Broadview
www.broadview.com.cn

筑墙

只需一点点安全常识 就能阻止网络犯罪

李铁军 著

反病毒工程师12年的一线作战经验

国内第一本写给普通网民的安全科普读物

傅盛 金山网络CEO **倾情**
陈睿 金山网络副总裁 **推荐**

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

筑墙

只需一点点安全常识
就能阻止网络犯罪

李铁军 著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

这是一本写给普通网民的信息安全科普读物。在生活中，我们总会为自己所处的网络环境安全担忧，在网购支付过程中是否被骗、手机上网是否会无端中毒、新兴的二维码扫描是否安全……这些问题一直困扰着大部分普通网民。

本书将以各种生动、真实的案例，教给大家在使用计算机、移动终端的过程中，如何才能防止不被侵犯，安全使用网络。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

筑墙：只需一点点安全常识就能阻止网络犯罪 / 李铁军著. —北京：电子工业出版社，2014.1
ISBN 978-7-121-21909-2

Ⅰ. ①筑… Ⅱ. ①李… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 274701 号

策　　划：张慧敏
责任编辑：徐津平
文字编辑：杨　璐
印　　刷：北京天来印务有限公司
装　　订：北京天来印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：720×1000　1/16　印张：10　字数：134 千字
印　　次：2014 年 1 月第 1 次印刷
印　　数：5000 册　定价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

长年和病毒、木马、钓鱼网站，这些网络黑色产业打交道，深知普通网民在这些专业网络犯罪团伙面前有多脆弱。

最早，那些病毒开发者是以炫耀技术为目的，比如，CIH 病毒就是早期计算机病毒的佼佼者，这个病毒中首次出现了可以破坏主板 BIOS 的数据，让崩溃的 BIOS 初始化系统失败，中招电脑给人的感觉就像主板电路物理损坏，中毒电脑不去送修的话，就无法开机。CIH 病毒还会尝试将硬盘所有物理扇区的数据都用垃圾信息替换掉，以彻底破坏计算机硬盘数据，不过，因为在重写数据的过程中导致系统崩溃，所以硬盘上的大部分数据可以被修复还原。

在蠕虫病毒时代，病毒作者发现一个高危系统漏洞之后，不是像今天这样去入侵大型计算机网络而获利，而是立刻编写一个让网络堵塞、瘫痪的蠕虫病毒，让蠕虫病毒沿着计算机网络快速、自动地复制传播，病毒作者的目的只是为了显示自己有能力让网络瘫痪而已。当然，这种蠕虫攻击会给商业公司及政府机关的网络造成严重的经济损失。比如，国内某次 ARP 网络蠕虫攻击就曾经造成中国大陆多个机场的自动检票系统失灵，并在同一时段，令所有机场陷入混乱。

在 IM 软件未成为流行应用的时候，电子邮件的使用更为普及，邮件蠕虫曾经严重泛滥，甚至出现了 Mydoom 邮件蠕虫和 NetSky 邮件蠕虫的开发者之间的竞赛，两个蠕虫之间相互消灭，竞相传播。在企业电子邮箱充满垃圾邮件，无法提供正常电子邮件服务的时候，病毒的增长戛然而止，竞争结束了，病毒开发者设定了在某个特定时间停止传播病毒。

前面这些是病毒开发者个人英雄主义的时代，病毒开发者高超的开发技巧赢得

了软件工程师的尊敬，普通网民也视病毒开发者为软件天才。

后来，写病毒不再是高深的技巧，制造病毒的门槛在降低，一部分人开始尝试利用病毒获得经济利益，而且这种收益非常惊人，它比许多正当的职业更容易获得商业上的成功。因此，吸引了越来越多的人从事病毒黑色产业。

最典型的灰鸽子木马养活了成千上万的不法分子，用灰鸽子控制上万台肉鸡的组织动不动就对一些网站发起DDoS攻击(拒绝服务攻击，令网站无法提供正常服务)，他们可以轻易得手，可以公开出售DDoS攻击服务：有人愿意花钱购买DDoS服务来攻击商业对手。

一些人利用灰鸽子入侵他人计算机，通过收集商业秘密和个人隐私数据来进行买卖。专业为灰鸽子提供升级加壳免杀服务的程序员也能获得丰厚回报，甚至一些人转型为灰鸽子教师，开班收徒，赚学费也弄到了不少钱。

