**案例一：积分兑换诈骗**

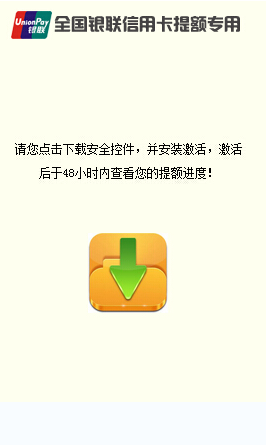
【案例回放】

2015年4月6日，北京的杨先生收到一条由某电信运营商发来的积分兑换短信，内容如下：“尊敬的用户您好：您的话费积分3160即将过期，请手机登陆web-10086.com/bank激活领取现金礼包。中国移动”

见到短信是由自己手机号所在运营商的号码发送的，因网址与真实网址近似，杨先生并没有过多的怀疑，就用手机打开了网址。进入的也是一个标题为“掌上营业厅”的页面，页面要求填写姓名、身份证号、信用卡卡号、交易密码、预留手机和卡背后三位等信息。



杨先生按照要求填写了相关信息后，点击下一步，又进入了一个标题为“全国银联信用卡提额专用”的页面。继续填写信息后就被要求下载一个安全控件（实际上是木马程序）。



当王先生一切都按照页面提示提交信息后，页面就进入了一直等待的状态。不久后，王先生就收到多笔消费短信，提示自己的信用卡被消费了7739元。

【网警解读】

这是一起典型的“伪基站+钓鱼网站+手机木马”的网络诈骗。骗子首先用伪基站伪装成电信运营商的号码，向受害者发送了带有钓鱼链接的诈骗短信，诱使受害者在钓鱼网页上输入包括身份证、信用卡等一系列个人敏感信息，最后又在钓鱼网页上以信用卡安全控件的名义，诱骗受害者在手机上下载了一个木马。检测显示，这个木马的主要作用就是劫持用户手机收到的银行发送的验证短信。骗子利用同时骗到手的信用卡账号、密码、卡背后三位（信用卡背后的三位密码，很多银行的信用卡，提供这三位信息后就可以进行消费）和手机验证码，就可以成功的利用网上银行或手机银行来盗刷受害者的信用卡。

实际上，积分兑换只是伪基站短信诈骗最常见的一种形式，其它常见的形式还有银行U盾升级、银行卡积分兑换等。

【网警提示】

由于有伪基站技术的存在，因此，即便是自己熟悉的客服号码发来的短信，也不能轻易相信。特别是当短信中有网址链接时，一定要谨慎打开。最好是向服务商的官方客服渠道核实之后再查看。

不论是银行还是电信运营商发送的活动短信，通常只会要求用户填写账号、密码，或手机号，不会要求用户填写身份证号这种非常敏感的信息，更不可能要求用户填写信用卡信息。

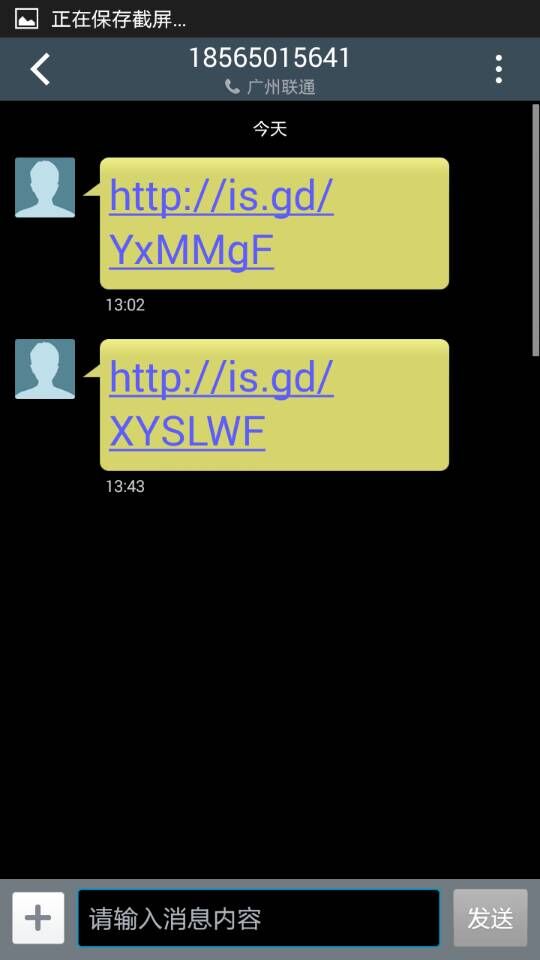
银行的U盾通常是不需要升级的，更不存在不升级就将失效的问题，所有类似U盾升级，银行电子密钥升级的短信基本上都是由伪基站发送的诈骗短信。

