2012 年浏览器安全及发展形势报告

360 安全中心

360 安全浏览器

2013 年 3 月 26 日

摘　　要

2012 年，360 安全中心拦截钓鱼网站访问 81 亿次。其中，360 浏览器共拦截钓鱼网站攻击 39 亿次，比 2011 年的 23 亿次增长了 69.6%；共拦截挂马网页访问 4237 万次，较 2011 年下降了 86%。数据显示，网页挂马数量持续萎缩，而钓鱼网站数量则大幅增长。钓鱼欺诈已经超过网页挂马，成为用户上网浏览安全的首要威胁。

搜索引擎仍然是钓鱼网站传播的主要途径，比例高达 43.2%。竞价排名是使钓鱼网站登上搜索结果前面几条的主要方式。

钓鱼网站的生存周期大幅缩短，已经从 2011 年的平均 50 小时左右，下降到 2012 年的平均不到 12 小时。2012 年下半年，开始出现一大批“闪骗”型钓鱼网站，其生存周期甚至缩短至 6 小时以下。这种“闪骗”型钓鱼网站呈现“精准定位”、“迅速出击”、“骗完就闪”的三大特点，针对性极强，一旦诈骗成功或被安全软件拦截，就会快速消失，用户极易上当受骗，且不易防范。

“在线风险分析”是防范“闪骗”型钓鱼网站的一种有效方法，360 安全浏览器在这方面已经率先推出了网站身份认证和“照妖镜”等功能。

Cookie 能方便用户上网，是互联网服务发展的重要基础，但一些网站联盟通过在数十万家网站部署跟踪代码，将用户上网行为记录在 Cookie 中，跨站跟踪用户上网行为，在对“跨域 Cookie”数据分析后，进而推送“精准”广告。由此引起了公众对于滥用网络跟踪技术的强烈担忧。相应的，反跟踪技术的研发和应用也成为浏览器安全性能的最新发展方向。

数据劫持是 2012 年集中爆发的另外一类安全问题，主要包括网页缓存劫持、运营商广告劫持、网页内容劫持、DNS 解析劫持和广告佣金劫持。数据劫持，不仅干扰用户的正常上网，而且存在诸多安全隐患。解决数据劫持问题，需要网站、运营商与浏览器厂商的共同协作。

帐号保护存在安全隐患已经成为多数浏览器的薄弱环节。网络帐号是每个用户在互联网上的身份标签，同时也是绝大多数黑客攻击和窃取的主要目标。目前网民常用的浏览器中，有相当一部分存在严重的帐号安全隐患。提高浏览器的帐号保护能力迫在眉睫。

免责声明

本报告为 360 安全中心发布的研究数据和分析资料。主要数据来源于 360 安全中心系统、360 浏览器监测系统，360 客服中心，以及网络公开资料。报告针对 2012 年中国浏览器安全状况进行统计总结，并发布安全趋势研究结论。

本报告可供任何个人、政府相关部门及行业机构、企事业单位参考，但对于本报告所阐述之内容、数据及分析结果，360 安全中心不承担与此相关的一切法律责任。

目　　录

第一章　浏览器安全形势整体分析

根据艾瑞统计，超过 98%的互联网用户使用浏览器上网。浏览器是中国网民上网的主要工具。随着安全软件的高度普及与安全浏览器的广泛应用，网页挂马等传统安全威胁日渐减少，而以钓鱼欺诈、网络跟踪、数据劫持等为代表的新型安全威胁日渐突显。此外，帐号保护已经成为多数浏览器安全的薄弱环节。

1.　钓鱼欺诈成为浏览安全的首要威胁

2012 年挂马网页的攻击形式已经大为缩减，根据 360 安全中心的统计，钓鱼网站的数量还在大幅增加，2012 年 360 安全中心共拦截钓鱼网站攻击 81 亿次，比 2011 年增长了 273%。与此同时，全年共拦截挂马网站访问 4237 万次，比 2011 年的 3 亿次下降了 86%，挂马网页拦截量仅为钓鱼网站拦截量的 5‰，而且挂马网页比钓鱼网站更容易被安全软件和安全浏览器所拦截，从实际危害来看，钓鱼欺诈已经超过网页挂马，成为用户上网浏览安全的首要威胁。

钓鱼网站的生存周期呈逐年下降趋势，从 2011 年的 50 小时左右，下降到 2012 年的平均不足 12 小时。2012 年下半年，出现大量“闪骗”型钓鱼网站，这类钓鱼网站的生存周期甚至不足 6 个小时。

网址云安全目前仍然是防范钓鱼网站和挂马网页最有效的手段；网站身份认证和在线风险分析等新型网站安全鉴定技术在浏览器中的应用，还为网民查看网站身份、识别新生的钓鱼网站提供了便捷有效的参考依据，比如，360 安全浏览器的“照妖镜”功能，可以在用户手动提交的情况下，实时检测并反馈当前网站安全性。这种功能对“闪骗”型网站起到了很好的抑制作用，能够更有效地降低钓鱼网站的存活时间。

2.　网络跟踪涉嫌窃取用户隐私

2013 年，3·15 晚会播出了一些公司通过跟踪 Cookie/Flash Cookie 等方式定位目标用户、精准推送广告的行为。尽管社会各界对 Cookie 隐私问题存在争议，但一些网站联盟跨站跟踪 Cookie，对用户造成一定的隐私泄露风险。比如在某搜索引擎搜索“糖尿病”，再访问其联盟网站时，随时可能出现“糖尿病”医疗广告，无疑会对用户造成个人隐私泄露的困扰。

目前，包括 360 安全浏览器在内的国内外多款浏览器已经发布了反跟踪功能，保护用户隐私。

3.　数据劫持造成安全隐患

用户上网遭遇数据劫持的现象越来越普遍，其中网页缓存劫持、运营商广告劫持、网页内容劫持、广告佣金劫持和 DNS 解析劫持是 2012 年出现最多的劫持现象。数据劫持不仅干扰用户的正常上网，甚至导致登录串号，主页被篡改，广告联盟佣金被窃取等安全隐患。此

