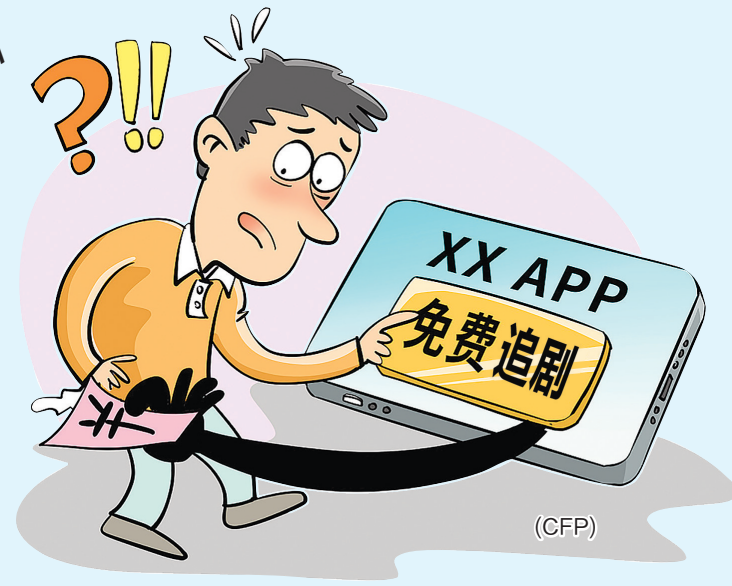
“观影神器”藏数字陷阱,用“免费追剧”APP须小心

侵了别人的权 丢了自己的隐私

“追剧党速藏,一个免费APP就够了”“下载观影神器,实现追剧自由”……在短视频平台、社交群组和网页弹窗中,这类极具诱惑力的宣传语随处可见,背后指向的却是各类来源不明的盗版剧APP。近日,中国消费者协会专门发布消费提示,直指此类APP不仅涉嫌严重侵犯著作权,还通过窃取个人隐私、植入恶意程序等方式,对消费者的信息安全和财产安全构成多重威胁。



(CFP)

诱饵 免费投喂背后藏猫腻

在短视频平台上搜索“免费追剧”,会弹出大量相关内容。评论区里,不少人主动晒出追剧截屏,并宣称“无广免费高清还可以投屏”,引来众多用户主动搭讪“求分享”。记者私信其中一个博主,对方很快发来操作步骤,要求下载一款浏览器,之后在搜索栏输入指定口令。

值得注意的是,对方故意在步骤中用“吓载”替代“下载”,用“刘兰气”替代“浏览器”,从而规避敏感词审查。一番操作过后,的确可以进入影视播放页面,但同时出现的还有大量不堪入目的色情广告。

在社交平台上,同样有用户以“免费追剧”为诱饵进行圈粉引流,并附上群聊二维码,邀请他人入群分享交流。记者尝试加入多个群组,发现群主会在置顶消息中分享一款APP,还强调“必须先搜指定口令,才可以激活使用。”

相比起这些操作而言,部分博主的手段更为隐蔽。记者以咨询者身份联系一名博主,对方很快便通过私信发来下载链接。点击后,平台提示其为第三方网页。记者询问是否可以从应用商店下载,对方表示“不能”。

打开相应链接,页面弹出一款影视APP的下载说明。其中提到,“放心下载下图所示软件:该软件为马甲包,升级后即正常使用;打开软件显示是否允许粘贴密钥弹窗,请务必选择‘允许粘贴’;请从后台退出APP,重新打开,即可获取最新版提示。”

陷阱 权限窃取暗中埋祸根

看似普通的免费追剧APP,究竟会带来怎样的后果?追剧爱好者徐女士下载后发现,自己的手机流量突然暴增。“明明都是在家连Wi-Fi看的,出门基本没用过,可还是很快就用掉100G,导致莫名被扣费。”她在社交平台上看到,不少人也有过类似遭遇,“即使不主动打开,也会在后台飞速耗流量”。

有媒体此前报道的案例中,周先生原本也只是想下载免费追剧APP,结果却被盗取钱财。当地反诈中心技术部门对手机取证分析后,确认其被植入了具备远程控制功能的木马程序,由此导致周先生的支付宝及银行卡共被盗刷数万元。

“一些APP只是披上了‘免费追剧’的外衣,本质上是电信网络诈骗的作案载体。”长期工作在反诈一线的北京市公安局朝阳分局刑侦支队民警王佳谈道,这类APP可能通过“免费追剧”诱导用户下载,安装时强制要求授权通讯录、短信、位置、相册等权限,部分还会暗中获取手机root权限,实现对手机的全面控制。随后,通过木马程序窃取用户支付软件账号、密码、短信验证码等信息,或直接远程操控手机进行转账消费。

