2010年中国网络购物安全报告

2010.12.21

金山网络
www.ijinshan.com

《2010年中国网络购物安全报告》

免责声明：《2010 年中国网络购物安全报告》是由金山网络安全中心、金山网络客户服务中心针对网民在网络购物的过程中，可能遇到的安全威胁进行整理、归纳、研究与分析所得。金山仅保证在其可掌握的数据、技术水平许可范围内出具本报告，如若本报告阐述之状况、数据与其它机构研究结果有差异，请读者自行辨别。

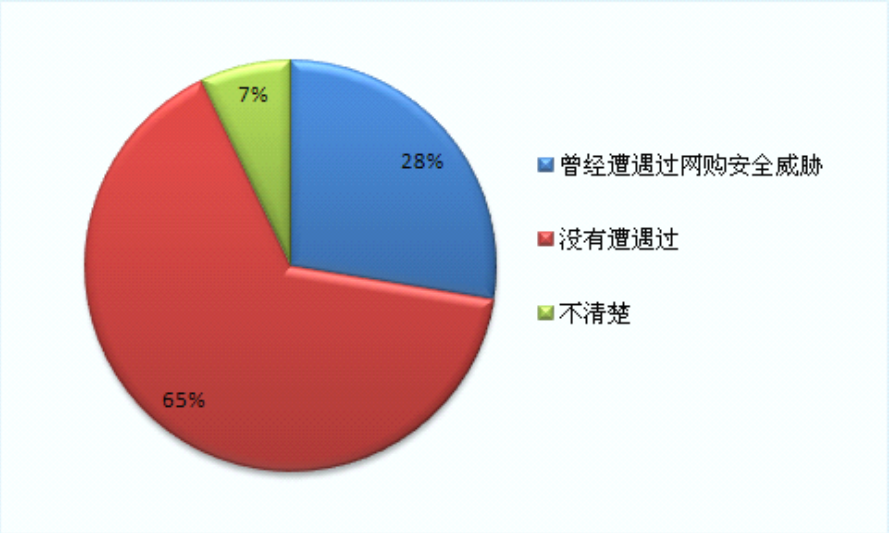
目录：

一、2010年中国网络购物安全状况整体描述

随着互联网的发展，网络购物作为一种消费时尚，逐步成为消费者购物的热门渠道之一。来自中国互联网络信息中心的数据显示：2009年我国网购市场交易规模为2500亿元，较2008年翻一番，而2010年网络购物的市场规模将超过4300亿元；网购人群也大幅度增长，2009年至少在网上买过一次东西的中国网民数历史性地突破了1亿人，达到1.08亿人，增长46%。而在2010年，使用过网络购物的互联网用户更是接近2亿人。网络购物已经成为发展最迅速，与网民利益最相关的网络应用。

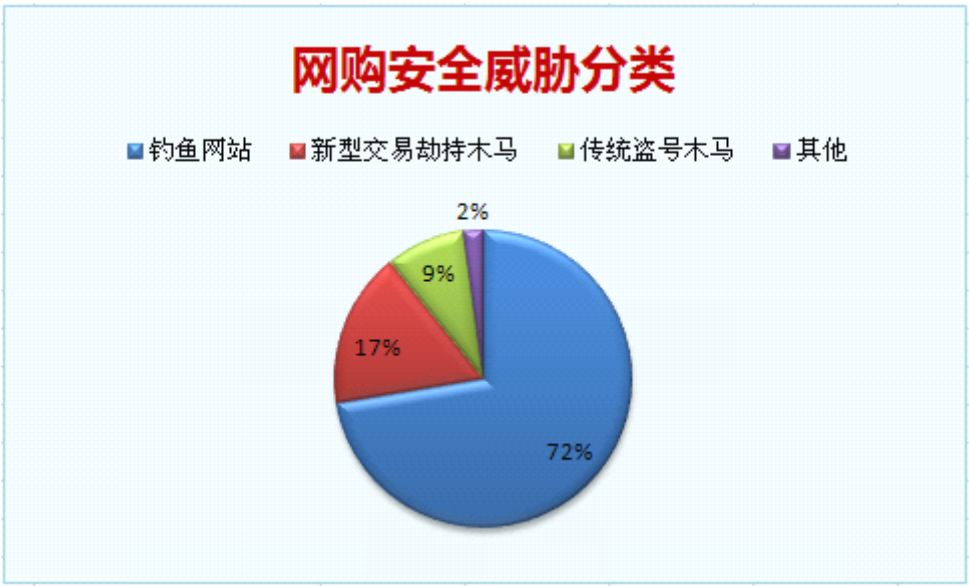
网络购物的火爆也引发了一系列的网络安全问题。相比之前的病毒、木马等通过控制“肉鸡”电脑或者盗取游戏、QQ 账号密码等信息，并通过交易获取经济利益的方式不同，不法分子对网络购物的利用和攻击无疑能够更直接的获取经济利益。

