网络时代的信息安全知识

何明芮 著

中国科学技术出版社
CHINA SCIENCE AND TECHNOLOGY PRESS

本书为四川省社科普及规划项目成果

网络时代的信息安全知识

何明芮　著

中国科学技术出版社
·北　京·

图书在版编目（CIP）数据

网络时代的信息安全知识/何明芮著．—北京：中国科学技术出版社，2017.5

ISBN 978-7-5046-7510-1

Ⅰ.①网… Ⅱ.①何… Ⅲ.①信息安全—研究 Ⅳ.①G203

中国版本图书馆 CIP 数据核字（2017）第 110453 号

责任编辑 王晓义 蒋宵宵
封面设计 孙雪骊
责任校对 杨京华
责任印制 徐 飞

出 版 中国科学技术出版社
发 行 中国科学技术出版社发行部
地 址 北京市海淀区中关村南大街 16 号
邮 编 100081
发行电话 010-62173865
传 真 010-62179148
投稿电话 010-63581202
网 址 http://www.cspbooks.com.cn

开 本 720mm×1000mm 1/16
字 数 130 千字
印 张 7.25
版 次 2017 年 5 月第 1 版
印 次 2017 年 5 月第 1 次印刷
印 刷 北京京华虎彩印刷有限公司

书 号 ISBN 978-7-5046-7510-1/G·751
定 价 40.00 元

前　言

信息是构成现今知识信息时代的基础资源，对人类社会的发展具有极其重要的意义。怎样保障人类社会合理利用信息已成为不容回避的基础问题，换而言之，即信息安全问题必须被提上日程并持续重视。不同的领域对信息安全的概念有着不同的阐述。在通常的经济和商业领域中，信息安全主要强调的是消减并控制风险到个体或组织能够接受的水平，以达到保持业务操作的连续性的目的，最终将风险造成的影响和损失降到最低。根本而言，信息安全最重要的任务是保证信息网络中的信息资源的安全性，保证信息系统本身的安全性。

信息安全问题具有相当广的覆盖面，从国家层面到个人层面都涉及信息安全问题，如从国家军事政治等机密安全，到企业商业秘密安全，再到个人信息的安全。尤其是目前网络普遍运用，信息安全与每个人的生活密切相关，如手机银行等业务由于操作便捷越来越受到人们的青睐，QQ、微信等业务几乎成为人人选择的交流方式，更不用说当我们外出旅游时，通过网络预订酒店、飞机票等业务。这些让我们享受网络便捷的同时，也给我们带来了个人信息泄露的困扰。例如，2014 年 5 月 13 日，小米陷入“泄露门”，被发现确有部分 2012 年 8 月前注册的论坛账号信息被非法窃取；2013 年 8 月，国内一大批快捷酒店开房记录被泄露，造成酒店客户相关信息在网上疯传；2013 年 11 月著名企业腾讯爆出 7000 多万 QQ 群数据公开泄露，造成大量个人隐私公开……

由此可见，了解信息安全知识，从多角度防范信息泄露的不良后果非常符合人们目前的实际需求。本书从个人层面和企业层面介绍信息安全知识，旨在让更多的人了解信息安全基础知识，树立并增强信息安全意识，防护个人和企业的信息安全。