王佳透露,恶意程序的作案手段还在不断升级。一些非应用商店下载的APP会搭载“共享屏幕”功能,当用户登录手机银行输入密码、验证码时,骗子能实时查看并记录,“还有些会让手机瞬间黑屏,使其处于完全被托管状态,用户无法察觉资金被转移的过程”。

此外,部分应用商店上架的小众APP也可能被利用。王佳表示,一些看似合规的应用会通过推送广告引流,点击后不仅弹出不良内容,还可能诱导用户下载其他恶意程序,或跳转至刷单返利、投资理财等诈骗界面,“它们本身不直接作案,而是作为引流平台,将用户一步步引入更深的诈骗陷阱”。

链条 精准诈骗黑产牟暴利

在盗版剧APP背后,藏着一条分工明确、环环相扣的产业链。从资源窃取、程序植入,到推广引流、非法牟利,每个环节都有专业人员参与,形成了完整的“灰色生态”。

在这条产业链中,“技术研发”是源头。不法分子专门破解正版影视资源的加密方式,非法复制后存储在私人服务器中,同时开发带有木马程序的盗版APP,将影视资源与恶意程序捆绑;随后由“推广团队”通过短视频平台、社交群组等多种渠道扩散,用“免费看剧”等噱头吸引用户下载;最后通过窃取信息、远程盗刷、精准诈骗等方式非法获利。杭州警方前不久破获的案件中,嫌疑人正是搭建了专属资源库网站,发展上千人的技术群组管理下游客户,向各类盗版APP运营者提供资源支持与技术服务,从中牟取暴利。

王佳透露,诈骗团伙在获取用户年龄、性别、消费习惯、地理位置等信息后,可能实施精准诈骗。例如,对年轻人推送刷单返利、网络贷款等骗局;对中老年人则重点推广虚假投资理财、保健品购买等项目;部分还会利用获取的通讯录信息实施敲诈勒索,比如诱导用户进行私密视频聊天并录屏,再威胁将视频发送给其亲友,要求支付“封口费”。

更令人担忧的是,这条黑产链条还在不断延伸。部分不法分子会将窃取的用户信息层层转卖,包含姓名、手机号、住址、支付习惯等信息的“个人信息包”,在黑产市场上可能被卖出不菲的价格。而这些信息又会被其他诈骗团伙利用,实施新一轮精准诈骗,导致用户面临连环损失。

“电信网络诈骗背后往往是整个犯罪集团在运作,他们分工明确、手段专业,不断翻新作案手法。”王佳提醒,每个人都可能成为目标,“有钱的会被诱导直接转账,没钱的也会被诱导贷款转账,最终导致个人的信息安全和财产安全受损”。

应对 出现异常可拔卡断Wi-Fi

面对盗版剧APP带来的多重安全威胁,消费者该如何筑牢防护屏障?王佳结合多年反诈经验,给出了具体的防范建议,提醒用户既要事前防范,也要掌握遭遇风险后的正确处置方法,避免损失扩大。

“恪守‘四不原则’是防范电信网络诈骗的核心,要做到未知链接不点击、陌生来电不轻信、个人信息不透露、不明APP不下载。”王佳强调,正规的影视资源需要通过官方平台观看,不要为了节省会员费而下载非应用商店的APP,“这些APP没有经过正规审核,风险极高,可能包含恶意程序和病毒”。

安装任何应用时都要谨慎授予权限,对于要求获取通讯录、短信、麦克风、摄像头、定位等敏感权限的APP要格外警惕。“很多恶意APP就是通过过度获取权限来窃取用户信息的,一旦发现APP存在异常权限申请,应立即卸载,并对手机进行病毒查杀。”王佳提醒,接到自称公检法、银行客服、航空公司等机构的电话时,不要轻易相信对方提供的信息,不要点击对方发来的链接,也不要下载对方推荐的APP。

一旦不小心下载了不明APP,发现手机出现卡顿、黑屏、自动弹窗等异常,或收到陌生扣款通知,又该如何应对?王佳表示,可以迅速拔出手机SIM卡,阻断骗子获取短信验证码。同时,断开Wi-Fi和移动网络,防止骗子继续远程控制手机,“还有一点也很重要,那就是尽快用家人的手机拨打银行客服电话,将名下所有银行卡挂失,之后再拨打110报警。挂失银行卡比更改密码更有效,可以直接阻断骗子的盗刷行为”。

(《北京晚报》)