**案例二：冒充客服/网购异常诈骗**

【案例回放1】

2015年4月16日，安徽省合肥市的王先生接到一个号码为18565015641的电话，对方自称是亚马逊的客服人员，因发现王先生的付款存在问题，所以需要王先生提供自己的银行卡号，给王先生退款，同时还要求王先生将发货方式改为货到付款。

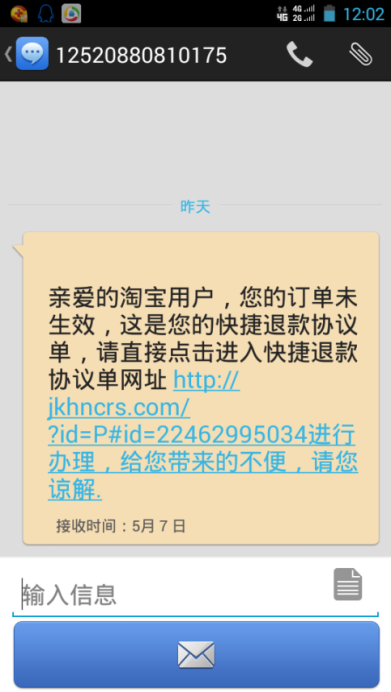
由于王先生恰好是刚刚在亚马逊网站购过物，而且对方也准确的说出了他所购买的商品信息，因此，王先生对于这个电话并没有产生什么怀疑。随后，该号码就向王先生发送了一个带有退款链接的短信，要求王先生在页面上进行退款操作。



王先生打开短信中的链接后，见到的是一个“支付宝支付异常系统”，王先生在该系统上填写了网银的账号、密码、验证码以及身份证等信息。随后，王先生就收到了银行的扣款短信，其网银账户被扣掉了228元。

【案例回放2】

2015年4月29日，江苏省盐城市徐女士在淘宝购物后，收到一条看似淘宝系统发出的短信。短信内容称：徐女士的订单未生效，可以进行快捷退款。徐女士点开短信中的链接后看到一个退款界面，要求填写姓名、身份证号、储蓄卡卡号及银行预留手机等信息。徐女士在填写相关信息不久后，收到银行发来的扣款短信，短信显示自己的银行卡被扣款3000元。



【网警解读】

此类诈骗是近期发案数量仅次于积分兑换的诈骗类型，无论是在PC端还是手机端都非常流行。在PC端，骗子主要是使用聊天软件冒充商家客服，而在手机端，骗子则主要是通过诈骗短信或直接拨打电话的方式冒充客服。

而所谓的“支付宝支付异常系统”、“交易异常处理中心”、“快捷退款页面”等都是骗子伪造出来的、原本就不存在的钓鱼网站。用户在这些网页上填写自己的银行卡账号、密码和验证码，甚至是身份证信息之后，骗子就可以利用这些信息盗刷用户的银行卡。

退款诈骗是一种成功率很高的网络诈骗形式，而成功率高的主要原因就在于骗子对受害人的身份信息和购物信息了如指掌，从而使受害者很难识破这种骗局。而造成这种情况的主要原因，就是因为互联网上有大量的个人信息泄漏。根据某互联网企业的统计，仅2011年至2014年底，已被公开并被证实已经泄漏的中国公民个人信息就多达11.27亿条，内容包括账号密码、电子邮件、电话号码、通信录、家庭住址，甚至是身份证号码等信息。

但是，被公开的这11.27亿条个人信息很可能只是冰山一角，未被公开的、在地下被偷偷使用和交易的个人信息数量可能还要更多。根据某第三方漏洞征集平台的数据统计，仅该平台上被报告的漏洞，就有可能导致23.6亿条用户个人信息泄漏。

【网警提示】

不论是淘宝、天猫还是京东，都没有所谓的异常处理流程或退款流程，还有类似卡单、掉单等词语也都是诈骗专用术语。

不要相信主动找上门来的客服电话或客服QQ，遇到问题应当通过官方客服电话进行咨询。

当有人告诉您交易存在异常时，应直接登陆电商网站并查询自己帐户的状态，如果系统给出的账号状态和交易状态没有异常，则不要相信陌生人的说法。

定期修改购物账号的密码可以在一定程度上减少自己遭遇退款诈骗的风险。

**案例三：网络兼职诈骗**

【案例回放1】

小李考上大学后一直想找个兼职，一日他在某QQ群中看到有人发布“高薪兼职，日赚300”的信息，遂与对方联系。对方自称是做“淘宝刷钻平台”，小李只需要去指定的淘宝店铺购买充值卡，对方会把货款退还给小李，确认好评后，小李将得到一定比例的佣金。购买次数越多，佣金返还比例也越高。

小李按照对方要求购买了充值卡后要求对方返款，但对方要求小李将充值卡的卡号和密码截图发送过来以验证小李确实购买了充值卡。小李未加思量便将充值卡的卡号和密码截图发送给了对方，但对方以小李的操作尚未满足返款条件为由，拒绝返款给小李，并一再要求小李继续刷钻，以满足返款条件。小李感觉自己可能被骗，想立即使用充值卡以挽回损失，但拨打充值电话后被告知，充值卡已经失效。

【案例回放2】

小王是大三学生，一日在浏览博客时无意中看到一篇名为“中国联通招聘网络兼职”的博客。博客称联通为扩大业务量和知名度招聘“刷业绩兼职”，回报率很高，并且醒目提示“不需要任何保证金”、“需要保证金的都是骗子”。

小王觉得博客内容规范，提示贴心，比较可信，遂通过博客上的QQ进行联系。对方自称为联通内部员工，为提升业绩招聘“刷业绩兼职”，只需去官方网站上购买联通充值卡，3张算一次任务，任务完成后会把货款退回给小王，每次任务可得15元佣金。对方还特别提醒小王不用担心被骗，因为就算不退还货款小王手里还有充值卡，也不会损失。

小王觉得对方说的有道理，于是就在对方发来的充值卡链接上花300元购买了3张充值卡，然后联系对方要求回退货款。但对方却表示，系统可能“卡单”了，只看到一张充值卡的交易记录，小王必须再购买三张才可以激活之前的订单。小王感觉不妙，立刻打电话充值，但系统提示卡号密码错误，充值卡都是假冒的。

【网警解读】

网上兼职诈骗，也称为刷信誉诈骗，大多是以简单的任务，高额的佣金，来诱惑受害者应聘兼职，随后用人工欺诈与钓鱼网站相结合等方式实施欺诈。为取得信任，骗子往往都会编造出神秘、灰色的身份，例如“淘宝刷钻平台”、“联通内部员工”等。有的骗子不仅会制作精致的兼职说明，而且还会“好心”的提醒受害者要当心上当，甚至会介绍各种防范兼职欺诈的方法，如：“需要保证金的都是骗子”、“一定要在收到返款之后再确认收货”等。但在实际特定的欺诈场景中，这些“好心”的提醒都没有什么意义，只是为了让受害者放松警惕而已。

在第一个案例中，骗子与淘宝卖家实际上没有任何关系，受害人小李在淘宝店铺中购买充值卡的过程是完全符合正规的购物流程的，所以淘宝店家没有任何法律责任。只不过，小李为了让对方确认自己购买了商品，将卡号和密码截图发送给了对方。对方立即进行充值，从而完成了欺诈。

这起案例中，小李及时发现问题并停止了交易，所以损失不是很大。但在以往的某些案例中，有些骗子会在受害人一开始只有小额投入的时候真的返利给受害人。而受害人一旦相信了对方进行大笔投入，则骗子就会立刻卷款消失。最终被骗几万、十几万的人都有。

在第二个案例中，受害人小王实际上是在骗子的诱骗下登录了钓鱼网站，而在钓鱼网站上购买充值卡，实际上就是将钱直接转入了骗子的账户中。如果小王按照骗子的提示，继续购卡“激活订单”的话，结果只会是继续被骗。

【网警提示】

找兼职要上正规的招聘网站，不要轻信QQ群、博客、论坛上看到的招聘信息；

不要从事不合法的兼职工作，否则不仅容易上当受骗，而且可能还会承担法律责任；实际上，刷点、刷钻、刷积分等都不合法，相关的网上兼职也基本上都是欺诈；

几乎所有通过截图方式证明交易成功的要求都有很强的欺诈嫌疑，因为，真正卖家完全可以通过查看交易记录来证实交易是否成功，而不会要求别人发截图。

**案例四：网络二手交易诈骗**

【案例回放】

王先生心仪某水果手机已久。一日，他在淘宝网上看到某卖家标出某二手水果手机的价格只需2600元，比别家便宜。他随即用淘宝旺旺与卖家联系，但卖家以电脑运行旺旺会卡为由，要求转到QQ上进行交流。

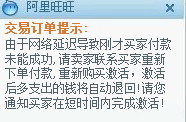
卖家告诉王先生，手机是前男友送的生日礼物，因分手后不想看到“伤心物”，故忍痛贱卖。王先生对卖家很是同情。不过由于担心货品质量和售后保障，王先生还是仔细询问了手机的序列号，并索要发票，卖家也一一提供。



王先生随后向卖家索要商品的实物照片，卖家表示室内光线不好，无法拍摄，并突然告诉王先生，有另外的买家想要买这台手机，并且能出更高的价格，但是如果王先生现在就能拍下付款的话，自己还是愿意以原价卖给王先生。王先生担心超值的手机被别人买走，立刻答应现在就拍下付款。

卖家发来一个“淘宝链接”（实际上是钓鱼网站）要求王先生拍下付款。王先生还特意仔细查看了链接，里面确实包含熟悉的“item.taobao.com”，于是使用中国银行网银付了款。但当王先生通知卖家自己已付款时，卖家却说没有收到交易通知。

王先生查看自己的淘宝交易记录，发现也没有刚才拍下的手机，此时，王先生开始焦虑不安，并向卖家询问。卖家表示，这是由于淘宝网网络故障“掉单”了，导致王先生的付款被支付宝暂时冻结，并发来了交易状态截图和淘宝旺旺的提示截图（实际上，淘宝不会发送此类信息），如下图



卖家告诉王先生，只需要再支付1元激活款，被锁订单就会被激活，同时又发来了那个2600元的商品链接要求王先生拍下付款。王先生询问为什么金额显示是2600元而不是1元？卖家非常确定的多次表示，2600元显示的是被冻结金额，王先生实际上只需付款1元，催促王先生尽快付款解锁。并发来“系统提示”截图和网银提示截图。





对于卖家的说法，王先生将信将疑，但最终还是按照卖家的要求，在卖家发来的商品链接上进行了付款操作。随后不到1分钟，王先生的手机便收到了银行发来的扣款2600元短信通知。此时，王先生实际已经支出了5200元。王先生感到自己上当了，立即找卖家质问。

卖家再次坚称没有欺骗王先生，并表示，可能是由于王先生的电脑网络问题导致连续付款错误。随即发来了一个名为“淘宝订单解锁”的文件（实际上是一个网银木马），说只有运行这个文件进行订单解锁，才能退回之前的款项。王先生退款心切，便接收并打开了这个文件。随后，王先生电脑上的某安全卫士提示此程序为木马，已经删除。

王先生再次向对方询问，对方却反问“是杀毒软件吧？”，“这是杀毒软件的误报”，“要首先关掉杀毒软件，再运行这个程序”。对方还向王先生提供了一个某搜索引擎“杀毒软件误报”的结果链接（<http://www.baidu.com/s?wd=360%CE%F3%B1%A8>）。



王先生看到搜索结果后，最终听信了对方的话，关闭了所有的杀毒软件产品，并再次接收和运行了对方发来的程序。

该程序提示王先生：只需要再次登录网银输入用户名和密码进行确认，不需要再进行支付。王先生按照提示操作，结果并没有等到款项被退回的消息，手机却收到银行发来的信息提示：一笔金额为1万元的扣费交易，由于账户余额不足没有成功。王先生此时才确信自己真的是上当了，立即挂失了银行卡，并拨打了110报警。

【网警解读】

这是一个十分经典的“钓鱼+木马连环欺诈”，骗子通过精心布局一步一步引受害者上钩，最终利用网银木马洗劫受害者网银资金。在上述案例中，如果不是账户余额恰好不足，王先生的损失还将扩大。

在上面案例中，骗子不仅利用受害人对淘宝规则的不了解进行了钓鱼欺诈，而且还利用受害人急于追回损失的心理，进行了逐步深入的诱骗欺诈，致使受害人被二次钓鱼，并最终关闭安全软件，放行了网银木马，险些造成更大的经济损失。此外，骗子在欺诈过程中，还利用了受害人的同情心理（自称失恋）、抢购心理、甚至还引用知名搜索引擎的搜索结果作为自己的欺诈说法佐证，骗局设计之精密，实不多见。

还有一点值得注意，这就是骗子对钓鱼网址的伪装。王先生在打开钓鱼网站之前，还特意查看了一下网址信息，其中包含“item.taobao.com”，为什么还会是钓鱼网站呢？

下图是骗子通过QQ发给王先生的钓鱼链接。其中，后半部分确实包含淘宝网页的网址信息。但是，根据HTML的相关规则，实际上，这个网址的前半部分才是真正会被打开的网页，而后半部分不过是一个无效参数。为了增加迷惑性，骗子还对前半部分网址进行了编码，普通用户很难分辨其对应的真实域名是什么。



【网警提示】

不要轻信明显低于市价的商品信息；

凡是要求使用QQ沟通的淘宝卖家，十有八九都是骗子。因为旺旺会拦截卖家发送的非淘宝链接，而QQ则不会；用旺旺与淘宝卖家沟通，被钓鱼的风险会大大降低；同时旺旺上的聊天记录也能成为交易纠纷的核查证据；

所有类似“卡单”、“掉单”、“付费激活资金”之类消息或截图信息都是欺诈信息；淘宝既不会向买家也不会向卖家发送此类信息；

网购过程中，不仅不要关闭安全软件，而且还应当开启专门针对网购设计的安全服务产品；

对于有一定网址识别能力的用户来说，识别网址安全性，一定要看网址中的第一个域名。遇到形如“http://%39%6D%70%2E%63%6F%6D/BOhm6?”这种有一堆“%”的域名就要加倍小心，因为正常合法的网址不需要这样的伪装。

**案例五：冒充老板/熟人诈骗**

【案例回放】

2015年6月27日上午8时30分许，一家医药公司出纳刘小姐，打开电脑登录QQ，看到公司“李总”QQ头像闪动，点开对话框，内容是提醒她“不要迟到，准点上班”。刘小姐有些心虚，不知如何回复。没一会，“李总”又发来信息：“公司账户上还有多少资金？”刘小姐回复：“300万。”“李总”指示：“好，立即转40万到这个账户。”

一个陌生账号发了过来，“有急事，你快点，转了账再找我签字。”“李总”的叮嘱让刘小姐不敢马虎，虽然操作违规，但她不敢多问，赶紧上网转账。没多久，她又按“李总”指示，向另一账户汇入100万元。

9时许，当刘小姐拿着140万元转账票据，找李总签字时，李总目瞪口呆，当天一早，他一直在接电话，根本没登录QQ，遂发现被骗。

【网警解读】

QQ冒充熟人尤其是老板诈骗，一直以来是出现比较多的诈骗形式，特点是作案手法简单，诈骗金额巨大。操盘手上网找到财务人员QQ号后，将木马程序植入广告，发送给受害人，一旦点击，木马程序会自动窃取QQ密码。

嫌疑人会在深夜受害人不在线时登录，对其QQ好友职业角色、对话语气语境等进行分析揣摩，选择老总级好友下手。他们一般会将老总QQ号删除，再加入和老总同样图标，同样网名的QQ为好友。实际上，受害人QQ上闪动的“老总”，早已易人，不仔细查看QQ号码，根本无法察觉。

此类诈骗，还包括冒充亲戚，朋友等熟人，编造生病、出车祸、手机欠费等等紧急情况，进行小额诈骗。

【网警提示】

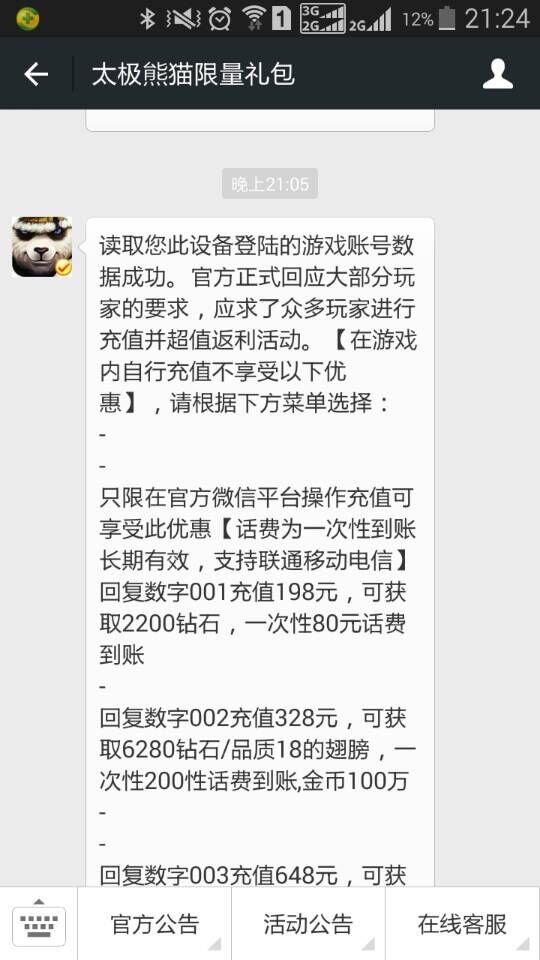
警方提醒财务人员，凡收到要求转账、汇款的信息、电话，必须核实对方身份，严格遵守财务规章才能进行资金操作。公司财会人员，应谨慎向外界透露职业和联系方式等私人信息，以防各类针对性的诈骗犯罪。

**案例六：虚假微信公众号AA诈骗**

【案例回放】

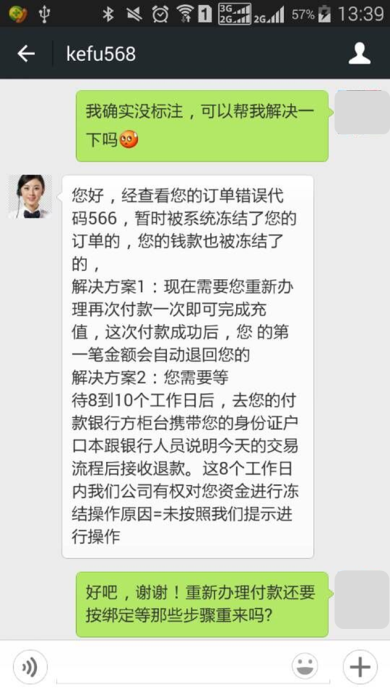
甘肃省酒泉市的邵先生是手机游戏“XX熊猫”的热心玩家。2015年4月27日，邵先生在微信上搜索“XX熊猫”时，偶然看到一个名为“XX熊猫限量礼包”的公众号。于是邵先生就添加关注了这个微信公众号。

关注该公众号后，邵先生看到一个充值兑换的优惠活动信息。信息显示：活动参与者可以选择多种套餐进行充值，充值后可获得非常优惠的游戏道具兑换与话费充值。同时，活动信息还提示，充值只有通过微信公众账号进行才有效，在游戏内进行充值是无效的。看到是微信公众号发布的信息，邵先生并没有过多的怀疑，就点击了活动公告参加优惠活动。活动采用的是AA付款的方式进行收费，邵先生在活动界面上购买了968元的套餐产品。付款后，从AA收款的消息界面上可以看到，共有8个人参与了这个活动，总共付款7744元。

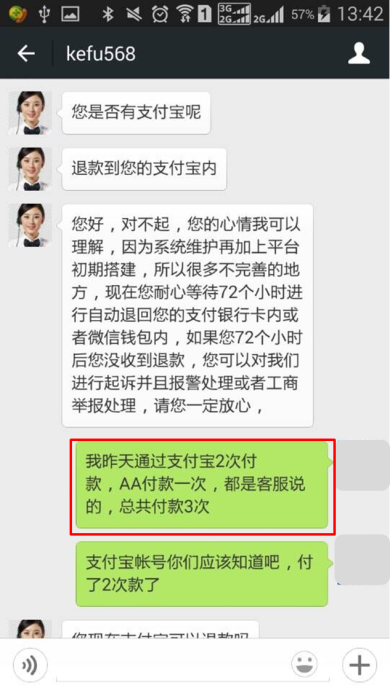


可是，邵先生刚刚完成付款没多久，就有一个自称是客服的名为kefu568的微信号联系了邵先生，并告诉邵先生其购买的商品出现了问题，资金已被冻结，需要给邵先生退款。此时的邵先生略微有一些焦急，便向这个客服号询问如何取回资金，并询问是否可以重新参加活动。

kefu568向邵先生提供了两种解决方案，一个是再付一次款，这样前一次的付款就会自动退回。另一种方法是等9-10个工作日后到银行去办理退款手续。



但邵先生认为这两个方法都很难接受，于是继续和这个客服号沟通。最后kefu568给邵先生发了一个二维码，要求邵先生用支付宝扫描一下这个二维码就可以完成退款。邵先生扫描了这个二维码后，账户中又被转走了968元，收款人为“李传利”。邵先生向kefu568询问是怎么回事，对方说表示可能还是交易异常，请邵先生再扫一次二维码。结果邵先生扫过二维码后，支付宝又被扣款968元。



kefu568劝说邵先生，要解除异常，就必须继续充值或扫描二维码退款。邵先生觉得这个是个无底洞，拒绝继续操作。于是，kefu568告诉邵先生，72小时后钱会自动退款到邵先生的网银账户。次日，邵先生再次向kefu568询问自己的钱什么时候能退，对方则继续劝邵先生等待。又过了半天，邵先生发现kefu568已经联系不上了，而“XX熊猫限量礼包”的公众账号也找不到了。这才确信自己已经上当。