目　录

个人篇 …… 1

一、网购时个人信息安全防护知识 …… 1

1. 网购中个人信息泄露的渠道 …… 3

2. 个人层面基本网络安全技术 …… 6

3. 个人层面信息安全防护意识 …… 13

二、使用 QQ 等交友工具时个人信息的安全防护知识 …… 15

1. 常用交友工具介绍 …… 15

2. 使用交友工具时常见的陷阱 …… 25

三、使用智能手机时个人信息安全防护知识 …… 33

1. 智能手机病毒基本知识 …… 34

2. 智能手机常见信息泄密渠道 …… 35

3. 使用智能手机时的常见陷阱 …… 37

4. 使用智能手机时增强个人防范意识 …… 45

企业篇 …… 49

一、常见信息安全标准 …… 49

1. TCSEC 标准 …… 49

2. ISO 15408 标准 …… 50

3. BS7799 标准 …… 50

二、常见信息安全支撑技术知识 …… 56
1. 身份认证技术 …… 56
2. 加密(解密)技术 …… 59
3. 边界防护技术 …… 59
4. 访问控制技术 …… 60
5. 主机加固技术 …… 60
6. 安全审计技术 …… 60
7. 检测监控技术 …… 61
8. WPA(Wi-Fi Protect Access) …… 61
三、网络时代对企业信息安全防护的新挑战 …… 61
四、网络时代企业信息安全防护新对策 …… 83
1. 企业信息安全的主要威胁 …… 83
2. 企业信息安全防护新对策 …… 84

附录 1 我国个人信息保护相关法规 …… 89

1. 中华人民共和国宪法 …… 89
2. 中华人民共和国民法通则 …… 90

附录 2 信息安全技术公共及商用服务信息系统个人信息保护指南 …… 91

1. 范围 …… 91
2. 规范性引用文件 …… 91
3. 术语和定义 …… 91
4. 个人信息保护概述 …… 92
5. 个人信息保护 …… 94

附录 3 信息安全等级保护管理办法 …… 97

参考文献 …… 107

个人篇

网络时代，个人信息安全问题让人感到不安。2015 年，中国互联网信息中心最新全国互联网发展统计报告显示，中国网民互联网安全意识亟须提升，近九成用户个人信息曾主动泄露；智能硬件成互联网新趋势，但智能生活却面临着立体式攻击……我们已经习惯各种智能硬件丰富我们的生活，但信息安全问题已成为我们享受智能生活便捷的一大障碍。因此，从个人层面，知晓在常见上网渠道中的信息安全防护知识是非常重要和必要的。

一、网购时个人信息安全防护知识

【案例 1】网购现象 1

王××是一个漂亮善良的妹子，但不怎么熟悉电脑，天生又怕麻烦，所以很久没给电脑中的杀毒软件升级了。她经常上网购买自己喜欢的衣服等物品。在一次网购过程中，卖家给她发了一个图片，说这张图片能更清晰地看到衣服的细节。她也没多想就接收了该图片，哪成想，这是一张带有木马病毒的图片！可怜的王××因此被盗了账号和密码，损失人民币 700 多元。

【案例 2】网购现象 2

谭×是一名在校大学生，认为网购方便而且能有更广的选择面，所以一向喜欢网购不喜欢逛街。有一次在网上购买耳机的时候，卖家给他发来一个链接，让他往里面预付 10 元钱，说只要预付后就能享受店内更优惠的活动。谭×觉得 10 元钱数额很小，被骗了也没关系，于是爽快地付了钱，但随后发现自己支付宝里余额全没了。这下他才着急了，可是已经晚了，不良后果已

