

演唱会门票含泪转让不加价？有诈！

顶流歌手演唱会一票难求，却遇“好心歌友”原价转让门票……嫌疑人以“原价门票”为诱饵，在社交平台发布虚假信息，诈骗歌迷购票款数万元。近日，湖北省武汉洪山警方通过对一起警情进行深挖，破获7起演唱会门票诈骗案件。

“我有2张武汉站演唱会门票，临时有事去不了，都是歌迷不加价，只求去了现场帮我拍段视频……”近日，武汉市公安局洪山区分局洪山派出所接到唐女士报警，称其在某社交平台上看到有人出售某知名歌手演唱会武汉站的门票，后通过微信找对方购票，被骗1500元。

唐女士介绍，自己是这位歌手的忠实粉丝，因没有抢到票，感到十分遗憾。案发当日，刷小红书时，唐女士偶然发现有人出售偶像武汉站演唱会的门票，而且没有加价，便立即联系对方咨询购票事宜，生怕这2张票被其他歌迷抢走。

添加对方微信并支付750元定金后，对方发来一段快递工作人员将门票放进快递文件袋的视频，并称自己不能去现场觉得很遗憾，只求唐女士到了现场能发一段偶像的视频给他。唐女士觉得自己很幸运，遇到了不加价的



歌友，欣然支付了750元尾款，并期待着装有门票的快递能早点收到。

然而，两天过去，她迟迟没有快递的消息，多次催促，对方却提供不了快递单号。眼看演唱会的日期越来越近，唐女士向对方协商退款，但对方却坚称已经发货，提出唐女士必须拦截快递才能退款。此时，她意识到遭遇骗局，向警方报案。

接到报警后，洪山派出所民警立即展开调查。此时，对方的小红书账号已经注销。民警推断嫌

疑人很有可能通过相同的手法欺骗其他歌迷，为逃避惩罚而注销账号。

在洪山分局刑侦大队的支持下，办案民警对嫌疑人收款账号进行资金流分析，印证了此前的推断。系统显示，嫌疑人近期存在多个1500元左右的收款记录，疑似均为受害人购买门票的转账。民警对多名受害人逐个进行电话回访，发现其均为购买演唱会门票的受害者，其中大多为武汉地区的在校学生，且很多人还没有意识到被骗。

警方进一步调查发现，嫌疑人在上海徐汇区一银行办理了销户手续。经过对多条线索进行综合分析，民警确认目前身在上海的21岁福建籍男子魏某具有重大作案嫌疑。办案民警立即与上海警方取得联系，请求协助抓捕。

随后，上海警方抓获了嫌疑人魏某。武汉洪山警方立即赶往上海，对魏某进行讯问。经查，魏某沉溺于网上赌博，输光积蓄后无意间在小红书上看到了求购这位歌手演唱会门票的帖子，当即想出以虚假售卖演唱会门票的方式骗取钱财，在短短两天时间里，让7名歌迷中招，非法获利10500元。

日前，魏某因涉嫌诈骗被武汉洪山警方押解回汉并刑事拘留，案件正在进一步深挖之中。

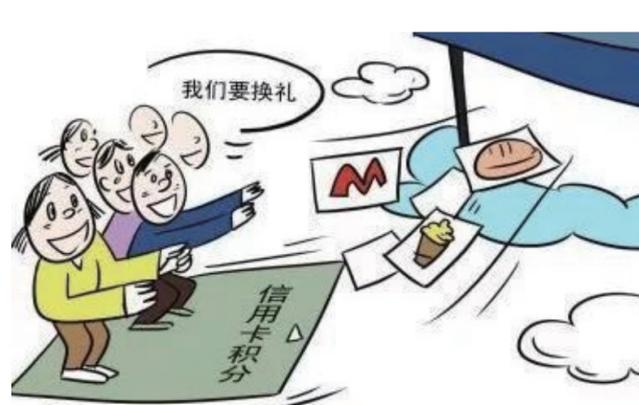
【民警提醒】

近期多地演出市场开启“演唱会时间”，人气歌手的演唱会往往“一票难求”。歌迷通过各种非正式渠道购票，不仅溢价严重，还会一不小心掉入诈骗陷阱。

理性“追星”，购票一定要认准官方网站，切不可轻信社交媒体上的“票务代理”和“黄牛”。

(来源:国家反诈中心)

