

每次选购新手机之前，小黑总会思考一个问题：到底是买iPhone还是安卓旗舰手机？

前些年，iPhone 手机与安卓手机差距巨大，在硬件性能、系统流畅性、软件安全性等方面，iPhone都高出安卓手机一大截。

如今，随着安卓旗舰手机不断更新黑科技功能，iPhone 在内存、快充、屏幕等领域渐渐被安卓手机反超。

现在，小黑优先选购iPhone 手机，多半看中了 iOS 系统安全性，毕竟是闭源系统，App Store中的软件安全性高，不像安卓系统，随便找个APK 文件包就能下载手机软件。



▲ 真 “Trezor” logo

原来，真正的 “Trezor” 根本就没有开发iOS版应用，这就让心怀叵测的骗子抓到漏洞。他们使用相同的名字，使用相似的图标，假装成真正的 “Trezor” 。

真正的“Trezor”图标为黑色门锁，而盗版“Trezor”图标只是将门锁颜色改成白色，同时加上一个绿色背景。



▲ 诈骗软件评分接近满分

名称一模一样，图标高度相似，功能还基本一样，这样的诈骗软件居然能够在App Store 正常上架，小黑心中满是疑惑。

对此，苹果表示，假“Trezor”应该是通过“诱饵与开关”进入App Store，使用了与真 Trezor 完全相同的标志和颜色。

在应对审查时，该应用自称是一款 iPhone 文件加密 App，不涉及任何虚拟货币。在提交假的Trezor之后，又把自己变成了一个加密钱包。

并非个例，诈骗 App 层出不穷

起初，小黑以为菲利普小哥遇到的问题只是个例，苹果App Store还是可以有效审查诈骗应用，直到小黑看到更多诈骗App 案例。



▲ 虚假App

在软件开发领域，有一个名词叫热更新，即不经过应用商店，在应用内部实行的即时更新。这种更新可大可小，不会涉及底层架构设计。

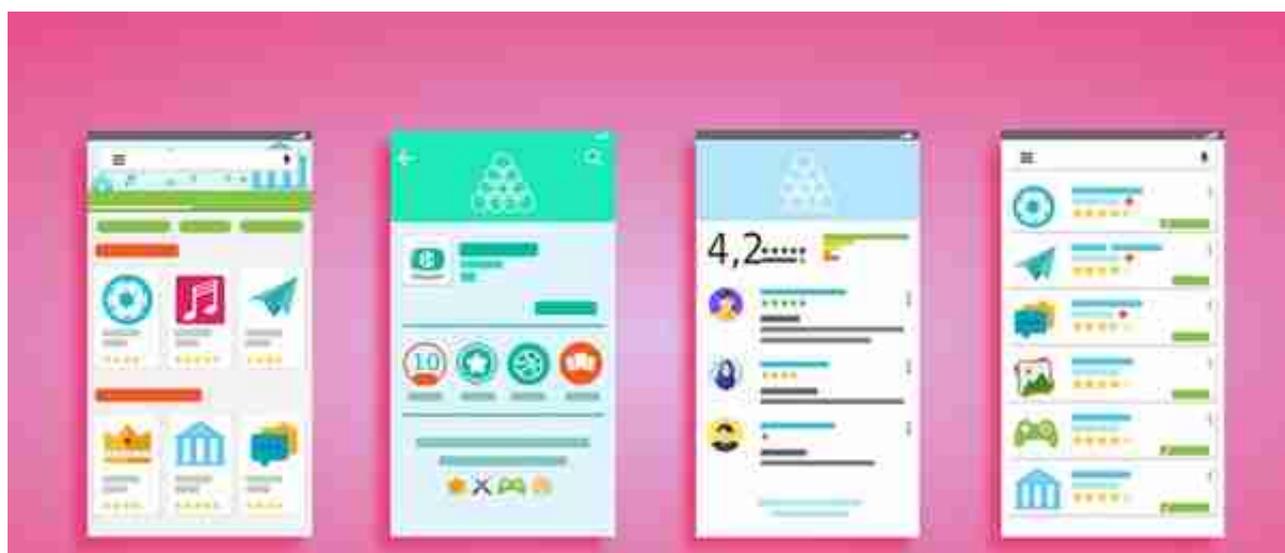
在App Store 中，热更新难以监管，很容易形成审查漏洞，不法分子可以肆意发布诈骗App，且不容易受到惩罚。

苹果本身，不仅对诈骗应用放任自流，事后也不会对其追责。

上述“Trezor”应用被骗的五位用户，一直在向苹果反映问题，至今没有收到答复。三年前被骗的牟大哥也是一样，去苹果客服申诉，仅仅被告知填一张表格，此后就再无消息。



通常来说，用户发现手机有风险都会想办法补救，这时该应用免费提供一个 7 天病毒扫描服务，随后将进行 Touch ID 验证。没有警惕性的小伙伴，可能直接验证通过。可在下方还有一行小字，写着免费试用结束后将每隔 7 天扣费 99.99 美元。



▲ 搜索排名

这些诈骗软件通过搜索广告，使得其在App Store 搜索排名虚高，甚至比业内部分常用软件还要高。同时使用大量小号评价刷分，伪造成信誉良好的模样。如此包装之后，用户在App Store搜索下载某类软件时，就很容易中招。

有报告统计，这些新型诈骗App已经骗走了用户超过4亿美元的金額。由此可见，此类诈骗应用已经普遍存在于App Store之中，苹果想要彻底整治它们，恐怕要下很大功夫才行。

如何打造铜墙铁壁

短时间内，小黑看不到苹果大规模整治App Store乱象的迹象。普通人若是想避免上当受骗，还要从自身做起，首先在下载App时一定要擦亮眼睛，仔细分辨用户名称、logo与开发者信息，尽量不下载小众应用。



在App Store 中可以下载该软件。打开软件，内部含有我要举报、报案助手、诈骗预警、身份验真等功能。首页下方内含大量诈骗案例，除了苹果App Store 软件骗局，还能学习电信网络诈骗、诈骗电话等多种骗局。装上这款软件，用户可以提高警惕，练就火眼金睛，打造安全防护铜墙铁壁！

软件的世界充满各种未知，安卓系统由于开源开放，打击诈骗App 无从下手。苹果iOS系统不开放旁加载功能，所有软件都需要从App Store 下载，居然也做不到有效防护。

小黑认为，苹果自身完全有能力加强App Store防护能力，从根源上杜绝诈骗App。虚假App已经严重影响苹果用户体验，如果苹果再不做改变，iOS系统安全优势或将不复存在！

图源：谷歌、苹果