病毒黑色产业变得越来越专业，分工也越来越清晰，从病毒制造、升级、传播、盗号、洗号、通过第三方游戏交易平台洗钱都有专业的人来干。

杀毒软件和病毒作者展开了激烈的技术竞争，杀毒软件的防御体系不断完善，病毒的破坏和入侵暂时减弱。网民人数多年来成倍增长，未来大概每个人都会成为网民。黑色产业获得成功的机会也在增长，因为大部分新增网民对网络安全缺乏足够的认识。在网络购物成为新时尚后，几年间，没有技术含量的钓鱼网站攻击给网民造成的危害就超过了病毒木马。

以往，一个攻击者可能需要一台电脑去尝试入侵。随身带着笔记本，总显得目标过大。现在，攻击者只需要一部安卓手机就可以办到了。也许，到贵公司前台面试，或者一个电梯工人、快递员，就可能通过装在口袋里的安卓手机干很多事。

现在，以病毒木马、钓鱼网站为首的黑色产业正在非常明显地向移动互联网转移。我们每个人使用的智能手机里，存储的数据已超过早些年的家用电脑。在手机上玩游戏、刷微博、逛淘宝和朋友聊微信、做银行理财。手机对攻击者来说，就是一个宝库。拿走手机里的数据，比小偷入室盗窃的难度小多了。

怎么办？科技的发展改变着我们的生活，难道为了安全就让我们放弃这些，回到过去吗？这怎么可能。把安全托付给安全软件就好了，我才懒得搞明白安全是怎

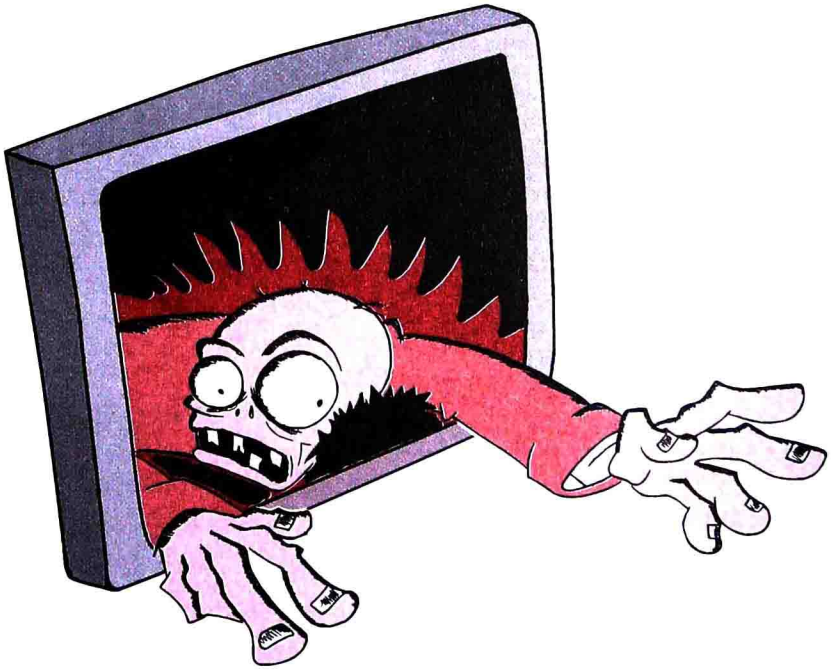
此为试读，需要完整PDF请访问：www.ertongbook.com

么回事。持这个观点的人大错特错了，安全是自己的事，如果你完全托付给安全软件，结果一定会令你失望，因为有许多攻击方法是安全软件不能解决的。比如，有人找你要银行卡号，你想都没想，就交给他了。你说，安全软件能搞定吗？

作为一个杀毒软件工程师，一直有一个梦想：每个人都不再依赖杀毒软件。一台没有安装杀毒软件的计算机，其性能会更好，如果只做正经应用，永远不染病毒的话。如果计算机里没有病毒、没有钓鱼网站，那些聪明的程序员就能做出改变世界的新应用，计算机网络能让人们的生活更美好。

实际上，你是可以做到不依赖杀毒软件的，这并不难。只需要掌握一点点安全常识，就能获得对病毒木马、钓鱼网站的免疫力。如果安全意识再强一点儿，用病毒木马、钓鱼网站来做黑色产业的人，准给饿死。