积分即将清零？小心是圈套！



“您的积分即将过期清零，现在可以用您的积分兑换精美礼品。”你是否收到过这种“积分清零”的短信？小心，这很有可能是诈骗！

近日，杨女士收到一条“积分清零”短信，称杨女士积累的18650分即将过期清零，为避免积分失效，可以点击链接限时兑换礼品。于是，杨女士点击链接进入到一个积分兑换页面，选好了要兑换的商品后，显示只能部分兑换积分还需要支付少部分费用。

杨女士按要求填写了姓名、电话号、身份证号、银行卡号、以及验证码等信息，随后又被要求下载一个安全控件安装后进行支付。杨女士按要求操作完，发现她的银行卡被人消费了2万多元。意识到被骗的杨女士立即选择报警求助。

【民警提醒】

诈骗分子用伪装的号码，向受

害人发送带有钓鱼链接的短信，谎称“回馈用户，积分可兑换精美礼品”，诱使受害人进入钓鱼网站输入身份证号、银行卡号、验证码等个人信息。随后，以“安装银行卡安全控件”等为由，诱骗受害人下载木马软件。这时，诈骗分子利用骗取到的银行卡号、验证码等信息，盗刷受害人的银行卡，借机敛财。

民警提醒，要仔细甄别。遇到“积分清零”的短信或电话要仔细甄别，若短信发送者为陌生号码时，切勿轻易相信。要保护隐私，凡是短信中附有网址链接的，一定要注意识别，不要随意点击，它们很有可能是仿冒的钓鱼网站。当遇到需要输入真实姓名、银行卡号以及验证码等隐私信息时，一定要多留心。如不慎被骗，请保留相关证据，并第一时间拨打110报警！

(来源:国家反诈中心)

网课能申请退费？

一女子中招被骗40余万元

随着网络兴起，线上学习成为了许多人提升自我的重要途径。然而，学海虽无涯，骗子也“奋进”，在“求学提升”过程中，他们早已布下罗网，伺机而动。

近日，广东省揭阳市一名群众就不幸落入不法分子织的骗网中，损失惨重。

陌生短信 引导进群

2022年12月，家在普宁的小吴在网上花费399元报名了“阔学培优”App网课。此后小吴一直在该App上学习。

直到近日，小吴意外收到一条短信息：【阔学培优】吴女士，您好，您很久未登陆阔学培优App进行学习，如果对课程不满意，可以加QQ群58***27，进群结算返还学费。

因小吴确实购买过该网课且没有进行学习，便没有怀疑真实性，按照短信提示加入指定的QQ群聊。

下载App 购买证券

进群后，群管理员称，申请退学费需通过“英大经办”App进行办理，并在群聊中发布下载链接。小吴下载注册账户后，便收到App客服“清退办专员”的私信。

对方以“审核退款资格”为由，向小吴索要其个人信息，随后对方称“退费需通过购买公司证券进行增值”的方式退款(购买多少钱证券，即可返还本金及20%的利息)，引导小吴注册账号并绑定银行卡。

施以小利 博取信任

小吴注册账号后，发现账号钱包有100元并能成功提现到银行卡。得到甜头的小吴更加确信对方是在帮自己退学费，按照对方提供的方案购买了1500元“证券”。随后对方向小吴发送一份回款协议，表示本金连同利息会分批到账，同时小吴账号收到600元回款，并成功提现至银行卡。

2次成功提现让小吴完全放松警惕。

操作错误 大额转账

见到有利可图，小吴在对方的指导下继续购买了1001元“证券”。对方以“清退学员较多需要随即匹配统一金额学员一起完成回款指标”为由，将小吴拉进一群

聊，群内一名“监管员”，一名“规划师”，4名办理回款学员(3个是托)。

小吴按照“规划师”的指引继续操作。对方以操作失误为由，要求小吴继续增加充值额度以寻求一次性汇款成功。

期间，小吴在对方诱导下多次向指定银行账户转账共计295201元。

沉没成本 继续转账

小吴已被高度洗脑，面对高达29万余元的巨额投入，不甘心的小吴无法接受自己被骗的事实，宁愿选择相信骗子的说辞：退款流程没有问题，只要再次转账后即可进行资金清退。小吴再次向骗子转账，企图挽回前期投资。