2010年，随着网络购物的发展，针对网络购物的安全威胁已经成为影响互联网安全的重要形式。在2010年，有近28%的互联网用户遭遇过虚假钓鱼网站、诈骗交易、交易劫持、网银被盗等针对网络购物的安全攻击。



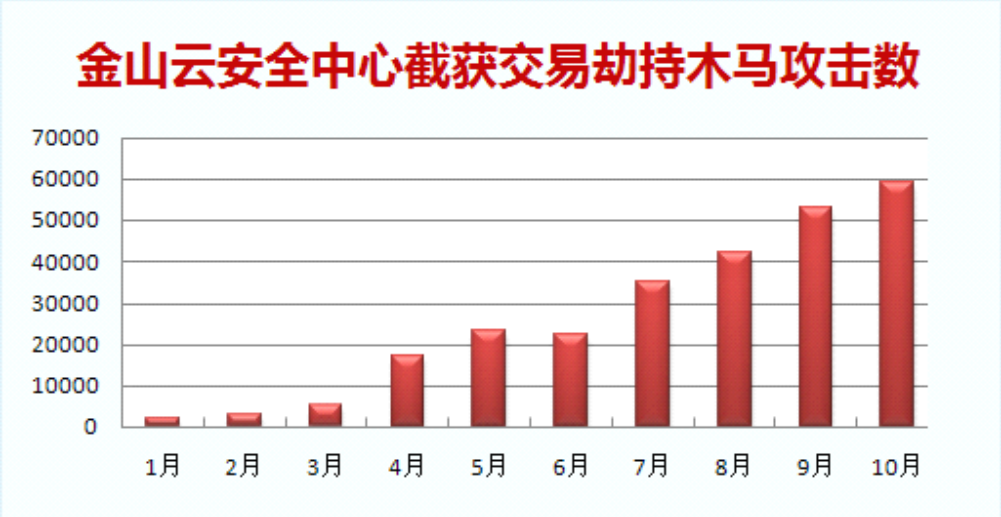
全体互联网用户中遭遇过网络购物安全威胁的比例

据金山网络安全中心最新调查统计数据显示，目前影响我国消费者网络购物的安全威胁主要包括三大类：钓鱼网站、新型交易劫持木马、传统盗号木马。其中，对网络购物用户威胁最严重的还是钓鱼网站，网络购物用户遭遇的所有安全威胁中有72.4%是以钓鱼网站进行的；而占第二位的是新型交易劫持木马，占所有威胁的16.8%，是2010年增长最快的安全威胁，也是让网络购物用户最防不胜防的攻击手段；最后，盗取网络购物账号或者网银账号的木马占威胁总数的8.7%。从整体变化发展趋势来看，钓鱼网站威胁一直处于平稳增长的态势，新型交易劫持木马数量则呈现了快速增长，而传统的盗号木马威胁则在逐步减少。