外，数据劫持现象也对网站和浏览器的信誉造成了一定程度的损害。要解决数据劫持问题，需要网站、运营商和浏览器的共同努力。

4. 帐号保护成部分浏览器安全薄弱环节

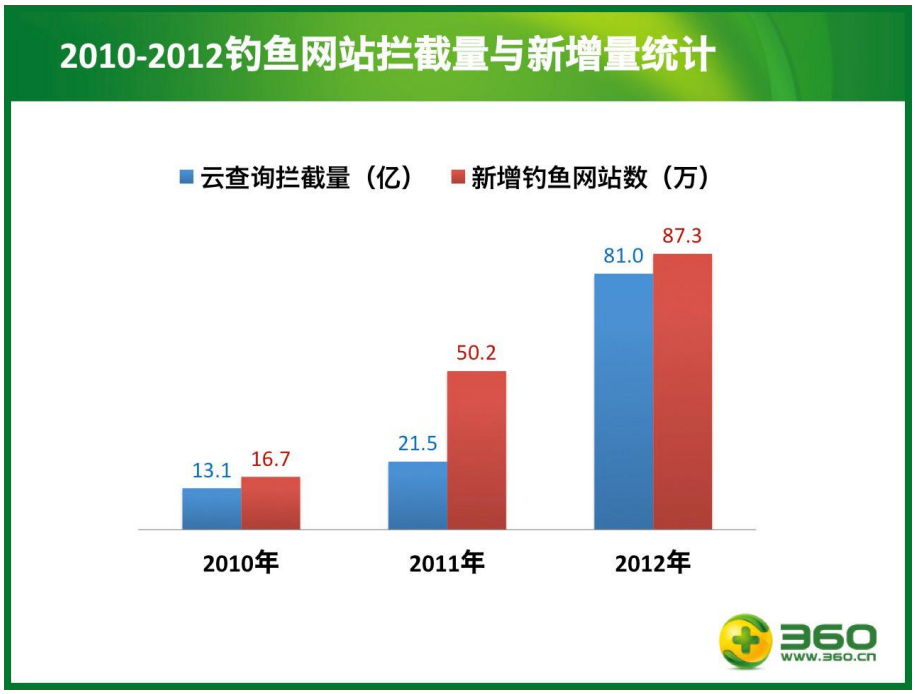
仿冒官网、盗号木马、Cookie 窃取和网站拖库等多种因素严重威胁用户的上网帐号安全。但很多常见的浏览器并没有对用户的上网帐号进行有效的安全保护，甚至部分知名浏览器还对用户帐号进行明文保存，极易被黑客入侵和窃取。浏览器的帐号安全保护功能急需加强。

在接下来的各章中，将分别对钓鱼网站、网络跟踪、数据劫持和帐号保护等几个方面的问题及相应的浏览器安全技术的发展进行详细的介绍和讨论。

第二章　钓鱼网站成为浏览安全首要威胁

（一）　钓鱼网站增长近 3 倍

网页挂马和钓鱼欺诈是威胁用户上网安全的两大主要形式。2012 年，钓鱼网站拦截大幅增加， 360 安全中心共拦截钓鱼网站攻击 81 亿次。其中，360 浏览器共拦截掉钓鱼网站攻击 39 亿次，比 2011 年的 23 亿次增长了 69.6%。



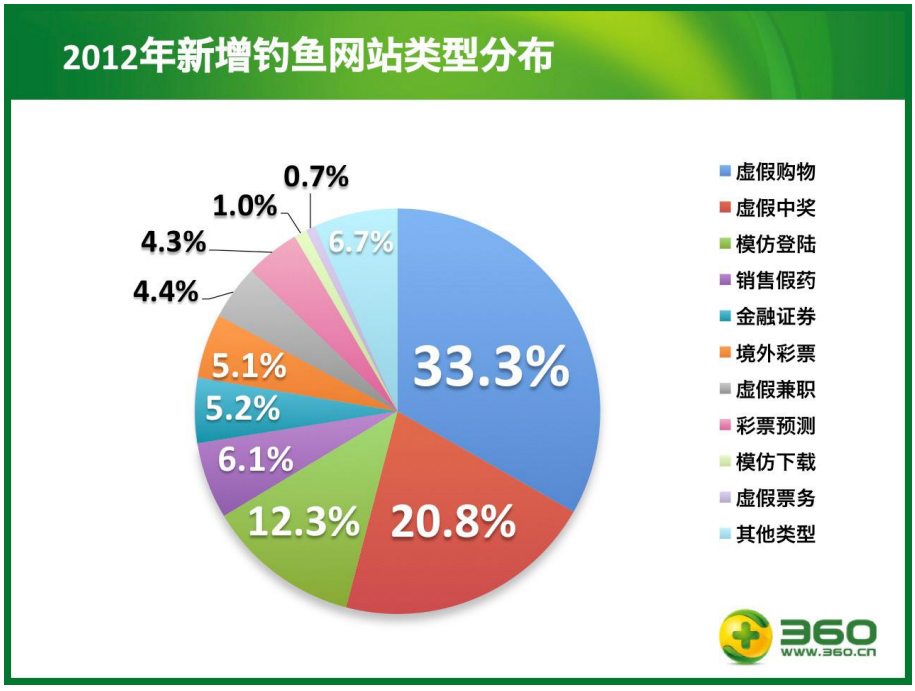
与之相比，2012 年，360 安全中心共拦截挂马网页访问 4237 万次，相比 2011 年的 3 亿次下降了 86%。其中，360 安全浏览器拦截挂马网页 2100 万次，相比 2011 年的 2 亿次下降了 89.5%。挂马网页拦截量仅为钓鱼网站拦截量的 5‰。

从全年统计来看，2012 年新增钓鱼网站数量比 2011 年增加了 74%。从实际危害来看，钓鱼网站已经超过网页挂马，成为用户上网浏览安全的首要危害。

自 2010 年以后，随着安全浏览器的普及程度大幅提高，配合安全软件的共同使用，挂马网页的攻击成功率急剧下降。2011 年，360 安全中心对挂马网页的拦截量为 2010 年的 12.9%，而 2012 年拦截量再次下降，仅为 2011 年的 14.0%。

（二） 钓鱼欺诈已成为电子商务最大毒瘤

从钓鱼网站的类型分布上来看，虚假购物仍然以 33.3%的比例居钓鱼网站排名的榜首，紧随其后的是虚假中奖和模仿登录类钓鱼网站。排名前三的钓鱼网站占到钓鱼网站总量的 66.4%。值得一提的是，2011 年排名靠前的各种博彩类钓鱼网站的排名明显下降，而模仿登录类钓鱼网站比例却大幅上升，占 12.3%。



