包装诈骗信息 引诱开通授权

自动扣费 扣你没商量

在数字支付便捷普及的今天，各种关于自动扣费的骗局正悄然酝酿。无论是年轻人还是老年人，都容易成为骗局的受害者。其中，有当事人警惕心不足、观察不仔细的原因，也有平台安全提示不够到位的问题。尽管事后回顾时能发现蹊跷，但身处于骗局之中，普通人实在难以分辨。

想买低价会员 却被盗刷500元

回想起前段时间的一次被骗经历，高先生现在还有些后怕。本想着“薅点便宜的羊毛”，没想到最后被“薅”的竟然是自己。

高先生看视频时，发现一部网剧需要开通会员才能收看。相比于直接在网站上开通会员，他依稀记得，在二手交易网站上，也会有一些卖家以相对低廉的价格售卖视频网站的会员。去二手交易平台一搜索，还真找到了不少卖家。

对比各家，高先生发现其中有一家的价格相当便宜，虽然卖家并未标注“信誉良好”，但他也没太在意。付了几元钱的开通费之后，对方发来了一个领取会员资格的二维码。扫码之后，界面跳转到了Apple服务的开通付款授权，高先生此时隐约感觉到了不对。

“如果当时在这一步停住就好了，因为我没看明白授权是什么意思。”但高先生之前并未在二手平台购买过其他网站的会员，他下意识地以为，开通授权指的是让对方能帮自己开通会员，于是便点了开通。

没想到，在接下来的十分钟里，高先生的手机开始不断收到扣款通知，而这些扣款全都流向了一个他从未玩过的网络游戏，单笔金额从几十到上百元不等，损失很快达到了500元。

高先生立马意识到自己的支付软件被盗刷了，赶紧联系了支付平台的客服。在对方的帮助下，高先生解绑了一个根本就不属于他的Apple账号，这才让损失没有进一步扩大。“最后我才弄明白，我扫的那个码，做的那个授权，其实是把我的支付软件绑定在了骗子的Apple账号上。对方之后的任何消费，刷的都是我的支付软件，而且都是免密支付。”

App要求授权的说明模糊隐蔽易被忽略

套路简单有效 用户极易中招

麦女士的父亲，到底是怎么落入陷阱的？因为当时父亲收到的垃圾信息都已删除，麦女士推断，应该是一些平台自动向父亲推送了购买会员的功能，父亲误点之后才开通了自动扣费服务。

记者在应用商店搜索发现，有不少App是需要付费之后才能下载的，相对来说还容易避开。还有些App确实如麦女士所料，虽然下载时完全免费，但内置了VIP会员的开通服务。比如一些网络短剧平台，点击观看一部网剧，刚开始的几集还是免费收看，可到了之后的收费集数，界面上就跳出了一个购买会员的选项，其中第一项就是“官方推荐”的连续包月服务。

还有些App则更加离谱，下载完成后，点进去的第一步就是要购买会员，之后才能正常使用。但在购买流程上，平台却耍起了花招。比如一款提供“养生指导服务”的App，页面上会有一个大大的按钮，写着“开始免费试用”。但在按钮的旁边，却有一行非常不起眼的小字：“每周仅需48元，可随时取消。”而一旦用户点击开始试用，系统就会跳转到自动续费的开通界面。如果是辨别能力差的老人，可能还以为是在填写什么注册信息。

这些骗老人的App，用的是“小字套路”，如果仔细观察，发现陷阱倒也不难。而高先生遭遇的套路，连年轻人都会中招，到底是如何做到的？记者本以为，这项骗局会相当有技术含量，可经过测试才发现，想要完成行骗竟然异常容易。

记者通过很简单的方式，就能调取出远程绑定支付平台的二维码，而这就是高先生在二手平台交易时收到的二维码。在记者调取出的二维码旁边，倒是会提示“支付宝扫码安全验证”等提示，但骗子显然把这些信息都截取掉了，只剩下了一个二维码。

