



警惕手机里的“李鬼”，

下载 App 需谨慎

□ 慎 君

“扫码下载 App，获取国家投资补贴项目信息”“分享 App 下载链接邀请新用户，领百万现金奖励”“专属理财助理邀您下载 App 捞金”……看到这样的广告，你是不是很心动？然而，隐藏在这些“福利”外壳下的，往往是信息泄露、财产损失等危险后果。

近期，工信部反诈工作专班会同有关部门开展 App 反诈电子标识试点工作，2023 年 9 月至今，累计监测发现约 1.7 万款仿冒 App。不法分子为牟取不当利益，在未经版权所有人同意或授权的情况下，仿造正版 App，诱骗用户下载安装使用。仿冒 App 一直是制约移动互联网健康发展的毒瘤，其往往通过植入病毒等方式，违规采集个人信息、获取手机权限、偷跑流量或盗打电话，甚至转移用户资金、盗取钱财。

据了解，此类仿冒 App 迷惑用户的套路主要分为两类：一种是追求 1：1 高仿，使用与正版相同或高度相似的名称和图标，具有很强的迷惑性；另一种是虚构某正版 App 的国际版、特价版，以掩盖差异，降低用户的警惕性。近年来，仿冒 App 引发的诈骗案件多发，主要涉及投资、理财、网贷、刷单、博彩、交友等类型。

工信部反诈工作专班提示，不法分子还经常铺设国家政策出台、政务活动、投资理财等场景，以此实施诈骗。比如，浙江台州警方破获的一起仿冒个人所得税 App 诈骗案中，不法分子在个税申报高峰期假冒正规政务软件，套取用户姓名、身份证号、通讯录等关键信息，实施更加精准的诈骗活动。

随着技术手段的不断迭代升级，不法分子利用工具批量生成仿冒 App，通过广撒网的形式提高安装率、保留率，规避安全合规审核和监管，已经形成一条运作熟练的黑色产业链。不仅如此，据工信部反诈工作专班技术专家介绍，不法分子先上架一个看似正规的 App，之后通过动态加载修复补丁或更新内置网页后台等手段，换成仿冒 App，以一种更为隐蔽的方式躲避安全合规审核，一般称为 App 的“热更新”，即所谓的“马甲”App。

那么，用户应当如何应对此类仿冒 App，守护好个人信息和财产安全呢？一是下载时，不点击没有明确来源的链接，不扫描来历不明的二维码，确保从正规官网或应用商店下载 App；不轻信所谓的点赞、挂机赚金币等应用，这些应用通常有很高的诈骗和病毒传播风险。二是安装和注册时，认真阅读服务条款和授权协议，谨慎授权相册、位置、通讯录等敏感数据。三是在使用过程中，一旦发现下载的 App 有异常，或相关页面提示存在风险，要极为慎重，拒绝一切形式的提前转账；同时要保持手机操作系统的更新，及时修补手机安全漏洞。🔒

（资料来源：人民网、央视新闻、《北京日报》等媒体报道）

责任编辑 / 达洁玉