

双十一轰轰烈烈的来了，过冬的粮草清单已经打出来，各种信用卡蠢蠢欲动。不过，俗话说：冲动是魔鬼，在这个网购热浪席卷全国的时候，融360还是要提醒大家：理性谨慎用卡，不要一不留神，掉入有心人的陷阱。本期给大家揭秘干货：网购常见骗局！

骗局一：虚假客服用退款退货为由，引你进入钓鱼网址
不法分子通过非法渠道获取了你的网购信息（必须要唾弃下隐私保护现状），跟你联系，说因为某些原因，要给你退款/退货，然后给你一个钓鱼网站链接，你点击进入，以为是自己在秘密的输入账号、密码、动态密码等信息，实际上这些信息已经被不法分子一览无余了。融360支招：网购退货/退款一定要通过商户的官方渠道，比如淘宝上的退货/退款是在淘宝个人账户栏目里，不要随便点击别人发给你的链接，更不要轻易加陌生人的其他联系方式。

骗局二：利用二维码，植入木马病毒到你手机中

有些信誉度低的商户，会利用双十一大促，给出红包或各种优惠活动，但是活动需要信用卡持卡人用手机扫描二维码才可以。实际上这些二维码中植入了木马病毒，你一旦扫描，病毒就立刻在手机里扩散，并监控了手机的各类应用。现在大家的信用卡基本上都是靠手机APP（官方APP、第三方管理软件等）在管理，一旦这些信息被人监控，给你造成的损失将难以估计。

融360支招：慎扫二维码，除非是你确认安全的来源。

骗局三：利用低价短信，吸引你点击钓鱼网站

网购多了，手机经常会收到各种低价促销信息，有些是常用的商户发来的，有些发信人则是不甚明了，还带着链接。这时候要小心了，不要随便点击链接，一旦点击进入，很可能是个钓鱼网址，你看到价格果然很便宜，爽快付款。殊不知，这是别人的圈套，要么这些款项有去无回，要么你付款的信用卡账号信息已经被人掌握。

融360支招：不要点击不明来源的人发给你的链接。

骗局四：冒充电商商家，谎称积分兑换，骗你点击钓鱼网址

不法分子通过短信/聊天工具/邮箱等方式，告知你有积分兑换礼品的活动，只要点击网址进入就可兑换，你高兴的点进去，然后输入了自己的信用卡账号、密码、手机号码等信息，然后，就没有然后了。。。融360支招：无论是什么情况，不要随便点击不明来源的链接，如果需要查询或兑换个人账户的积分信息，一定要登陆电商的官方网站操作。

骗局五：提供公用WIFI 盗取你的信用卡信息

鉴于手机购物的方便性，我们可能随时都会有想要剁手的行为，有时候担心手机流量，就会各种找WIFI。如果遇到非正规渠道提供的无密码公用WIFI，卡友们要留心了，已经有很多前车之鉴：嗨皮的用完无密码公用WIFI手机支付后，信用卡被莫名盗刷了！融360支招：一尽量不在逛街时网购，二即使真的需要也尽量不要用公用

WIFI，三如果以上都不满足，请自觉开通信用卡短信实时提醒功能，以便第一时间知道账户是否被盗刷。

骗局六：冒充银行谎称银行系统升级等原因，要求提供你的信用卡信息 网购正嗨皮，接到电话，来电号码显示是某银行官方客服，告诉你银行系统升级改造，需要客户提供下个人信息，然后取得了账号信息后，好心的提醒你需要更改下密码或者重新输入密码，然后，你的信用卡就华丽丽滴被盗刷了！融360支招：银行不会因为自身系统升级、改造等原因，要求你输入密码等个人信息，也不会要求你进行模拟交易，一旦接收到此类信息，请自觉回避。

骗局七：以帮你提高额度为由，要求你提供信用卡信息 粮草清单长又长，信用卡额度有点慌，这时候忽然有人告诉你可以帮你提高额度，你会不会很高兴的提供自己的卡片信息给他？提供？你就上当了！融360支招：小伙伴们要谨记信用卡额度提升，只有银行一个渠道，其他通通不可信。融360提醒：骗局设计的这么有看点，小融也是醉了。总之，双十一很嗨皮，我们的打算是：通过这一天的血拼，以低价获得一冬的粮草。本身是个很划算的事情，不要因为各种各样的一时不慎，给自己造成更大的经济损失。简单来说，手段就是几句话：购物用官网、不随便点击不明链接、慎扫二维码、不用不安全的网络。信用卡用卡是个理性的事情，希望我们能够一直保持一颗清醒的头脑，不给骗子们可趁之机，护好自己的钱袋子。