经造成。那个链接指向的网站上有木马病毒，当谭×在该网站上输入自己的账户和密码时，就已经掉进骗子挖好的陷阱里了。

【案例3】网购现象3

熊×的大学专业是计算机，因此一向对网站敏感。

一次，他在淘宝上打算购买一件衣服。当咨询卖家时，卖家自动回复说：店内太忙，请和客服QQ：××××××××联系。

他很喜欢看中的那件衣服的样式，所以就在QQ上和客服联系了，并与客服谈妥了价格。随后，对方给他发过来一个链接，说是详细介绍那件衣服。

由于专业习惯，熊×仔细察看了一下该网页，居然发现它是模仿淘宝的虚假网页，据他事后说一般人很难分辨出真假。

熊×觉得很庆幸，幸亏自己懂一些计算机基础知识，否则当自己毫无防备地输入自己的信息后，账号和密码肯定就落到骗子手里了，自己账号上的钱肯定也就保不住了。

【案例4】网购现象4

有一天，成都市的崔先生网购了一部手机。在等待手机到货的过程中，崔先生突然接到一个陌生电话，对方自称是来自商家的一名员工，并准确报出了订单的详细信息，如购买手机的型号、手机的成交价以及收货住址等。然后，对方告诉他，根据崔先生的订单情况，崔先生现在已有资格成为本公司会员并办理会员卡，办理会员卡需要交纳500元，同时可以享受公司所有商品的2~7折优惠，还会赠送给崔先生一套礼品，并且保证货到付款。崔先生很高兴地答应了，挂了电话后突然想起还不清楚赠送礼品的具体内容，于是找出当时手机购物网站提供的客服电话拨打过去，哪知客服回答说他们企业从未搞过类似办理会员卡的优惠活动，并提醒崔先生说已经有客户因此上当了，现在骗子非常猖獗。

【案例5】网购现象5

2015年7月，兰州的吉先生网购了一台打印机。不久后，一个自称是商家客服的人给吉先生打电话，告知，因为商家系统临时升级维护，导致近段时间的订单都失效了，为了不让客户受到损失，现在需要吉先生填写退款协议并且办理退款。吉先生信以为真，在QQ上打开了对方发来的办理退款的链接，并按提示输入了自己的私人信息，如银行卡号及密码等，甚至也输入了发到手机上的短信验证码。刚输入这些信息不久，就被银行告知关联的银行

卡已被消费了 3000 元。

作为一种新兴的消费购物模式，网络购物具有比传统消费购物模式更多的优点，如便宜的价格、更多选择的品种、不出门就可收货的便利性等，这些特性充分满足了人们快节奏的生活需求，从而受到越来越多消费者的欢迎。然而也正是这种随时随地足不出户就可以购买到自己所需商品的购物方式，出现了各种个人信息安全泄露事件，案例 1 至案例 5 只是网购中个人信息安全泄露案件的冰山一角，这些信息安全泄露事件给消费者带来了不容小觑的损失。那么在网购过程中，如何能有效地保护好自己的个人信息，尽可能地做到安全购物呢？首先，需要了解网络中个人信息泄露渠道；其次，须要提升个人层面基本网络安全知识；最后，加强个人层面信息安全防护意识。从而达到更充分地保障网购生活安全性的目的。

1. 网购中个人信息泄露的渠道

一般来说，网购过程主要包括注册、登录、浏览网页、填写订单以及网络支付等步骤，如图 1 所示。

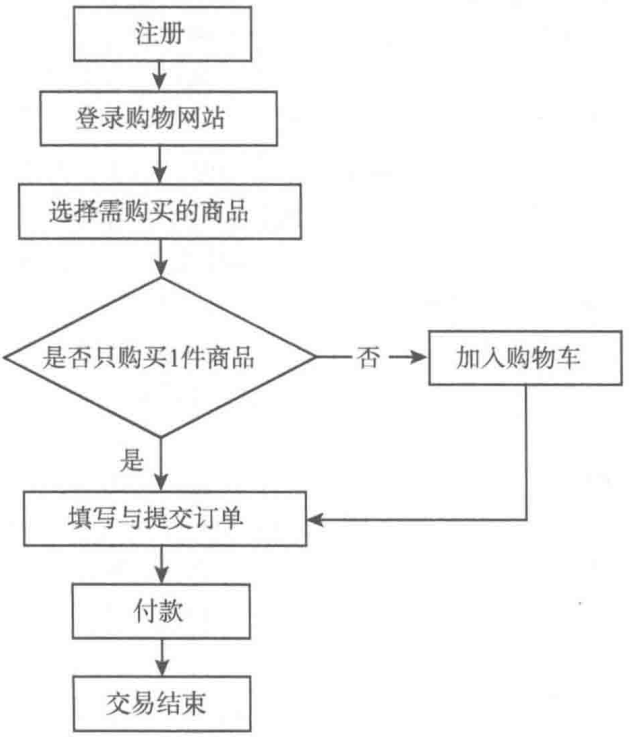

图 1　网购流程图

根据图1所示网购流程图，针对每一网购步骤，详细分析其所存在的具体安全风险如下。

（1）用户注册和登录

在进行网购之前，消费者必须做的第一件事情就是：在相应的网站填写个人相关信息进行注册。成功注册后才能登录相应网站进行购物活动。通过注册，商家可以轻易地获取个人相关信息。

