2023.09.13 星期三
责编/曹吟秋 版式/杨丽丹 校对/谢禄林
贵州法治报

明明没有网上购物，但却收到了快递包裹，里面不仅有小礼品，还有一张中奖率是百分之百的刮刮卡。这些快递是谁寄来的？真有这样的好事吗？记者用自己的亲身经历给出了答案。

警惕！

不明快递里100%中奖的刮刮卡是诈骗

快递中的刮刮卡100%中奖 兑奖则需扫描二维码

近日，记者收到了一份神秘快递，里面有一份小礼品，一封感谢信，还有一张刮刮卡。感谢信上称，这是一份感恩回馈客户的谢礼，并邀请客户参加“邀您一起刮豪礼”的活动，最高可获得1万元的现金奖励。

记者拿着收到的快递来到北京市公安局刑事侦查总队，找到之前采访过的反诈民警，探寻神秘快递背后隐藏的秘密。

在民警的见证下，记者刮中了一个18元的现金红包和奖品水果。在刮刮卡上写着，如果要兑奖需扫描上面的二维码。

北京市公安局刑事侦查总队十支队民警高山介绍，这是最近高发的新型电信网络诈骗，犯罪嫌疑人的作案手段就是邮寄一个陌生快递，并附赠一张100%中奖的刮刮卡，一旦扫码领奖，就是被骗的开始。

记者随后扫描二维码时，出现一行绿色的小字：“此二维码已通过安全验证，可以放心扫码。”

民警提示，这其实是个有迷惑性的细节，这行小字让被害人觉得这个二维码是安全的。但实际上，这些字是被设计制作在图片上的，没有经过任何系统验证。

利用红包福利诱人进群 记者因询问过多被踢出群聊

记者扫码联系上所谓的“美团客服”后，客服首先要求提供中奖手机号和获奖刮刮卡的照片。民警表示，这是因为诈骗分子发送快递时已经有了被害人的手机号等个人信息，再次提供手机号和照片，就可以实施精准诈骗。

客服告诉记者，水果礼品约一小时内可以送达，但是现金红包要加入到一个商家微信群内领取，进群后还可以参与不定时的红包雨、现金抽奖、生活电器试用等活动。

随后，记者扫描客服提供的二维码加入了一个微信群。记者观察，群里不停有新的“中奖者”进入。但是，除了管理员发布的“红包稍后统一兑换”“保持安静”等提醒以外，没有其他人发言。当记者对奖品配送、红包兑换等问题提问时，还受到了群聊管理员的警告。

记者还发现一个细节，这个活动的举办方号称是淘宝，而扫码后的客服人员却显示来自美团。对此，记者向客服人员进行咨询，对方则表示，这是商家联盟合作推出的回馈老用户活动。

很快，群里已经有所谓中奖者晒出了自己收到的礼品，有牛奶、食用油。记者刚想询问自己的礼品为什么没有收到时，却发现被移出了群聊。民警分析，这是因为记者向客服咨询的问题太多。“客服感觉到你的逻辑性很高，防骗意识比较强，所以就把你踢出群聊。”当记者询问客服人员，自己为什么会被移出群聊，对方也没有再进行回复。

随后，记者分别致电了淘宝和美团的官方客服，询问他们是否举办过此类回馈活动。平台客服人员明确回复：没有直接邮寄礼品、刮刮卡扫码抽奖的活动，也不会无故联系用户要求加群、派发红包等。

与利用刮刮卡诈骗手段类似的，还有“惊喜盲盒”骗局等。骗子会给用户邮寄“惊喜盲盒”，里面有伪造的微信红包，引诱被害人点击APP的下载链接。

如果真的扫了二维码，点开了下载APP的链接，又会发生什么呢？

刮刮卡实为刷单诈骗引流工具 被害人被骗走20多万元

今年7月，徐女士收到了一张刮刮卡，之后她不但扫了码、进了群，还下载了做任务的APP。她发现，在APP的任务群内，人数竟有1800多人。“直观看，这就让你觉得参加这个活动的人特别多。”

在收到一些小额返利后，徐女士开始相信这个活动是真实的。在客服的诱导下，徐女士开始在APP中完成一些大额任务，比如给贫困地区捐款等。“比如你先捐助30块钱，然后截图给客服，他不光把30块钱返还给你，另外再多给你20块钱，说这个是商家给予你奉献爱心的补助。”

徐女士说：“你就觉得这好像是特别公益的一件事，特别急于赶紧把它完成好。实际上当时已经感觉到这个事不对，但是也都有那种侥幸心理。”