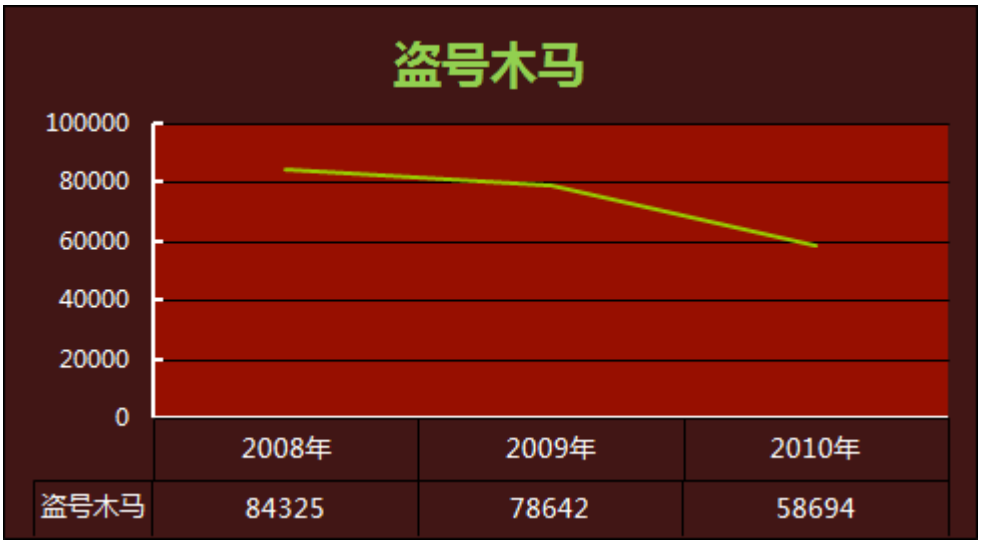


另据金山网络安全中心云网址鉴定系统统计数据显示，2010年1-10月，平均每天新增的与网络购物相关的钓鱼网站约为1500个。其中典型的诈骗方式主要分为三大类：低价诱惑、交谈诈骗、电话诈骗。据统计，低价诱惑类网购钓鱼网站约占40%左右，交谈诈骗类钓鱼网站近年来上升明显，约占32%，而400电话诈骗类钓鱼网站约占18%。

此外，新型交易劫持木马是2010年刚刚兴起的一种网购威胁。通过在正常的网络购物交易过程中给消费者电脑植入木马，将消费者的网上付款流程直接引向假网银网站或者假的第三方支付网站。在消费者以为完成了正常的购物流程后，才发现卖方没有收到货款。这种方式很隐蔽，也让消费者防不胜防。据金山网络安全中心以及客户服务中心最新统计数据显示，2010年交易挟持类木马已经从最初的1个，发展为近千个不同种类的木马，每天金山云查杀系统截获的交易劫持型木马攻击用户电脑在2000例左右。



而传统盗号木马近年来逐步走向“没落”。伴随着反病毒技术手段的不断提升，盗号木马通过盗号进行牟取经济利益的成本越来越高，因此传统盗号木马的数量也在逐步减少。2008年，中国互联网共截获与网购相关的盗号木马84325个，2009年为78642个，而进入2010年，前10个月，这个数字已经下降为58694个。



网购安全威胁与日俱增与网购经济的繁荣存在紧密的联系。数据显示，截止到2010年6月底，中国电子商务市场交易额达到2.25万亿元。而黑客已经就网购安全威胁形成了一条完整的产业链条。依据金山网络安全中心的安全威胁监测和统计，在2010年有超过1亿用户曾遭遇过至少一种针对网络购物的安全威胁，带来直接经济损失将突破150亿元， 网购用户的人均经济损失也由2009年的80元上升至150元左右。

总结：纵观2010年中国网络购物的安全威胁主要表现为三大特征：1、以窃取用户直接经济利益（如现金、网银的真实财产）为目的的安全威胁逐渐成为主流，随着网络购物规模的迅速扩大而普遍化；2、以钓鱼网站为主要形式的网络欺骗仍然是网购安全威胁的主要形式；3、新技术的应用使得用户在网络购物安全问题方面防不胜防。

二、2010年影响网民网络购物安全的三大威胁

网购三大安全威胁之钓鱼网站

1、什么是钓鱼网站？

钓鱼网站是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的网址以及页面内容，或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的网页代码，以此来骗取用户银行或信用卡账号、密码等私人资料。

钓鱼网站制作和发布流程：制作一个钓鱼网站成本只有几十元

钓鱼网站的源码只需几十元即可买到，近年，在网络上也出现了批量生成钓鱼网站的工具。而钓鱼网站使用的域名（网站地址），也大多可以免费申请。钓鱼网站的生存周期一般只有几天，当钓鱼网站被安全公司拦截或被停止域名解析后，“钓鱼者”可以很快将网页内容切换到另一个域名，继续实施诈骗。