觉察被骗 损失惨重

期间，对骗子抱有一丝希望的小吴再次向对方指定的银行账户多次转账共计131171元。

转账后，小吴等来的不是“资金清退”，而是骗子贪而不厌的索要：“中国税务”要求转账补缴税款。小吴这才如梦初醒，发现被骗共计425672元。

【民警提醒】

诈骗分子通过非法手段获取培训机构用户信息，筛选诈骗目标对象，发送短信、点名道姓，告知报名课程可以申请退费以此获取信任；以购买理财产品获利返还学费、充值返利、做任务等理由，引导受害人点击陌生网址链接下载虚假App，填写个人信息、银行卡等资料进行注册。诈骗分子引导受害人向对方指定的多个“个人账户”继续追加资金，随后又以操作完成后一次性返还、操作错误、账户冻结、解冻金等理由不断诱导受害人转账的方式实施诈骗。

民警提醒，正规的退款流程，一般是以原路退还的方式将钱款退至本人缴费账号。如接到自称是培训机构工作人员主动退费的电话时，一定要保持警惕，不要加入陌生的QQ群、微信群，不要点击陌生链接，更不要相信任何理由的转账要求，要求转账的退款都是诈骗！

(来源:国家反诈中心)

“杯子快递”不是“馅饼”是诈骗



没有在网上下单购物，却莫名其妙收到一件快递……近日，一些市民遇到了这样一件稀奇事，有的收到指甲剪，有的收到手机支架，还有的收到杯子。警方提醒，这是一种骗局，收到这样的快递件，千万不要扫描物件上的二维码，以免掉入骗子的陷阱。

“快递盒是破的，打开掉出来一个破得掉渣的搪瓷杯，杯子上印着‘美团优选’的宣传活动。我经常通过美团下单，但美团优选从没用过。”张女士很奇怪，自己最近并未网购，却莫名收到一个杯子快递，快递盒的面上还有寄件方的地址、电话，但怎么都联系不上寄件人。

扫描搪瓷杯上的二维码，添加上自称“美团在线客服”的工作人员。对方声称：“只要提供本人手机号，就可以免费领取大米、食用油、蔬菜等物资。”跟着工作人员的话，张女士被加到名为“美众优选”的微信群，“管理员”开始布置任务……看着这些操作，张女士回想起之前社区民警入户反诈宣传的话，意识到自己遇上了骗子，果断退出微信群，联系了官方客服。

经过与美团官方的电话求证，张女士得知，美团没有直接邮寄礼品、水杯、水果、毛巾之类的活动，更不会通过客服或微信联系用户，要求加群来派发红包等。所以，寄快递的人无疑就是骗子。

无独有偶。近日，林女士也收到一个附有二维码的杯子快递，上面写着“xx百亿补贴活动”。她没多想就扫了二维码，添加了一位陌生好友。对方拉她加入一个群聊，按照要求浏览店铺刷单转账。做了2单任务后，她觉得收益不错且还能提现，于是放松了警惕。

接下来，林女士按照“客服”的要求，继续刷单转账。待转账13万余元后，“客服”以操作失误为由，

让她再转7万元才能提现。在“客服”的哄骗下，林女士依旧不疑有他，连续转账，结果被骗20万余元。

【民警提醒】

诈骗分子通过非法渠道获取到受害人的相关信息：姓名、手机号、收货地址等，并邮寄带有二维码的水杯。用邮寄的方式广撒网，只要扫描了杯子上的二维码就可能落入诈骗分子设下的圈套。有的诈骗分子还会冒充电商平台客服再送一袋米、一箱水果或洗衣液等礼品，让受害人对他们深信不疑。领取到免费礼品后，有人可能会认为这是电商平台送来的福利，没有多想就扫描对方提供的二维码，加入骗子所开设的聊天群。

随后，自称“客服人员”的QQ、微信会主动来添加好友，通过私聊给受害人派发任务，开始会有小福利，刷单几百块返现几十块，任务完成即可领取红包让受害人先尝点甜头；等受害人彻底放下戒备后便被引诱下载软件、充值垫付，完成佣金更高的兼职任务，一步步走进刷单诈骗的陷阱。往往刷了几千、几万元的大单后，不法分子会以“系统卡顿”“任务超时”“操作失误”等理由告知受害人无法提现需要继续充值；等受害人多次尝试均无法提现时才知后觉自己被骗了，但为时已晚。事实上这都是骗子的剧本，受害人根本无法提出本金和佣金。

民警提醒，“杯子快递”骗局其实就是刷单返利诈骗。刷单本身就是一种违法行为，贪图小利往往会遭受重大损失。如果收到这样的快递，千万不要扫上面的二维码。在扔掉杯子、宣传页前务必将杯子、宣传页上的二维码涂抹掉，避免有人捡到后被骗。

(来源:国家反诈中心)



浙江省文明办