

信用卡诈骗的手段层出不穷，最近又有一种新的诈骗手段浮出水面——不法分子以信用卡退款名义骗取卡片信息，再实施网络盗刷，喜欢网络购物的持卡人可要当心了。

莫名接到退款要求

钟爱网络购物的陈小姐前两天接到一个电话，来电人自称是某购物网站工作人员，因陈小姐此前在该网站上的一次购物交易未成功，现在要退款给陈小姐。而陈小姐日前的确在该网站买过一件家用电器，也没注意到付款后有什么交易不成功的提示。陈小姐想，既然工作人员要给她退款，又不是跟她要钱，也就欣然接受。

这个所谓的网站工作人员表示，要往信用卡里退款还要陈小姐提供一系列的信息，如陈小姐的信用卡卡号、有效期、安全校验码等信息，最后还要陈小姐提供手机动态支付验证码。陈小姐突然意识到，这些信息都告诉他，那不等于将这张信用卡交给他一样了吗？对方完全可以利用这些信息实施网络盗刷。想到这里，陈小姐惊出一身冷汗，赶紧挂了电话，再打电话咨询银行和购物网站客服人员，结果银行和网站客服人员都明确表示这人一定是个骗子，幸亏陈小姐没有将所有信息和盘托出。

虚假退款定有漏洞

据了解，随着网络购物的日益兴盛，近期的确发生过多起不法分子冒充支付宝等网站工作人员以交易未成功需退款的名义，通过电话向持卡人实施网络盗用。那么持卡人收到类似骗取信息的来电该如何防范呢？

建行信用卡专家介绍，不法分子在实施网络盗用时有几点主要特征持卡人须留意，如支付宝等第三方支付网站均有统一规范的客户服务热线，不法分子实施诈骗时使用的电话号码通常为匿名登记，不同于官方网站公布的电话信息；在网络支付过程中，退款交易不需要客户输入支付密码、手机动态密码等关键信息，但不法分子往往利用客户退货心切的心理，诱导客户输入上述信息；为加强网络支付的安全性，银行同第三方支付均推出了手机动态密码验证功能，该功能仅限于通过网络支付页面输入，银行同第三方支付的工作人员不会以人工电话方式同客户核实此类信息，而不法分子往往通过人工电话的方式联系客户，诱骗上述关键信息。

退款也应提高警惕

陈小姐事后回忆，此前她在网上购物也有过几次退款经历，多数都很简单，直接在她的订单中点击“退款”按钮，写明退款原因，卖家几天内就处理了退款事宜，已

付款项会自动退回，并不需要银行卡号、密码等信息。

上述信用卡专家表示，持卡人如遇到此类信用卡退款要提供信息的情况，一定要引起高度警惕，切勿提供信用卡信息及支付验证码，同时注意银行发送的交易提示短信，谨防被骗。信用卡信息及手机动态验证码属于信用卡支付验证的关键信息，应妥善予以保管，不要轻信以退款、网站升级等名义骗取关键信息的陌生来电。一旦发现被骗，请立即致电客服热线，冻结账户，避免和减少损失。

专家提醒，不法分子获取客户想退款的信息有几种可能的途径，首先是持卡客户中了不法分子发布的木马病毒，电脑中信息被窃取；其次是通过QQ聊天工具，在虚假的网络界面中聊天；还有可能是通过一些虚假的网络连接；最常见的就是不法分子直接致电客户，以商品有优惠退款为由让持卡客户意识松懈，从而泄露银行卡信息。