2、2010 年钓鱼网站三大特点

（1）高伪装性

网页伪装是钓鱼网站制作者最早采用的手段。近年来，伴随着网民网络安全意识的提升，传统的域名伪装法被网民所熟知。2010 年，钓鱼网站的伪装性不断加强，伪装的办法也不断翻新，一些钓鱼网站使用了多次跳转，这种网页成功欺骗了若干聊天工具内置的安全识别系统，令广大网民防不胜防。

（2）病毒式推广

钓鱼网站制作成本很低，但推广钓鱼网站有一定难度和门槛。钓鱼网站制作者和病毒、木马以及流氓软件的传播者相互勾结，通过病毒、木马、流氓软件来弹出钓鱼网站的广告，为钓鱼网站带来“人气”，令大量用户进入陷阱。针对特定目标的钓鱼网站会通过一些聊天工具、贴吧、论坛或网络游戏内置的聊天频道来推广。

（3）技术含量提升

之前的钓鱼网站几乎没有什么技术含量可言，钓鱼者为了增加网络钓鱼的成功率，2010 年开始尝试将一些病毒木马技术引入到钓鱼的过程中，如交易劫持木马利用正常软件的安全漏洞来实现自动加载，在网购用户最后的支付环节，直接将木马创建的交易单贴在正常交易单的前面。

3、钓鱼网站的黑色产业链分析

伴随着互联网应用的日益广泛，互联网上的“钱”越来越多。而钓鱼欺诈的方式与传统的病毒产业链相比，整个钓鱼欺诈过程，一个人即可完成，钓鱼者可以更直接、更快速的获取经济利益。

钓鱼欺诈流程：钓鱼网站代码贩子（木马作者）——钓鱼网站经营者——通过流氓软件产业链为钓鱼网站带流量（或通过游戏内置的聊天频道、虚拟物品交易平台推广）——诈骗受害者钱财或个人信息——收集出售个人信息——获取利益

4、三类典型的网购钓鱼网站欺诈形式：低价诱惑、交谈诈骗、电话钓鱼

2010年1-10月，平均每天新增的与网络购物相关的钓鱼网站约为1500个。其中典型的诈骗方式主要分为三大类：低价诱惑、交谈诈骗、电话诈骗。据统计，低价诱惑类网购钓鱼网站约占40%左右，交谈诈骗类钓鱼网站近年来上升明显，约占32%，而400电话诈骗约占18%。

（1）低价诱惑——1980 元的 iPhone4 陷阱

1980 元的 iPhone4 是不是有点不敢相信？没错，这就是网络钓鱼者的新伎俩。低价是网络钓鱼者屡试不爽的杀手锏。最常见的是低价商品诱惑，骗子往往通过超低价诱饵吸引购买者登录假冒的商品销售网站，进而引导用户输入网银账户密码，实施诈骗。

案例：

小黄看网上 iphone 手机越来越火，很想买一款。一天，小黄无意中在某个讨论 iphone 4 的论坛上看到 iphone4 秒杀的广告，点击后发现这里卖的 iphone4 只有市价的一半。仔细端详之后，决定汇款购买，他按网页上提示的流程下单后迟迟收不到货，电话和邮件投诉均没有回音，和朋友交流后才知已经上当。

（2）交谈诈骗——　一毛钱的陷阱

交谈诈骗又称聊天过程中钓鱼，最常见诈骗方法是买家与卖家在沟通的过程中，通过聊天工具发送假冒的钓鱼网页，引导用户在假冒的网页上进行支付。2010 年，又出现了一种隐蔽性更强的钓鱼陷阱。即卖家要求买家先汇款一毛钱或一块钱下定单。不少买家很可能因为定单价值只有一毛钱或一块钱而放松警惕，点击骗子提供的链接后，会打开与下图类似的支付窗口，这个窗口和正常在线支付窗口完全一致，请特别注意一下支付金额为 0.1 元。很多人并不在意的一毛钱汇款，实际是个大陷阱。买家无意中将自己的信用卡号、支付密码和信用卡背面的三位数字直接提交给钓鱼网站，骗子就可以用这些信息盗取用户的银行卡，可以轻易实现银行卡的离线交易。