这是我打算写《筑墙——只需一点点安全常识就能阻止网络犯罪》这本小册子的初衷，不用担心安全的网络会给你带来更多欢乐！



目 录

1 不懂安全的人上网多久会沦陷 /1

曾经有个朋友在微博上问：“不懂安全的人上网多久会沦陷？”，网友的回复五花八门，有人说，可能要一天。也有人说，这要看这个人上网做什么，也许只需要几分钟，这台电脑就不再属于他了。

2 可怕的电脑摄像头 /9

本章给朋友们讲述一类经典的木马：远程控制木马，也有人称之为后门程序。也是迄今为止，最令人恐惧的恶意程序。

3 屠龙刀不见了 /15

网络游戏产业的兴旺成就了一批打钱代练工作室，一些人没日没夜地在虚拟世界创造虚拟财富，再通过专业虚拟物品交易网站将收集的虚拟资产出售变现。有外国媒体给专业打钱工作室起了一个响亮的名号：“金币农夫”。

4 生活将不再美好——吓死人的 PPT/21

图片或 PPT 文档，会不会给电脑制造麻烦呢？当然是会的，恶意软件传播者的确会在图片中捆绑病毒，也会将后门程序隐藏在 Office 文档中，让你打开文档就中毒。

5 密码疑云 /25

亲爱的读者朋友，正式开始本章之前，笔者想提几个问题，你经常访问的网站服务有多少？你是否记得每个服务的登录密码。接下来的内容与每个人的信息安全，甚至人身安全均有密切关系，本章不包含任何晦涩难懂的密码学知识。

6 免费 WiFi，你敢用吗？ /33

要是走在哪里都有免费 WiFi 使用，一定很方便。于是，就有黑客尝试去破解 WiFi 密码，也很容易得手。如果你碰巧还在使用比较古老的无线路由器，你的无线路由器就可能被黑客破解。

7 厌恶排队，把银行柜台搬回家 /39

网民真的可以轻易使用网上银行吗？有担心网银的安全问题吗？这就是本章需要讨论的内容。

8 网购达人是怎样炼成的 /51

据《31 次中国互联网络发展状况统计报告》提供的数据，截至 2012 年 12 月底，我国网购用户规模已达 2.42 亿人，比 2011 年增长了 24.8%。有过网购经验的网民占到 42.9%，也就是将近一半的网民尝试过在线购物。

9 先生，有你的包裹 /63

什么是电信诈骗呢？这仍然多多少少与网购有关。

10 最爱你的人伤你却最深 /69

本章还是从一类最常见的诈骗案例开始，这个案例源于微博的真实诈骗。“儿子”表示有机会出国留学，通过手机 QQ 和老爸联系需要一笔钱。

11 拜托，只想早点回家 /77

火车票预订，大部分人会选择 12306 订票网站，但是，总有些钓鱼网站会伪造成火车票订票网站，他们会留下联系电话，欺骗想回家的人拨打电话。

12 智能手机需要安全软件吗 /85

据国内安全厂商统计，安卓手机病毒呈现高速增长态势。2013 年第 2 季度末共收集安卓病毒样本 800 万个，较第 1 季度末的 500 万个增长 60%。2013 年第 1 季度又是 2012 年全年的 3.2 倍，2012 年又是 2011 年的 7.6 倍。

13 关于手机支付的安全问题 /95

本部分内容不针对任何第三方，相反，笔者一直是手机购物、手机支付的支持者。本章的内容志在帮助手机用户在享受手机支付、手机购物的同时，保障资金安全。

14 无线路由器与安全 /105

在本章的最后，一定给使用路由器接入的朋友一个建议：重新设定路由器的用户名和登录密码，不再使用默认值，这样攻击者就不会轻易得手了。

15 没文化的小偷惨了 /111

当你的手机被盗，在手机有锁屏密码的情况下，小偷尝试解锁手机失败时，安全软件会自动使用手机的前置摄像头连续拍照，再将照片上传到服务器或发送指定邮箱。

16 微信支付与代打飞机 /119

在 PC 互联网的时代，QQ 号是事实上的网络通行证。在网络世界，QQ 号就如现实生活中经常要用到的身份证一样重要。很可惜的是，不少网民并不像保管身份证一样在意 QQ 号的安全。

