2011上半年
中国网络购物安全报告

2011.8.18

金山网络
www.ijinshan.com

目录

2011 年上半年中国网络购物安全报告

网购安全问题想必大家都不陌生，每天网购盗窃事件在你我身边都有发生，网购形势不容乐观。那么网购盗窃的手段都有哪些呢？我们又能如何防患于未然呢？针对这些问题，我们完成了《2011 年上半年中国网络购物安全报告》。

数据来源：

1.金山云安全中心的统计数据；

2.业界公开调查报告；

3.网购受害者维权 QQ 群调查统计受害情况。

一、 主要结论

金山网络分析 2011 年上半年网购安全形势后得出如下主要结论：

(一) 68%网民被盗金额在 500 元以下

网购受害者维权 QQ 群调查数据显示，有 67.9%的受害者被盗金额在 500 元以下。因为受损金额较小，消费者投诉无门时，往往自认倒霉。行窃者的行为长期得不到法律制裁，是网购盗窃猖獗的原因之一。

(二) 40%被盗者怪罪于购物网站

通过微博、QQ 群、论坛了解受害者对被盗过程的描述，发现有 40%的被盗者怪罪于购物网站，20%的用户认为是杀毒软件的责任。

(三) 聊天工具传播的网购木马上千次/天

网购木马的传播方式比较单一，目前只发现通过 QQ 或淘宝旺旺等聊天工具传播，尚未和其他木马捆绑传播，因此传播量相对稳定。金山网络云安全中心监测数据显示，2011 年上半年，网购木马每天通过 QQ 或淘宝旺旺发送的数量达上千次。

(四) 病毒集团完成网购盗窃只需 5 分钟

据受害者回忆和电子商务网站提供的数据，从网购开始接触骗子，到最终被盗，大概需要 5-20 分钟左右的时间。如果杀毒软件能够在尽可能短的时间内对网购木马或者钓鱼网站等问题做出响应，很多网购被盗案是可以避免的。

(五) 钓鱼网站半年增长 10 倍，拦截量超过病毒木马

金山云安全中心的拦截数据表明，今年上半年，新增钓鱼网站的数量和拦截量均比去年同期增长了 10 倍左右，由此可以看出网购的火爆程度。钓鱼网站的拦截量是病毒木马报警次数的 15-20 倍，钓鱼网站已经超过病毒木马，成为最严重的安全威胁。

二、 概述

(一) 网购用户迅猛增长吸引病毒集团加速转型

2011 年上半年，中国的互联网有一个较大的转变，人们对网络娱乐消费的热情，更多地转向了商务活动，电子商务今年上半年热情高涨。投资、并购，电子商务领域热钱涌动；新的细分市场的电商网站不断出现；团购更是点燃了人们的消费热情。

这些最根本的就在于网络购物和网上支付的用户规模的不断壮大，而这种壮大也吸引着病毒集团加速转型，不断提高诈骗、盗窃网购人群技术手段、扩大受害者人群等等。

据中国互联网信息中心（CNNIC）最新统计数据，截至 2011 年 6 月底，中国网民规模达到 4.85 亿，其中，网络购物用户规模达到 1.73 亿，使用率提升至 35.6%，半年用户增长 7.6%；网上支付用户数从去年年底的 1.37 亿增至 1.53 亿，半年增加 1607 万，用户增长 11.7%。团购用户数从 2010 年底的 1875 万增长至 2011 年中的 4220 万，半年增长率达到 125%。

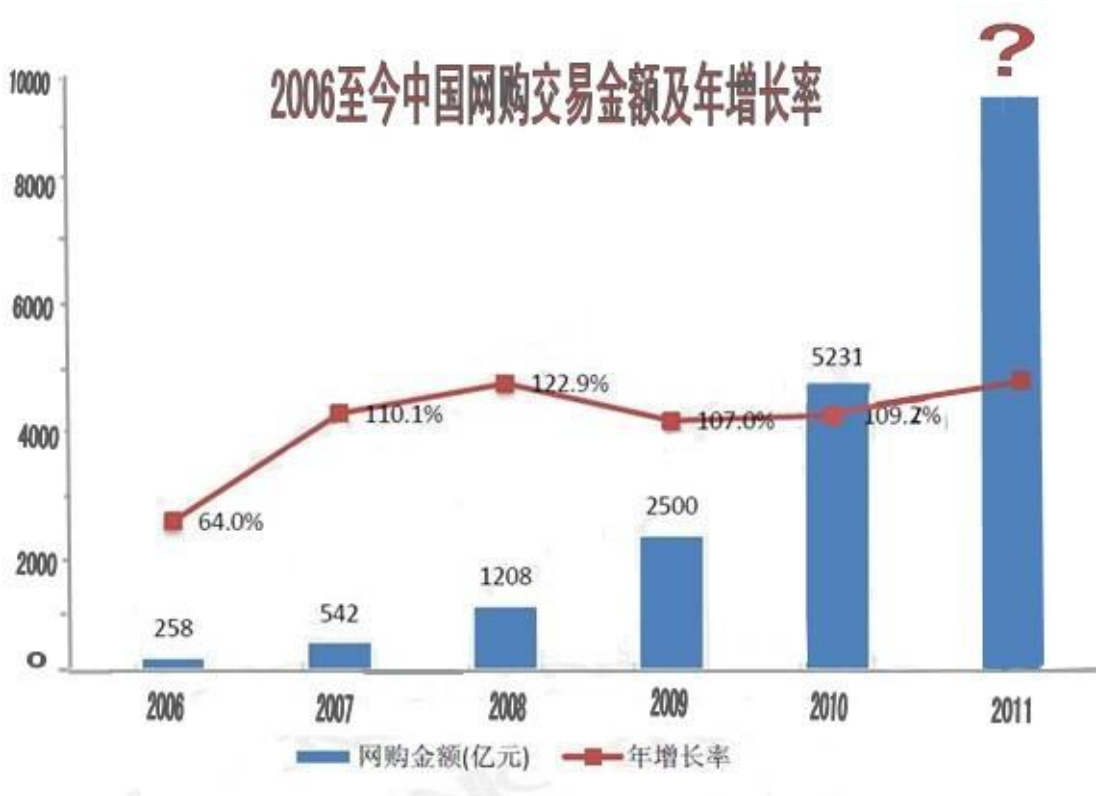

图 1：2006 年至今中国网购交易金额及年增长率

中国网络购物市场交易金额已经连续 4 年实现了成倍增长，至 2010 年交易金额达到 5231 亿元，较 2009 增长 109.2%。相信今年仍会保持这样的增长势头。

(二) 每 12 个网民就有 1 人网购被盗

随着网购在网民中的渗透率日益增加，网上流转的资金快速增加，针对网购的一些不安全因素也在不断滋长。这其中最多的便是消费欺诈和网购被盗。

据 CNNIC 统计，2011 年上半年，有 8%的网民在网上遇到过网购被盗，该群体规模达到 3880 万人，也即每 12 个网民中就有 1 个遭遇过网购被盗！网购安全的问题不容忽视。

一般来说，网购盗窃主要通过两种技术手段实现：网购木马和钓鱼网站。今年上半年，这些安全威胁均增长迅猛。

据金山网络云安全中心统计数据显示，每天监测到的网购木马传播量就达到上千次，钓鱼网站更多，上半年检测到的钓鱼网站服务器主机数近 19 万，拦截钓鱼网站的访问量更高达近 30 亿次，相当于每天拦截 1600 万次。与去年同期相比，不管是钓鱼网站服务器主机数与拦截访问次数均增加了 10 倍之多。

随着网络安全黑色产业链的集团化作战趋势越来越明显，网购的危险因素越来越多，欺诈手法也层出不穷，安全形势仍然十分严峻。病毒集团也正与安全厂商在技术和速度上激烈对抗。

三、 上千名网购被盗者深度调查

(一) 68%网民被盗金额 500 元以下

2011 年 5 月到 7 月，金山网络通过微博、论坛、QQ 群和 1062 名网购被盗的受害者进行调查访问，这些受害者分布在全国各地，甚至连西藏、宁夏、青海、海南等都不例外。

1062 名网购诈骗受害者合计被盗金额达 3651090 元，被盗金额在 500 元以下人数占 67.9%，说明网购诈骗仍然以小额诈骗居多。

受害者回忆被盗过程，绝大部分人估计被盗时花了大约 5-10 分钟和骗子沟通，在骗子的指导下进行在线转帐操作。

因被盗额度多数偏小，达不到立案标准，使得诈骗行为得不到法律制裁，受害者无可奈何，只抱怨自己运气不好或责怪自己没能识别骗术。

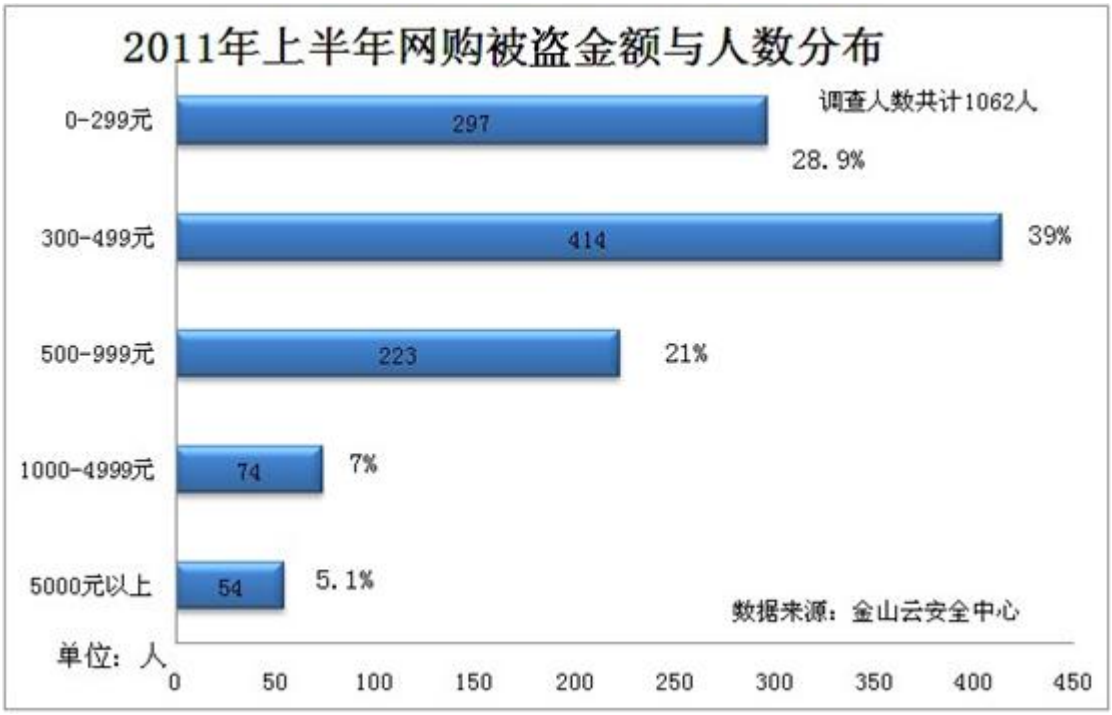

图 2：2011 年上半年网购被盗金额与人数分布

(二) 60%网购盗窃在购物聊天时发生

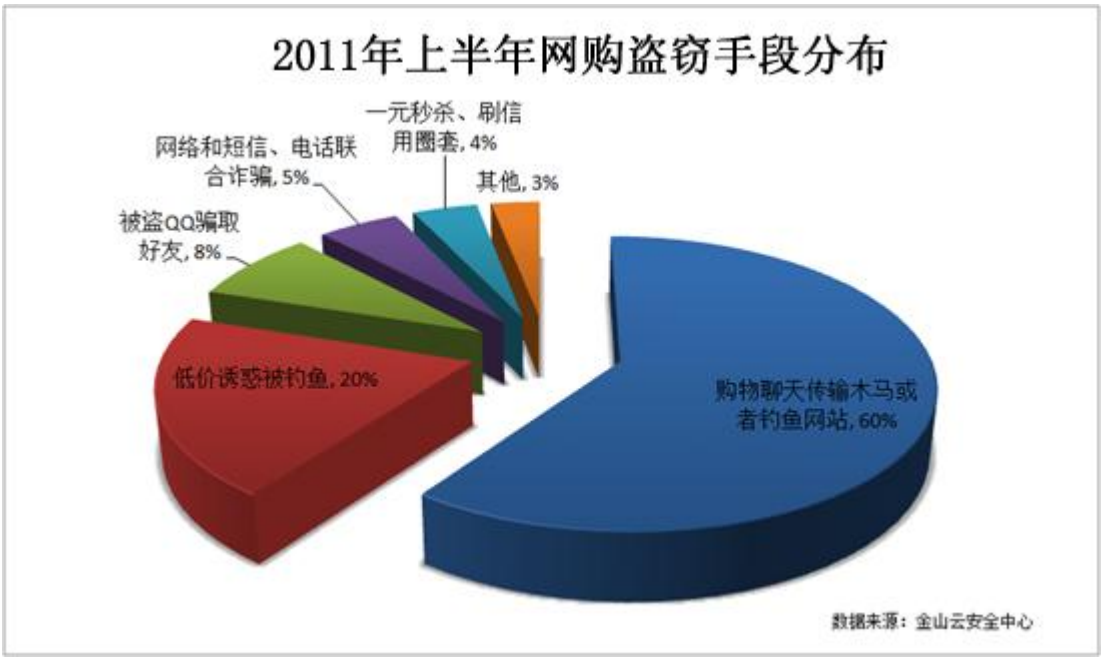

图 3：2011 年上半年网购诈骗手段分布

网购欺诈的手法多种多样，骗子通过百度知道、贴吧、SNS 社交网站（微博客、开心网、人人网等）发布钓鱼网站信息。当网民搜索相关商品交易信息时，可能访问到骗子蓄意制造的欺诈内容。

接下来的盗窃过程多数会用到 QQ、淘宝旺旺等聊天工具。骗子利用网民贪便宜、朋友信任、恐惧等天性，诱使网民上当，然后辅以技术手段，实施盗窃骗取钱财。

2011 年上半年，通过网购聊天传输木马或者钓鱼网址实施盗窃的案例增势迅猛，已然成为当前网购盗窃最为常用的手法，占所有作案手法的比例达到 60%。

其次，低价、打折、优惠等手法虽然传统，但对大多数网民来说仍有非常的杀伤力。利用低价陷阱引诱网民点击访问，网民多会在不明真相的情况下将账款直接打到了骗子账户中。目前，这种诈骗方式占比仍达 20%。

(三) 40%受害者网购被盗怪罪购物网站

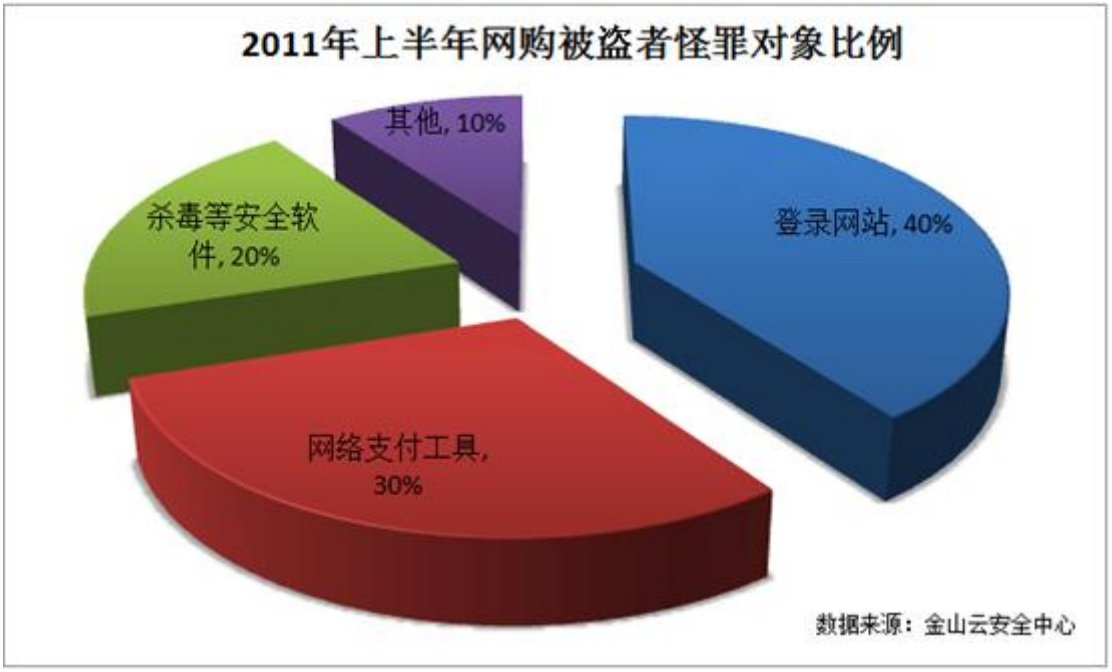

图 4：2011 年上半年网购被盗者怪罪对象比例

网购被盗的网民首先会归罪于案发的网络应用，比如淘宝网、在线订票网站等，这部分占比达到 40%；其次，网民抱怨的是网络支付工具未能保证他们的资产安全，比如支付宝、财付通、网上银行等，占比达 30%；只有约 20%的网友会怪罪电脑中安装的杀毒软件没有起到网购安全防护作用。

CNNIC 统计显示，国内超过 95%的网民都安装了杀毒软件、网购保镖等工具，但网民网购受骗的案例每时每刻仍在发生，有很多网友中了木马或者登陆钓鱼网站，在得到了杀毒软件的提醒之后，却轻易地按骗子的提示关闭了杀毒软件。

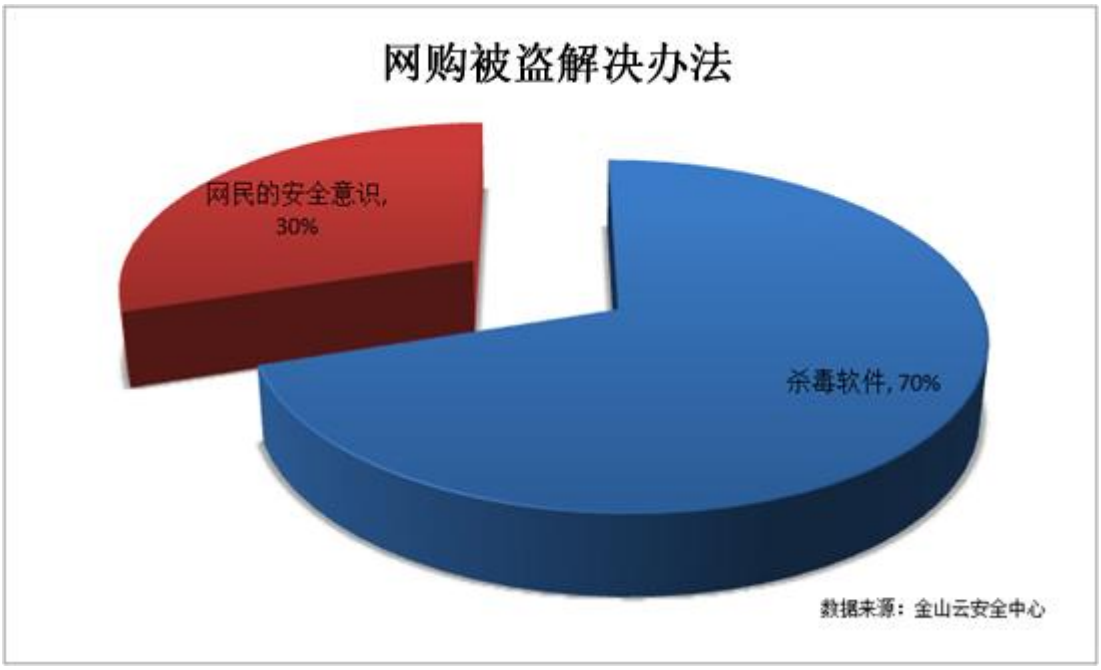

图 5：网购被盗解决办法

虽然网购盗窃手法千奇百怪，但最基本的技术手段无非是网购木马和钓鱼网站，而针对这两种风险，杀毒软件完全有能力、有责任解决。

杀毒软件有能力较好地解决 70%左右的网购风险，当然有些诈骗手法只能依靠网民的安全意识来解决，比如有好友在 QQ 中要求借钱消费。据公安方面统计，这种类型的诈骗上当者众多，基于社会关系的直接诈骗，杀毒软件无法从技术上解决。