案例：一毛钱莫名变 1 万元

小涛想在网上购买一张价值 100 元的手机充值卡，拍下之后付款到卖家的支付宝，卖家叫小涛登录某网站，用网银汇款 0.1 元到他的账户里，说是用来提取单号，通过单号来提取充值卡卡密。小涛心想：既然都付了 100 元钱到支付宝上了，也不在乎那 0.1 元了。于是按提示支付，可多次出现超时问题，当初以为是电脑浏览器问题，于是和那位卖充值卡的卖家说，让他的“技术人员”加小涛 QQ，加了后，一番交谈，小涛进入了“技术人员”所提供的支付网站，登录网站后，在付款的前一刻，支付金额清清楚楚写着“0.1 元”，按了付款后，一分钟内，手机收到银行的短信，内容说“银行支出 10000 元”！

视频：一毛钱钓走三万五
http://video.sina.com.cn/v/b/19372661-1512571704.html

（3）电话诈骗——400 电话也有假

将网络诈骗和电话诈骗结合的典型例子是机票预订，不少人喜欢通过航空公司的在线机票代理预订机票。当网民点击一个看起来很正常的机票预订网站，在这些网站提交订票信息时，往往会弹出服务器忙之类的出错信息，这是骗子在诱使你电话联系客服，一番电话之后，就会有人将票款转到骗子帐户。受骗者永远无法收到机票，在新浪微博和腾讯微博每天都能发现有人因为这个原因遭受损失。

案例：400 电话被“易容” 成骗子挡箭牌

网友小常在网购机票时不慎被骗千元。小常是网上搜到的这家特价机票网站，打开页面是400 的订购热线，自己一直认为 400 开头的电话应都是可信、安全的。而 5 折深圳飞北京的机票在国庆长假高峰很难订到，这家网站承诺网银汇款就可立马出票。而网银汇款后就再也打不通网站显示的 4006 定购热线。

视频：400 号码助钓鱼网站骗取信任
http://www.letv.com/ptv/vplay/607602.html

金山网络安全专家防范建议：
1、对超低价、超低折扣、中奖等诱惑要提高警惕，避免贪图便宜而落入圈套；
2、收藏经常访问的在线购物网站，在网站提交含有个人信息的内容时，检查一下浏览器地址栏，看看是不是自己所熟悉的地址；
3、启用专业安全软件，如永久免费的金山毒霸，及时更新，防止点击钓鱼网站链接；
4. 如果安全软件对正在访问的页面弹出警告，应立即中断交易；
5、网购确定付款时，检查收款方帐户信息是否正确。不要轻易按对方电话的安排，使用 ATM 或网银转帐功能付款。

三大网购威胁之新型交易劫持木马

交易劫持是2010年新兴的一种网购威胁。据金山网络安全中心以及客户服务中心最新统计数据显示，2010年交易劫持类木马发展迅速，木马变种近千个，而此种网购威胁所影响到的网购者也与日俱增。

1、新型交易劫持木马特点

（1）技术含量高

交易劫持木马的一个重要特点是利用正常软件的安全漏洞来实现自动加载。2010 年，dll 劫持漏洞被发现，逐渐发现相当多的互联网软件存在这种安全漏洞，而消除这些漏洞有相当