事实上，向网站提供基本个人信息这一行为对于消费者而言肯定存在安全风险。首先，由于信息的不对称，消费者永远无法确切了解自己的个人信息会怎样被网站使用，也不可能知道网站向消费者所承诺的隐私条款是否得到了切实的执行。其次，在网上提供个人信息的行为让消费者相关信息和隐私遭受侵犯的可能性增加，甚至存在个人身份盗用的风险，最终导致财务受到严重损失。

然而，消费者向网站提供个人真实信息又是网购过程中必不可少的一环，因为这是消费者能够获取网站进一步服务的必要条件。

（2）选择需购买的商品

在消费者通过浏览网页来选取自己所需商品的过程中，网络浏览器都会将消费者访问过的痕迹在网络服务器的日志上留下记录，如曾经访问过的网页信息、曾经访问过的图像信息等。网络服务器日志记录的内容包括：消费者的网络地址和传递查询的URL[①]等信息。

Cookie[②]文件是在消费者网络浏览过程中产生的一类常见文件，利用Cookie文件网络服务器能标记带有识别信息的网络浏览器，网络浏览器就可以准确地识别消费者，使消费者的浏览体验变得更为便捷。在消费者的一方，消费者经常使用的浏览器和账户的组合会被Cookie文件所标示；在商家的一方，商家可通过Cookie软件跟踪消费者的网上具体操作，也就能得知特定消费者所购买商品的详细信息、会经常浏览网页的内容以及消费金额和次数等。

此外，在选取商品的过程中，消费者经常遭遇到的一类现象就是图片和视频广告。实际上，这些广告都是网站的网页中嵌入的第三方内容，不仅可以为商家带来不菲的广告收益，还可以跟踪消费者的网上购买行为，为商家分析消费者网购行为提供数据。那么，在指定的网页中，增加一小段HTML

① URL是Uniform Resource Locator的缩写。在WWW上，每一信息资源都有统一的且在网上唯一的地址，该地址就叫URL，它是WWW的统一资源定位标志，就是指网络地址。

② Cookie文件：存储在用户本地终端的数据。

和服务器记录消费者的访问痕迹并利用 Cookie 文件来标记浏览器就是很平常的事情了。无疑，由于这些第三方广告和嵌入式内容的存在，消费者个人信息泄露的风险会再次增加。

（3）填写与提交订单

无论是购买一件商品后直接提交订单，还是使用网站购物车购买多种商品后一起提交订单，正确填写订单都是完成网购的必要步骤。订单上则有消费者详细的商品信息和送货信息。其中，通过订单中的商品信息，商家可分析出消费者的购物倾向和经济状况等内容，从而对消费者进行有针对性的市场推广活动；送货信息则要求消费者填入正确的地址和联系电话，那么，这些真实的个人信息不可避免地会被商家和物流方清楚地知道，这必将导致个人信息泄露风险的增加。

（4）付款

实际上，在交易过程中的付款就是消费者如何将自己的账户资金转移到商家账户的过程。目前，由于各种支付方式的出现，网购中的付款也成为相当便利的过程，消费者可以无需现金，也不需要出门，只要拥有一台可以上网的计算机即可，利用那些方便的电子支付工具，用于购物中的资金结算和流通即可完成付款这一行为。这一环节亦是目前网购过程中个人信息安全风险最大的一环。

目前，在消费者网上支付环节中，主要存在三类影响较广的安全威胁：传统盗号木马、钓鱼网站和新型交易劫持木马。早在《2014 年上半年中国网络购物安全报告》就显示出，现今人们主流的消费方式已变为网购消费，同时木马犯罪产业的攻击对象也发生了改变，从原来的游戏盗号改变为现在的网购消费者，通过构建钓鱼网站，结合木马劫持、电话诈骗等方式，从而达到盗取网站资金的目的。