【网警解读】

这是一个连环陷阱的骗局：骗子首先冒充游戏官方的微信公众号骗取玩家关注，之后向玩家发送AA收款链接要求玩家付款。玩家付款之后，骗子又通过虚假的微信客服号以交易异常、继续付款才能退款为由，诱骗玩家反复付费。玩家拒绝再向AA收款付费后，骗子又给玩家发送了一个支付宝的转账二维码链接，用户扫描该链接并确认后，实际上是通过支付宝又向骗子支付了一笔新的费用，从而陷入反复被诈骗的困境之中。

在这个典型案例中，我们看到，邵先生本人先后被骗了三次，被骗金额为2904元。而参与AA收款的一共有8个人，另外七个人至少每人也被骗了968元，加上邵先生的损失，骗子在这样一起诈骗中，至少骗得了9680元。

与2015年春节期间流行的AA收款红包诈骗不同，在这种新型诈骗中，骗子没有对收款链接的名称进行任何伪装，而是明确的告诉玩家这是一个付费送礼包的活动。由于骗子使用的是微信公众账号，利用了玩家对公众账号的信任，所以才能得逞。

【网警提示】

不能认为微信公众账号都是可信的，关注公众账号时，不仅要看账号的认证名称，还要看认证的机构是否为出品游戏企业。

微信AA收款，目前还不具备直接为第三方游戏账号充值的功能，所以，通过微信活动获取礼包的行为都具有一定的风险性。

在向微信公众账号付款之前，最好首先联系游戏官方客服进行确认。这是最为安全保险的一种方法。

任何所谓的需要通过再次付款才能得到退款的说法都是诈骗行为，正规企业向消费者退款是不可能要求消费者再次付款的。

任何时候都不要扫描陌生人从聊天工具中发来的二维码，不论是QQ、微信，旺旺还是其他的聊天工具。因为二维码本质上就是一个网址链接。如果没有欺骗行为，对方完全可以直接在聊天工具中发送网络链接，而没有必要费劲的制作二维码。发送二维码的目的就是为了绕过聊天软件的网址安全检测机制。

**案例七：二维码购物单**

【案例回放】

河南的淘宝店主王先生某一天在网上售货，有买家说要和同学一起购买多款商品，担心买错款式，他们就用手机做了一个二维码清单，这样王先生用手机一扫描就能知道他们要买什么了。然而，王先生用手机扫描完二维码后就跳转到一个文件下载页面，等安装并打开名为“购物清单”的apk文件后，看到的却是乱码，根本没有任何商品信息。

****

王先生再去联系对方，对方已经下线了。但仅仅几分钟以后，王先生却收到网购充值卡成功的短信提醒，同时电脑也弹窗提示说他的支付宝在异地登陆。忽觉事儿有蹊跷的王先生赶紧尝试修改支付宝密码，可这才发现密码已被人改掉。

事实上，王先生遭遇了典型的二维码钓鱼欺诈，当他下载并运行了所谓的“购物清单”文件后，暗藏的apk木马就成功入侵了他的手机。

【网警解读】

利用二维码实施木马钓鱼的伪装性很强，这种钓鱼方式主要针对的是淘宝卖家。骗子以买家的名义联系受害者，并以看上了受害者淘宝店铺中多件商品的名义发来二维码，要求受害者用手机扫描后即可看到详情。受害者卖货心切，扫描二维码后，其实是下载了一个手机木马。该木马会拦截并窃取受害者的验证码短信，黑客利用验证码短信，并通过其他渠道获取受害者身份证号，即可盗刷受害者的支付宝账户。

二维码是当下流行的一种流行事物，但多数人并不知道，二维码实际上只是一个网址链接的二维形态。而且网上有很多制作二维码的工具，制作一个二维码并没有什么难度。

【网警提示】

不要轻信陌生人发来的二维码信息，如果扫描二维码后打开的网站要求安装新的应用程序，则不要轻易安装；

与陌生人进行网上交易或交流时，不要轻易的更换交易或交流的平台。比如本案中，双方的交流就被骗子强制要求从PC上突然跳到了手机上。这种突然而且没有必要的平台转换，实际上就是为了把受害者吸引到一个他不熟悉的环境中，从而更方便的实施诈骗。