

## 工行安庆分行开展“3.15 消费者权益保护教育宣传活动”

## 关于警惕疫情防控期间金融诈骗的风险提示

近期,有不法分子借机利用新冠疫情防控相关工作实施诈骗,由于诈骗手法被“包装升级”,使得消费者更加难以识别,容易被此类新型诈骗所侵害。为保护消费者权益,工商银行安庆分行在此总结了四种常见的手法,提醒各位消费者擦亮双眼,提高风险防范意识,保护自身信息安全和财产安全。

**手法一:假冒流调人员谎称疫情流调**

流行病学调查(简称“流调”)作为最重要的疫情防控工作之一,每位市民都有义务配合。不法分子看准了这个可以获取个人信息的机会,打着“流调”的幌子要求市民提供合理范围以外的信息,进而实施诈骗。不法分子伪装流调时,往往会询问以下信息或要求操作以下步骤:1.询问财产等与疾病传播不相关的问题;2.发送二维码要求扫描;3.索要银行卡号、密码或短信验证码;4.发送链接要求点击;5.推销产品或编造理由要求付费;6.要求加入QQ群、微信群;7.要求转账和进行“资金核查”。

**手法二:假冒机构人员谎称拥有“特效药”**

不法分子假冒药物研究(医疗)机构的名义,推广所谓防疫“新药”、保健品、防疫中草药;或者用假冒伪劣药品贴上外文标签,冒充国外研制的新药,谎称对预防新冠肺炎有非常好的功效,诱导用户购买以及在钓鱼链接中输入个人敏感信息,进而骗取个人财产。

**手法三:冒充老师混入家长群**

不法分子潜入班级家长群,通过设置与老师相同的头像和昵称,利用中午或晚上休息时间,假冒老师以疫情防控期间学校提前收取学费、培训费、资料费为由,引导家长们用微信或者支付宝扫描转账,造成群体受骗;或者找部分家长私聊,发送虚假缴费通知,骗取钱财。

**手法四:假冒医院人员谎称亲友患新冠**

不法分子谎称是医院的工作人员,以受害人的亲友患“新型冠状病毒肺炎”,现已被隔离,在医院救治为名,要求受害人向其提供的账号汇款缴纳“住院费”,以此骗取受害人钱财。

上述行为严重侵害了消费者信息安全权和财产安全权。针对以上四种诈骗手法,工商银行安庆分行提醒消费者从以下几方面做好防范:

一是注意识别正规“流调”与伪“流调”。正常的“流调”过程中,工作人员会询问以下问题:1.个人信息,比如姓名、年龄、家住哪里、家里有几口人、现在位置等;2.健康状况,例如近期可有不适,近期是否就医,是否有发烧咳嗽等异常情况,是否做过核酸检测等;3.疫区旅游史,比如是否去过疫区旅行、经停过,到过的地方等;4.疫区居住史,例如老家在哪儿,是否回去等;5.病例密切接触史,比如同乘旅客、近距离交流、居家成员等;6.交通工具,比如近期是否乘坐飞机、火车、汽车、轮船等;7.其他对疾病防控有用的信息。消费者如果接到询问超出上述范围的“流调”电话,请一定要提高警惕,不透露自己的财产信

息和短信验证码,不点击任何链接或扫描二维码,更不能进行转账。

二是注意针对疫情目前尚未研发出特效药。消费者不要相信陌生人口中所谓的“特效药”等信息,更不要通过网上银行、微信、支付宝等方式进行转账。

三是注意对各种微信群、QQ群人员的身份识别。群组管理员要加强入群管理,及时清理不相关的群成员;家长和老师要注意个人账户信息的保护,不将个人账户等敏感信息透露给未经核实身份的人员或公开在互联网上;家长们缴费、转账要认准学校,并注意核实老师的真实身份,主动去官方验证缴费通知的真实性;缴费前要和学校、老师通过电话等方式确认,不向陌生人账户转账;一旦发现被骗,要注意留存证据,及时报警并通知群成员。

四是注意提高警惕,接到陌生电话要求缴费时要注意核实医生的真实身份。可以通过查询医院官方对外公布的电话联系等方式进一步确认,主动去官方验证缴费通知的真实性,不向陌生人账户转账。

## 打好宣教“预防针” 提高防骗“免疫力”

近期,不少不法分子蠢蠢欲动,企图利用小恩小惠对老年客群进行虚假宣传,实质是扰乱金融秩序,侵害消费者合法权益。工商银行安庆分行提醒广大金融消费者提高风险防范意识,远离非法金融活动。

**手法之一:发放“降价”“领取优惠券”链接**

购物网站纷纷推出预售活动,其中不乏“领红包,享优惠”等类的宣传词,不少不法分子从商家此类优惠活动入手,开展电信诈骗活动。比如,诈骗分子发送“预先降价”等短信,短信中提出“点击链接领取优惠券”等文案,然而链接中多含有木马病毒,会盗取个人信息以及银行卡信息,造成用户经济损失。

**手法之二:“红包”陷阱 收集个人信息**

有时我们会收到红包链接,但是通常需要先关注或者转发N个好友微信群,达到一定金额方可提现。此类链接往往在用户大量输出私人信息后只获得微薄收益,甚至一无所获,而不法分子则以此非法收集了更多的个人信息。

**手法之三:谎称可以信用卡“提额”**

诈骗分子多瞄准目前广受消费者欢迎的各大银行信用卡作为诈骗

噱头,谎称可以提升信用卡额度,要求用户先扫码付款收取额外费用,或者利用虚假短信、客服和银行网站界面,通过客户输入信息获取客户银行卡、身份证和CVV码等个人信息,诈骗客户卡内可用额度。

**手法之四:“客服”退货诱惑**

“退款不退货”这个行诈手段近几年在网购人群中屡试不爽,不法分子在获取到用户购买记录后,谎称为该商品客服,提出该商品存在质量等问题,向客户索要银行卡等个人信息进行退款不退货的补偿,在客户提供给“客服”手机验证码后,银行卡余额将被全部划走。

上述行为侵害消费者合法权益,影响恶劣,工商银行安庆分行在此提示消费者谨记:

敢为人“先”,也要擦亮眼睛。预售活动是商家为吸引消费者打造的预热活动,消费者应只相信正规购物平台的优惠活动,对陌生网站与短信链接发送的优惠链接保持警惕,更不要好奇心作祟,点开领取,步步陷入陷阱。

“红包”为什么那样红,“血”的教训染红了它。目前盛行的“红包雨”席卷各大社交平台与好友群,信息鱼龙混杂,让人眼花缭乱。您要识别真伪信息,任何需要提供个人信息的红包链接都有电信诈骗的嫌疑,不要好奇心作祟,误入钓鱼网站,泄露个人银行卡信息,最后非但没有获得

优惠,反而损失惨重。

不要让提“额”,提走的是消费者的金额。信用卡额度提升是通过正规渠道办理的,一般银行等正规机构会根据用户征信报告,资产情况以及收入等多方面的信息考量,来为用户进行提额审核与办理。请您不要相信任何非正规机构的提额承诺,认

准官方渠道进行办理。

退款有道,认准官方平台。如有退货退款等申请需求,请认准官方平台进行操作,不需要提供任何私人信息以及手机验证码,经平台简单操作后,款项会自动回到付款账号,任何要求添加私人社交联络方式的操作均有诈骗嫌疑。