1）传统盗号木马。通过病毒木马感染消费者的计算机，伺机窃取淘宝或支付宝 ID 以及银行卡等消费者个人隐私信息。但是，目前这类安全威胁正在逐渐减少，其中不断升级的反病毒技术手段功不可没。

2）钓鱼网站。钓鱼网站最大的特点是不法分子通过仿制真实网站的 URL 地址和网页等内容，达到鱼目混珠的目的。怎样吸引消费者进入这些仿冒网站，价格牌是不法分子的首选方式，一旦消费者认为自己“占了便宜”，并完成了汇款，“卖家”就会消失得无影无踪。

相比与传统盗号木马，钓鱼网站欺诈过程制作成本更低廉，且更简便。对“钓鱼者”们来说，可将仿冒网页内容很快切换至不同的域名，从而规避安全拦截或被停止域名解析；对消费者来说，一般很难辨别这些具有极高相

似度的钓鱼网站，因此难免上当被骗。

3）新型交易劫持木马。现在这种新兴的网购安全威胁类型已经超过了钓鱼网站，是增长速度最快的网购安全威胁。一般情况下，不法分子会先注册甚至直接盗用其他网店，仍然利用价格牌的方式吸引消费者点击进入，在貌似正常的网购交易过程中，将木马中植入到消费者的计算机中。这类木马会一直监视消费者的浏览器，只要消费者进行网上支付行为，就会被引向假冒网银网站或者假冒第三方支付网站，从而劫持消费者的购买资金。消费者自以为完成了购物流程，但实际上商家并没有收到货款。对消费者来说，很难提防这种隐蔽的方式。

同时，我国法律监管对于网上支付也存在着不少漏洞，尤其是第三方支付平台模式来说，银行并不能对其有效的监管，成为法律的一个灰色地带，需要相关法律法规规范其行为。

2. 个人层面基本网络安全技术

从以上网购过程中个人信息泄露渠道知识中来看，掌握基本的网络安全技术是可以在一定程度上减少个人信息泄露安全风险。下面介绍两种个人层面的基本网络安全技术。

（1）Cookie 文件

1993 年 3 月，网景公司的前雇员 Lou Montulli 发明了 Cookie 文件。

服务器生成 Cookie 文件并发送给浏览器，浏览器会将 Cookie 的 key/value 保存到某个目录下的文本文件内。当浏览器设置为启动 Cookie 时，只要用户请求同一网站就会发送该 Cookie 文件给网站服务器，这样服务器可以知道用户是否是合法用户以及是否需要重新登录等。

当然，用户可以自行改变浏览器的设置，决定使用或者禁用 Cookie。

以微软 IE 浏览器为例，可根据以下步骤来对 IE 进行设置，以达到使用或禁用 Cookie 的目的：“工具—Internet 选项—隐私—高级”，详见图 2 与图 3。

在图 3 中，可以看出可以通过不同的设置策略来决定 Cookie 的实际运行状态。

Cookie 最典型的应用是判定用户信息以及简化登录手续，网购中“购物车”之类的处理则是 Cookie 另一个重要应用。在一段时间内，当用户在同一家网站的不同页面中选择不同商品时，这些信息都会写入 Cookie 文件中，在最后付款时方便提取相关信息。在高级 Cookie 的运用中，网站服务器甚至可以分析每个用户 Cookie 文件的具体内容，调整所显示的内容，将用户感兴趣的内容放在前列。由于这种利用用户个人信息的目的大多是统计的需要，不

一定会引起用户的直接损失。鉴于此，并没有相关法律约束 Cookie 与用户隐私权受侵害的问题。目前，甚至有的网站要求用户必须开启 Cookie 以后才能正常使用。

