针对电脑用户的安全意识电子月刊

OUCH!

本期导读

- 概览
- 获取APP
- 权限
- 更新APP

安全使用移动APP

概览

平板、手机之类的移动设备已经成为了我们在个人和工作生活中使用的主要技术之一。移动设备之所以如此强大，是因为我们有上百万的APP供我们选择。这些APP让我们变得更高效，让我们能够及时同他人交流、分享，我们也能靠它们来培训或者教育，或者仅仅是找点乐子。然而，伴随这些APP的强大功能的还有风险。下面是一些安全使用、维护移动APP的方法。

客座编辑

Chris Crowley是一位独立顾问、SANS认证讲师和课程作者。他活跃在Twitter（@CCrowMontance）和Google+上（+ChrisCrowley）。

获取APP

首要方法是，确保你总是从一个安全的受信任的源下载它们。记住，几乎任何人都能创造一个APP，所以你得对你获取它们的地方额外留意。网络罪犯已经在制作和传播看似合法实则受到感染的移动APP上颇有“造诣”。如果你安装了其中一个受感染的APP，那么这些罪犯将能控制你的移动设备来读取你的邮件、窃听你的对话、获取你的联系人信息等等等等。而只从知名的受信任的源下载APP，将能降低你安装受感染的APP的机率。你或许并未意识到的是，你移动设备的品牌决定了你的选项。

对于iPad、iPhone之类的苹果设备而言，你只能从苹果商店这个托管环境下载移动APP。这样做的优点是，苹果对移动APP和它的作者能进行双重安全检验。尽管苹果无法侦查到所有的坏蛋或所有的受感染的移动APP，这种托管环境有助于显著减小你安装受感染APP的风险。此外，如果苹果找到了商店里的一款受感染的应用，它将迅速移除它。Windows Phone用了类似的手段来管理应用。

安全使用移动APP

安卓设备则不同，它允许你从互联网上的任何地方下载移动APP，从而给你更强的灵活性。然而，随之而来的还有更多的责任。你得在你下载、安装的APP格外小心，因为不是所有的这些APP都被检测过。Google的确也维护了一个托管的移动APP商店，它和苹果的类似，叫Google Play。你从Google Play上下载的程序已经接受了一些检测。因此，我们建议你只从Google Play上下载安卓APP。避免从其它网站上下载，因为包括网络罪犯在内的任何人都能轻而易举地制作和传播恶意APP，并且骗你安装它们，让它们感染你的移动设备。作为一层额外的保护，反病毒软件值得你考虑考虑。

要想安全地使用移动APP，关键之处就在于只从受信任的源安装APP，并且确保它们保持更新，并且你核验了它们所请求的权限。

为了进一步降低风险，避免全新的少有人下载或少有正面评价的APP。APP上线的时间越长或者收到的正面评价越多，它就越能被信任。此外，只安装你需要并且要使用的APP。问问你自己，你真的需要这款APP么？每一款APP不仅会带来潜在的新漏洞，还会造成隐私问题。如果你不再使用一款APP，那就从移动设备上删除它——如果你之后发现你需要它，你总能把它装回来。

最后，你可能像越狱或者root你的移动设备。这是一种入侵系统并且安装未经许可的APP或者改变内置功能的过程。我们强烈建议你别这样做，因为它不仅会绕过或者消除你移动设备内置的安全控制，还经常会使保修和售后服务条款失效。

权限

你从受信任的源安装了一款APP之后，下一步就是确保它被安全配置了并且在保护的隐私。安装且（或）配置APP经常会涉及到让你授予特定的权限。在授权之前，总是想想，你的APP真的需要这些权限来干它的本职工作么？比如，一些APP使用定位服务，如果你允许一款APP获取你的地理位置信息，你就可能让APP的制作者跟踪你的踪迹，他们可能像其他人兜售这些信息。如果你

安全使用移动APP

不想授权，那就去看看商店里的其它APP，看看有没有能满足你的要求的。记住，你有相当多的选择。苹果设备允许你在“设置”或者在运行时修改一些权限，例如访问地理位置信息；Windows和安卓设备则不痛，它们采取的是一种要不全盘接收要不就什么也没有的策略，如果你不授予一款APP它所注明的所有权限，你就不能安装它。

更新APP

移动APP，正如你的电脑和移动设备操作系统一样，必须要更新且保持最新。罪犯总是在不停地寻找APP中的弱点，找到之后对其进行利用；制作你的APP的开发者也制作并发布更新来修复这些漏洞，保护你的设备。你检测、安装更新越频繁越好。大多数平台让你配置你的系统，让它自动更新。我们强烈建议你这样设置。如果这不可行，那么我们建议你至少没两周检查一下APP更新。然而，在你的APP更新的时候，你也要检查它们可能会要求的权限。

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

《社会工程学》：	http://www.securingthehuman.org/ouch/2014#november2014
《如何处理掉你的移动设备》：	http://www.securingthehuman.org/ouch/2014#june2014
《保护你的平板电脑》：	http://www.securingthehuman.org/ouch/2013#december2013
常用安全术语:	http://www.securingthehuman.org/resources/security-terms
“SEC575：移动设备安全课程”：	http://www.sans.org/sec575

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


securingthehuman.org/blog


/securethehuman


@securethehuman


securingthehuman.org/gplus