建一个方案

建议与你信赖的家人或朋友说说你的愿望，比如临终细节。除此之外，对你的数字资产和线上账号进行盘点和记录。如果你没有提前告诉你的家人如何登录这些账号，那么在你去世后，他们将很难登录或注销这些账号。比方说，你愿意让你的家人看不到这么多年来你在线存储的家庭照片和视频吗？

一个方法是将你的线上足迹记录在密码管理器中。这样能安全地保存你所有的用户名和密码、信用卡以及其他的敏感信息。密码管理器的目的在于让创建、存储、使用密码和安全问题变得更简单。与其他方式相比，这种方法为你记录电子足迹提供了一个强有力的工具。有了密码管理器，你甚至还可以进行设置，与其他信任的家人分享所有或某些密码。如果这样做让你觉得不自在，

那么你可以把访问密码管理器的方式记录下来，然后封装在信封里，在你去世后由遗嘱执行人或者信任的家人打开。这样一来，他们便可以进入你的密码管理器，进而访问你的各类账号和存储在其中的信息。

另外，一些网站提供了确定遗产或可信赖联系人的选项。比如，Facebook允许其用户提前确定是否希望在去世后删除或保留自己的账号。保留则意味着仅对现有好友可见，为朋友们提供了一个回忆往昔的空间。最后，你可能需要跟专门从事电子遗产继承的律师或遗产规划师打交道。

继承电子资产

你可能需要恢复或登录最近去世的朋友或家人的线上账号。我们建议你在采取行动前先咨询一下律师或其他家人的意见。其他家人如果看到你没有征求他们的意见便采取了行动，可能会很沮丧。在这之后，确定你能找到的密码。家人是否将密码写了下来或者存在某处？如果没有，你是否可以打开他们生前使用并且依然保持登录状态的电脑或移动设备？如果不可以，你很可能需要前往每一个网站尝试登录已故之人的账号。这通常需要提供死亡证明和直系亲属关系证明文件。在某些情况下，你无法登录账号或访问存储其中的数据，而只能将其删除。每个网站对这种情况的处理都不尽相同，这会是一个耗时的过程。

在今天这个数字化的世界，我们在进行未来的遗产规划时，除了实物资产，我们还应该考虑到数字资产。

特邀编辑

Cheryl Conley是网络钓鱼和意识方面的专家，曾在Lockheed Martin帮助打造和管理网络钓鱼项目。她目前为SANS安全意识团队提供支持，持有SSAP(SANS安全意识专家)证书。



资源

密码管理器：<http://www.sans.org/u/Y5Y>
让密码变得简单：<http://www.sans.org/u/Y63>

OUCH! 由SANS SecurityAwareness出版，并以 [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) 许可证分发。只要您不修改内容，您可以随意分发本通讯，或者将其用于您的安全意识项目。有关翻译或更多信息，请联系 www.sans.org/security-awareness/ouch-newsletter。编辑委员会：Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley