微信“砍价”0 元购。

不是

殊不知，许多“砍价”链接真实目的是获取用户的个人信息，用户最后不仅不会收到奖品，反而有可能被骗。早前，李女士在朋友圈里看到一个儿童驼背矫正器的“砍价”活动。随后，李女士将“砍价”链接转至朋友圈及各个群里，请求朋友帮忙砍价。当产品砍至0元时，链接却打不开了。东西买不到是小事，泄露信息出现隐患才是真正担心的。有网友也表示，曾在帮朋友砍价时填写个人信息并关注对方的公众账号，结果没多久就收到诈骗短信。在日常生活中，应当警惕需要输入个人信息的网页链接或者陌生人发送的图片、消息。需确认所登录的页面为官方渠道方可执行操作。尤其是连接免费Wi— Fi 时，不要进行手机网银操作。此外，不要轻信低价商品促销等信息。对于显著低于正常价格的商品和服务，要注意信息甄别、慎重购买。

“货到付款”有猫腻，应先仔细核对信息及所寄物品。

是

市民王女士早前收到一个由“北京众泰4S 店”寄来的包裹，快递单上写着“众泰4S店赠品”，但需货到付款。由于此前王女士确实购买了相应的汽车，背景信息基本吻合，以为真是4S店寄来的汽车赠品便没有怀疑，向快递员支付了39元“快递费”。但打开包裹后王女士却发现，寄来的是假的移动充值卡，经联系核实后，才发现4S店从未寄过所谓“赠品”。此类诈骗针对具有网购经历的网民，投递名目主要以“重要文件”“饰品”“洗漱用品”“赠品”为主，而实际的“货到付款”包裹中，往往只有假冒伪劣商品，成本极低，只要受骗者支付了“快递费”，骗子就稳赚不赔。被骗者即使发现了骗局，由于受骗数额小，也往往不会选择报警。市民一旦接到需要货到付款的快递时，应先仔细核对信息及所寄物品，对于来历不明的快递一律拒收，以免上当。此外，消费者在网购以及办理业务时要增强保密意识，不轻易透露自己的身份证号码、手机号码、家庭住址等信息。在日常工作中，有关自己个人信息的快递单据等不要乱扔，应先撕毁或者涂黑再予以丢弃，以免被不法分子利用。

免费“清粉”扫二维码存在盗取风险。

是的

近日，有微信用户收到“免费帮你清理微信僵尸粉”的信息，点击链接并关注相关公众号后，对方会对清理步骤做简单介绍或发送教程视频，查看步骤后，需要用户回复确认是否清理。待微信用户确认清理后，客服会发送一个临时二维码。而此二维码不能直接识别，需要将它发送至其他手机或用其他手机拍照，再进行识别。一旦用户识别二维码，用户的手机就会收到电脑登录手机微信的确认界面，如果用户确认登录后，对方的电脑可以直接登录用户的微信，对方可以用用户的微信开始群发消息，筛选僵尸好友。用这种方法“清粉”风险非常大，因为“清理僵尸粉”信息中的链接，很有可能是手机病毒，用户点击之后微信号可能被盗。如果你的微信绑定了银行卡，在点击链接时，一旦黑客破解了你的支付密码，就能盗取你的钱财。此外，如果骗子以“清粉”为由在电脑上登录你的微信，就可以用你的微信号以生病、出车祸、急用钱等为由向你的朋友群发信息进行诈骗。

捡到“银行卡”支付滞纳金就可以自由存取。

不是

近日，有一类新型骗局正在“流行”。在路上捡到一个信封，打开看里面有银行卡和密码。当你心动找ATM取款机查看时会发现密码正确，并且有很大的一笔余额。如果心生贪念想取钱，自动提款机会显示“不予承兑”，当你打信封上开户行的电话时，对方会回复你需要缴纳一定费用滞纳金，然后便可以自由存取了。但当你转钱时，银行卡仍然显示“不予承兑”，此时，你便已经上当。骗子通过银行卡复制器复制出伪卡，伪卡的磁条信息是使用之前办理的真实未激活的信用卡，而捡到卡的人一旦对卡内余额心动，按照要求支付滞纳金，打过去的钱就会收进骗子的口袋。此外，还有很多不法分子通过伪基站冒用法院、银行、公安等电话，打电话或发短信，称需要交纳某某款项，市民遇到此类诈骗应先拨打相关部门的电话或到办公地现场求证。

回复短信可能导致银行卡被盗刷。

不是

回复短信不会让手机中毒，但是短信中的链接可能会让手机下载木马病毒。互联网金融支付安全联盟的专家解释，短信是通过运营商系统中转的，单纯回复短信在现阶段不会造成手机中毒。是该市民点击了短信中的链接，导致手机下载了木马病毒，并通过后台监听系统泄露了手机银行转账短信验证码，造成资金损失。去年年底，郑州某消费者发现自己有两张银行卡通过手机银行被转账12次，合计5000余元。该消费者表示，前一天曾接到附有网址的陌生短信，内容是“某某某老同学，你的照片”。这位消费者看到对方叫出自己的名字，就点击了短信中的链接并回复一条短信：“请问你是？”结果在短短30分钟内，钱就被转走了。于是不少人担忧：仅仅回复一条短信就会造成银行卡被盗刷？专家提醒，消费者收到中奖、积分兑换、话费充值、信用卡提额等内容的短信，一定要通过官方途径确认并完成操作。为避免手机中毒，可以安装手机防病毒软件。

接听或回拨陌生来电可能收取高额电话费。

不是

针对“接听或回拨陌生来电可能产生高额吸费”的传言，工业和信息化部早在2008年就曾辟谣，表示这种情况基本不存在可能性，这其实是不法分子为推销所谓群呼设备，利用互联网所做的欺诈性宣传。但是，狼来了的故事仍然年复一年地上演，仍有相当一部分人深信接听或回拨陌生电话会被收取高额话费。事实上，无论是回拨以400还是以区号开头的固定电话，都不存在高额吸费的情况。回拨后往往都是声讯台录音，要么推销贵金属、理财、贷款等，要么是“您中奖了”之类的诈骗电话。消费者完全不用理会。

登录骗子网银可锁定骗子银行卡。

不是

网银被锁仍可由ATM提款。有网友在QQ上发消息称，收到骗子要你转账汇款的短信后先别删除，查查它发来的卡号是哪家银行的，然后登录该银行的网上营业厅，输入该银行卡号，密码随便填。只要填错3次密码，此卡在24小时内就会被冻结。如果有闲工夫，每天给他来3次，骗子就不能得逞了。看到这么解气的办法，很多网友拍手称快，跃跃欲试。但是，银行业内人士表示，银行卡查询密码和取款密码的功能是不一样的，查询密码输错只能限制登录网银的操作，不能限制ATM渠道的取款。

连续汇1分钱整倒骗子。

不是

利用手续费整骗子只是个传说。通过手机银行转账，金额小于10元，手续费都不能选择收款方扣收。也就是说，每次只汇1分钱，每次2元手续费，直到骗子账户“卡壳”是行不通的。此外，“1分钱转账整倒骗子”还有另一个前提条件，那就是骗子的账户里有余额。因为只要银行从骗子的账户里扣不到手续费，这笔转账就会被判定为交易失败，所汇的1分钱会退回汇款人账户，骗子则不会被收取任何手续费。实际上骗子账户里有余额的情况是很少的，除非正好有其他受害者给骗子汇了款，且骗子还来不及转走，否则就是一个空账户。

遇上匪徒，倒输密码能自救。

不是

倒数密码只会锁定银行卡。互联网金融支付安全联盟的专家介绍，虽然确实有人开发了这一技术，但目前为止并没有被应用在任何一台ATM机上。在ATM机上倒输密码只会提示密码错误，而且连续三次输错取款密码银行卡还将被锁定。专家提示，银行的ATM机都装有摄像头，北京的许多ATM机上还装有报警装置，遇到突发情况，取款时尽量让歹徒暴露于摄像头之下，以留存对方的容貌信息，待自身安全后，及时报警。

低价销售游戏装备很有可能是骗局，这是真的吗？

是

近年来针对虚拟网络游戏的诈骗案件不断增多，常见的诈骗方式一是低价销售游戏装备，犯罪分子利用某款网络游戏，进行游戏币及装备的买卖，在骗取玩家信任后，让玩家通过线下银行汇款的方式，待得到钱款后即食言，不予交易;二是在游戏论坛上发布提供代练信息，待得到玩家提供的汇款及游戏账号后，代练一两天后连同账号一起侵吞;三是在交易账号时，虽提供了比较详细的资料，待玩家交易结束玩了几天后，账号就被盗了过去，造成经济损失。

陌生网友约到酒吧咖啡厅有可能是酒托骗局。

是

2012年9月，外地青年小张和自称小樱的女网友相约在郑州见面。等小樱确认小张按照事前的要求带了银行卡，就把小张领到二七区交通路上的一家咖啡厅，点了开心果、果盘等食品。女网友的温柔甜美让小张意乱情迷，不一会儿就消费320元。小樱酒量惊人，杯杯红酒豪爽入肚。但每次酒杯快要见底的时候，小樱都会让服务员上酒，小张也是一遍遍刷卡结账。当晚5小时内，愣头愣脑的小伙子先后刷卡消费10次，共计17620元。犯罪分子专门挑选男性网友,利用其寻找“对象”、“情人”、“一夜情”等欲求心理,取用暧昧网名通过网络聊天引诱见面消费,使其不知不觉落入圈套。同时利用男性爱面子、不愿为人知晓等心理弱点,迫使被骗男性“甘心情愿”吞下苦果,被迫进行高额消费。

扫描陌生人给的二维码可能会下载木马程序。

是

这是近期发生的最新网络诈骗案件。用扫描加微信方式，在受害人手机里植入木马程序，进而获取受害人的支付宝账户信息，此后进行修改支付宝账户密码并转走账户内资金。这类骗局属于高科技骗局。对于任何好友发来的不明链接或图片，都不能轻易点击，以免被不法分子在手机中植入木马程序。2013年8月4日晚上10点左右，经营网店的张先生接到阿里旺旺的一个用户发来的信息，称要购买家具，随后对方称需要用手机接收购买清单，通过旺旺发送了一个二维码让张先生扫描加其为微信好友。张先生用自己的安卓手机扫描后跳出安装提示，他当时没有在意内容就点击了确认。然而，他并未加到对方微信，且对方旺旺也迅速下线。直到第二天，张先生才发现支付宝账户(与手机绑定)内的49812.01元被人转走。警方通过调查发现，原来张先生手机被嫌疑人植入了手机木马，该木马启动后，从手机系统后台拦截短信，并转发至指定手机号码(受害人手机自木马启动后接收不到短信)。嫌疑人据此修改支付宝账户密码并转走账户内资金。经过大量前期侦查，苏州警方在广东和贵州成功将嫌疑人梁某和高某抓获。经审查，从今年3、4月份起，高某以盈利为目的，先后多次制作非法控制计算机信息系统的程序贩卖给梁某等人，实施了多起诈骗。

网上提供特殊的稀缺的信息资源，如划定中奖号码范围、提供黑马股票信息、高额回报工作信息等大多是骗局

是

骗子在互联网上发布虚假网络服务信息，提供特殊的稀缺的信息资源，如划定中奖号码范围、提供黑马股票信息、高额回报工作信息，要求加入会员，支付保证金，甚至代为保管资金等。一旦有人上套，拿到资金后他们会迅速玩起失踪。前不久，市民周师傅退休在家。闲着无事，听同事说，现在可以买点股票，于是他动心了。之前从来没有炒过股，没有经验怎么办?他想到了在网上找一名师傅教教自己。在看到所谓上海某某证券有限公司一长串的专家能手名单和“优秀成绩”后，周师傅十分放心地把自己的积蓄交给对方帮助打理，满心欢喜地等着高额利润回报，先后被对方以入会费、保证金、股金等名义骗取人民币50多万元。

被告知在抽奖活动中奖，很大概率是骗局

是

这是最常见也最高发的诈骗方式。这一骗局，主要利用人性贪婪的心理，编造各类中奖故事，逐步骗取被害人的资金、账号，并会利用人的侥幸心理连续地编造故事进行欺诈，直到被害人彻底失望放弃为止。住在市区的张先生，在上网时收到一封邮件，称其在游戏中中奖，奖项是一台三星笔记本电脑和38000元现金，邮件中还留下了中奖查询电话。收到邮件后，张先生通过中奖查询电话同所谓的“公司客服”联系，对方要求他预交1000元物流保证金，并且要求在3小时内汇款到帐，否则等于自动放弃。为了获得奖项，张先生按照对方的要求将钱汇入对方指定的账号。此后，对方又以要交保证金、个人所得税等名义要求他继续汇款，总计30000余元。

网购时卖家给的其他网站的链接，要谨慎点击

是

此类案件防范比较困难，普通网民在支付的时候很容易被假的网站蒙蔽，轻易地输入自己的卡号和密码，信息全部被犯罪分子获取，被骗以后所有的银行资金全部被转移，损失巨大。市民余先生在家上网时，想要购买一张移动充值卡，于是他用支付宝拍下一卖家的充值卡商品，之后便用淘宝旺旺与卖家取得联系。对方并没有马上给余先生移动充值卡密码，而是要求他到一个网上交易平台支付0.1元提取一个订单号，余先生也没多想，便打开对方提供的网站，选择支付了0.1元。到了第二天，余先生查询自己的银行卡，发现里面突然少了35000元人民币。

网络交友中，我们应该给相聊甚欢的人完全的信赖吗？

不是

对于网络上相聊甚欢的人，我们也应该留一个心眼。有一些犯罪分子利用互联网发布信息，或和被害人进行聊天，编造各类故事，设置感情陷阱，骗取对方信任，或者博取对方同情，骗取钱财。这一骗局游走在法律和道德边缘，被害人因面子问题，很多时候都羞于报案，公安机关进行打击缺乏证据。家住苏州吴江的卢某在“世纪佳缘”等大型聊天交友网站注册账号，谎称自己是退伍军官，自身条件优越，骗取多名女性的信任后，以投资和救急为名，诈骗作案多起，被害人不仅损失金额巨大，同时身心又受到了极大的创伤。

公安局打电话告诉你涉嫌洗黑钱，已经成为通缉犯，需要配合调查洗清嫌疑，你应该主动配合吗？

不是

此类诈骗先提前通过非法渠道获得取得获得受害人的个人信息。然后通过网络改号软件伪装成公安局电话群发短信或者拨打用户手机，接着以涉嫌洗钱、法院传票、信用卡透支、邮包藏毒等方式恐吓受害人，接着再以帮助受害人洗脱罪名为由要求对方转账；也会通过木马病毒的方式，直接控制用户电脑进行转账操作。警方不会打电话办案，更不会要求汇款转账，所有警方打电话办案的都是诈骗。2014年9月12日，有小龙女之称的著名影星李若彤的经纪人邓小姐接到自称是“内地公安局”的来电，通知她因为涉嫌贩毒、洗黑钱等罪已经成为通缉犯 。随后，为配合调查，她在对方的指示下，登陆钓鱼网站后将某内地账户的银行U盾插到电脑上，几秒黑屏后，她收到银行提示短信，该账户上的100万已被全部转账。

超低价商品，见到就要把握机会，这是真的吗？

不是

请不要相信任何低于实际价值商品的信息，不到任何非正规网站购物。有些诈骗分子通过各种淘宝等电商渠道发布超低价商品真实链接，当有用户上钩后，通过短信等方式将虚假网址链接发送给用户，由于诈骗分子所给的虚假链接前半部分和真实网站一模一样，因此一般用户很难区分此类链接的真假，当用户点击购买后，其实是将钱直接打给了诈骗分子，根本收不到任何货物。据《北京晨报》报道，2014年11月18日，首都网警破获了一起利用淘宝网低价商品虚假链接，骗取事主钱财的诈骗案件。犯罪团伙通过互联网交易平台，疯狂作案300余起，涉案金额200余万元。

航班被取消，机票要求改签，点开短信中的链接就可以退票多退200元。

不是

“航班取消”诈骗一般采用“伪基站”群发航班取消短信，以退票多退200元为诱饵让用户点开短信中留下的“钓鱼网址”或者假冒航空公司的400电话让受害人放松警惕。钓鱼网址的页面一般与航空公司页面几乎完全一样，一旦输入了账号、密码，就会被盗取资金。不回拨短信中的任何航班改签400电话，查询航班信息以官方客服电话、官方网站信息为准，不点开任何陌生网址。2014年11月，央视报道了一起信息诈骗案，贵阳的张女士收到了一条“机票改签”的短信，她随后拨打了短信中预留的400电话，对方告知因天气原因导致她的航班取消，并表示可以帮她办理改签，让她登录“官方网址”进行改签操作，当张女士在对方提供的网址上完成改签之后，手机收到了一条银行提醒短信，她卡里的17万元被转走。

公共场合的免费WiFi便利又好用，能连就连。

不是

请不要轻易接入任何无密码WIFI，不在公共场所打开手机WIFI功能。有些黑客先是配置一款无线路由器，设置一个公共的免密码连接的钓鱼WiFi，当有用户登录至该WiFi后，利用手机安全漏洞，黑客即可获得手机的完全控制权。当用户在手机上输入支付宝账号和密码的时候，这些极其重要的账户认证信息就会被黑客所获取，其中就包括用户的支付短信验证码，从而进行下一步的转账和盗刷。据人民网11月27日电，据陕西省榆林市神木县公安局永兴派出所官方微博官方微博消息，日前，江苏扬州一市民的银行卡在不到2天内，竟交易69笔，6万元不翼而飞！警方发现，这与他曾在公共场所连接免费WiFi有关。

收到10086的短信，说可以用积分兑换现金礼包。

不是

据新华网2014年11月25日报道，武汉十堰刘女士近日手机接到一条来自“10086”的短信，短信称：“尊敬的用户：您已满足兑换249.36元现金大礼包，请登入点击下面链接，网络商城，根据提示下载并安装点击允许，即可领取”。刘女士当时没有理会，隔天后刘女士的手机上再次收到相同短信。刘女士想到可以兑换现金，于是便点击下载安装并进入这一网站，随后网页上弹出要求输入银行账号、密码及身份证号等信息，刘女士按照要求进行输入。没过多久，她发现卡上1.6万余元被人通过网银分5次全部消费。犯罪分子通过“伪基站”伪装成10086群发积分兑换现金的诈骗短信，并在短信中内置一个钓鱼网址；用户看到10086发的短信后便放松了警惕，按照短信要求登录钓鱼网址，并输入了个人信息（身份证号、手机号、银行账号密码）；然后，诈骗分子通过电商和支付平台，发起购物申请，通过快捷支付功能完成了银行卡盗刷。