捐款的任务都在几百到几千元不等，徐女士完成了几个任务之后，在APP上都显示有返现到账。随后，客服又发布了更大金额的任务。

徐女士回忆，这项任务由五人共同完成，要求每个人充值上万元。但是，任务有时间限制，只要有人超时，任务就算失败。失败了就要五个人一起再做下一个充值任务，才能把之前投进去的钱拿回来。民警表示，其实这里有一个心理学的效应——沉没成本。“她这个时候如果不再充值，可能之前的钱都收不回来了。但如果再继续充值，钱就有可能会拿回来。”

当20多万元全部打了水漂，徐女士才意识到自己真的被骗了。民警告诉她，群里其他晒奖励的人、和她一起做任务的人都是托。

民警调查发现，徐女士遭遇的正是典型的刷单诈骗，而这张100%中奖的刮刮卡，则是刷单诈骗的一种引流方式。

警方提示：小心“馅饼”变陷阱

民警调查发现，犯罪嫌疑人是通过步步设局来诱导被害人的。

第一步：通过互联网黑灰产业链获得潜在被害人信息。

第二步：以知名互联网企业的名义快递廉价礼品，并附上刮刮卡和入群二维码，赢得被害人好感。

第三步：设计所谓的“安全扫码页面”，打消被害人顾虑，诱导被害人扫一扫。

第四步：冒充知名企业客服，诱导被害人参与非法刷单等诈骗活动。

民警提示，收到陌生快递时一定要提高警惕：“要看是不是自己购买的。如果是赠品，一定要跟官方客服核实。如果不是，很有可能就是骗子寄来的诱饵。”

新型骗局层出不穷，为了诱人上当受骗，骗子也会不惜投入成本，这也使得这些骗术越来越难识别。然而，只要我们坚信没有天上掉馅饼的好事，不贪小便宜、不轻易转账，遇到没听说过的事和亲人朋友们先聊一聊，那么我们掉入诈骗陷阱的几率也会大大降低。

（据央视新闻微信公众号）

延伸阅读 认识三种新型骗局

记者 曹吟秋 整理

一 FaceTime冒充金融客服诈骗

近期，上海市接到多名市民报警，均称遭遇了陌生人打来的FaceTime电话诈骗。

诈骗分子通过FaceTime联系受害人，冒充京东金融、支付宝、微粒贷等金融平台客服，或是冒充银监会工作人员，以国家政策调整为理由，以个人征信为威胁，要求受害人进行注销账户、消除贷款等操作。

之后，引导受害人下载腾讯会议、zoom等各类具有实时屏幕共享功能的APP，打开不明网址联系在线客服，诱骗受害人将钱款转至指定账户，或引导受害者从银行或其他网贷平台进行贷款，承诺资金审核后会将钱款返还，待转账完毕，就将受害人拉黑、失联。

【如何防范】

1. 不接听陌生FaceTime电话，可关闭手机FaceTime通话功能。

2. 选择官方正规平台，进行独立的账户开户和注销操作。如接到任何平台“客服”的电话，不要轻信，应返回官方平台或拨打官方客服电话，联系工作人员核实情况，在官方平台进行独立操作。

3. 保护个人隐私，警惕视频共享。身份信息、银行账户、验证码、各类密码和人脸识别信息要小心保管，绝不透露。警惕下载不明软件、APP进行屏幕共享的操作，正规平台不会使用该方式“教学”。

二 冒充好友诈骗

微博经常互动的好友，突然在平台私信你请求帮助，看着熟悉的账号名、头像和说话方式，你并没有心生疑虑，从而落入对方精心布置的陷阱。（其他社交平台也会有类似骗局）

不法分子会注册一个全新的微博账号，盗用微博头像以及个性签名但昵称前多了一个“。”或“-”等。新的账号迷惑性强，极易上当受骗。

骗子会私信仿冒对象列表好友，或者发表一些相同的内容，并@仿冒对象互动较多的好友，使得受害人误认为这是自己的微博“好友”，从而实施精准诈骗。诈骗分子会以“微博代付”“手机漫游被限无法订票”等各种理由骗取信任，诱导受害人帮忙垫付资金。

【如何防范】若在社交软件上遇到好友要求转账汇款时，一定要先通过电话、视频、面对面等方式验证对方是否为本人！如对方以“不方便通话”“情况紧急”“信得过”等种种理由予以回避，则应当提高警惕，切勿碍于人情而盲目相信对方，不经核实切勿向对方支付钱款。

三 AI诈骗

诈骗分子通过各种渠道收集受害人及其熟人的信息，如姓名、电话、社交账号、照片等利用AI换脸技术，将自己或他人的面部替换成受害人熟人的面部，并利用AI拟声技术，将自己或他人的声音转变成受害人熟人的声音。通过社交软件或电话联系受害人，并以视频方式进行信息确认，让受害人放松警惕，并以各种理由诱导受害人转账汇款，如借钱、投资、紧急救助等，并催促受害人尽快操作。收到钱款后诈骗分子便立即消失，切断与受害人的联系。