大的难度，数字大盗病毒正是利用 dll 劫持漏洞的典型代表。病毒会利用一些正常软件来实现自动运行，这种启动方式可有效逃避某些安全软件的行为拦截功能。

（2）点对点传播

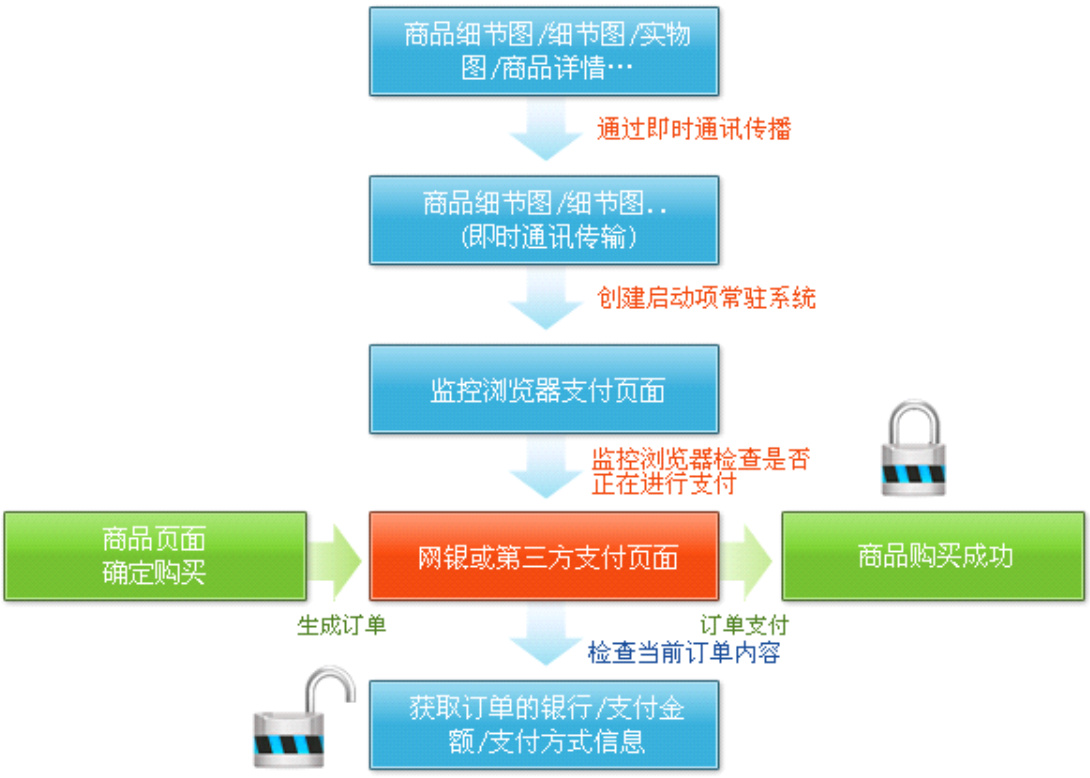
交易劫持木马一般采用一对一传播的方式，如买家与卖家在进行沟通的过程中，通过聊天工具等将伪装成细节图、价目表的木马发送给对方。因此，交易劫持木马并没有出现大规模爆发的态势，这也让木马作者更难被捉拿归案。

（3）成功率高

有了前期买家跟卖家的良好沟通，买家的警惕性会下降，而一旦接收并打开了卖家传递过来的木马，中招的几率非常大，因为劫持创建新的交易单时和正常的交易过程几乎没有区别。如果买家电脑上安装的杀毒软件没能阻止数字大盗病毒的运行，被骗取钱财的可能性接近 100%。

