

OUCH!

本期摘要

- 安全设置
- 安全维护

平板电脑安全使用手则

概述

恭喜你得到了一个新的平板电脑！这项技术为人际交流、网上购物、看电影、玩游戏以及一系列其他活动提供了强大而便捷的渠道。由于平板电脑很有可能成为你生活的重要组成部分，甚至取代你的个人电脑，我们为您提供几个确保平板电脑和个人信息的安全的步骤。

客座主编

Lori Rosenberg在开发针对员工和顾客的信息安全教育材料和培训领域有着丰富的经验，并且致力于探索新型有效的方法来分享她的所得。关注她的Twitter账号：[@infoSecLori](#)。

安全设置

或许你会不相信：你的平板电脑所面临的最大风险不是来自攻击者，而是来自你自己。相比被黑客攻击，平板电脑被弄丢的可能性更大一些。所以，为了保护你的平板电脑，头一件该做的事就是开启自动锁屏功能。这意味着每一次使用平板电脑，你都必须要用强密码、手势密码或者指纹来解锁。这确保了即便你的平板电脑遗失，没有人可以访问它，从而保护了里面存储的个人信息、移动应用以及其他内容。在你开启了自动锁屏之后，以下是几个其他小贴士：

1. 安装或者开启能够通过互联网远程追踪平板电脑的软件。这样，如果你的平板电脑遗失，你还有机会通过互联网连接并查找到它的位置，或者最坏打算也可以远程删除所有个人资料。
2. 更新你的设备并且开启自动更新以确保其始终运行最新版本的操作系统。攻击者乐此不疲地寻找软件的漏洞，而软件提供商也不断地提供更新和补丁来修复漏洞。因此使用最新的操作系统和移动软件增加攻击的难度。
3. 初始化平板电脑时，请关注各种设置，尤其是隐私设置。平板电脑的一大安全隐患就是给其他人提供了追踪、锁定设备所在位置的能力。我们建议你一开始关闭所有的地理位置追踪，然后再开启你

平板电脑安全使用手册

认为必要的软件，比如导航软件或者找周围餐馆的软件。大多数软件并不需要你的实时位置。

- 大多平板电脑和软件都把你的信息存储在云端。因此，你需要清楚个人数据存储在哪儿以及是怎样被保护的。例如，你最不希望发生的事情就是包含地理位置的个人相片被上传到互联网让全世界都能看到。请将云端的任何信息都默认成不能被共享，然后再单独开启你想要分享的那些。
- 平板电脑不断地将你的app与手机或笔记本电脑等其他设备进行同步。同步可以是一个非常便利的功能，但是请注意哪些app或者功能应该被同步。如果你开启了自动同步，那当你在办公的时候，看到之前在平板电脑上访问的网站和创建的标签页出现在你的电脑浏览器上时，请不要吃惊。



保证平板电脑的最佳方式就是开启锁屏功能，检查隐私权限和使用最新版本的软件。

安全维护

在安全设置了平板电脑后，以下是帮助你长期维护其安全性的一些关键步骤

- 永远不要越狱或者攻击你自己的平板电脑。这将避开大量的安全控制从而使其失效，进而使你的平板电脑变得易攻击。
- 只从可靠的资源下载你需要的应用软件。对于iPad而言，只通过iTunes进行下载。这些软件在上架之前就已经被苹果公司审查过。对谷歌的平板电脑而言，我们建议你只从Google Play下载软件，同理。亚马逊的平板电脑只从亚马逊应用商店下载资源。虽然你可以从其他网站下载到应用软件，但是这些没有经过审查故而有可能被感染。最后，无论你是从哪里得到的资源，一旦你不再需要这个应用或者用的很少，我们建议你将其删除。

平板电脑安全使用手册

- 在安装一个新的应用软件时，确保你审查并设置了相关的隐私选项，就像你之前在设备初始化时一样。仔细对待每个应用软件可以获取到的资料和权限。比如，你刚下载的应用真的需要获取你的所有朋友和联系人信息吗？如果你觉得某个软件的权限设置不合理，另找一个能够满足需求的替代。另外，定期查看软件的权限设置以确保没有变化。

平板电脑是个强大的工具，我们希望你能享受和使用其带来的便捷。以上一些简单地步骤能够长久地保证你和设备的安全。

了解更多

订阅OUCH! 安全意识月刊，查看OUCH!往期内容，以及了解有关SANS安全意识方案的其他内容，尽在<http://www.securingthehuman.org>。

Dyn is a cloud-based Internet Performance company. Dyn helps companies monitor, control, and optimize online infrastructure for an exceptional end-user experience. Through a world-class network and unrivaled, objective intelligence into Internet conditions, Dyn ensures traffic gets delivered faster, safer, and more reliably than ever.

相关资源

安全使用移动APP:	https://www.securingthehuman.org/ouch/2015#january2015
密文:	https://www.securingthehuman.org/ouch/2015#april2015
安全使用云服务:	https://www.securingthehuman.org/ouch/2014#september2014
处理掉你的移动设备:	https://www.securingthehuman.org/ouch/2014#june2014
SANS每日安全小贴士:	https://www.sans.org/tip_of_the_day.php

OUCH!由SANS Securing The Human出版，遵从“[知识共享许可协议3.0（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。

编委：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻译：陈柳希



securingthehuman.org/blog



[/securethehuman](https://securethehuman)



@securethehuman



securingthehuman.org/gplus