

目前,国内疫情持续好转,大家在做好防控的基础上忙着复工复产,一些骗子也借机打着“防疫”、“复工”等旗号,将老骗术翻新升级,频频下手。据国家反诈中心公布,截至上月底,全国公安机关累计侦破利用疫情实施电信网络诈骗案件14786件,抓获犯罪嫌疑人6605名,累计涉案金额超过4.88亿元。4月13日,公安部召开电视电话会议,部署全国开展以打击治理电信网络诈骗犯罪等为主要内容的“云剑-2020”行动,要求坚决遏制电信网络诈骗案件高发反弹势头。

# 购物群卖万元“特效药” 假理赔骗走31万 疫情下老骗术穿上新衣裳

## 骗术1

### 购物群里的“特效药”要价一万

近日,一位男士报案称,自己本想购买预防治疗新冠肺炎的“特效药”,结果却被诈骗近万元。

此前,诈骗嫌疑人多次打电话,向这位男士推销新冠肺炎“特效药”,声称“效果很好”。担心疫情严重,事主轻信对方,并约定见面交易。对方带来了42颗绿色药丸,要价1万元,经讨价还价后以9000元成交,该男子以微信支付转账。但钱打过去后,对方就“失联”了。警方经侦查,将诈骗嫌疑人抓获刑拘,嫌疑人供认自己兜售“特效药”骗财。

同样在购物群里上当受骗的还有刘先生夫妇。两人加入了一个拼购群,群里有自称是“某国际著名保健品公司中国区代理负责人”,给大家解答新冠肺炎方面的问题。刘先生夫妇担心被感染,就单独加对方为好友请教。对方透露,有“秘密渠道”可搞到国外研制、专门预防感染新冠肺炎的保健品。夫妇俩赶紧询问能否购买,对方表示前面还有200多

人,为避免哄抢不能声张,连自己子女也不能说。夫妇俩便向对方转账4.5万元,购买“一次服用一辈子都不会感染此类病毒”的良药,但对方迟迟不发货。夫妇俩觉得不对劲,在群里询问,发现还有六七人也这样掏钱买了所谓的保健品。就在此时,大家发现推销者“失联”了。

#### 骗术拆解

公安部刑侦局提示,疫情防控期间,大家都迫切地希望能出现可治愈或防范疾病的药品。不法分子假冒政府部门或防治新型冠状病毒肺炎部门来电,推销假冒防疫药;或假冒药物研究(医疗)机构,在网上推广所谓防疫“新药”。事实上,国家相关机构针对疫情研发的所有药品均会通过官方渠道公布,不可能私下联系大家。遇到打着“推销药品”旗号的骗子,未核实其真伪前,决不要相信。

## 骗术2

### 接“银行”来电卷入大案

被骗女子张欣(化名)近日接到一家“银行”来电,对方称要“查证”她银行卡被盗用的事。起初,张欣半信半疑,就给家里打电话询问。经过一番商量,张欣父母建议应配合对方查清事实,以免被诬陷或盗刷。所以当“银行”再来电时,张欣很配合地进行了“查证”,没想到自己竟卷入大案。

所谓的“银行”工作人员好心地电话转到“广州公安”,张欣与一名“韩警官”联系上,通过聊天软件添加好友后,“韩警官”出示了警官证。

这位“韩警官”表示相信张欣,但称检察院已跟进,还发来了全英文“通缉令”。

一见“通缉令”,张欣更慌了,连忙配合“远程笔录”。“韩警官”告诫,这是机密案件,让张欣坚决不能向任何人透露。张欣就没敢再给家里打电话。当张欣把自己的身份信息、银行卡信息发给了“韩警官”,对方核实确认后,发了一个网址。张欣点进去后,发现自己的“刑事拘留批捕执行书”和“冻结管收执行命令”弹出来了,她彻底吓傻了。就在这时,家里人紧急联系张欣,并发来她遭遇电信诈骗的提示消息,反复要求电话联系,张欣这才回电。

原来,经北京市公安局海淀分局反电信网络诈骗犯罪中

心工作人员反复沟通,张欣的家长明白孩子被骗了。工作人员联系不上张欣,让家人帮忙联系。反诈中心工作人员让张欣赶紧查余额。她急忙通过手机银行查看余额。还好!反诈中心为她申请了银行卡保护措施,她的3张银行卡内的20余万元一分没少。张欣想起“韩警官”发来的照片,反复查看才发现“警官证”是后期处理的。

之后,张欣又按照反诈中心人员的提示,把骗子拉黑,进行手机杀毒木马病毒,修改网银和银行卡的密码等操作。临近傍晚5点,张欣和家人确定保住了血汗钱,万分感谢民警,也表示以后遇到诈骗电话会当即挂断。