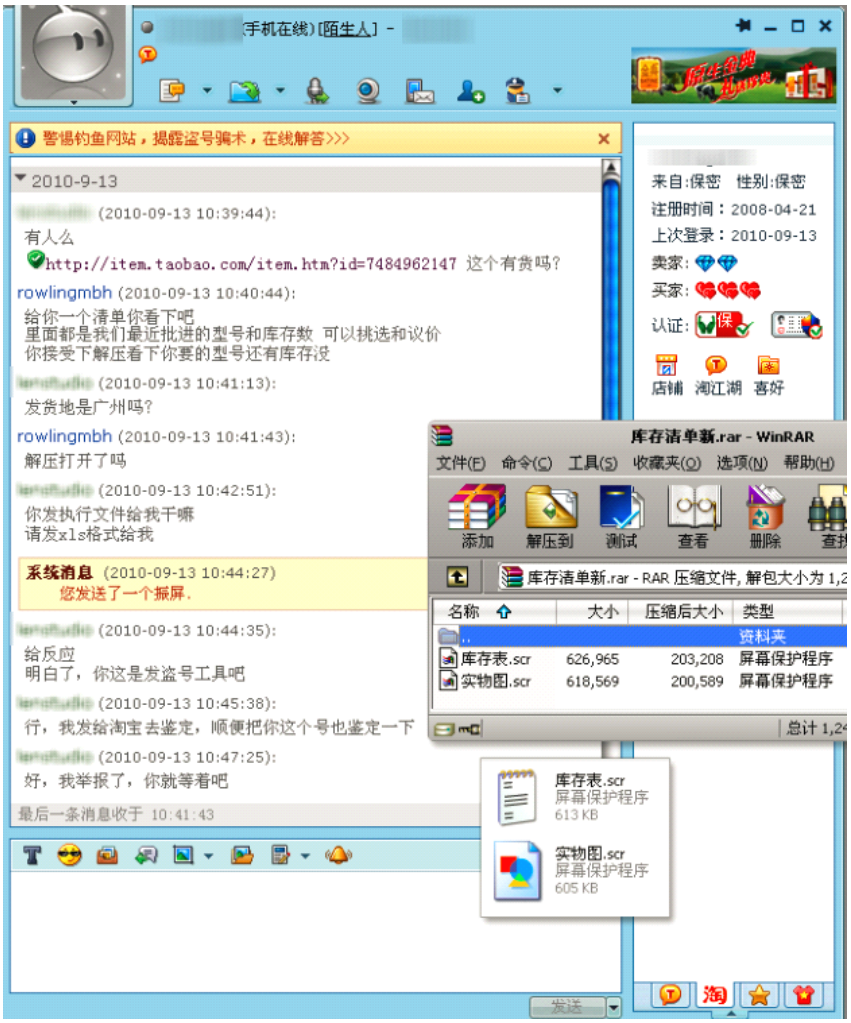
2、新型交易劫持木马的欺诈流程

新型交易劫持木马的作案流程基本一致：在交易过程中，买家执行了对方发过来的文件（木马），在继续交易时，木马会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。



3、典型新型交易劫持木马——数字大盗

特征描述：最早的数字大盗被截获的时间是 2010 年 6 月，受害者还不算多。该木马目前看仍然没有大面积扩散，点对点的传播控制了木马传播的广度，使木马作者也隐藏的更深。金山网络安全中心担心该木马的攻击方式如果公开，将会对在线购物安全构成严重威胁。



传播：最早的数字大盗木马是利用了某安全软件网络查看器的设计缺陷，通过某安全软件的网络连接查看器(带数字签名)来启动自身，可以绕过绝大多数安全软件的拦截。此后发现，更多存在漏洞的互联网软件被数字大盗作者利用，数字大盗木马的危害将长期存在，因为相关软件即使升级也无法阻止病毒作者继续利用这些业已存在漏洞的软件。

金山网络安全专家防范建议：

1. 交易时，如果对方要发文件给你，千万要小心。若发送的文件是 exe、pif、scr 等可执行程序的扩展名，应立即将对方拉黑。发送可执行文件的，基本可以断定为骗子；

2. 点击确认支付按钮时，一定要检查收款方信息，如果不是你购物时熟悉的收款方，应立即取消交易；

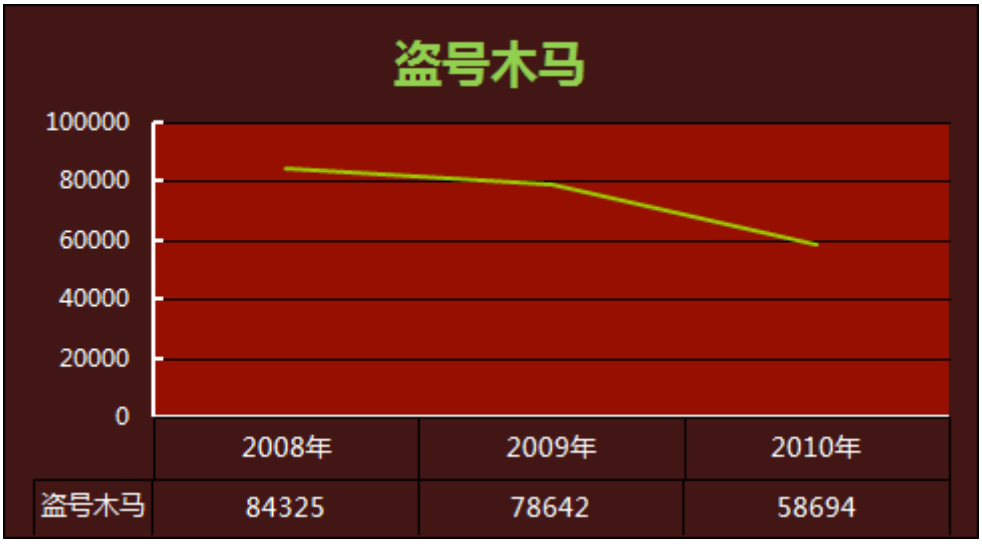
3. 交易过程中，若本机安装的杀毒软件有弹出报警消息，应立即中止交易。

三大网购威胁之传统盗号木马

盗号木马对于网络购物来讲是比较传统的威胁，当网购用户感染病毒后，病毒木马会窃取网

民的淘宝 ID、支付宝 ID、QQ 号、银行卡信用卡信息，再伺机窃取用户资产。

传统盗号木马近年来逐步走向“没落”。伴随着反病毒技术手段的不断提升，盗号木马通过盗号进行牟取经济利益的成本越来越高，因此传统盗号木马的数量也在逐步减少。2008年，中国互联网共截获与网购相关的盗号木马84325个，2009年为78642个，而进入2010年，前10个月，这个数字已经下降为58694个。



