针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 概览
- 隐私
- 安全

社交媒体

概览

诸如Facebook、Twitter、Instagram、LinkedIn等社交媒体是你和世界各地的人们认识、交流以及分享的绝佳资源。然而，随之而来的还有风险，并且这种风险不止针对你，还有你的家人、朋友和公司。本期，我们将解释这些危险是什么以及如何安全使用这些网站。

客座编辑

Tanya Baccam是一名长期的安全顾问。她担任SANS作者及讲师一职已有十多年，创设了包括 SEC502、SEC542、SEC401、MGT414、AUD507在内的诸多课程。你可以在Twitter（@tbaccam）上关注她。

隐私

有关社交媒体的常见问题就是保护个人信息。潜在的危险包括:

- **影响你的未来**：一些组织会在进行背景考察的时候搜索社交媒体网站。令人尴尬或内容不当的照片或帖子，无论多么老，总有可能让你与受聘或升职失之交臂。此外，许多大学对申请者也采取类似的考察手段。隐私选项可能并不会保护你，因为这些组织可能会要你赞或者加入它们的主页，某些帖子可能还在多个网站有存档。
- **针对你的攻击**：黑客可能会分析你的帖子，并借此获取你或你公司的信息。例如，他们能利用你分享的信息猜测你密保问题的答案，以重置你的密码，创建钓鱼邮件，或者伪装成你给你公司内的其他人打电话。此外，这些攻击还可能影响到现实世界，比如确定你在哪工作、居住。
- **不慎对你的公司造成损失**：罪犯或竞争者可以使用任何你发布的关于公司的敏感信息来对抗你的公司。此外，你的帖子可能会损害你公司的名誉。务必在发布任何有关你的工作的内容前查看你的公司政策，毕竟你发的帖子还有可能会被监控。

限制你的分享就是最好的保护。是的，隐私选项都提供一些保护，但是它们常常不知所云且在你不知情的情况下经常变更。你认为是私人的可能很快就因为各种原因而变得公开了。此外，你的帖子的隐私性仅与你分享的人的安全

社交媒体

性相当。你分享的朋友或联系人越多，你信息公开化的可能性越大。你应该假设你发的任何信息都将公开并且成为互联网上的一个永久性的部分。

最后，留意朋友们发了哪些关于你的内容。如果他们发了你不喜欢的内容，让他们删掉。如果他们拒绝或者忽略你，那就联系社交媒体网站，让他们帮你删掉。同时，在发关于别人的内容时你也要懂得尊重。



社交网站有意思并且功能强大，但是务必在分享的内容和对象上留个心眼。

安全

除了隐私问题，还有一些方法供你保护你的社交媒体账号和网上活动。

- **登录**: 用独一无二的强密码保护你的每一个账号，并且不要将密码告诉任何人。此外，许多社交网站支持加固的验证方法，例如两步验证。只要可能，就启用这些方法。最后，不要用社交媒体账号登录其它网站，否则如果其它网站被黑，那么你的所有账号就有危险了。
- **隐私设置**：如果你使用隐私设置，那么务必定期检查它们。社交网站经常变更隐私设置，你很容易就犯错。此外，许多APP和服务让你能给你的帖子标注地理位置信息（即geotagging）。如果你希望不公开你的物理位置信息的话，定期检查这些设置。
- **加密**：社交网站使用HTTPS加密来保护你的访问连接。像Twitter、Google+这些网站默认会启用这点，其它网站可能需要你手动设置。查看你社交媒体账号的设置，只要可能，就将HTTPS设定为默认的连接方式。
- **邮件**：有些邮件声称自己来自社交网站，对此你要保持怀疑，这些可能是黑客发送的虚假邮件。应对此类消息的最安全的方式就是从书签或其它方式直接登录社交网站，然后从网站上查看和回复任何消息以及通知。
- **恶意链接/诈骗信息**：对社交网站上的可疑连接或潜在诈骗保持警惕。不法分子通过社交媒体展开攻击。仅仅因为是一个朋友发的，并不能保证消息就一定是他们的，因为他们的账号可能被入侵。如果某个家人

社交媒体

或朋友发送了一条奇怪的消息（如被抢劫了现在需要钱）而你无法核验其真实性，那么就打他们手机或用其它方式确信消息真正来源于他。

- **移动应用**：绝大多数社交网站都提供APP。确保你从正规网站下载，并且你的手机受强密码保护。如果你的手机遗失之后被解锁，那么任何人都能通过你的手机访问你的社交网站并且以你的身份发布信息。

社交网站是与世界沟通及保持联系的绝佳方式。如果你遵循我们提供的这些建议，你应该就能有一个更加安全的在线体验。想了解更多关于如何安全使用社交网站或如何上报未授权的行为，请查看你社交网站的安全页。

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
安全使用手机应用:	http://www.securingthehuman.org/ouch/2015#january2015
教孩子理解网络安全:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook安全:	https://www.facebook.com/safety

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