而在扫码之后，会进入开通付款授权服务的页面，这也是高先生感到有些“蹊跷”的步骤。这时，系统会弹出一个安全提示：“请确保这是你本人的Apple账户，开通后将为该Apple账户下所有付款行为进行授权。”记者将这个截图发送给了高先生，他表示，当时好像有这么一个提示，但他以为这里所说的账号是自己的账号，并不知道指的是骗子的账号。

随后点击开通授权，如果之前开通了面容支付功能，在用户面对手机的一瞬间，授权就开通完成。之后，支付软件就绑定到了骗子的账号上，整个过程连1分钟都用不了。

自动扣款数月 老人不知来源

有些骗局是专为年轻人设计，还有些骗局盯上的则是老年人。麦女士的父亲已经70多岁了，平时会用一个智能手机发发微信，看看新闻和视频。但因为操作不熟练，眼神也不太好，每过一段时间，父亲的手机上总会出现一些不知是从哪里下的App，麦女士只能时不时检查一下父亲的手机，帮他删一删。

有一次在帮父亲做完手机的清理之后，麦女士无意间发现，父亲的手机消费记录里，居然有三个不明平台的自动扣款，每月扣十几元到数十元不等，而且已经扣了好几个月。问了父亲，他根本不知道这三个签约是什么意思，又是怎么签上的。

“我怀疑他是在用手机的时候误点了什么广告链接。老人不太懂，有时也不会仔细看。骗子就是利用这一点，专门骗老年人。”想到这一点，麦女士有点气不打一处来。她首先在父亲的手机里关闭了自动扣款服务，随后又通过支付记录的信息查到了扣款来源公司，气愤地给对方拨打了电话。有两家公司明显是“做贼心虚”，很快就同意了退款。但还有一家死不认账，最后款也没能退回来。

“人家跟我说，他们是一个提供健康服务的公司。我父亲下载了App，扣款是我父亲同意的，他们也提供服务了，说他们是诈骗，他们不认。”但事实上，麦女士的父亲根本就不知道那款App是干什么的，更别提享受什么所谓的服务了。但因为老人实在说不清楚是怎么开通的自动扣费授权，麦女士一时也拿不出认定对方是诈骗的证据，最后只能吃下这个哑巴亏。在麦女士看来，这类自动扣费的陷阱，相比于单笔金额的诈骗更加可恶。“如果不是我检查我父亲的手机，还不知道扣费要扣到哪年哪月去。”

安全提示不足 缺少防控手段

记者随后在二手平台上，找到了不少售卖低价视频网站会员的网店。其中，有些正规的卖家，会要求买家在支付时提供手机号，以协助开通对应的会员。还有些卖家，则会像高先生遭遇的那样，在收到付款之后发来一条信息，里面可能是一个链接，也可能是一个二维码。如果卖家有意诈骗，通过这种方式，可以引导买家进入设计好的诈骗页面。

回顾被骗的过程，高先生表示，从事后分析的角度，肯定能发现有不合理的地方，也有自己应该多加注意的地方，但在当时真的很难分辨骗子的套路。而在安全提示方面，系统也有做得不到位的地方。“首先，为什么手机能这么简单就开通免密支付，而且还是远程开通？另外，为什么在绑定的时候，系统没有提示您绑定的是哪个账号，而是直接绑定成功？”

记者将这几个问题也询问了手机厂商的客服，对方表示，高先生遇到的情况并非个例，客服此前已经收到过多个类似的投诉。远程绑定支付平台的办法确实是存在的，也容易被骗子利用，目前仅能告诫用户，不要点击陌生来源的链接或扫二维码。

“那现在有没有一种办法，能让我的支付平台上个锁，不去绑定任何的手机账号？如果能上锁，不就不会被骗了吗？”记者向手机厂商以及支付平台的客服提出了这个问题，但双方均表示，目前没有这种安全措施。

（莫 凡）