四、 金山云安全系统数据分析

虽然网购盗窃者的手法有很多种，但真正从网民手中骗走资金，最根本的技术手段只有 2 种：网购木马和钓鱼网站。网购盗窃的 7 成是被钓鱼网站欺骗，被网购木马直接抢钱的约 3 成。但是，因为网购木马的特殊功能，可以给受害者造成严重损失。

(一) 每天通过聊天工具传播的网购木马上千次

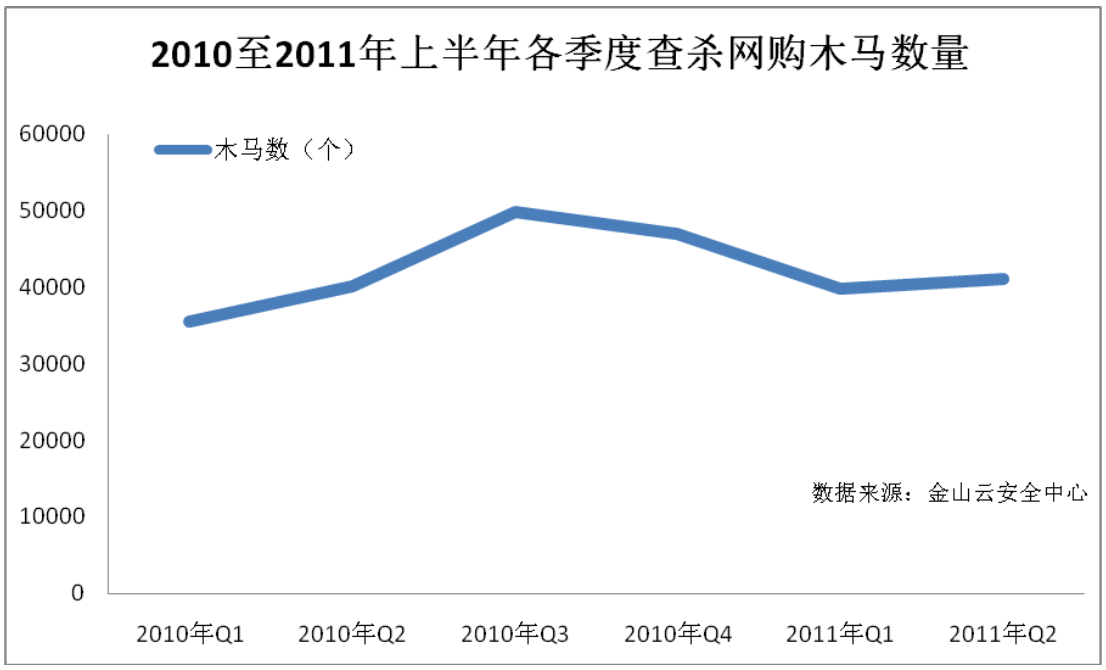

图 6：2010 至 2011 年上半年各季度查杀木马数

所谓网购木马，是指盗窃者将细节图等文件发送给买家，程序运行后会在后台篡改支付链接到指定的第三方支付。一旦中毒，直到病毒清除之前，所有购物交易都将被木马劫持到骗子指定的第三方支付。骗子还借口卡单或支付宝维护，受害者为一个定单反复支付。

网购木马的传播方式比较单一，目前只发现通过 QQ 或淘宝旺旺等聊天工具传播，尚未和其他木马捆绑传播，因此传播量相对稳定。金山网络云安全中心监测数据显示，2011 年上半年，网购木马每天通过 QQ 或淘宝旺旺发送的数量达上千次。

网购木马的绝对传播数量虽然不是很多，但盗窃者往往进行的是点对点攻击，极易上当受骗。若受害者电脑安装的杀毒软件未及时拦截，网购木马诈骗成功率就接近 100%。据此推算，金山网购保镖每天可减少网民损失 50 万元。

(二) 钓鱼网站增长 10 倍，3 成假冒淘宝

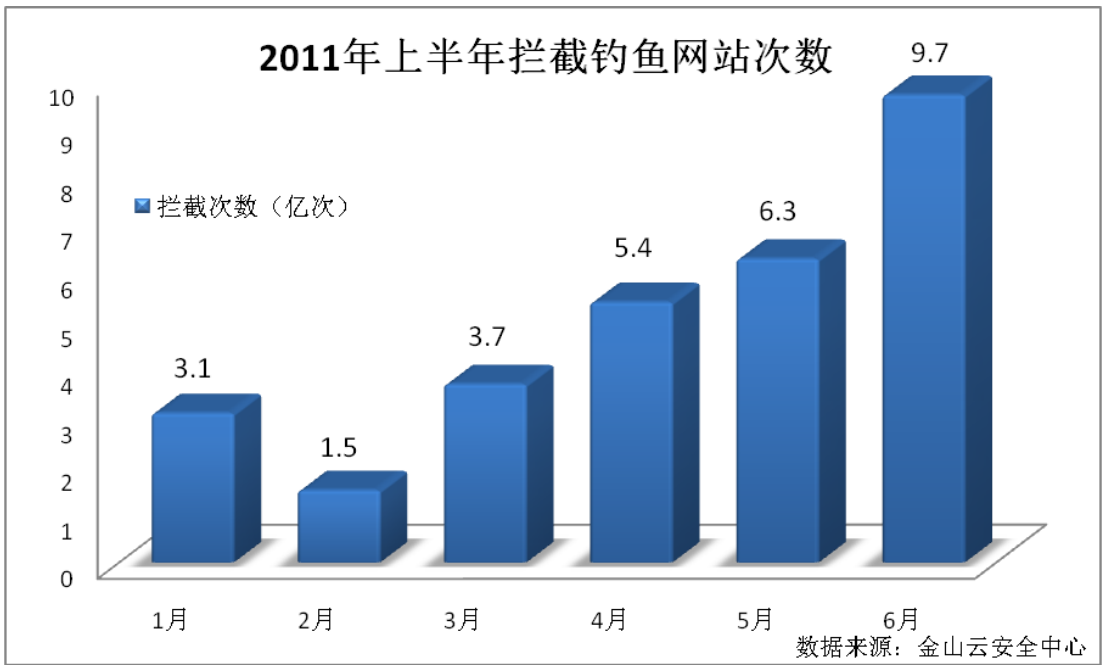

图 7：2011 年上半年拦截钓鱼网站次数

钓鱼网站，是指仿冒网络银行、购物网站的假冒网站，假网站的内容几乎可以达到乱真的程度。网民在钓鱼网站提交自己的网银信息、购物网站帐号密码等，会被钓鱼网站后台盗取，骗子会引诱网民给钓鱼网站上根本不存在的交易付费或转帐到骗子帐户。

金山网络云安全中心监测数据显示：2011 年上半年，监测到钓鱼网站服务器主机数达 18.97 万个，拦截钓鱼网站访问量高达 29.75 亿次。平均每周拦截钓鱼网站的访问量在 1.2 亿~1.8 亿次之间，大约是同期病毒木马拦截次数的 15~20 倍。与去年同期相比，钓鱼网站服务器主机数与拦截访问次数均增长了 10 倍之多。

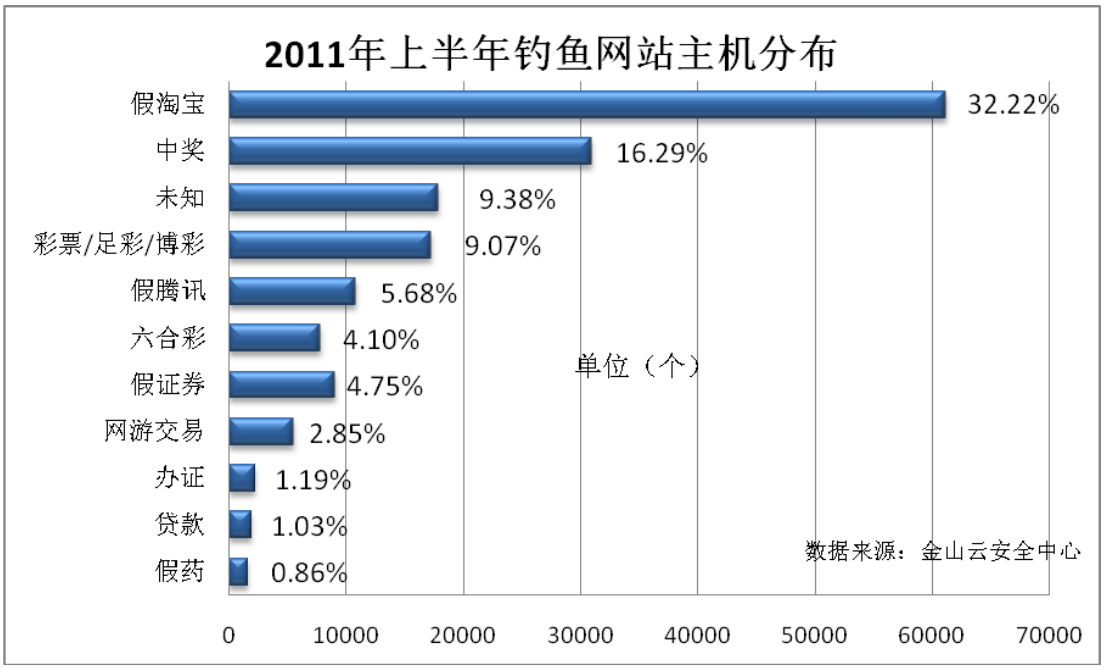

图 8：2011 年上半年钓鱼网站主机分布

今年上半年，钓鱼网站的数量和访问量整体依然保持高速增长，每周新增服务器主机数 5000-10000 个，而每个主机可以建设多个网站因此，钓鱼网站增速更快。

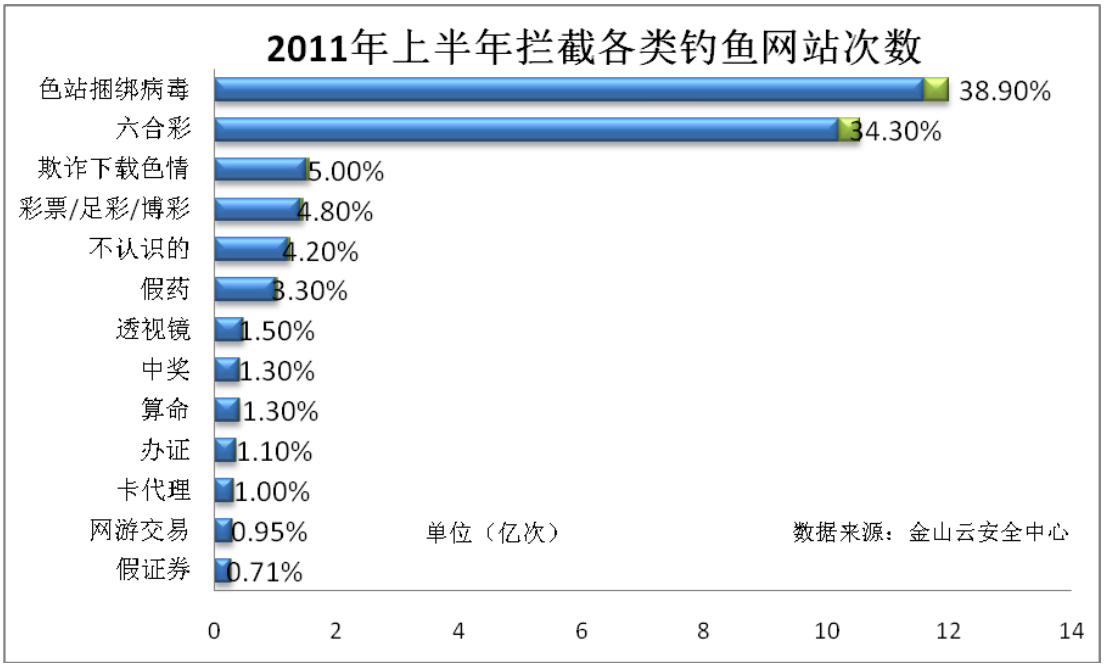

图 9：2011 年上半年拦截各类钓鱼网站次数

在所有钓鱼网站中，与网购相关的大约为 45%。其中假淘宝店约占 32%，QQ 好友被盗后发生的购物诈骗 5%，假网游交易平台 3%，假药店 1%，假旅行社、机票销售 1%，假团购网站 1%。

由于淘宝是开放的 C2C 平台，也没有统一的客服，因此针对淘宝钓鱼网站和网购木马最突出，2011 年上半年，金山网络安全中心监测到假淘宝网站服务器主机数量超过 6 万个。

(三) 钓鱼网站主要采用 P2P 传播模式

针对网购的钓鱼网站传播渠道与传统的病毒传播有很大不同。传统病毒一般依附于访问量较高的网站，比如色情网站、视频或软件下载站等，属于比较典型的一对多的 Web1.0 式的传播方式。

钓鱼网站的传播方式因此更类似于互动的 Web2.0，采用 P2P 传播模式。一般来讲，网购钓鱼网站的传播渠道主要为 QQ、淘宝旺旺等聊天工具，以及电子邮件、短信、论坛和博客、微博客、网游聊天频道等。

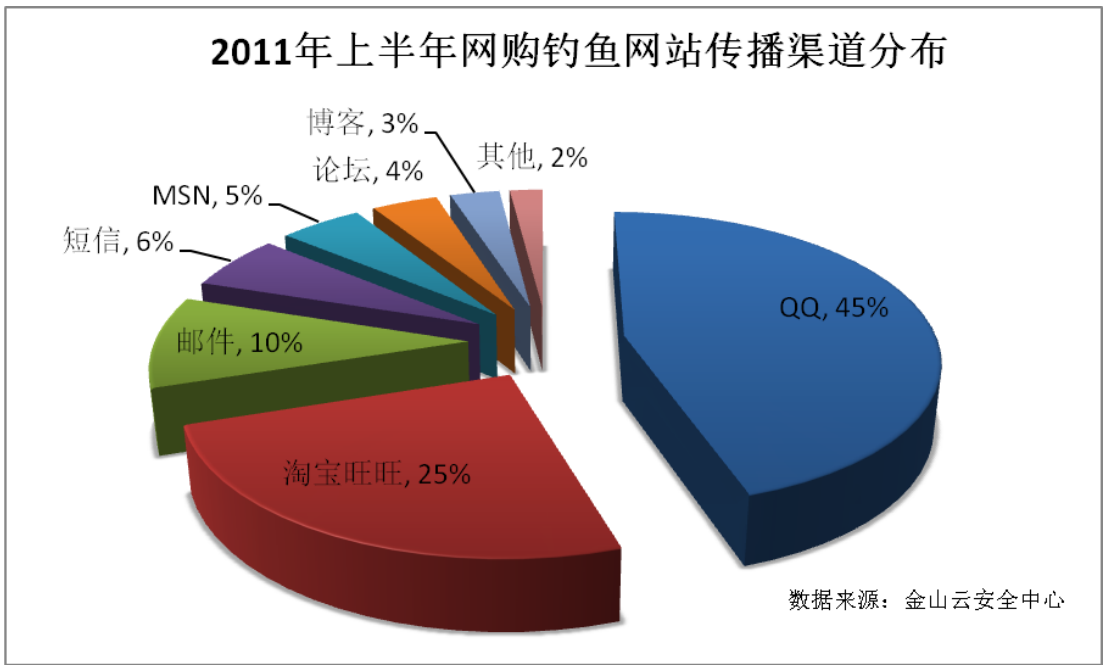

图 10：2011 年上半年网购钓鱼网站传播渠道分布

今年上半年，诈骗者通过聊天工具传输钓鱼网址的案例非常突出，占所有传播渠道的 3/4。如果某个网民的 QQ 号或旺旺号被盗，好友被盗的概率就会大增。

骗子会假冒被盗者的身份向好友行骗，行骗的手段有很多：给好友传输木马文件或者钓鱼网址，将木马或钓鱼链接在 QQ 群中共享，修改 QQ 的签名、发送带广告地址的文件夹行骗等。若遭遇这种情况的网民缺少怀疑和防范，就可能上当受骗。

五、 病毒集团 3 大新特色

今年上半年，网购木马、钓鱼网站等黑色产业链的集团化作案趋势愈加明显，由此不仅带来了钓鱼网站等数量的快速增加，也使得它们的作案手段愈加专业。

目前，网购欺诈呈现出三大主要趋势：木马、钓鱼网址更新越来越快，传统安全软件应接不暇；木马样本的体积制作得越来越大，试图绕过杀毒软件的云技术；整个作案速度越来越快。

(一) 10000:1 的数量战

一般来说，网购木马均有个病毒母体，一个新病毒的制作需要较高的技术水平，新增的速度不会很快，但该病毒进行版本更新是非常简便的，就相当于更换一个“面具”，进行简单的“加壳”、“加花”，稍微更改下程序代码即可。

目前，很多病毒集团制作了相应的程序，可瞬间对木马进行大量的版本更新。网购木马的更新从原来的每周一次更新已经升级到现在的每日多次更新。一个木马母本往往可以生成几十个新木马，有的更多为几百个，甚至几万个。

病毒集团更新网购木马版本，几乎不花费任何成本，但传统杀毒软件却需要对所有的新版本木马重新进行鉴定识别。从一个新版本木马的出现到被传统杀毒软件鉴定为危险程序，往往需要几个小时甚至更久，这期间就可能有大量的网民不幸“中招”。

钓鱼网站也存在类似的更新加快的情形，病毒集团利用批量制作钓鱼网站的工具，简单点击即可快速生成多个钓鱼网站。

病毒集团首先会挑选一些高质量的淘宝店，只需要点击几次鼠标，就将这个淘宝店的所有内容批量生成十几个、几十个完全相同但 URL 网址不同的钓鱼网店。而钓鱼网站的推广还会借助病毒程序来完成。比如木马修改用户系统，直接在网民桌面弹出钓鱼网站。

传统杀毒软件虽然可以拦截钓鱼网址，但拦截方法是基于用户举报，拦截效果有限：主动向安全厂商举报钓鱼网址的网民很少。而钓鱼网址的生存周期普遍不超过一周，收集的大量网址，也会很快失效。

(二) 网购木马游击战绕过杀软防线

除了与安全厂商展开数量上的较量之外，网购木马还在如何绕过杀毒软件的防御上下了很多功夫。

为了对抗第一代采用 MD5 识别的杀毒软件，木马作者会随机修改网购木马的大小，使 MD5 验证很快失效。作者还会把木马的体积做到数十 MB，甚至数百 MB，这是对抗杀毒软件云技术的方法：因为越大的软件计算 MD5 越慢，上传到云服务器也越慢。

还有网购木马会利用正常软件来启动自身，用以绕过一些安全软件的主动防御。

(三) 完成网购盗窃只需 5 分钟

由于集团化作战，诈骗者的作案速度大大加快。而同时，网购木马和钓鱼网站又通过快速增加数量和增大体积，来拖慢传统杀毒软件的鉴定速度，为自己赢得作案时间。

据电子商务网站报案数据统计，诈骗者从诱使网民上当至完成骗取钱财整个过程平均只需要 20 多分钟，最短的不过 5 分钟！

而很多杀毒软件从收集一个新的未知文件到鉴定为病毒，并更新至网民电脑病毒库中，一般需要几个小时，甚至几天，而这时诈骗活动早已完成，诈骗者早已逃之夭夭。

六、 网购盗窃手法大揭秘

网民在网购的过程中被盗的经历五花八门，但金山安全中心专家指出，从技术角度来说，网购盗窃技术手段主要有两种：传输木马病毒和制作钓鱼网站。

（一） 网购木马

木马分为两种：一种是以交易劫持为主的网购木马，一种是以盗取 QQ、网游等账号为目的的盗号木马。其中前者感染量与日剧增，而后者的威胁逐步下降。

1. 常用手法

网购时，往往习惯和卖家进行沟通。诈骗者更倾向于使用 QQ 而不是淘宝旺旺，并以各种名义给买家传输文件，比如衣服照片、货品清单、折扣登记、礼品赠送等，借口不一。

骗子装扮的卖家发送的文件多为网购木马，买家打开这些文件（木马）后，在接下来的交易过程事，木马会盗取买家的淘宝 ID 等个人隐私，创建一个新的隐藏的交易单，这个交易单会抢在正常交易单之前被提交。

在整个过程中，买家完全看不到交易信息被篡改，会直接将货款打到犯罪分子指定的帐号中，不知不觉就上当受骗。网购木马的打劫就好比在超市购物，却把货款付给了假冒的隐身收银员，而超市和其他顾客都看不见这个收银员，一致认为这个被盗的客户在说谎。

2. 木马技术分类

a）盗号木马

盗号木马主要通过潜藏在网页中或是图片及一些文件里，通过受害者打开网页或是打开卖家发来的文件，盗取网民的淘宝 ID、支付宝 ID、QQ 号、银行卡或信用卡信息，然后伺机窃取用户资产。

b）早期交易劫持木马

这类木马是最早发现的网购木马类型，大小一般为 30MB 左右，用图片或 Office 图标做掩饰，在整个网购木马中占比约为 20%。

此类网购木马不需要借助任何其他文件，所有操作都由自己完成，通过淘宝旺旺、QQ 等将以“实物图”等命名的文件发给买家，买家打开就会直接运行木马程序。

c) “压缩包炸弹”类网购木马

最近发现的网购木马的新形式，主要采用两种方式逃脱杀毒软件的查杀。

首先，它将自身体积由原来网购木马的几十 MB 增大至上百 MB，有的整个文件达到 400MB 左右，文件体积的增大会极大地影响传统杀毒软件的查杀结果；然后，病毒作者再用稀有的压缩格式对病毒进行多层循环打包。

这类网购木马在最后一层打包后会重新命名为实物图等一些会诱导买家点击的名字，让受害者自行解包运行，此类木马在网购木马中约占 45%。

d）利用好压等软件漏洞来执行的网购木马

这类网购木马的策略主要是依附于正常的有数字证书的应用程序（比如好压），由正常程序间接运行网购木马，以躲避杀毒软件的拦截。该木马在传播时将自己的病毒 dll 文件命名成 HaoZip.dll，连同正常的好压软件（exe 文件）一同打包。

用户收到文件后，运行好压的 exe 时会自动加载 HaoZip.dll 文件，而这个 dll 文件，正是网购木马自身。作者为了骗用户点击，会把好压的 exe 文件命名为“实物图/高清图”等诱导用户点击。

此类木马在网购木马中约占 30%。

(二) 钓鱼网站

钓鱼网站通常是一些正规银行及电子商务网站的克隆网站，也就是我们所说的“山寨版”，目前钓鱼网站是构成网购安全威胁最主要的一部分。

1. 常用手法

a) 购物聊天传输钓鱼网站

消费者网购时，很多人选择和卖家在 QQ 或者旺旺聊天，收到卖家给发送的各种链接，而钓鱼网站就会掺杂其中，页面通常会模仿淘宝、拍拍、支付宝、财富通等购物相关的网站，引导消费者在假冒的网页上进行支付。

b）网络和短信、电话联合诈骗

骗子首先群发短信，谎称受害人有一笔交易发生，建议网民访问相关网站处理。若网民信以为真，就会访问钓鱼网站。按提示操作，就可能损失金钱或其它敏感信息。

c) 被盗 QQ 骗取好友

骗子利用木马盗取用户的 QQ 号，再冒用他人身价给 QQ 好友群发消息，让好友代付购物。或者在 QQ 消息中发送钓鱼网站链接，好友不知实情，就可能会帮忙付款，最后钱财成功掉入了犯罪分子的口袋里。

d) 低价诱惑被钓鱼

消费者在淘宝网等某些购物网站上买东西时，会发现有的店里的东西比商场里或是其他店里卖的便宜，然后就被极低价格固定了思维，直接点击支付，买下了商品，事后才发现东西没有拿到，钱也不翼而飞了。

e) 一元秒杀、刷信用、删差评圈套

很多不法分子批量伪造各种“秒杀网，淘宝秒杀，一元秒杀”等站点，诱惑用户去点击，然后引导受骗者输入网银、支付宝、财付通账号密码，然后盗取用户的个人信息，致使资金全部卷入黑客的钱袋里。

另外很多店家的信誉很高（实为钓鱼网站），其实是通过一些刷信誉软件等来刷信誉，让你掉入他的陷阱中。还有一些骗子声称可以删除差评，而实际上要么发送网购木马，要么使用钓鱼网站实施诈骗。

2. 钓鱼网站分类与案例

钓鱼网站制作技术简单，成本非常低，只有几十块钱，但它主要是利用人们的心理来实行诈骗。目前网上猖獗的钓鱼网站主要有以下几种：

a) 假淘宝骗走了我的 2000 元钱

一般淘宝钓鱼网站域名里面会有 taobao 字样，但是和真的网站域名不同。如下图，此钓鱼网站地址中虽然有“taobao.com”等字样，但真正的域名为 com-oecea.co.cc。但很多网购者看到 taobao 字样便信以为真，放弃了防备。

图 11：假淘宝网站不仅页面相似，地址中也包含 taobao.com 字样。

案例：张小姐在淘宝网上某家店里看中一款手机，价格为 2000 元，比商场里卖得便宜得多（一般卖 4500 左右），而且卖家级别为 2 个皇冠。在旺旺上联系店主，连发数遍，都只得到店家的一个自动回复：对不起，我很忙，请联系我的业务 QQ，号码为××。

张小姐直接用 QQ 联系了卖家，收到了卖家发来的一个链接，打开一看，是和淘宝页面上一模一样的网页，上面也有她想要的那款手机。并且卖家告诉张小姐，可以直接在上面拍。张小姐按照卖家描述的流程付了款，然后她又立刻登陆到第一次登陆的淘宝页面上，发现没有自己的交易信息。她马上查看了自己的网银，发现 2000 元已经不见了。

b) 谁偷走了我的网游装备？

图 12：456 游戏网的钓鱼网站与真网站让人真假难辨

网游的火爆使很多网络公司都想分这一块蛋糕，更有一些仿冒网站如防盛大、防 456 游戏王等，使大量的网游迷们受骗。

案例：如上图，456 游戏网的山寨网站与真正的几乎一模一样，域名地址也非常相近。当菜鸟玩家小李进入网站后发现和官网一样，便失去了防御的心理，等输入了账户和密码后大约 10 分钟后发现自己游戏账号被盗，积累多时的装备也都被盗走了。

c) 山寨银行短信钓鱼

民航、医院、银行等机构都会有自己的官网，来方便人们自助办理某些业务，也省去了专门去这些地方办理业务的时间，于是这些钓鱼网站的山寨版本就应运而生。

图 13：假银行网站借助短信引诱网民上当

案例：今年初，上海市金山区居民钱女士在家中收到一条手机短信：“尊敬的用户，您的动态 e 令已过期，请您在三日内登陆以下网址进行升级，逾期将不予办理。”钱女士于是根据手机短信中提到的网址上网进行升级，后来发现自己的三万多元被人转走。

d) 小团购的大陷阱

图 14：假冒团购网站拉手网的钓鱼网站

团购钓鱼网站主要分为两种：仿冒知名团购网的钓鱼网站和自己制作的假团购网站，以第一种为主。

案例：2011 年 7 月 18 日，金山毒霸云安全中心监测到伪装成团购网站的钓鱼网站正在通过一些论坛、博客和 QQ 群传播。不少团购消费者被假拉手网欺骗，欧先生就是受害者之一。7 月初，欧先生在拉手网上团购了云南三日行的票，只需 1500 元。当他用网银付完钱之后等了 20 分钟左右，发现没有收到确认短信，也没有看到团购网上的确认信息，打客服电话发现是空号。这时他才意识到自己被盗了。

e) 微博中奖卷走巨款

图 15：新浪微博也遭山寨钓鱼

随着微博的火热，既催生了有关的营销方式，就是微博营销，在评论回复中插入广告，但是这其中也隐藏着许多钓鱼网站的链接。据金山云安全中心统计，目前每天冒出的微博钓鱼网站高达几百个，有时甚至达到 500 个/天。

一般链接前的广告特别吸引人，一旦点击链接，就会进入他们的钓鱼网站的页面里，进而上当受骗。另外一种是发布消息，说你已经被新浪微博选中，成为几等奖幸运用户，请点击查看通知，这种一般都属于虚假中奖诈骗消息。

案例：李先生某天和往常一样打开微博，结果发现微博通知自己被选为幸运用户，将获得大奖，请尽快与客服联系。客服电话是×××，在两个小时之内办好手续，只收取 5 元的手续费。他觉得新浪是一家很正规的一家公司，不可能是骗人的，而且打了电话之后，了解了基本上的领取流程。点击通知下面的一个连接，然后找出相关的窗口，输入了自己的网银账号和密码，付了 5 块钱，就坐等大奖的到来。孰知他等了一个星期都木有到，他才意识到受骗了，当他去查自己银行账户时，发现自己银行卡里的 10 万元钱已经没有了。

七、 购物安全解决方案

网购诈骗案件的出现给经常网购的人们敲响了警钟，网民宜熟知防骗要点减少上当。

(一) 网民防骗须知

1、购物时看网站。

钓鱼网站终归是假网站，可尝试多点击几个页面，以发现网页是否有错误。钓鱼网站的登录框通常无法校验数据真实性，可尝试随意输入字符，如能登录，则可判定为假网站。

2、看信誉等级和相关评价。

若卖家只有 QQ 号、电子邮箱、手机号码，无固定地址，一般不要轻易交易。

3、看价格，忌贪小便宜。

4、不盲目相信未知的电话、短信，去正规网站核实。

5、聊天过程中不轻易打开卖家发来的文件或链接。

6、不轻易泄露自己的个人身份信息。

7、尽可能使用第三方担保支付，如支付宝、财富通。先支付，后收货的交易方式应三思而后行。

8、若发现被盗，应立刻联系网银或支付平台，请求终止交易冻结资金，然后去报警。

(二) 金山毒霸网购保镖

金山毒霸 2012，内置专业的防骗利器：金山网购保镖。

图 16：金山毒霸 2012（猎豹）内含网购保镖功能模块

1. 99 秒鉴定所有未知文件和网址

网购木马快速更新版本，并随意增加垃圾代码来增加文件体积，这使得传统杀毒软件的响应时间过长，往往无法及时拦截骗子发送的网购木马。据淘宝方面提供的数据，和对受骗者的调查，大多数诈骗在 5-20 分钟内完成。

金山毒霸 2012 可实现 99 秒鉴定所有未知文件，从而令网民被网购木马欺骗概率大大下降。

针对网购相关的钓鱼网站肆虐，传统杀毒软件依赖于用户上报，显然，无法做到及时响应。金山毒霸和众多浏览器厂商、腾讯、淘宝等深度合作，在云服务器中自动采集和鉴定钓鱼网址。再通过浏览器、聊天工具、杀毒软件来阻止网民访问钓鱼网址。

2. 金山网购保镖十层立体防护

金山毒霸 2012 内嵌网购保镖功能，采用十层立体防护策略，可防止支付页面被篡改、拦截欺诈购物网址、查杀网购木马以及自动清理网购痕迹，有效保护网购时面临的安全威胁。这十层防御体系如下：

第一层：禁止未知风险进程运行；

第二层：下载和聊天传输云保护；

第三层：快速鉴定未知风险程序；

第四层：实时监控系统进程状态；

第五层：网购木马高启发式鉴定；

第六层：防风险程序注入浏览器；

第七层：防支付页面被篡改功能；

第八层：拦截钓鱼，挂马黑网址；

第九层：防止键盘输入时被记录；

第十层：自动清理网购历史痕迹。