17 小游戏也有大阴谋 /125

在我们购买的手机中，一般内置了若干个安卓应用商店的客户端。只要把手机接入网络（WiFi、3G、数据），就能很方便地在这些市场上挑选自己感兴趣的软件来安装。国内的安卓软件市场鱼目混杂，各种山寨应用、盗版游戏充斥其中。

18 窃听风暴：手机后门对你了如指掌 /131

出于满足某些需要，一些人试图对密切监视自己的亲人、上司、客户或商业竞争对手。以往，要达到这个目的，可能需要雇佣私家侦探，或者非法购买一些所谓的间谍窃听装置。现在，随着智能手机的普及，监听他人行踪变得异常简单。只要将一些手机监听软件安装在别人手机上，就可以对监视目标的一切了如指掌。

19 ROOT？越狱？有必要吗 /139

经常有网友会问，我买了一部安卓智能手机，有朋友说 ROOT 之后会更好用，也有人告诉我千万别 ROOT，我不知道什么叫 ROOT，我该怎么选择呢？好，今天我们要讨论的，就是一个非常关键的话题，手机 ROOT。

20 二维码真的一扫就中毒吗 /145

仅仅一个扫码动作，是不会造成恶意软件运行的。至少到目前为止，安卓系统还没有暴露出类似漏洞可以实现扫码后立即自动下载自动运行有害程序。而用户完成软件下载之后，就只能寄希望于安全软件了。

此为试读，需要完整PDF请访问：www.ertongbook.com

1

不懂安全的人
上网多久会沦陷

不懂安全的人上网多久会沦陷

曾经有个朋友在微博上问：“不懂安全的人上网多久会沦陷？”，网友的回复五花八门，有人说，可能要一天。也有人说，这要看这个人上网做什么，也许只需要几分钟，这台电脑就不再属于他了。

在回答这个问题前，让我们先看看普通网民的电脑有什么情况吧。

一台崭新的电脑系统大概来自这几种不同渠道：第一类渠道是电脑城或网上电子商城购买的品牌机或笔记本电脑，新买的电脑已经预装了 Windows 7、Windows 8；第二类渠道是在朋友或电脑城装机商的帮助下购买的兼容机，预装了盗版的 Windows 系统（操作系统可能是 Win XP、Win 7、Win 8 的任一版本）；第三类是其他情况，比如公司的 IT 部门统一配置的系统，或者，一些比较懂系统管理的网民自己 DIY 配置的电脑系统。

在这些电脑上除了预装的 Windows，一些最常用的软件，比如聊天工具、办公软件、下载工具、视频播放软件等也多半预装在里面。在春节放假去亲戚朋友家看到，每个家庭都会用电脑上网看电影、聊天、打游戏。这些电脑几乎 7×24 小时连接在互联网上，不联网独立运行的电脑一台也没有看到。

由于这些电脑只要打开电源就时刻连接在互联网上，在搞网络安全的人看来，这些电脑就存在被不明攻击者入侵的可能。这些电脑非常容易被入侵的一个关键因素在于使用了盗版的 Windows 系统。

盗版 Windows、安全漏洞与病毒入侵

不久前，看到过一个有争议的资料，国外某些研究机构报告说，中国软件行业盗版率有 80% 之多。笔者就有不少朋友不习惯电脑里预装的 Windows 7，在小区找电脑维修人员将正版操作系统换成了盗版 Windows XP。

互联网上每天都有一些攻击者在四处漫游，他们喜欢使用一些黑客工具对互联网的某段 IP 进行随机的扫描侦察，当他们发现某处存在防御弱点时，便会伺机入侵。这就好比有形迹可疑的人在社区漫无目的地闲逛，当他发现某户人家门窗没关好时，就可能尝试入室盗窃。大量盗版的 Windows XP，就像没有关好门窗的房间，随时有被入侵的可能。

不光 Windows、Office 这种软件存在漏洞时可能导致电脑被入侵，当一个软件普及程序很高时，比如杀毒软件、下载工具软件、聊天工具、视频播放软件、输入法软件、浏览器软件，如果这些软件存在安全漏洞，就会被入侵者利用。