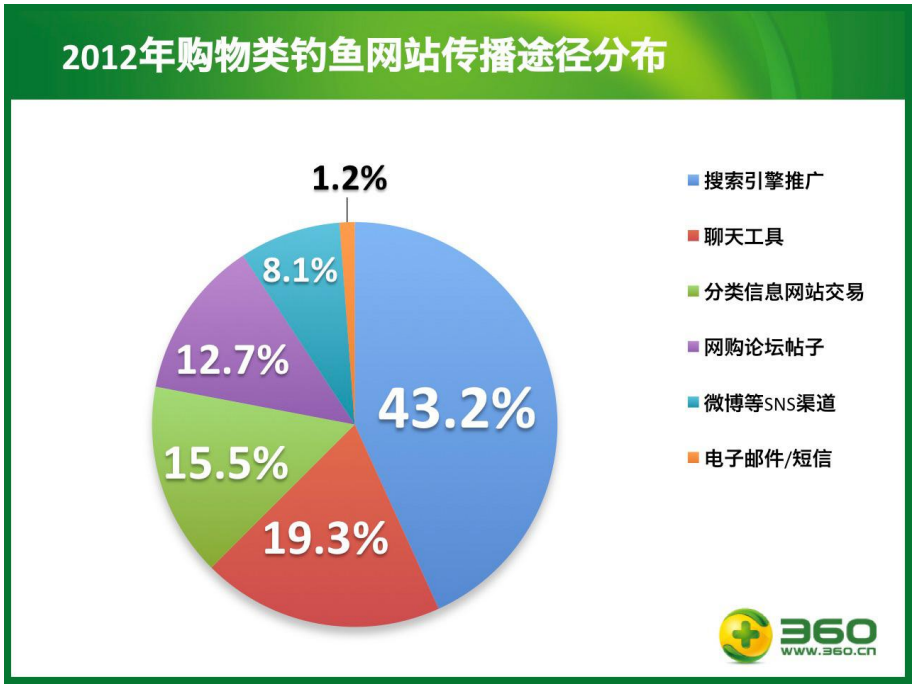
2012 年，网购相关产业蓬勃发展，网购呈现出迅猛增长势头。据 CNNIC（中国互联网络信息中心）发布的第 31 次《中国互联网络发展状况统计报告》数据显示，目前全国 5.64 亿网民中，网购用户规模达到 2.42 亿，比例高达 42.9%。网购用户的大幅增长，也吸引了钓鱼网站的关注。

钓鱼网站通过制作仿冒网站，盗取网民真实资产、虚拟资产，滥用网络资源，给网民造成了巨大的损失。据清华大学网络与信息安全实验室的分析，仅 2011 年就有 1.07 亿网民受到钓鱼欺诈网站影响。2012 年，据 360“网购先赔”服务数据统计，钓鱼欺诈网站对每位受

害者造成的平均经济损失高达 658 元。据此推算，2.42 亿网民中即使仅有百分之一的受害用户，那就将造成每年近 16 亿元的直接财产损失！

（三） 搜索引擎成钓鱼网站传播主要途径

360 安全中心综合用户举报与“网购先赔”案例发现，钓鱼网站通过搜索引擎传播的比例达到 43.2%；此外，不法分子通过聊天工具一对一或聊天群发送钓鱼网址，通过分类信息网站、论坛、微博发布低价商品信息，诱骗用户访问钓鱼网站，也是其重要传播渠道。



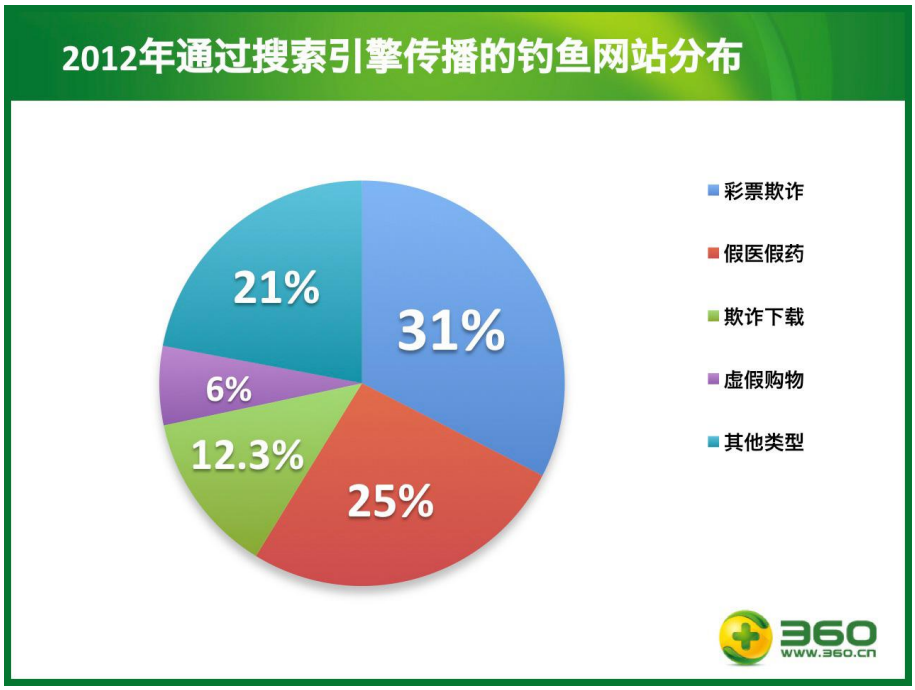
钓鱼网站通过搜索引擎进行传播的方式主要有两种，一种是黑链植入 SEO（搜索引擎优化），一种是直接利用竞价排名系统。

1. 黑链植入 SEO。简单的说就是黑客首先入侵政府、高校等在搜索引擎中权重较高、但自身安全性较差的网站，在网站页面植入自己的网站链接和关键词，并且巧妙隐藏使人不易发现。但搜索引擎在抓取页面信息时，却会抓取到这些隐蔽的链接，从而使钓鱼网站权重提高，在搜索结果中排名靠前。

2. 利用竞价排名系统进行推广。由于某些搜索引擎审查不严，使得钓鱼网站的制作者可以直接在竞价排名系统中购买关键词，让自己的网站排在搜索结果的顶端，从而让网民误入钓鱼网站。

黑链植入 SEO 需要一定的技术水平，而且成本较高，见效较慢，一旦被网址云安全系统拦截，很多先前的工作也就白做了。而通过竞价排名系统购买关键词，则更容易在一定时间内进入搜索结果的首页甚至首条，技术门槛相对较低，而且灵活多变。因此，绝大多数钓鱼网站作者都是首选通过竞价排名系统在搜索引擎上传播。

下图给出了通过搜索引擎传播的钓鱼网站类型分布。



对于不熟悉互联网的电脑用户来说，鉴别钓鱼网站应首先确定网址来源是否可信。如果是通过搜索引擎或陌生人发布的信息打开的网址，而且其中带有中奖、低价打折商品等诱惑信息时，应向他人求助核实。

（四） 钓鱼网站生存周期再次下降

360 安全中心的统计显示：钓鱼网站的平均生命周期在 2011 年约为 50 小时，而 2012 年则大幅下降至平均不足 12 小时，到 2012 年下半年，开始出现一大批“闪骗”型钓鱼网站，这类网站的生存周期极短，甚至不足 6 个小时。

