双十一打折秒杀满天飞，购物狂欢迷人眼。退款诈骗、到付快递陷阱、有毒红包或是二维码、假冒兑换积分的链接剁手族们可不要忽视这些陷阱哦，才能买得放心舒心省心。远离这些骗局，来看看四大常见的网购陷阱。

一、退款陷阱

【案例】王女士前几天网购了几件心仪的衣服，第二天手机收到了一则奇怪的信息，说因为支付宝系统升级被冻结了，交易出现了卡单，没有支付成功。而赵女士所付的钱，需要通过点击短信里的一个链接完成退款。王女士看到短信里确实是自己的淘宝ID，衣服款式也是对的，就没太怀疑。但当她点击了那个链接，网页显示让她输入银行卡号时，她忽然想到最近电信诈骗比较猖獗，便立即点击了取消。随后，她打开了淘宝，向商家询问情况是否属实。客服称根本没有支付宝系统升级这一回事，退款一说更是子虚乌有。值得庆幸，王女士没有上骗子的当。

解析：从往年的双11情况来看，退款骗局已经成为了投诉量最大的诈骗案例之一。一些不法分子浑水摸鱼，通过不法途径窃取买家的交易信息，并冒充卖家发送退款信息，诱骗消费者点击钓鱼网站，从而达到诈骗的目的。而破解这个骗局的方法其实很简单：只要向卖家询问是否真的有退款的情况就可以了。

二、到付快递陷阱

【案例】今年10月，大学生李双收到了一个神秘的包裹。那段时间，李双并没有在网上购物，也没有朋友曾说过要寄包裹给她，所以收到短信时，她有些疑惑。当时我也问了很多人，都说没给我寄东西。李双说，包裹到时，自己正在外地的家中，便委托室友帮拿包裹。室友去拿包裹时，对方告诉她，包裹是到付的，需要支付30元快递费。李双十分好奇包裹到底是谁寄来的，便让室友先帮自己支付30元。不久后，李双回到学校，兴致勃勃地打开了这个神秘包裹，却发现包裹里除了一些废纸和塑料，什么都没有。此时，她才知道上当受骗了。

解析：双11后很长一段时间，购物党都在不停收取快递。此时，一些诈骗分子开始乘虚而入，利用人们的好奇心理，赚取到付费。到付的圈套其实很简单，诈骗分子
收取
较高的快
递费用，但包裹里
其实只有废纸或是一些价格十分低廉
的东西。

破解该骗局的方法：首先是不能贪图小便宜，如果到付的包裹不是自己在网上订购或是朋友寄的，就要多个心眼，尤其是遇到支付费用超过一般快递费用时，更是要特别小心，最好选择当面验货。如果对方拒绝验货，就很有可能是骗子，此时应当果断拒绝支付。

三、有毒红包或是二维码陷阱

【案例】市民小冯前段时间就收到过一个微信好友发来的红包，页面跟微信钱包十分相似，点击后出现了一个恭喜你成功领取红包58元窗口。小冯真以为领取到了红包，还有些沾沾自喜。谁知过了不久，他才发现手机已经被植入了木马程序，绑定的银行卡已经被诈骗分子转走了2000多元。

解析：将红包大盗手机木马伪装成微信红包，窃取手机用户的银行卡号等信息，也是非常常见的诈骗方法。双11期间，各类红包更是满天飞，卡友们需要擦亮眼睛，注意甄别，千万不要相信来源不明的红包，对于好友发送来的所谓的帮拆红包的链接，也最好核实后再点击。破解办法：如果不慎点击了木马红包，应第一时间关闭手机网络，立刻修改网银、支付宝等密码，去正规手机售后部门刷机或重置相关系统，以彻底删除木马病毒。

四、兑换礼品陷阱

【案例】近日，小李遇上了一件美事。她经常在同一家网店购买东西，所以当她接到自称是该店客服发来的兑换礼品的信息时，便没有多想，点击进入后，便按照相关提示，一步步填写支付宝、银行卡号及密码等。原以为填完后就能得到免费的礼品，谁知没多久，却等来了银卡的扣费信息：她卡里近千元全部被划走。随后，小李致电该店铺，才发现根本没有所谓的礼品兑换活动。

解析：利用所谓的兑换礼品诱骗消费者点击钓鱼链接，已经是一个比较老套的电信诈骗手段了。诈骗分子还会冒充10086或是银行的官方号码，给对方发送诈骗短信，诱使受害者在钓鱼网站上输入个人的敏感信息，有时还会诱使他们下载木马，劫持用户收到的银行卡验证信息，从而实施诈骗。破解办法：对于此类网购骗局，一定要做到不轻信、多核实，千万不要在网站上填写身份证号码、银行卡密码这些非常敏感的信息，以免被不法分子利用。

【卡片推荐】

????????????????????????????5?=1?????????????

??????????5??

????5?=1????????????