信用卡不仅能预订机票、酒店，进行网络购物，还能在众多实体店刷卡得到实实在在的优惠，积分还可兑换一些礼品，因此使用信用卡消费的市民越来越多。当前，正值年底购物的高峰，也是信用卡诈骗、盗刷案件的高发期。一秒通专业融资顾问在此提醒广大市民，千万保护好自己的信用卡，谨防被骗。

泄露消费验证码被刷走1万余元

去年12月29日，刘女士在江东区东胜街道家中接到一个自称是淘宝售后客服的电话，说刘女士之前在淘宝网店购买的一件货物无法结算，需要她再次输入一遍银行卡信息才可以正常结算。刘女士于是按照对方提供过的网站再次输入相关信息，不久就收到一条6位数的消费验证码。对方又说结算审核过程中需要这个验证码，于是刘女士主动把该号码发过去，但之后对方再也联系不上。刘女士一查银行卡，发现被刷走1万余元。

家住海曙区的唐女士也有类似遭遇，去年12月31日16时左右，她在某KTV娱乐时接到一名女子打来的电话，对方自称是某银行的工作人员，因为唐女士使用的信用卡刷卡记录良好，达到银行可以提升信用额度的要求。唐女士按对方要求填好信息，不一会儿，另一名自称是该银行VIP客服经理的男子打电话来，说唐女士的流水账单没有达到要求，需要她再提供两份流水账单，于是唐女士根据要求进行网上消费一次。事后收到扣费短信，唐女士发现数额不对，仔细审查才发现手机被强制安装了一个病毒软件，个人信息全被盗走。

再来看下鄞州张先生的惨痛遭遇，1月1日下午2点左右，他收到一条来自0085259 34331的短信，内容显示为张先生预定的宁波飞深圳的航班因机械故障取消，要求他及时联系航班客服4006016722进行办理改签或退票。张先生立即拨通电话，根据对方的提示通过网上银行进行操作。事后没多久跟朋友说起这事，朋友称这可能是诈骗。张先生马上查询银行卡内数额，发现少了将近40万元。

一年破获通讯（网络）诈骗案件1808起

据统计，截至去年12月20日，我市共破获通讯（网络）诈骗案件1808起，抓获犯罪嫌疑人305名，打掉犯罪团伙17个，冻结赃款333.29万元。同时，紧急止损被骗资金人民币237.4万元，封停了800余个诈骗电话号码。

针对通讯（网络）诈骗高发态势，市公安局成立了“心防工程”建设工作领导小组，从去年5月起，全市金融安全“心防工程”建设暨防范宣传集中活动在全市范围内启动。截至目前，全市金融机构营业场所LED滚动显示、ATM机屏幕滚动宣传、防诈骗警察“提示岗”等等基本到位。自专项建设活动开展以来，我市已成功堵截诈骗案件142起，挽回经济损失300余万元。

然而，随着使用信用卡人群基数越来越大，对信用卡管理不善的、不明晰信用卡使用规则的、个人信息保管不合理的、安防意识不强的人也越来越多，尤其是一些中老年人，因为接触时间不长，不够熟悉常规操作，加上不法分子“洗脑”和“忽悠”能力越来越强，上当受骗仍然时有发生。

涉“卡”诈骗主要有三种

细分各类案情的关键点后可以发现，以“卡”为中心的作案手段，从作案结果来看可以分为三种，分别是操控持卡人、盗取卡面信息和骗取交易验证信息。

操控持卡人

他们会先以某某客服、民警、邮政人员、法官等身份出现，告知法院传票、银行卡被冻结、包裹藏有违禁品等，因为这些事情日常生活中市民接触和了解不多，容易信以为真，最终被洗脑后按照对方要求主动汇钱。

一秒通融资顾问提醒：首先要谨记，正规单位或部门提出需要处理问题时肯定要当面沟通，因为这牵涉到审核事件真实情况、文件内容修改或签字等，电话最多只是用于通知个人具体时间地点。另外还需记住，对方让你对着“空气”聊天半天后，最终提出让你去银行汇款转账，这种情况下可以断定就是诈骗。

盗取卡面信息

我们在非实卡消费场合，比如通过电话或网络预订机票或境外酒店时，其实只需提供信用卡卡号和后三码，核对个人信息后即可消费（前提是信用卡未设密码）。后三码在卡背面签名栏末尾处，有一排反斜体数字，前四位为卡号末四位数字，后三位即为后三码，其作用是在交易过程中核实卡的真实性。一旦这些信息泄露被不法分子所得，对方就有可能通过这些信息进行信用卡盗刷。

一秒通融资顾问提醒：针对此类骗术，市民最好先记住后三码，然后抹去或用胶布将它隐藏起来，切忌泄露卡号、有效期、后三码等信息或将其记录在电脑里，以防被病毒软件攻击盗取；在没有保护措施的情况下，最好不要让信用卡离开自己的视线，以防关键信息被抄走。

骗取交易验证码。一般网上支付，跟信用卡绑定的手机就会接收到6位数的验证码，只要再次输入它，才能支付成功。验证码是为了保障市民网购的安全性，但不法分子同样通过设局欺骗市民把验证码发送给他，最终骗走钱财。

一秒通融资顾问提醒：验证码是网上交易整个过程的最后保障，市民朋友一定要小

心对待，在接收到验证码后，仔细审查交易情况是否属实、支付金额是否合理等，一旦发现疑点，应立即停止交易。