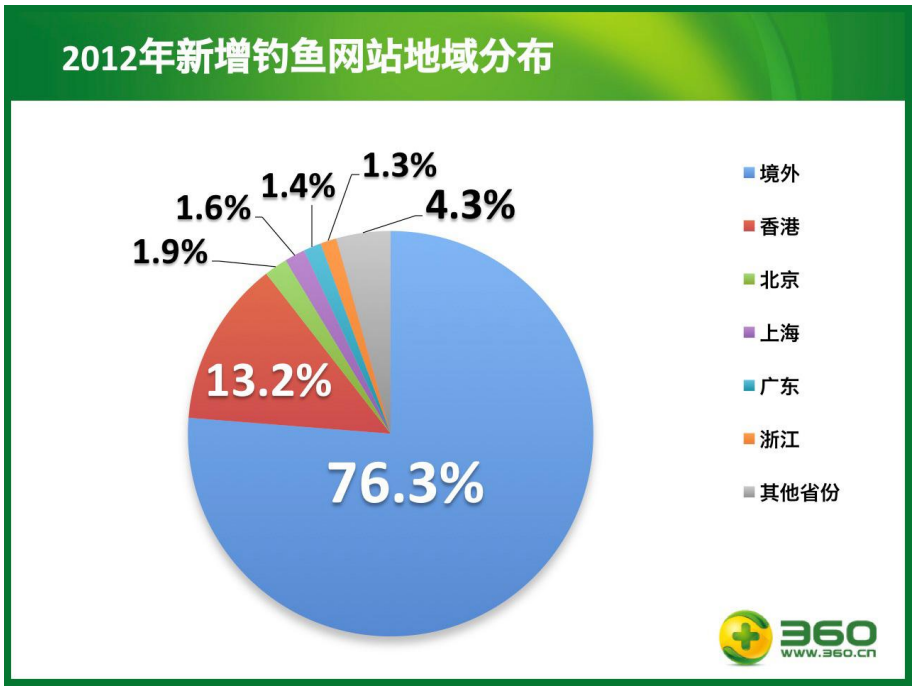
“闪骗”型钓鱼网站一般呈现三个主要“精准定位”、“迅速出击”、“骗完就闪”特点，即精准定位攻击人群，把握机会迅速引诱用户上当，成功诈骗后网站迅速下线。

（五） 钓鱼攻击时间、地域分布特征

1．钓鱼网站多数来自境外

据 360 安全中心统计，在新增钓鱼网站中，境外网站占 76.3%，香港网站占 13.2%，二者之和接近 90%。这些地区的域名、服务器等网站基础设施管理相对宽松，使得钓鱼网站建设门槛较低、监管难度较大。

就国内而言，相对科技技术比较发达的北京、上海、广东、浙江等地，新增钓鱼网站占比也较高。



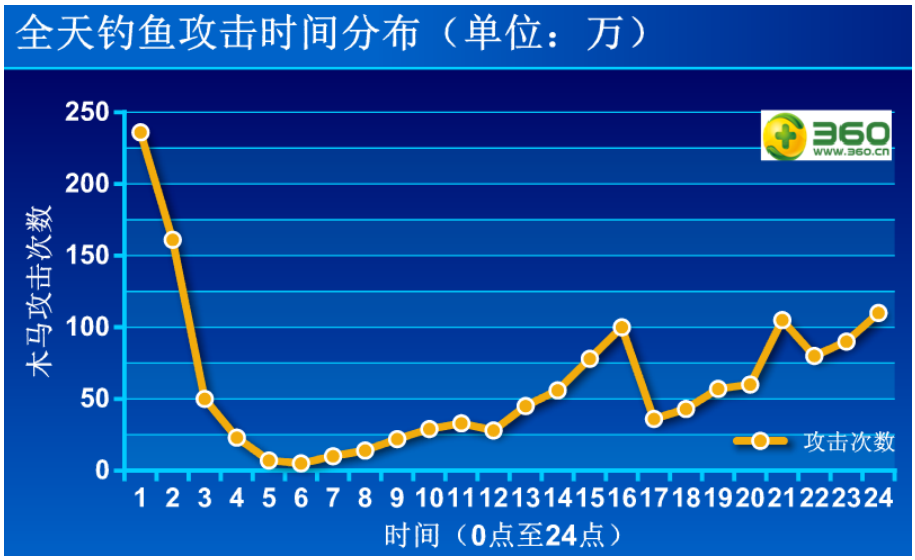
2. 网购有高峰 星期四是“最危险的一天”

（1）星期四是网购钓鱼拦截最高的一天

据 360 安全中心统计，在每周七天时间中，网购钓鱼拦截量最高的一天并不在周末，而是星期四。据分析，这可能是因为在这一天用户网购热情最为高涨，所以遭遇钓鱼攻击数量也最多。

（2）一天中三个购物危险时间段

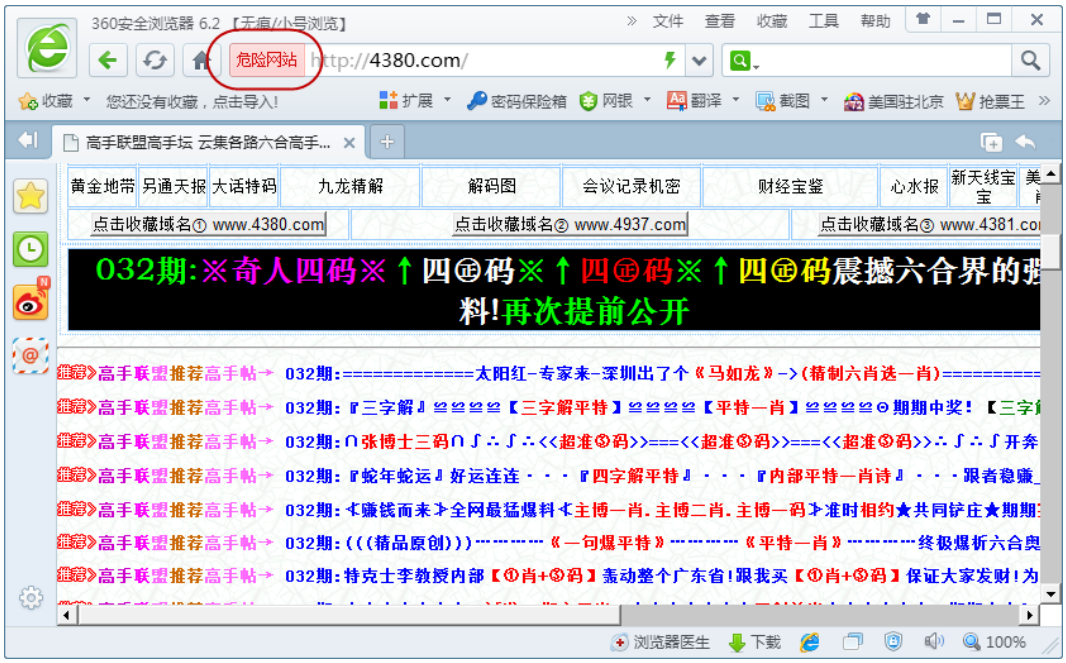
在一天当中，网购拦截的高峰时段是下午 16 点，晚上 21 点，凌晨 1 点，工作日为主。同样道理，这也和用户网购习惯密切相关。用户调查显示，这三个时间段恰好也是用户一天中网购较为集中的时间。



（3）拦截次数最高的网站——被拦截近 700 万次

境外钓鱼网站 4380.com 是被 360 浏览器拦截次数最高的钓鱼网站，2012 年仅 360 安全浏览器就累计拦截了该网站 692 万次。

从页面设计和内容构成来看，被拦截次数较多的网站大多具有以下一些共同特点：含有大量钓鱼广告，网站多为六合彩、彩票、算命类网站，此类网站抓住了部分人群的暴富、迷信等心理特点，通过钓鱼欺诈广告的方式，诱导用户上当受骗。这些网站的特点多为页面设计相对简单，文字内容罗列，充斥大量短时间致富、美女等信息，例如下图 2012 年拦截次数最多的钓鱼网站 4380.com：



