

您的移动设备安全性如何？

我们大多数人都有智能手机，但又有多少人真正思考过这些移动设备所面临的安全威胁？移动设备容易遭受多种多样的威胁。如今，骗徒日益频繁地攻击移动设备，并借助恶意应用程序定向入侵您的手机。他们无所不用其极，在您毫不知情的情况下顺利盗取个人和商业信息。

即使您下载了安全或防病毒应用程序，也不能单靠这些服务保护您的智能手机。要预防移动设备的隐私和安全问题，改进您的移动设备安全实践才是最佳的防御方法。

如何改进我的移动设备安全实践？

请始终谨记以下最佳实践，将移动设备遭到攻击的风险降到最低：

1. **务必随时更新手机操作系统。**经常更新操作系统，有利于修复安全漏洞。操作系统过时会导致安全漏洞未被修复，许多恶意威胁正是由此而来。
2. **小心应用商店里的恶意应用。**官方应用商店会定期移除含有恶意软件的应用程序，但有时这些危险的应用会逃过法眼，并被不知情的用户下载。做好调查，阅读评论，留意下载量。切勿从非官方应用商店的来源下载应用程序。
3. **确保应用程序不会请求访问与功能无关的手机信息。**在下载应用程序前，这些应用通常会请求提供有关文件、文件夹、其他应用程序及数据的权限列表。不要盲目批准这些权限。如果您觉得这些权限请求没有必要，那就在应用商店中寻找替代应用。
4. **无密码或弱密码保护。**许多人仍然不用密码锁定手机。假如您的设备丢失或被盗，窃贼就能轻而易举地访问存储在手机上的所有信息。
5. **谨慎使用公共 WiFi。**凭借强大的科技，骗徒能够窥探您的一举一动。避免通过公共 WiFi 登录网上服务或进行任何敏感交易（如银行业务）。