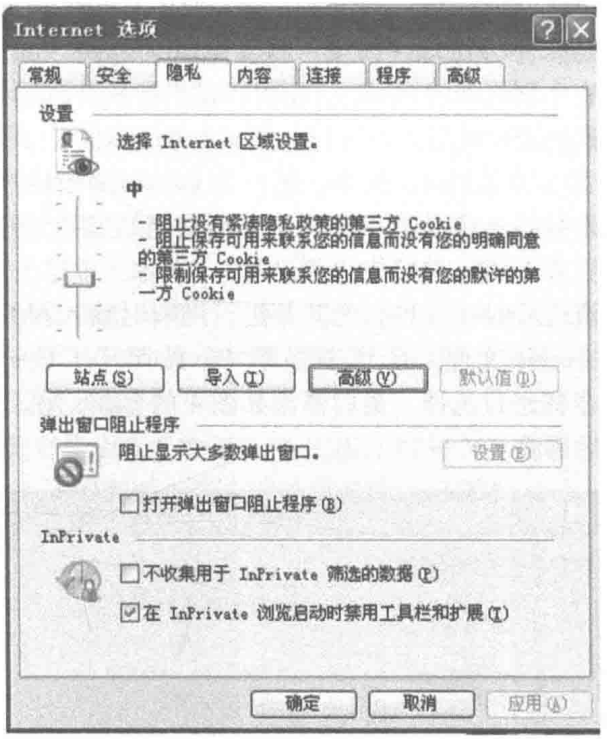

图 2　IE 浏览器如何设置 Cookie 1

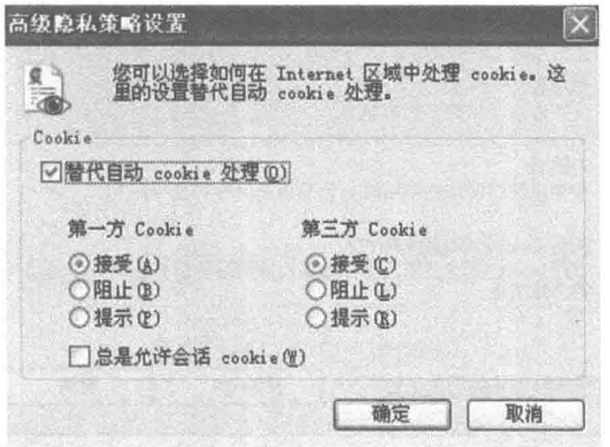

图 3　IE 浏览器如何设置 Cookie 2

那么，作为普通上网用户，我们应该怎样做才能尽可能地保障自己的信息安全呢?

首先，在浏览器中正确设置 Cookie 策略。一般情况，用户可将滑块（见图 2）调整到“中高”或“高”的位置。需要使用 Cookie 信息最多的是论坛站点，如果用户从来不去论坛，甚至可将安全级别调到“阻止所有 Cookie”的位置；为了禁止个别网站的 Cookie，则可以单击按钮“编辑”，将要屏蔽的网站添加到对应的列表中即可。在按钮“高级”的选项中（见图 3），可设置第一方 Cookie 和第三方 Cookie，其中，第一方 Cookie 是指用户正在浏览网站的 Cookie，第三方 Cookie 则是指用户非正在浏览网站发给用户的 Cookie，一般情况下，对第三方 Cookie 选择为“拒绝”。

其次，及时清理 Cookie 文件，尤其是进行网购时输入相关银行卡信息后一定要及时清理 Cookie 文件。在 IE 浏览器中，按照“工具—Internet 选项—删除历史记录”步骤进行选择，最后弹出如图 4 的界面，在 Cookie 文件前打钩进行选择，最后删除。