3．钓鱼网站出没时间“黑白分明”

360 安全中心监测发现，近来钓鱼网站也变得越来越狡猾，他们根据用户上网习惯，选择最“恰当”的时间行骗，以提升诈骗成功率，逃避监管。

（1） 白天高发钓鱼：“兼职”

据 360 安全中心监测发现，早 8 点到晚 20 点这一时间段冒充“兼职”的钓鱼网站的拦截量较大，晚上 20 点之后拦截量则大幅减少。据分析，学生等用户群多在白天这个时间段在网上搜索兼职，因此钓鱼网站会选择在这个时间段出现。

（2） 晚上高发钓鱼：“充值”、“充话费”

360 安全中心监测发现，晚间 20 点至凌晨 1 点，搜索“充值”、“充话费”等关键词，会出现较多钓鱼网站，其中 22 点之后是高发时段。此外，每月的月底和月中是用户充值高峰期，这个时间段钓鱼网站的拦截量也是最高的。下图为晚上 20 点之后“充话费”钓鱼高发：

4. 2012 年钓鱼攻击最多的网站新特点

（1）利用消费者贪便宜的心理行骗；

（2）多包含彩票算命类信息，用暴利诱惑用户；

（3）闪骗：骗完就关站，逃脱侦查，一般 12 小时内关站；

（4）网页包含海量外链，用关键词诱骗用户点击；

（5）域名放在海外，逃避监管。

（六） 网址云安全是拦截钓鱼网站有效方式

由于钓鱼网站普遍呈现模仿官网、不含危险代码、数量每年成倍增加、生命周期不断缩短等特点（可参照附录 3），仅仅依靠本地安全机制是很难解决钓鱼网站的识别与拦截问题。就目前的技术手段而言，网址云安全技术是最有效的解决方案。

以 360 安全浏览器为例，用户电脑会定期更新经过 360 安全认证的可信网站白名单，当用户访问不在白名单中，可能存在风险隐患的网址时，360 浏览器会把网址进行不可逆的加密处理，然后与云安全服务器上的“恶意网址库”进行比对，发现是恶意网址就对用户进行报警提示。

（七） 网站身份鉴定重要性日趋增强

对于不法分子最新制作出来的钓鱼网站，以及使用多层隐蔽技术的钓鱼网站来说，任何安全软件都无法确保第一时间 100%识别拦截。因此，提供有效的参考依据，协助用户识别钓鱼网站也是很重要的方法。

我们打开一个网页，一般只能看到这个网页的网址和网页上的内容，对于这个网站是否合法，注册机构或个人是谁，都很难了解。这也为网络安全带来了巨大的隐患。而网站身份认证技术则可以有效解决这一问题，帮助用户识别和防范钓鱼网站。

按照相关法规，国内经营的网站均需在工信部进行 ICP/IP 备案，目前的备案类别主要分为：军队、政府机关、事业单位、企业、社会团体和个人等等若干种。ICP/IP 备案信息实际上就是政府颁发给网站的一张身份证，这些信息均可以在工信部网站进行查询。另外，多数欧美正规网站支持“VeriSign认证”等国际认证，这些国际认证也可以帮助用户分辨国外网站的安全性。

通过适当的方式向用户展示网站是否拥有合法认证以及合法认证的具体信息，将十分有助于网民分辨网站的安全性。下图就是 360 安全浏览器为北京协和医院官方网站进行的身份鉴定：

360 浏览器还联合了多家权威认证机构，提供经过审核的其他身份信息，例如医院、政府、银行、品牌官网等资质信息。目前，这项安全鉴定技术已经得到了工信部的大力支持。

对于并未取得安全认证，也没有被加入云端网址库黑白名单的网站，其安全性也是未知的。为确定此类网站的安全性，只有通过在线风险分析技术，帮助用户快速鉴定一个未知的网站内容的安全性。 解决钓鱼作者利用安全厂商还没来得及分析网站内容的空窗期进行欺诈钓鱼。

360 安全浏览器新上线的“照妖镜”就具有在线风险分析能力，借助于 360 安全软件拦截网站经验，通过机器智能学习并总结钓鱼欺诈网站的特性。当用户访问安全性未知的网站时，可通过“照妖镜”功能实时监测网站安全性，确定网站安全后即可放心访问。如果访问被“照妖镜”确定为安全的网站时仍然上当受骗，可通过 360 安全浏览器的网购先赔功能索赔，最高每年可享受 72000 元赔付基金。

第三章　网站跟踪威胁用户隐私安全

（一）　“网络跟踪”问题引起关注

2012 年年初，谷歌公司被爆利用苹果公司 Safari 浏览器的漏洞，绕过该浏览器的隐私设定，跟踪用户的上网习惯。随后，FTC（Federal Trade Commission，美国联邦贸易委员会）对谷歌侵权一事展开了调查。8 月， FTC 要求谷歌缴纳 2250 万美元的罚款并彻底停止追踪用户上网习惯的侵权行为。11 月，美国旧金山地方法院批准了 FTC 的这一处罚决定。而美国的“消费者监察”机构则认为这一处罚太轻，FTC 应该对谷歌至少处以 30 亿美元的罚款。

Google 此次被罚事件，使大型搜索引擎利用网络跟踪技术追踪用户上网习惯的问题曝光在公众面前。2013 年 3 月，央视 3·15 晚会也集中曝光了一批利用 Cookie 跟踪窃取用户隐私信息的互联网公司，并由此引发了人们对网络跟踪可能严重泄露个人隐私的普遍担忧。

早在 2011 年 11 月 W3C （World Wide Web Consortium）就提出了两项标准的初步草案，它们的目的是保护 Web 用户的隐私，以及让用户可以选择退出 Web 跟踪系统。2012 年 10 月 2 日，W3C 发布“禁止跟踪”的最新标准草案，根据该标准草案，用户可以选择禁止被网站跟踪。W3C 认为该标准有利于改善用户在互联网上的体验，减少用户网络隐私被侵犯或遭泄露的可能性。

（二）　网络跟踪的原理与危害

A 和 B 是两个域名不同的网站。如果用户在访问 A 网站时，回传的页面内容中却包含对 B 网站的访问请求，则称该用户对 B 进行了跨域访问；如果用户对 B 网站的访问请求中包含足以标识用户个人身份的信息，则可以说：B 网站对该用户实施了跟踪。下图为跟踪技术基本原理

网络跟踪是在用户不知情的情况下进行的。事实上，跟踪者通常会与众多网站组成联盟，并在每一个盟友的网页中部署自己的跟踪代码。用户无论访问联盟中的哪个网站，都会被跟踪。而跟踪者则会根据收集到的各路信息对用户进行特征分析，之后与同盟者分享分析结果，并据此进行精准的广告投放。