金山网络安全专家防范盗号木马：

1. 最好收藏常去的银行网站、在线购物网站。最好不从陌生的邮件或聊天工具收到的网站链接点击进去；

2. 保护电脑安全：安装专业杀毒软件，如永久免费的金山毒霸等，并及时更新病毒库。在许多银行的网站上都免费为用户提供“网银病毒专杀工具”，专门针对盗取网银信息的木马病毒；

3. 保护密码：正确使用数字证书，证书可以存放在电脑里，也可以存放在硬件介质 USBkey 里。如果存放在电脑里，就要保护电脑安全。如果存放在 USBkey 里，注意使用后要及时拔出。

三、有关网络购物安全问题的解决办法

安全问题已经成为影响网购消费的一个重要话题。登录各大购物网站的论坛，网购被骗的案例比比皆是，欺骗的方式也五花八门。一个用户从登录购物网站到选择商品，再到与卖家沟通、付款，每个环节都有可能潜伏着安全风险。这也给网购安全问题的解决提出了很多挑战。

金山网络作为较早关注网购安全的专业安全厂商，针对网民在网络购物的过程中，可能遇到的安全威胁进行深入研究与分析，目前已经针对网购过程中的安全风险提出了多重解决方案。

（一）技术层面解决方案

1、网址云安全智能反钓鱼

对于网络钓鱼欺诈的技术查杀，金山网络安全实验室经过长期研究，分析了网络钓鱼目前最常用手段，找到了对付网络钓鱼欺诈的最佳解决方案（如图所示）：

这个方案的核心技术在于可以通过服务端的自动收集和自动识别，来有效拦截有可能被网民访问到的网络钓鱼网站。目前每天阻止网民访问钓鱼网站的次数已超过40万次。同时有效修复因不慎访问钓鱼网站导致的安全问题，通过金山毒霸2011组合防御可有效拦截各类"钓鱼"欺诈网址！

2、网购木马专杀——针对性拦截更有效

金山全系列安全产品均集成了下载保护功能，当用户通过 IM 工具、下载工具传播程序时，会自动对要传播的文件进行安全检查，及时收集和识别其中的病毒木马，当一个网址或文件被判定为恶意欺骗下载链接或病毒文件时，该恶意网址和文件的传播会立即被千万级的用户网络所阻止。

针对数字大盗这样典型的交易劫持木马，金山毒霸还提供了特别的解决方案——当检测到交易页面被跳转、通过淘宝旺旺或 QQ 传输了一个敏感的程序文件、网购用户在打开某个程序文件后有特别的程序释放等等，这些关键环节，金山毒霸会及时报警，最大限度避免网民受数字大盗这种木马加钓鱼网址的双重攻击而遭受损失。此项功能将在即将发布的金山毒霸SP5最新版中全面集成。

（二）行业层面——互联网厂商联合对抗网络欺诈

1、安全厂商与网购厂商、浏览器厂商的大力合作

一直以来，金山与电子商务厂商、浏览器厂商保持着良好的合作。2009年12月9日，金山联手傲游浏览器以及电子商务平台淘宝网、支付宝，共同推出国内首个网购安全平台。通过凝聚四方多项安全技术，充分满足多层次用户的需求。

2、金山卫士开源计划——拦截钓鱼欺诈无处不在

为了让更多的互联网应用可以吸取金山网址云安全系统的成功经验，金山决定向全社会开放金山云安全客户端应用框架以及服务端应用接口，任何互联网软件只要申请成为金山开源计划成员，就可以无偿使用。

在不久的将来，我们将看到：能拦截钓鱼网址的聊天工具、邮件客户端、搜索引擎、浏览器和下载工具。金山开源计划可以让互联网变得更安全，钓鱼网站的危害将被有效遏制。