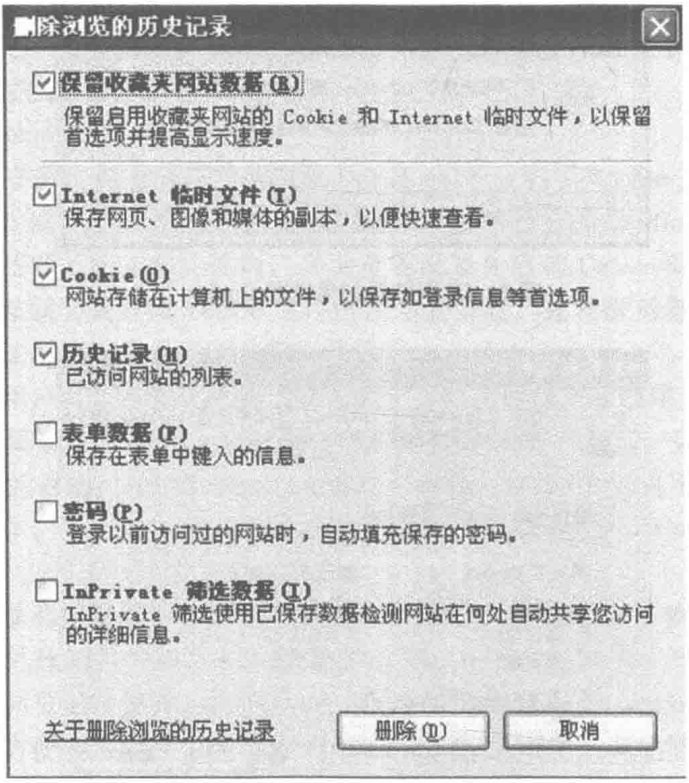

图 4　如何删除 Cookie 文件

（2）防火墙

防火墙（Firewall）是由 Check Point 创立者吉尔·史威德（Gil Shwed）于 1993 年发明并引入国际互联网的。它是一种隔离技术，是指一种将内部网络和公众访问网络（如 Internet）分开的方法，并确定在两个网络通信时执行的一种访问控制尺度。根据用户的需求，依照特定的规则，能够同意或者拒绝外部数据进入内部网络，最大限度地阻止网络黑客访问用户的网络。其中，防止内部信息的外泄是防火墙基本功能之一，因此，为了保障自己的信息安全，在电脑中安装防火墙是我们应该采取的基本措施之一。

目前网络上提供很多免费防火墙下载，比较常见的防护墙有 360 防火墙、瑞星防火墙以及天霸防火墙等，其中 360 防火墙比较受个人用户的欢迎。360 防火墙是集成在 360 安全卫士中，是一款保护用户上网安全的产品，它拥有云安全引擎，解决了传统防火墙频繁拦截和识别能力弱的问题。下面具体介绍 360 防火墙的设置步骤。