网络跟踪的一种最常见的形式就是 Cookie 跟踪。而所谓的 Cookie 跟踪，是跟踪者通过联盟或付费等方式，将其跟踪代码嵌入到大量网站中，收集这些网站用户的网页浏览记录、

停留时间、购物商品等个人信息，记录在“跨域 Cookie”数据中。跟踪者可以通过对“跨域 Cookie”数据的分析，一定程度上掌握用户的行为特征和上网偏好，并可以据此谋取特定的商业利益。

网络跟踪就像是在网民生活的每一个角落里都装上隐蔽的摄像头，对上网者的一举一动进行全程监控，而用户不仅对监控行为毫不知情，对监控者的身份也是一无所知。网络跟踪虽然已经广泛存在，但目前仍然处于法律和监管的真空地带，可能严重威胁用户的个人隐私安全：

首先，跟踪者的身份是不受约束的：谁有能力与网站结成联盟，谁就可以发布跟踪代码；第二，跟踪行为是不受约束的：跟踪者可以根据自己的需要，任意采集用户信息，任意记录用户行为；第三，跟踪记录的用途是不受约束的；第四，跟踪者没有保密义务：尽管跟踪记录与分析结果涉及大量用户隐私，但跟踪者不但没有任何保密义务，而且还会与联盟者分享结果，从而可能造成用户隐私的二次泄露、三次泄露。

（三） 反跟踪成为浏览器安全新需求

微软在 2012 年 8 月就曾宣布，IE10 浏览器将默认开启防止跟踪功能。至此，浏览器的反跟踪功能已经成为行业安全的新标配。截至 2012 年底，包括 360 安全浏览器、火狐浏览器和 Safari 浏览器在内的国内外多款主流浏览器均已发布了自己的反跟踪功能。

从技术角度看，防范网络跟踪有两种基本的方法：一个是禁止跨域访问，一个是清理 Cookie 数据。不过，单纯的跨域访问并不一定构成网络跟踪，如果不做辨别的禁止所有跨域访问，将可能导致网站的某些正常功能无法使用。类似的，如果总是无差别的清除所有 Cookie 数据，也会使用户上网非常不方便，并可能引起其他一些网站登录问题。

事实上，如前所述，除了跨域访问之外，网络跟踪还有另一个构成要件，就是用户信息采集，二者缺一不可。因此，浏览器并不需要禁止所有的跨域访问，而只需要禁止那些采集或携带了用户身份信息的跨域访问请求，就可以阻止网络跟踪。

类似的，浏览器也并不需要随时清理所有的 Cookie 数据，而只需要自动清理那些“跨域 Cookie”数据，就可以使跟踪者无法连续的追踪同一用户，从而防止 Cookie 跟踪。

下图是 360 安全浏览器自带的隐私保护器，通过隐私保护器可以一键清理网站 Cookie/FlashCookie/跨域跟踪日志，保护用户隐私：


隐私保护器
Cookie使用日志
Flash cookie记录
跨站跟踪日志
网站隐私保护器
清cookie 反跟踪
一键全面清理网站Cookie，阻止网站跟踪！
网站访问Cookie通常用于商业广告投放，防止隐私信息泄露，建议定期清理
一键清理
Cookie使用日志
清理访问cookie记录，避免网站跟踪！
366条
查看详情
Flash cookie记录
Flash cookie就是记录您在访问Flash网页时候的信息，普通方法无法清除
23条
查看详情
跨站跟踪日志
跨站跟踪记录主要用于商业目的，用于内容定制，精准广告推荐，web统计等
261条
查看详情
央视315曝光Cookie隐私泄露，360安全浏览器全面抵制网络偷窥
查看详情>>

第四章 数据劫持与反劫持

数据劫持通常是运营商为了特定的商业利益而采取的一种技术策略。数据劫持的形式多种多样，常见的包括：页面缓存劫持，插入广告劫持，DNS 解析劫持，广告佣金劫持，网页内容劫持等等。下面就对一些常见的数据劫持现象及其危害进行详细说明。

（一） 缓存劫持与登录串号

为了节约带宽，减少网络传输负担，一些中小运营商会将部分热门网页缓存在本地服务器上。当有临近用户请求相关内容时，运营商的本地服务器会直接将缓存页面发送给用户，而不是到网站服务器上去请求数据。这种技术被称为运营商缓存劫持。

如果缓存机制审核不严格，将含有用户帐号信息的网页缓存到了本地服务器，那么后面访问的用户就有可能登录到前面用户的帐号中去，这种现象就是登录串号。登录串号现象广泛的存在于网页浏览、即时通信和电子邮件系统中。

（二） 运营商广告劫持

某些运营商会在正常的网页传输过程中，额外插入一些附加广告，以谋取商业利益。这就是插入广告劫持。由于普通网页传输一般采用 HTTP 方式，而 HTTP 协议对传送内容是不加密的，这就给中途劫持数据并插入广告创造了可能。

插入广告劫持通常不易被发现，因为普通用户很难识别哪些广告是来自网站的，哪些广告是中途插入的。不过，当用户打开原本完全没有广告的网页时也看到了广告，插入广告劫持的事情也就被证实了。

（三） 网页内容劫持

当用户打开某个网址时，地址栏显示的网址是正确的，但内容却是被篡改过了。这就是内容劫持。内容劫持实际上也是利用 HTTP 不加密传输的特点，中途对整个网页内容都进行了替换。下图是 2012 年 10 月接到的一个报告案例。用户访问 360 网址导航，结果打开的却是搜狗网址导航。

（四） DNS 解析劫持

DNS（Domain Name System）是域名解析系统的缩写，作用是将网站域名解析为指定的

IP 地址。而 DNS 劫持就是篡改域名解析的结果，将用户访问转向到其他 IP 地址。最为典型的 DNS 解析劫持现象就是：用户想要登录一个网站，结果却登录到另一个网站。下图是 2012 年 12 月报告的一起案例，用户原本想要打开 360 搜索，结果却登录了“hao123”网址导航。

问题表现：

1.在IE或Chrome中访问so.360.cn，自动跳转到http://www.hao123.com/?src=10003201_hao

2.在FF中访问so.360.cn，自动跳转到http://www.hao123.com/?src=10003205_hao

我看过hosts文件，看过环境变量，这是我能猜想到的地方，都很正常。 系统自启动项里也没发现值得怀疑的东西。在注册表里面搜索10003201_hao 这个src id，以及so.360.cn这个URL，均无果。

