OUCH! | 2020年2 月

社交媒体隐私

概述

大多数人绝不愿意走进一个喧闹的房间，然后向素不相识的人透露自己的私人生活细节——不论是自己的健康状况，还是亲朋好友的姓名、年龄或学校位置。但这些人却往往会毫不犹豫地将同样的信息发布到社交媒体上。过度分享影响的不仅是自己的个人生活和职业生涯，也包括亲朋好友的生活。

社交媒体是联络、分享和学习的绝佳场所。然而，仅确保安全可靠地设置了社交媒体隐私并不足以保护自己。一旦将信息发布到网上，你便失去了对它的掌控权。你需要了解哪些信息会被收集，它们又如何被他人使用。下面提供了一些隐私注意事项，使用社交媒体时你要慎重考虑：

隐私设置：仔细为你的所有社交媒体帐户创建隐私设置并经常检查，特别是在服务条款和隐私政策发生变更时。请记住，即使你对哪些人可以查看你的帖文进行了稳妥的设置，你的所有信息仍然会被收集、挖掘并存储在社交媒体平台服务器上，而且或许永远存储在那里。

隐私树：社交媒体设置不能防止朋友、亲戚和同事查看你的帖文，再将这些帖文与他们的朋友圈共享等等。

家人分享：人人都爱谈论自己的朋友和家人。但发布生日会恶作剧照片或者健康和行为问题可能会造成霸凌（尤其对未成年人而言），并且影响他们的个人生活。

信息分享：如果服务“免费”，那么你就是其产品。调查表明，你在网上的一切活动都可能会被出售给他人。

位置服务：签到数据可能被添加到其他个人数据中，形成你的生活和习惯的档案，这可导致跟踪纠缠并让你暴露于其他骚扰行为。此外，要留意你发布的任何照片或视频中包含的位置信息。

人工智能：AI、社交媒体和营销推广三者相辅相成。市场营销者现在利用从你的上网习惯中收集的信息，向你推送聚焦于你最近一次搜索或购买的广告，因而能继续加深对你的了解。

数字化死亡：一个人离世后，如果没有亲友维护或删除其帐户，其网上资料可能会更容易受到恶意人士的盗用。个人隐私不仅仅在于本人，影响范围也会延伸到家人和朋友。

意外泄露：你发布的关于你自身的相关信息可能会披露你的许多个人经历，因而能透露你的在线机密安全提示问题的答案。

隐私远不止在社交媒体帐户中设置隐私选项那么简单。你分享的信息越多，分享你的情况的人就越多，被公司、政府和其他机构收集和使用的信息就越多。自我保护的一种最佳方式，是慎重考虑和限制自己分享的内容，以及他人对你情况的分享，不论你使用什么样的隐私选项。

特邀编辑

Cathy Click为财富全球500强公司制定安全意识计划已有超过14年的经验。Cathy喜欢探讨复杂的技术话题，并将它们转化为易于理解的语言，帮助人们加强自己的网络安全。

资源

电子遗产：http://www.sans.org/u/Z2G
通过社交媒体实施欺诈：http://www.sans.org/u/Z2L
备用重要信息？：http://www.sans.org/u/Z2Q