经常有黑客高手试图挖掘这些软件的漏洞，正义的黑客会及时把发现的漏洞通知给软件开发商，要求软件开发商尽快修补。而另一类黑客则会迅速利用不为人知的软件漏洞大肆入侵，控制成千上万台电脑组成僵尸网络，或者把漏洞信息高价出售给另一群攻击者。

黑客远程入侵与蠕虫病毒爆发

历史上曾经有多款国外杀毒软件的系统漏洞被小范围披露，黑客针对这些漏洞开发出批量抓鸡工具（就是简单扫描实现大批量入侵的攻击程序）。运行这些攻击工具，可以在很短的时间内实现批量入侵。

现在，你的电脑中毒可能和你本地的操作一点关系也没有。黑客可以在数千里之外，将木马后门程序植入那些存在安全漏洞的电脑里，从而完全控制这些电脑的资源。有许多普通人刚配置好的个人电脑就是这样被入侵的。

一些资深老网民可能记得这种经历：电脑开机没多久，屏幕上就弹出一个对话框，RPC 服务中止，Windows 将在 60 秒内重启。重启之后，再次重复这一过程。这就是大名鼎鼎的冲击波蠕虫病毒自动攻击联网的 Windows 电脑系统漏洞造成的结果。

2003 年，据楚天都市报报道，武汉政府网与武汉经济信息网 7 月 23 日突然瘫痪，与其链接的市党政机关群 82 家单位办公受到严重影响。相关技术人员查明，入侵病毒是一种变异的蠕虫病毒，身份无法确定但其性质与美国电影《黑客帝国 2》中的“史密斯”病毒极为相似，可大量进行自我复制，以堵塞网络通道。

据悉，病毒入侵现象在 22 日下午 4 时许已零星出现，大规模入侵于 23 日凌晨爆发。记者 23 日上午 8 时至 9 时数次尝试登录两网站，未果。事发后，该中心立即组织技术人员连夜清除病毒，但该病毒也同时在三镇多个地区出现。

武汉市信息中心负责人接受记者采访时表示：种种迹象表明，此次病毒入侵很可能是黑客入侵且人数众多，有关人员正在核实并追查源头。据了解，因武汉经济信息网站主要是提供商业服务信息，所以不排除有商业竞争对手恶意破坏。而该中心一位工作人员透露，此前，曾有人冒充应聘人员混入中心，并对中心人员有过此类威胁。

几天后，中新网 7 月 27 日电，武汉市公安局网监处 26 日证实：武汉政务网此前一度瘫痪是防毒措施不健全，被病毒侵入所致，与传闻的黑客入侵无关。

网警调查后发现，自 22 日下午 4 时起，该网站遭到 MS-SQL 蠕虫病毒入侵，由于防毒措施不健全，与其链接的有关委办局及区级政府安装的 MS-SQL 2000 数据库服务器未安装补丁程序，导致部分网络上的服务器感染病毒，并相互传播，产生大量无用信息包（垃圾访问包）访问政务网防火墙，半小时内就达 2 亿多个，阻塞了武汉政务网与互联网之间的通道，使用户无法正常访问。

上面这个看起来惊心动魄的攻击案例，就是运行在 Windows 系统上的 SQL Server 服务器软件未打补丁造成的。比起黑客的随机扫描行为，蠕虫病毒就像一头被激怒了的莽撞的大象，在互联网上一路狂奔，随机闯入防守脆弱的网络，然后造成严重的破坏。

当年的 SQL 蠕虫王曾经取得辉煌的攻击成果：

1．美国花旗银行的 13000 个自动柜员机（ATM）中的多数不能处理客户的交割业务；

2．泰国、日本、韩国、马来西亚、菲律宾和印度都发生了网络堵塞，导致网络速度缓慢；

3．日本广播协会 NHK 电视报道，严重的网络堵塞使日本部分互联网连接发生瘫痪；

4．在韩国，几百万互联网用户因大韩电信和南韩电信指挥传输的电脑无法运作而受影响；

5．在中国，信息产业部新闻处和国家计算机中心有关人士证实，北京、上海、四川、广东等大部分省市的网络不同程度地发生故障；

6．蠕虫病毒发作 5 天后，英国的市场调查机构估计，全世界范围内因此造成的直接经济损失达到 12 亿美元。

近年来，蠕虫病毒的爆发机会越来越少，成为几乎被人遗忘的病毒。其中一个非常重要的原因在于正版的 Windows 操作系统中，已经集成了性能优良的 Windows 防火墙。Windows 防火墙有效地阻止了蠕虫病毒发送的攻击数据包，避免了网络堵塞，使蠕虫病毒的传播被阻止。