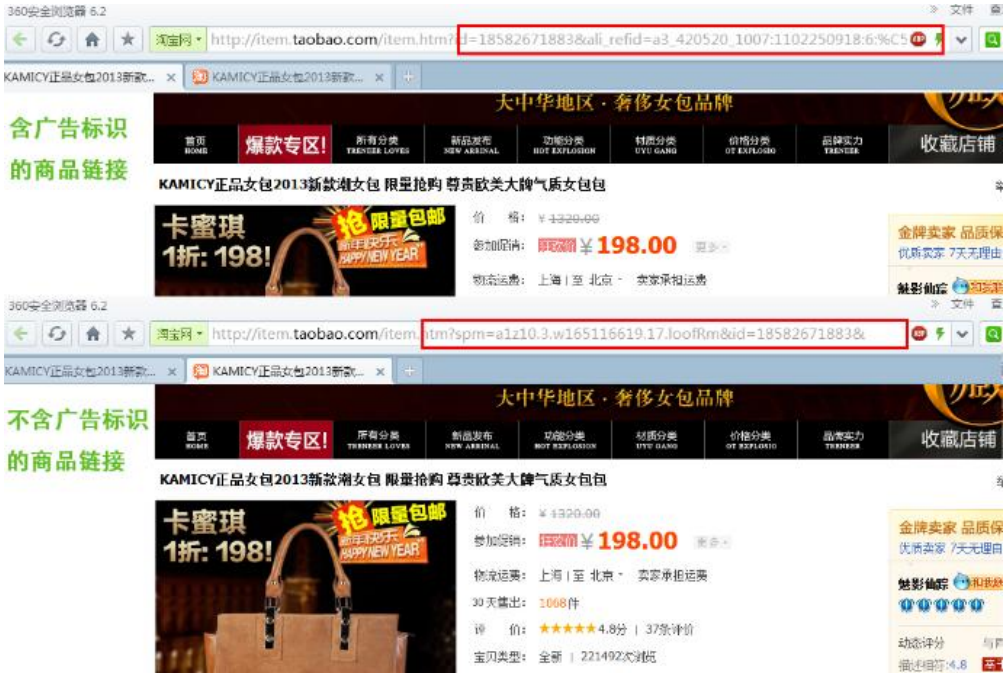
系统为Win7 x64，常驻软件是ESS防火墙。

这就是我能描述的全部已知信息。

（五） 广告佣金劫持

广告佣金是指网站加入广告联盟，并在其网站加入广告内容进行推广，产生点击后获得的一笔广告费用。比如，我们通过某个网页上的广告点击进入了一个淘宝卖家的店铺，那么一旦交易成功，淘宝卖家就需要按照一定的比例向广告发布者支付广告佣金，即淘宝客盈利模式。另外，很多网站也会加入一些广告联盟，通过在其网站上加入联盟广告并引导用户点击，联盟广告主就会根据网站中广告的实际点击，给网站支付广告佣金。

用户通过广告链接打开的商品页面，与直接通过自身页面打开的商品页面，内容虽然完全相同，但网址会有所区别。下图就给出了一个淘宝商品的示例。



如上图所示，通过广告链接打开的商品页面，网址会比原始网址长出一部分，这一部分就是广告商的身份标识。如果没有这段身份标识，消费者购买商品的货款就会全部属于卖家。而有了这段身份标识，货款中的一部分就会自动打入广告商的账户。

而所谓的广告佣金劫持，就是当用户并没有通过广告链接或推广链接进入特定网站时，却被人为的在网址中加上了广告商的身份标识，进而导致本应属于商家的资金被秘密打入广告商的账户。

在用户电脑没有感染木马病毒的情况下，广告佣金劫持通常是发生在用户请求的传输过程中。广告佣金劫持是一种特殊的劫持现象，由于这种劫持既不会改变商品内容，也不会改变商品价格，对消费者不构成任何危害，因此也很少遭遇消费者投诉。但这种劫持却侵害了商家的合法权益，在 2012 年遭遇了大量商家，特别是淘宝店主的投诉。

由于广告佣金劫持实际上也是在中途对的明文数据进行修改，浏览器本身很难进行鉴定和分辨。

不过，需要补充说明的是：广告联盟通常还会规定：只要用户通过广告链接打开了某些店家的网址，那么在一定的有效期内，该用户不论通过什么形式再次访问这个店铺，一旦交易成功，店家也需要向广告商支付佣金。比如，消费者通过广告链接进入了一个店铺，而在消费者与店主沟通时，店主又通过聊天工具向消费者发送了某些商品的链接，那么消费者即使是通过店主发来的链接购买商品，店主也需要支付广告佣金。这种情况并不属于广告佣金劫持。

（六） 数据劫持的危害与反劫持

数据劫持的问题广泛存在，不仅威胁用户的上网安全，同时也会对网站的信誉和商业运营造成破坏。不过，由于数据劫持通常是发生在网络传输过程中，因此，单纯依靠客户端或浏览器的安全机制很难实现有效的防范。解决数据劫持问题，需要运营商、网站和浏览器的共同配合。

首先，网站可以对页面中的用户名和密码等敏感数据进行独立的加密传输，之后由浏览器进行解密并填回到网页的特定位置，这就可以有效的避免登录串号现象；

第二，网站在发送网页时可以对网页进行数字签名，浏览器可以通过对数字签名的验证来鉴别网页是否在传输过程中遭到篡改；

第三，运营商也应当加强服务器的规范管理，尽量避免可能对用户带来骚扰或安全隐患的数据劫持。

不过目前，国内尚没有统一的行业规范来解决数据劫持问题。

第五章 浏览器登录安全

（一） 网站帐号面临多种安全风险

网站帐号是每个用户在互联网上的身份标签，同时也是绝大多数黑客攻击和窃取的主要目标。普通网民的网站帐号主要面临以下几种形式的安全威胁。

1. 仿冒官网

钓鱼网站中的一个主要类别就是仿冒知名网站，诱骗用户输入帐号和密码。一旦用户在钓鱼界面中输入，帐号和密码就会被黑客窃取。比如，下图就是一个仿冒 QQ 安全中心的钓鱼网站截图。

2. 键盘钩子

键盘钩子，泛指那些可以监视用户键盘输入的木马病毒。一旦用户在登录界面中输入帐号和密码，就会被木马程序秘密的记录下来，并发送给幕后黑客。

3. 盗用 Cookie

某些网站存在安全漏洞，使得一台电脑上的 Cookie 数据也可以在另一台电脑上使用。也就是说，黑客可以把您电脑中的 Cookie 数据复制到他的电脑中，并使用您电脑上的 Cookie 数据来登录相关网站。尽管黑客并不知道加密后的 Cookie 数据中具体的帐号和密码信息，但同样可以以您的身份登录网站，并以您的身份发布信息，直到这些 Cookie 信息过了有效期。

4. 网站拖库

网站数据库信息被黑客集中盗取的现象被称为拖库。而黑客拖库的主要目标就是用户的帐号和密码。自从 2011 年底天涯、CSDN 等多家知名网站被曝拖库后，2012 年，国内外又有数家知名网站先后被曝拖库。另据 360 网站安全检测平台（http://webscan.360.cn)的统计数据显示，75.6%的国内网站存在高危安全漏洞。而存在高危安全漏洞也就意味着网站非常容易被拖库。

