OUCH!
每月安全意识通讯
SANS SECURITY AWARENESS

处置你的移动设备

概述

手机、智能手表和平板电脑等移动设备以令人惊讶的速度不断进步和创新。结果是，一些人频繁更换他们的移动设备，每年都会。不幸的是，人们经常没有意识到这些设备上有多少个人数据。下面，我们将讲述你的移动设备上可能存了什么，以及在你处置它们之前，应该怎样安全擦除上面的数据。如果你的移动设备是你的雇主发给你的，或者上面存有与工作相关的数据，那么务必要先与你的上司确认如何恰当备份和按处置流程处置它们。

你的信息

移动设备上储存的敏感数据比很多很意识到的要多，甚至远远超过你电脑上储存的。

⚠

- **你住在哪，在哪工作，以及去过哪些地方**
- **你地址簿里每个人——包括家人、朋友和同事——的联系方式详情**
- **接听、呼出、语音邮箱、未接来电等呼叫历史**
- **短信，以及安全聊天、游戏、社交媒体程序中的聊天会话**
- **网页浏览历史、搜索历史、cookie 和缓存的页面**
- **个人照片、视频和录音**
- **储存的密码和你银行、社交媒体、电子邮箱的访问权**
- **年龄、心率、运动历史、血压等健康相关的信息**

擦除你的设备

无论你如何处置你的移动设备简单删除数据是不够的，取而代之的是，你应该安全擦除你设备上的所有数据。实现这个的最简单的方法就是重置你的设备。不同设备的重置功能不同，下面是两种最常见的设备的重置方法。

在重置前确保你开启了设备上的加密功能，这是一种更安全的方法。在新出的移动设备上，最简单的做法是启用屏幕锁（希望你已经这样做了）。最后，我们非常建议你在重置前备份你的设备。

- **苹果 iOS 设备：设置 | 通用 | 还原 | 抹掉所有内容和设置**
- **Android 设备：设置 | 隐私 | 恢复出厂设置**

SIM 卡和外置存储卡

除了你的设备外，你也需要考虑如何处理你的 SIM（Subscriber Identity Module，用户识别模块）卡。SIM 卡是移动设备用来连接手机或数据网络的。当你擦除你的设备时，SIM 卡仍保存有你账号的信息，并且和你绑定。如果你迁移到新设备，并且仍使用原来的电话号码，那么和你的电信运营商聊聊，看怎样转移你的 SIM 卡。如果不能这样做，那么你应该留着你的老 SIM 卡，然后物理销毁它，以防他人盗用它来冒充你，然后获得你的信息或账号的访问权。最后，一些 Android 设备可以使用可移除的 SD（Secure Digital，安全数码）卡来扩充存储空间。在处置你的移动设备前，移除这些外置存储卡。这些卡经常可以在新移动设备上复用，或者通过 USB 转接器，作为电脑的通用存储使用。如果你不能复用你的 SD 卡，那么像对待你的老 SIM 卡一样，我们建议你物理销毁它。

如果你对上述方法有任何不确定的地方，或者你设备上的重置选项不大一样，那么你可以带着你的移动设备去你购买的店里，然后让受过培训的技术人员来帮你。最后，如果你要丢弃一个设备，那么考虑一下能不能不丢，而把它捐出去。有许多非常不错的慈善组织，它们接受二手移动设备，并且还有很多手机提供商在店里设有丢弃娄。

特邀编辑

Christopher Crowley（@CCrowMontance)是一位华盛顿特区的独立顾问，专注于安全运维领域。他偶尔会发推和写博客。他有一本关于安全运维中心的书将于近期出版，敬请关注。他是 SANS Institute 的一位高级讲师。

资源

SANS 课程：对你的移动设备进行渗透测试：	https://sans.org/sec575
SANS 课程：高级智能手机取证课：	https://sans.org/for585
FTC 关于处置移动设备的建议：	https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device