在一些盗版 Windows 操作系统中，盗版商竟然默认关闭了这个重要的防御工具，那些自以为是的盗版软件发行者认为 Windows 防火墙的性能不佳。而且，随着盗版组织商业模式的变化，这些人还会蓄意给盗版 Windows 留下后门，比如给所有安装这个盗版系统的用户分配相同的用户名和空密码，盗版组织在用 Ghost 灌装的盗版 Windows 中预装商业软件来获利。

现在，安全厂商观察到的蠕虫病毒已经和以往大不相同，随着社交网络的广泛使用，利用社交网站的安全漏洞传播恶意程序或者钓鱼网站成为一种新型攻击——XSS 蠕虫。

在 Twitter 和新浪微博，都曾经多次遭遇黑客恶搞，攻击者发现微博程序存在 XSS 漏洞（一种跨网络域的漏洞攻击），攻击者制作了一个特别的攻击页面，通过微博评论将攻击网址发送出去欺骗其他网民点击。点击之后，立刻被攻击成功，所幸这个利用 XSS 漏洞攻击的黑客并无恶意，中招微博用户只会关注这个攻击者账号，并自动转发一条带攻击链接的微博。于是，在短短的 1 小时左右，新浪微博就有数万网民遭到攻击。这就是新型 XSS 蠕虫的形态之一，攻击者可以将攻击链接设定为钓鱼网站，或者通过 XSS 攻击传播病毒下载链接，攻击者能制造和冲击波蠕虫病毒类似的轰动效应，可能导致非常严重的信息安全事件。

另外，国内安全厂商金山毒霸还发现有攻击者利用 QQ 群空间来制造蠕虫病毒。病毒作用利用 QQ 的快速登录功能，自动在后台登录 QQ 群，将病毒程序文件副本上传到中毒用户的所有 QQ 群中，由于 QQ 群共享文件具有自动分享的能力。QQ 群的成

员会看到一个新文件被分享了，病毒可能伪装成一部热门的电影视频或者一个搞笑的图片来欺骗其他人点击。如果有人双击打开病毒上传到QQ群共享空间的恶意程序，便会立刻中毒，新感染的病毒再将自身上传到若干个新的QQ群空间，这类新蠕虫病毒就能在非常短的时间内迅速通过QQ群实现传播。

本章总结

现在，聪明的读者大概知道本章问题的答案了：不懂安全的人上网，电脑沦陷的时间最短可以只是几分钟。

在移动互联网日益风行的今天，蠕虫病毒会重新在手机上泛滥吗？暂时还没看到，因为现在的攻击者，其攻击目的不是制造网络瘫痪，而是直接牟取经济利益。发起大规模攻击的可能性仍然存在，如果某款普及率很高的应用软件被发现存在严重安全漏洞，蠕虫病毒就可能在一夜之间卷土重来。

网民该如何防御这种攻击呢？其实这并不难，不是安全专家，也可以有效防御电脑被攻击。

第一，建议网民使用正版操作系统，如果你买的品牌机、笔记本已经预装了正版Windows，那就充分使用它，别把正版的格式化，再装一个盗版的系统。预装的系统已由专业人员配置了防火墙系统，在出厂之前，一些Windows安全漏洞已经修补妥当，被入侵的可能性相对较低。

第二，如果不得不使用盗版Windows，联网前先在控制面板中启用Windows防火墙，联网后，第一时间使用Windows Update描述安装系统补丁。笔者曾经看到不少朋友在Windows提示需要下载安装补丁时，总是去点“否”，不由得为他们的安全捏把汗。看完这篇文章的朋友，你是不会这样做的，对吧？

第三，关注一些与信息安全有关的新闻，当安全厂商发布重大警报时，早做防范，避免自己的电脑成为牺牲品。

第四，对于QQ群中出现的新鲜事件，收敛一下好奇心，避免打开未知的可疑程序而中毒。记住，任何一个不清楚其用途的可执行程序，都不要轻易双击它。在杀毒软件报告可能有危险时，应按提示停止运行。

此为试读，需要完整PDF请访问：www.ertongbook.com