两分钟买买买了“100亿”后，要当心这些骗局！

和往年一样，众多网民在疯狂购物后将迎来这三件事，“退款”“寄快递”“二手交易”，越来越大的交易量也被一些不法分子盯上，还设计了种种套路，稍不留神就会中招。警方提醒广大网民，买买买一时爽，购物后要防范以下网络诈骗：

■ 退款诈骗

如果你在抢购后，突然接到自称卖家的人打来电话称：您的网购交易存在异常或无法发货，需要给您进行退款或解除交易异常。不用怀疑了，你极有可能正在遭遇近年来最流行的网络诈骗方式：退款诈骗。一旦按照对方的指示，打开网页或进行某些操作，就很有可能面临资金账号被盗或网银资金被盗的风险。

所谓的“卡单”、“掉单”、“交易异常”、“解冻订单”、“异常订单处理” 等词汇全部都是诈骗专用术语，淘宝、京东等正规电商的网络交易平台上不会出现这些词汇。

警方提醒：如果遇到交易异常或发货缓慢的情况，一定要拨打电商网站的官方客服电话进行咨询，切勿相信陌生人打来的电话或发来的短信，更不要轻易点开陌生人发来的网址链接。

■ 二手交易诈骗

抢购如此热闹，自然少不了“网购黄牛”的身影。不少黄牛参加网上抢购，目的就是把低价到手的商品，加价之后再转手倒卖出去。

在抢购之后的一个星期内，二手交易诈骗极有可能大幅增加。骗子们会在各种同城网站或二手交易网站上发布消息，谎称抢购的便宜货自己不想要了，想要加价、同价、甚至低价转让手中的商品。消费者一旦与这些骗子搭上钩，骗子就会诱骗消费者在虚假的二手交易网站上进行交易。待消费者付款后，骗子就会逃之夭夭。更有甚者，一些骗子会在买家索要交易订单、发票或实物的照片时，向买家发送木马病毒文件。用户一旦运行这些文件，网银或支付账户就有可能遭到盗刷。

警方提醒：进行二手交易，一定要到正规的二手交易网站进行。对于陌生人发来的二手交易平台链接要提高警惕，谨慎打开。此外，如果要向卖家索要发票照片或实物照片，请一定要求对方在聊天窗口中截图查看，切勿直接接收对方发来的任何文件。如果已经接收了，也一定要先对文件进行杀毒扫描之后再打开。

■ 中奖诈骗

如果是平日里收到中奖短信，可能绝大多数人都不会相信。但抢购之后，以“您在某某电商参与抢购抽中大奖”的名义向您发送的诈骗短信，你就很有可能会相信。抢购后的半个月至一个月的时间里，各中奖诈骗短信都可能会呈现持续高发的态势。

警方提醒：接到此类信息如有疑问，请拨打电商网站的官方客服电话进行咨询或确认，切忌直接拨打短信中的联系电话，也不要轻易点开短信中任何网址链接。

■ 虚假快递诈骗

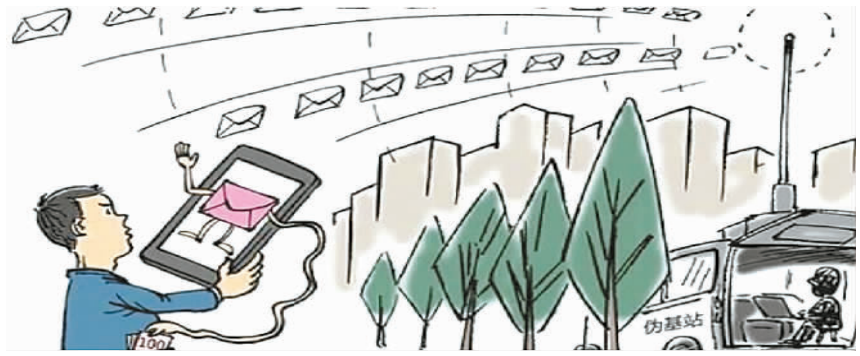
按惯例会收到大量的包裹，大家最翘首以盼的快递打给你电话说快递到了，但骗子也会看准这个机会冒充快递员，且能够准确说出你购物的信息，让你深信不疑，再用快递丢失、损坏等借口，谎称对客户进行赔付，伺机骗取钱财，或者是到付的加快递，骗取钱财。

警方提醒：接到此类信息如有疑问，请拨打快递的官方客服电话进行咨询或确认，切忌完全听信电话内容，也不要轻易点开短信中任何网址链接。

（“警民直通车上海”微信公众号）

警惕诈骗短信 不要上当受骗

冒充通信运营商客服，以感恩回馈等方式诱导点开链接；冒充银行客服，以电子密码器失效等方式种植木马；以聚会照片等方式，传播病毒；冒充电商客服，以降价促销等方式吸引点击链接……是短信最常见骗术，警方详解提醒：年底骗子又开始猖獗活动，别上当！



1、冒充通信运营商客服

以积分兑换、感恩回馈、话费余额不足等方式种植木马

诈骗短信中所提供的链接地址多为含有10086或1(字母L的小写)0086等字段的地址，令收信人误以为是官网链接而进行点击。

2、冒充银行客服

以积分兑换、电子密码器失效等方式种植木马

诈骗短信中所提供的链接地址大多系仿照银行官网地址申请，网址中含有ICBC、CCB等银行简称或95588/95533等银行客服电话，令收信人误以为官网进行操作。

3、冒充同学、好友、同事

以聚会照片、整理的资料、帮忙查看合同等方式种植木马

此类案件中，犯罪分子往往以熟人之间日常聊天的语气，称“整理了同学聚会的照片”、“发电东西留念”、“推荐个很不错的网站”或者“帮忙审看下合同/资料”等方式，诱惑收信人点击木马网址。部分案件中，由于犯罪分子通过非法渠道获取了手机机主的信息，会在短信称呼机主的名字，从而增加欺骗性。

4、冒充学校或老师

以查看学生成绩、平时表现等方式种植木马

此类案件中，犯罪分子冒充学校老师，以提供给学生家长查询成绩、平时表现的网址方式，诱惑收信人点击木马网址。个别案件还会利用特殊的时间节点冒充高考、期末考试查询网址进行诈骗。

5、冒充电商客服

以购物返礼、降价促销等方式种植木马

此类案件中，犯罪分子通过假冒京东、淘宝等商家进行购物返礼、积分兑换或者谎称自己有某某物品，因资金周转等原因降价甩卖等方式，诱惑收信人点击木马网址。

6、冒充交通部门

以通知交通违法的方式种植木马

此类案件中，犯罪分子以提醒收信人交通违法并提供违法照片等链接的方式，诱惑收信人点击木马网址。另外，犯罪分子往往还会利用通过不法渠道获取的公民个人信息（如手机号码关联的机主姓名、房产、机动车等）实施犯罪活动，令任防不胜防。

7、爆料、恐吓、激将

通过威胁恐吓等方式种植木马

此类案件中，犯罪分子往往以威胁恐吓的语气，声称 “你老公/老婆有外遇了”、“瞧你做的好事”或者“你朋友的手机中木马了，有照片”、“我与你老公/老婆真心相爱，有照片为证”等，诱惑或刺激收信人点击木马网址链接。

8、猛图、爆图

利用彩信种植木马

此类案件中，犯罪分子往往发送一张图像较小或者比较有诱惑力的照片，手机持有人点击查看后会自动跳转至含有木马病毒的网址。

9、代办大额信用卡

伪装信用卡申请文件种植木马

此类案件中，犯罪分子声称可以办理大额度信用卡，将木马链接伪装成信用卡申请协议等文件，诱骗收信人点击安装。

（“防范宣传先锋”微信公众号）

“顺丰快递”被扣押？有可能是假的！

前几天，张先生接到一自称顺风快递客服电话，称其邮寄的包裹内有“十八张身份证”，涉嫌违法。感到莫名其妙之时，“客服”随即将电话转接到“公安局”，所谓的林警官说的更严重，称张先生个人信息泄露，涉嫌重大洗钱案，张先生被这突如其来的电话给吓到了，这究竟是怎么回事？此时林警官表示，如需证明清白，需登入警方的资金审查网站，信以为真他登入网站后，将银行账户、密码填入，瞬间卡内的15000元被转走。

当然这所谓的“顺丰客服、林警官”都是假的，这是一起典型的电信诈骗案件。短短一周内有5位被害人被假冒的“顺丰快递”所骗，损失巨大。

顺丰快递公司对此也发出了警示公告：

一、顺丰的客服电话只能呼入，不能呼出，如接到4008111111来电均非顺丰速运官方电话。

二、顺丰工作人员来电只与您沟通与顺丰业务相关信息，也不提供转法院、公安等第三方服务。

三、顺丰服务热线：4008111111 官网www.sf-express.com。

治安总队提醒请将此信息转给身边的家人、朋友，特别是常帮子女代领快递的家中老人。警方发现，近期冒充“快递”、“邮政”客服谎称邮包未领取或包裹内含有 “身份证、信用卡、毒品”等违禁物品的诈骗案件集中多发，如接到此类电话、短信要求您汇款、转账的都是诈骗，如有疑惑，请联系社区民警或直接拨打110。

（社区安全屋为平安加油）

微娱乐

离奇的爆炸

音乐家皮特的家中发生了爆炸案，所幸皮特没有受伤。福尔摩伍在现场发现，爆炸的是一玻璃杯，里面装了一些火药。可是让人奇怪是的室内没有任何火源，也没有发现引爆装置。皮特说自己当时正在练习一首小号曲，当吹到高音部分时，就发生了爆炸。福尔摩伍仔细观察了一下爆炸残留物，马上就知道凶手是如何引爆的。

上期微娱乐答案：少女被关在窗户朝北，即面对丘陵的那间屋子里。这从少女所说的“夜晚会有风吹进来”这句话可以得到证实。海岸一到夜晚，陆地上的气温要比海面的温度容易冷却，这种凉的空气就从丘陵向海上流动，所以从朝北的小窗口吹来阵阵清风。反之，白天由于陆地很快变热，风就改从海上吹来，而在早晚气温相同的时候，海岸上就处于无风状态了。

公告

五里桥派出所为民服务信息公告

五里桥派出所地址：
中山南一路1109弄3号
邮编：200023
辖区报警电话：110
治安咨询电话：
021-63010589
（24小时接受咨询）
户籍咨询电话：
021-63014624
（早上8:30-晚上8:00）
五里桥派出所网址：
http://pcs.police.sh.cn/wsjws/gweb/index_gzz.jsp