【如何防范】以AI为基础的诈骗手法越来越多，群众要提高自我防范意识，避免上当受骗。眼见≠真实，如果有陌生人或熟人通过电话或视频联系你，并要求你提供个人信息或转账汇款要保持警惕，首先，要核实对方身份，不能仅仅因为一通电话或者一段视频就轻易相信；其次，不要轻易在网上泄露自己的社交圈子和私密照片，避免被不法分子利用；最后，不轻易提供人脸、指纹等个人生物信息给他人。一旦发现风险，及时拨打110报警！

评论

共筑防范电信诈骗“防火墙”

近日，电影《孤注一掷》爆火，该片以海外网络诈骗全产业链内幕为主题，引发了观众对网络诈骗的深刻思考和警惕。习近平总书记曾对打击治理电信网络诈骗犯罪工作作出重要指示强调，要坚持以人民为中心，统筹发展和安全，强化系统观念、法治思维，注重源头治理、综合治理，坚持齐抓共管、群防群治，全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任，加强法律制度建设，加强社会宣传教育防范，推进国际执法合作，坚决遏制此类犯罪多发高发态势，为建设更高水平的平安中国、法治中国作出新的更大的贡献。

整治电信网络诈骗，归根到底还应有法可依。《中华人民共和国反电信网络诈骗法》于2022年12月1日起施行。明确了各级政府和有关部门责任，从国家层面建立反电信网络诈骗工作机制，统筹协调打击治理工作，全方位筑牢反电信网络诈骗法治防火墙。实践证明，为人民群众织密个人信息的安全网才能防患于未然。譬如，湖北省通信管理局认真贯彻落实习近平总书记重要指示精神，严格按照《中华人民共和国反电信网络诈骗法》规定开展工作，2023年上半年，湖北省拦截省外境外诈骗电话累计35.2万次，日均近2000次，将1.8万个电话号码纳入来话黑名单管理；封堵涉诈网站、域名1538万个，累计阻断省内网民对涉诈域名的访问64.9亿次，撑起人民群众通信安全“保护伞”。打击治理电信诈骗的号角正在持续吹响，在法律利剑的高悬之下，优先寻求重点领域的突破，加速构建更健全的预防体系，全力遏制电信网络诈骗的嚣张气焰，实打实地增强社会安全感。

防范电信诈骗在有法可依的同时，行业治理的助力也必不可少。各电信企业、银行、支付机构、互联网企业等应承担风险防控责任，建立反电信网络诈骗内部控制机制和安全责任制度，加强新业务涉诈风险安全评估。目前，中国人民银行推出“国家反诈中心”APP、96110预警劝阻专线、12381涉炸预警劝阻短信系统、全国移动电话卡“一证通查”服务、云闪付APP“一键查卡”、反诈名片、全国互联网账号“一证通查2.0”这七大反诈利器，多角度共编防诈安全网；中国移动公司积极开展断卡行动，把好入网关，全面排查清理高风险电话卡、物联网卡，规范端口短信、呼叫转移等重点业务，同时加强技术反制，及时监测、发现各类违法行为，并进行一键封堵，助力反电信网络诈骗工作。利民之事，丝发必兴；厉民之事，毫末必去。天下无诈，是人民群众心之向往，相关行业领域要主动谋划积极作为，面对层出不穷的犯罪手法，结合自身行业领域特点，不断创新应对思路和方法，才能切实增强打击工作质效，确保战果最大化。

面对电信网络诈骗，事后打击不如事先防范，快破案不如不发案，多追赃不如不受骗。因而，积极宣传、广泛动员，有针对性地开展反诈知识宣传至关重要。今年6月15日，中宣部、公安部共同启动“全民反诈在行动”集中宣传月活动，进一步加强反诈宣传力度，不断提升群众防骗意识。譬如，陕西渭南市公安局在抖音进行反诈直播；山东理工职业学院开展校园反诈骗短视频比赛；武汉经开区沌口街翡翠玖玺社区联合辖区派出所组织“全民反诈”公益观影活动……在各单位和社区反复加强反诈的宣教活动中、在各基层派出所发出的警情通报里，形成全民反诈、全社会反诈的浓厚氛围，从源头铲除滋生违法犯罪的土壤。只有通过不断的教育与宣传改变大众观念，让具有高度欺骗性的谎话变成一眼就可戳穿的笑话，大众才能提升对网络信息、电信信息的识别能力，这是“全民反诈在行动”的最终目的。

打击防范电信网络诈骗，预防为先。“全民皆兵”机制格局的建立势在必行，上下联动、多管齐下，群防群治、形成合力，在全社会形成“不敢骗、不能骗、骗不了”的良好态势，让电信网络诈骗无处遁形、无计可施。

（据荆楚网）