（二） 帐号安全的最新防护技术

浏览器的安全性直接关系到网站帐号的安全性。针对网站帐号的各种安全威胁，浏览器技术也在不断发展和升级。

针对钓鱼欺诈网站的各种防范技术，第二章中已经有详细的介绍，这里不再累述。而针对另外三种主要的安全威胁，可以采用下面这些些有效安全技术进行防护：

1. 帐号加密保存

大多数浏览器都有自动保存网站帐号密码的功能。这不仅仅是为了方便用户使用，从安全角度看，减少键盘的使用频率，可以大大减小被键盘钩子攻击的风险。另外，在本地保存用户帐号和密码，必须进行有效的加密，以防止被黑客破解。

2. 异地解码保护

浏览器在每次使用本地保存的帐号和密码时，需要对加密信息进行解密。但是，解码加密信息中需要包含由本地系统特征生成的随机密钥，这就保证了加密信息只能在本地电脑上进行解密，即使这些信息被黑客窃取，也无法在异地使用。

3. 动态加密保护

每次重启浏览器时，都会使用一个新的随机密钥对存储在本地的用户帐号信息进行重新加密。这种动态更新的密钥，可以在最大程度上防范暴力破解。

4. Cookie 管理

要防止 Cookie 被异地使用，根本方法还是要网站做好安全认证机制。不过从浏览器的角度来看，也可以考虑以下两种方式来保护 Cookie 信息的安全。

首先是提供 Cookie 清理功能，允许用户主动清理所有的 Cookie 信息。

第二是建议网站使用临时 Cookie（即 session Cookie）记录用户上网信息，跟永久 Cookie 不一样，临时 Cookie 不保存在硬盘驱动器而是存在临时存储器中，当浏览器关闭时，将被删除。

5. 云端加密保护

除了本地帐号管理外，浏览器还可以通过云端托管，使用户能够方便的在异地使用和管

理自己的多个帐号，这是浏览器登录管理的未来趋势。不过，云端托管多个帐号除了要考虑一般的加密措施外，还必须采取有效的安全机制防范“拖库”风险，防止用户帐号被批量窃取。

一种可行的技术方案是将密文与密钥分开管理：服务器上只保存加密后的数据和部分解码密钥，而另一部分密钥则仅由用户自己持有，不上传的服务器。这就可以使任何黑客在没有拿到用户密钥的条件下，即使盗走服务器上用户信息的机密数据，也无法进行正确的解码。

（三） 部分浏览器产品存在安全隐患

目前，在网民常见的浏览器中，有相当一部分存在严重的安全隐患，主要表现在以下几个方面：

1. 个别浏览器明文存储用户的帐号和密码，极易被黑客攻击和窃取；
2. 某些浏览器使用静态密码对帐号信息进行加密存储，容易遭到暴力破解；
3. 云端存储的帐号和密码信息不能防范黑客拖库。

360 安全浏览器在帐号安全保护方面进行了大量的研究和实践，并在功能模块“登录管家”中使用了上述全部最新的安全技术。特别值得一提的是，登录管家本地帐号加密机制采用了双层加密，即对帐号数据加密以后，对加密后的数据再进行一次加密。

2012 年 11 月， 360 安全浏览器的“登录管家模块”通过了中国信息安全测评中心 EAL2 级别认证（见附录 2），是国内第一款获此资质的浏览器产品。

附录 1　浏览器应具备的十大安全防护功能（2013）

防护功能	功能简介
挂马拦截	结合木马网址库、恶意脚本检测等防挂马技术，阻止木马病毒通过网站入侵电脑。
钓鱼拦截	比对恶意网址库，对假冒网银、网购等钓鱼网站进行风险预警；在网购时提高防护级别，拦截劫持浏览器的钓鱼盗号型木马，增强安全性。
下载安全扫描	文件下载前自动识别恶意下载链接，下载后对文件进行病毒扫描，保证下载文件的安全性。
开启系统级防护	开启微软 DEP、ASLR 和 SEHOP 等操作系统安全防护，防御 0day 漏洞攻击。
沙箱隔离	建立虚拟环境隔离病毒、木马，使其不会影响用户的真实电脑。
隐私保护	跨域访问拦截，不记录用户上网历史和 Cookie，防止用户被第三方网站跟踪，保护用户隐私安全。
密码保护	保护用户帐号登录安全的辅助工具。
网站身份鉴定	建立统一的网站身份认证机制，辅助用户识别网站真实身份，降低被欺诈的风险。
主页防篡改	保护浏览器主页，阻止恶意程序篡改主页地址。
广告过滤	在用户开启广告过滤的情况下，屏蔽各类病毒欺诈型广告。

附录 2　360 浏览器获中国信息安全测评中心 EAL2 认证

国家信息安全测评

信息技术产品安全测评证书

证书号：CNITSEC2012PRD0211

级别：EAL2

北京奇虎科技有限公司

（北京市西城区新街口外大街28号D座112室 邮编：100000）

360安全浏览器登录管家模块V1.2.0.1071

测评标准：GB/T 18336-2008《信息技术 安全技术 信息技术安全性评估准则》（idt ISO/IEC 15408:2005）

测评方法：《信息技术安全通用评估方法》（idt ISO/IEC 18045:2005）

测评报告编号：363CR20121012-EAL2

测评机构：中国信息安全测评中心信息安全实验室

此证书仅适用于该产品的上述版本或型号

签发日期：2012年11月19日

有效期至：2015年11月18日

批准人：

中国信息安全测评中心

附录 3　2013 年典型钓鱼网站示例

1. **假冒淘宝**——利用伪造商品页面诱骗买家支付，实际付款对象是不法分子的账户。有时此类钓鱼网站也会套取受骗者的帐号密码。

2. **假药网站**——伪造或凭空捏造权威资质证明，虚构患者疗效案例，集中在男性壮阳药、跨国公司名贵进口药、疑难杂症特效药、知名的中药处方药四大领域。

3. **网游交易欺诈**——以热门网游虚拟装备、游戏币交易为名，低价诱惑游戏玩家交易支付，骗取玩家钱财。

4. 模仿品牌官网——伪装时尚数码产品的官网或官方销售渠道，例如iPhone、iPad、小米手机等，以远低于正常价格的标价出售，递送假冒伪劣的山寨手机。

5. 手机充值欺诈——假冒移动、联通、电信等运营商指定充值中心名义，以“充100送50”等优惠活动吸引网友充值，付款后无法获得话费。

6. 假票网站——模仿航空公司官网、旅行社、票务公司、12306.cn火车票网站等，通过搜索引擎竞价排名或SEO推广，在人们搜索机票、火车票相关信息时排在前列，诱骗消费者向不法分子设置的个人银行账户汇款。

7. 假冒网银——这是对网购族财产威胁最大的一类钓鱼网站。不法分子以网银账户冻结、动态口令（E令）升级等名义，通过短信、邮件诱骗攻击目标登录假冒网银的钓鱼网站，套取账户、密码以及动态口令信息，再迅速在口令有效期内入侵受骗者网银账户将资金转走。