

近日，家住广州市天河区的市民刘小姐报料称，她在国内某家知名电商平台网购退货的过程中，遭遇自称售后服务人员的电话诈骗，被骗走人民币46272.96元。

记者调查发现，刘小姐的情况非个案。在一个名为“退货骗局受害者”的QQ群，有来自全国各地的网购者都称自己在该电商平台网购退货受骗，受骗数额从数千元到上万元不等。

事主：“退货页面”与官网无异

10日，刘小姐在国内某家知名电商平台购买了一瓶价值79元的爽肤水。14日9时许，收到货的刘小姐发现该爽肤水有部分液体漏出，遂决定退货。次日下午，刘小姐收到了一个自称是“售后客服”的电话。

刘小姐说，对方准确地说出了自己的姓名、所支付的订单、价格等详细信息。紧接着，“客服”发送了一条包含退货网址链接的短信，还让刘小姐加其QQ，称会指导她按步骤退货。由于“客服”准确描述了刘小姐的购物信息，她就没有多想便加了QQ并点开了短信中的网站链接。

“点开链接之后，那个页面看起来就和电商官网的登录界面没有任何区别，这更加消除了我的疑虑。”刘小姐说。

刘小姐登录后输入了用来接收退款的农行卡账号。

“网页显示需要输入验证码，但我输入网页上提供的验证码一直不成功，那个客服告诉我是系统在维修，会通过短信把验证码发给我。”刘小姐说。

在完成以上操作后，刘小姐连续收到了多条验证码，并依次输入到该界面。“后面还连续收到了两条‘中国农业银行’发送的验证码，称正在支付1000元的订单。”刘小姐说。在挨个填写完验证码之后，她收到了一条令她震惊的短信。

短信发布者署名“富国”，内容称刘小姐申购了46272.96元的“富国富钱包”货币基金，已经扣款成功。刘小姐称，这个数额正是她该账户的全部存款，当她再去农业银行查询账户余额时，发现已经分文不剩。

目前，刘小姐已经就该情况报警，警方正在调查当中。

其他受害者：均在退货时遭遇诈骗

记者在“退货骗局受害者”的QQ群里发现了类似刘小姐的情况。该群共有28个人，分别来自湖北、四川、河南、江苏等多个省份，他们通过该电商网站官方微博下的维权留言结识，大都是学生和参加工作不久的年轻人，受骗过程与刘小姐的基本一致，都是在退货阶段遭遇诈骗的。

“他们竟然能够完完全全地说出我的手机号码、购买的物品、收货地址等个人信息，所以我就相信了。”群里一位来自湖北的肖小姐说。她是一名刚刚参加工作的护士，被骗了5000元。“现在想想，一定是我们的个人信息被泄露了。”她说。

记者点开受害者提供的网络链接，发现其网页界面与电商官网界面相似度高达99%，虽然个别位置字体略有不同，但如果不仔细查看域名地址，几乎无法从页面辨别真假。

此前，曾有媒体报道今年5月24日，一位郑州的女大学生在该电商平台网购土豆切丝器，以相同的方式被骗走20万元。

记者致电该电商平台客服，客服人员表示，网站绝不会泄露客户信息，退款流程也会按照原路径退回，在退款过程中也不会索要任何的银行卡账号。

至于客户信息的泄露，该电商平台有关负责人表示，此次诈骗事件是黑客在其他网站窃取到用户数据（包括用户名、密码等），随后进行撞库攻击，伪装成客服进行诈骗。接到用户投诉后，公司第一时间积极响应，了解相关情况并建议用户报警。该过程中，公司一直在协调，并主动出具资料协助调查敦促警方加快调查进度。

专家：关键在于获取验证码

银行卡里的钱究竟是如何被刷走的呢？

对此，一位网络工程师表示，关键在于获取验证码。网络诈骗分子一般会诱导受害人将验证码告诉他们，或者通过病毒网页偷取受害人输入的验证码。诈骗分子掌握验证码后，之前设定的转账请求就能通过银行验证，完成转账。这整个过程，受害人并不知情。

相关专家提醒，在网上申请退货退款时，要注意以下几点：

第一，对陌生来电和不明短信网址链接要保持警惕，认清发送过来的链接，除了确定网页页面相同以外，一定要上网查看官方网址，如果不一样，不要随便点击。

第二，办理退货退款一定要通过官方途径，切勿登录来路不明的网站，银行验证码

一定不能随意透露给他人，不能随便输入银行卡号和密码。

第三，钓鱼网址的开头基本都为http，而正规支付网页的网址开头为https。正规的支付网页网址末端还有一个绿色的锁的形状，表示该支付为安全支付，钓鱼网址是没有这个小绿锁的。