#### 骗术拆解

海淀警方提醒,在接到陌生来电时要提高警惕,勿轻信秘密办案,不要听人摆布。警方办案一定是面对面,不会采取网络视频等方式制作案件笔录。遇任何核实您身份信息的来电,务必提高警惕。“资产清查”、“安全账户”等是电信诈骗常用的关键词,要做到不听信不汇款。特别是当对方提及退款、社保卡、银行卡等与金钱挂钩的词语时,要立即挂断电话,自行拨打官方电话核实。



## 骗术3

### “快递理赔”骗走31万

疫情防控期间,线上消费增多,骗子也瞄准了网购领域行骗。事主陈小姐网购后,物流显示快递已被签收,但她并未收到货。在向客服反映后,多日未解决。于是陈小姐拨打快递客服电话咨询,没有打通。

挂断电话15分钟后,陈小姐接到自称是某通快递理赔客服的电话。在陈小姐半信半疑时,“客服”说出了其购物信息和个人信息。

之后,“客服”给陈小姐一个微信公众号链接,要求其填写相关个人信息,以便尽快理赔。陈小姐按要求操作后,“客服”以原路返还为由,让她填写银行卡账号。但陈小姐按要求操作多次,都显示网络出错,操作失败。之后“客服”便索要她收到的手机验证码,称帮她后台操作。陈小姐没细看,就把收到的多个验证码发过去了。事后细看发现,信息显示的是“授权转账”。陈小姐急忙询问“客服”为何转走她卡里的钱?“客服”称只走流程,钱未转走,理赔成功后,金额自动恢复。陈小姐拨打银行客服电话查询发现,卡内24万元被转走,信息通知功能也被取消,导致资金被盗刷时,她无法第一时间察觉。

陈小姐要求“快递客服”返还资金。对方称,这需登录某粒贷平台。陈小姐心急之下没多想,按要求操作后,发现从该贷款平台被转走7万元,方觉被骗遂报警。

#### 骗术拆解

警方对该典型骗术进行了拆解。首先,骗子谎称“受害人的网购订单出问题”,诱骗受害人通过假平台转账付款。然后,骗子以“操作失误”为由,让受害人配合电商平台或银行,在钓鱼网站重新转账、填写验证码,从而盗取个人信息行骗。当受害人进入假链接界面,输入账号、密码等信息后,骗子在后台实时获取这些信息。骗子利用受害人的信息进行消费盗刷。

警方提示:遇“客服”来电称办理“退款、理赔”手续,可自行通过网购平台联系商家核实;不扫描对方发来的“二维码”,不提供付款条形码或18位数字付款码及银行短信验证码,不点来历不明的“网页链接”;发现资金被无故转走,尽快更改密码,联系银行等相关客服反映处理,并拨打110报警。

## 骗术4

### 有人盗用你的护照作案

“有人使用您名字的护照从越南入境某市并作案。”近日,青年小叶接到“某省户籍科警察”的一个来电,之后小叶按要求找到一个私密房间反锁屋门,开启视频通话,不料对方透露的案情却令他更加害怕。

当天下午他接到自称是“外省某地户籍科警察”的来电,对方报了名字、警号等。“有人使用您名字的护照从越南入境某市并作案。”“但我没办过这个护照,作案的也不是我啊!”“为了查清案情,注销护照,您必须前往我市做笔录。”

小叶一听非常害怕,表示去某市有困难。“你涉嫌外地的一起案子,现在对你制作远程笔录,此事不允许向任何人透露!”视频那边,一名身穿“警服”的男子与小叶通话,随后男子又向他提供了一个网站,让其登录配合“资产清查”。网址是对方口述的,对方称需要小叶登录输入信息,远程配合查询资金流水。为了摆脱涉案嫌疑,小叶按照视频中“警察”的要求,输入银行账户、身份证、登录密码、支付密码等个人信息。本以为只是查询账目流水,可当小叶输完信息后,却发现自己卡上的钱在瞬间全没了!

#### 骗术拆解

海淀警方向记者介绍,“涉嫌外地案件”“资产清查”“警察”视频办案,此案为近期升级版的冒充公检法诈骗犯罪。犯罪嫌疑人为了提升迷惑性,穿上假警服,利用视频通话的方式,对事主进行洗脑诈骗。

疫情防控期间,各类诈骗手段频出,但无论骗子怎样伪装,请大家牢记警方绝不会以电话、QQ、微信等方式侦办案件,更不会让群众下载来源不明的软件。

公检法办案没有“安全账户”,不会要求当事人以转账方式查验资产合法性。点击陌生网站前,要认准辨别网页链接,不要下载陌生软件,勿随意填写个人信息及银行卡账号、密码、验证码。

如果怀疑对方身份,可向属地社区民警求助或拨打110报警核实,以免财产损失。