1）首先下载安装 360 安全卫士正式版。打开 360 安全卫士，进入首页，点击安全防护中心，即可进入防火墙设置界面，见图 5。

图 5　设置 360 防火墙步骤 1

2）在防护墙设置中心点击安全设置按钮，见图 6。

图 6　设置 360 防火墙步骤 2

3）首先需要设置防火墙需要开启，如果关闭，选择对应选项即可，见图 7。

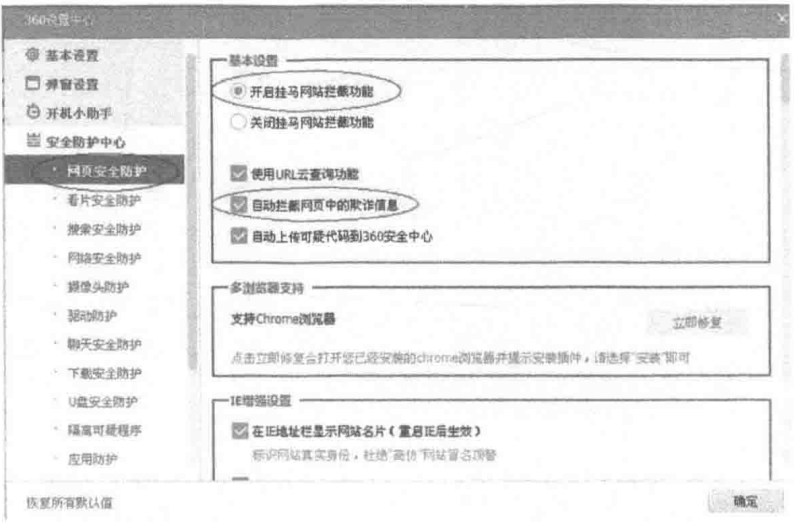

图 7　设置 360 防火墙步骤 3

4）网络安全防护中主要是网页木马防护，防止流量挂马网站，对于未知网站文件非常有用，当然也可以去掉复选框来进行关闭，见图 8。

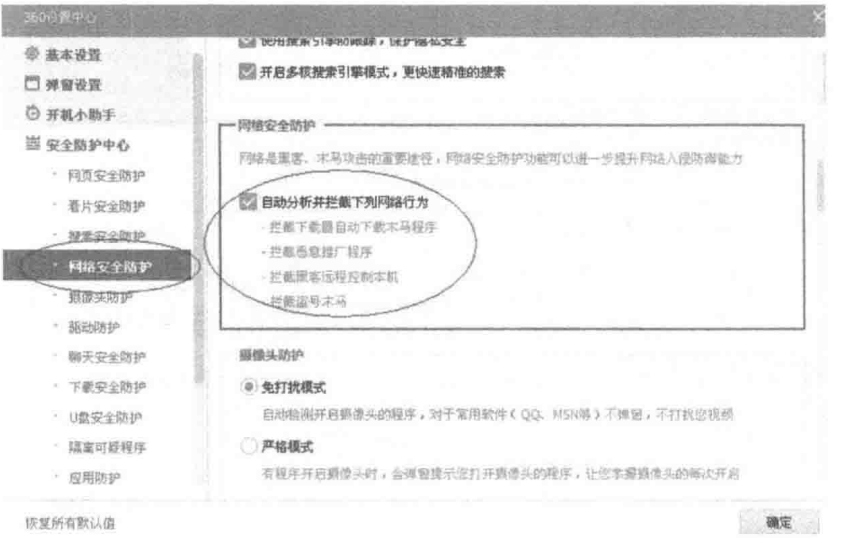

图 8　设置 360 防火墙步骤 4

5）隔离可疑程序：防止有些安装软件篡改用户的 IE 主页，同时可以拦截输入法木马，也可取消复选框进行关闭，见图 9。

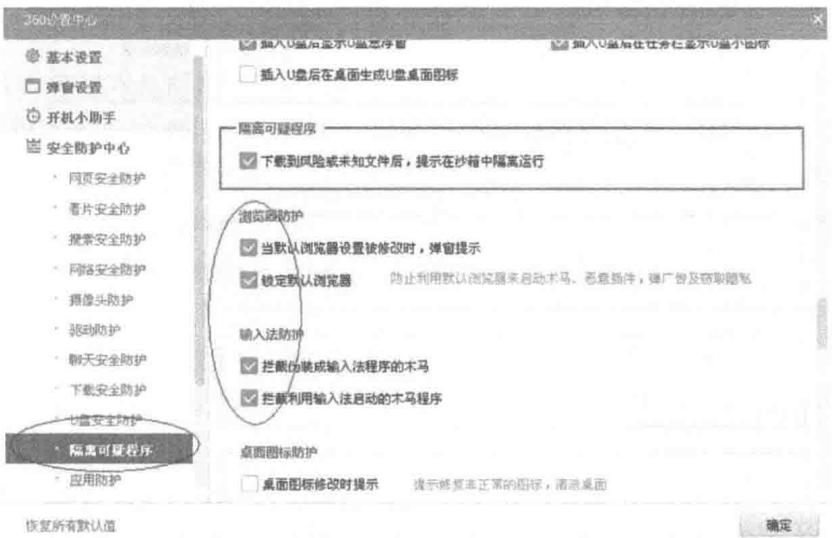

图 9　设置 360 防火墙步骤 5

6）下载安全防护：主要针对其他工具下载文件的检查，见图 10。