FOURTH EDITION

iParenting Media WINNER Award

家庭在线安全指南

作者：Marian Merritt

STOP | THINK | CONNECT™

Norton by Symantec

Marian Merritt

引言

我先生和我膝下育有三个可爱的子女，这三个子女都是我们家电脑的常客。孩子们时常挑战我对技术以及技术如何融入他们生活的认识和看法。我懂得互联网所带来的欢乐和危险。而当孩子们在网上打开自己的一片天地，不拘是寻觅新的游戏网站，下载音乐，还是通过自己的社交网络及文字聊天方式与朋友们交流，我恍然意识到关键在于要了解并时时关注我们的子女在做些什么。

我们都在设法管控我们子女越来越强的独立性，并尽我们所能为他们以及我们的电脑防范来自互联网的诸多严重危险。在这篇简短的指南中，我们将逐一了解那些最令人顾虑的互联网问题，但倘若您有兴趣进一步探究，我也将推荐一些网站和刊物，供您用来及时了解这方面的每日最新动态。您对这一主题感兴趣并愿意了解更多相关信息，实在是一件值得恭喜的事情。最让我心灰意冷的事情莫过于，家长们两手一摊，张口说道："这方面我孩子比我懂得多！" 您可以学到足够的知识，这样在需要求助于安全方面的专业人员和软件来平息事态时，自己也能够有所帮助并了解情况。

因此，无论您关心的是正在学习使用搜索引擎的小学年龄段子女，还是如何管控中学年龄段子女对社交网站日益严重的依赖，这些问题都在我们将要讨论的范围之内，我们将就每个主题为您提供一些易懂的提示和指南。*加油！*

Marian Merritt

作家、家长、诺顿互联网安全代言人

目录

家庭在线安全指南

第四版

从小到大

学龄前儿童（3-4 岁） 6
小学年龄段儿童（5-7 岁） 6
介于童年中期与青少年期之间的儿童（8-12 岁） 8
青少年（13-17 岁） 11
大学及更高年龄段子女 14
进行“光说不干”交流。 15

基础知识

网络犯罪是实实在在的犯罪 20
病毒、蠕虫和间谍软件 20
欺诈软件 22
点击劫持 22
Bot 真来了... 23
隐私信息和身份盗用 24
人际问题 25
网络欺凌和网络盯梢 25
保护您的密码 27
互联网猥亵者 29
性短信 30
安全浏览 31
保护无线网络 31
家长控制软件 32

风险

剽窃与作弊 34
文件共享、音乐和视频下载 34
社交网站 35
色情、赌博、种族主义、厌食和仇恨站点 37
数字声誉 38
青少年在线隐私保护 38
电子邮件 39
即时消息 40
手机安全 41
移动设备的安全 42
博客 43
数码照片与隐私 44
网上购物 45
网上和移动银行业务与帐单支付 46
在线打游戏和上瘾迹象 47
停下，思考，连接 47

重要提示

对成年人的重要提示 48
对孩子的重要提示 49

结束语

资源 50
其他务必了解的互联网安全资源 51

制造商资源：诺顿安全产品 52

Marian Merritt 54

从小到大

学龄前儿童（3-4 岁）

自从触摸屏智能手机和平板电脑问世以来，还未离开婴儿椅的儿童也可以轻松接触到技术。这并不意味着，在享受欢乐和享用教育应用程序的同时，风险没有随之而来。请注意您的小孩所用的程序。是否有广告出现？他们会不会单击一下按钮就购买了需要付出真金白银的加载项？如果他们按错了图标，他们是否会看到不良图像或播放包含不雅歌词的音乐？请使用家长控制设置，并密切注意您分给最小孩子的设备。还要防范这些设备被顺手牵羊，并使用屏幕保护膜和加垫外壳防止意外事故发生。

小学年龄段儿童（5-7 岁）

这是如今很多儿童开始接触互联网的年龄段。由于美国越来越多的学校设有电脑实验室并在教室内配备了 PC、Mac 或平板电脑，因此儿童对电脑的首次使用可能发生在学校里。其他一些儿童则是在父母或哥哥姐姐的引导下，在家里首次获得电脑使用体验的。5-9 岁的儿童平均每天花在网上的时间为 29 分钟。[1]

诸如 NickJr 和 Webkinz 之类的网站（常常包含在线游戏）吸引着最小的上网儿童们，甚至尚处在蹒跚学步年龄段的儿童也难抵其诱惑。有些网站几乎成了入门级的社交网络站点，因为它们提供了聊天及其他通信功能。幼儿家长起初应关闭这些功能。像 Webkinz 这样的领先站点之所以能流行起来，是因为它们为提供一个安全的环境付出了额外的努力，注意到这一点是十分有益的。在 Webkinz 营造的小世界内，家长们无需为幼儿“关闭”聊天工具，因为它们提供了一种双管齐下的方法。Kinz 聊天工具的脚本是完全预先编写好的，尽可放心地让儿童使用它来发送音符等内容、与小朋友们“聊天”。通过它来介绍聊天概念并开始讨论“网上礼仪”及安全做法， 再好不过。Kinz 聊天工具增强版是可监控的聊天工具，认为孩子已足够成熟的家长们依然不能在准予许可方面有所放松，并且始终都可以撤消许可。

1. http://joanganzcooneycenter.org/upload_kits/jgcc_alwaysconnected.pdf

要确保您的幼儿明白，即使他们是在自己钟爱的游戏或俱乐部站点的友好界面中操作，您也要限制他们的在线聊天。经过一段时间后，您就可以介绍与他们认识的人（例如叔叔、阿姨或小朋友们）进行聊天的概念——在此过程中一定要强化他们应经您同意后再在网上与任何新认识的人聊天的意识。

理想情况下，当孩子们处于这一年龄段时，您应向参与他们的家庭作业那样积极参与他们的在线活动。例如，在厨房、小房间或起居室等公共空间，您应确保孩子使用的电脑或设备在您的视线范围内。请谨记，随着我们越来越多地使用移动设备来访问互联网，单单设法监控一台静止不动的电脑已经不够了。家长控制软件可以帮助您限制当您不在孩子身边时他们可以访问的站点，或者他们使用藏在背包和卧室内的设备可以访问的站点。它所提供的控制功能还可以限制您不希望孩子透露的任何信息，不管是他们的名字、年龄、电话号码还是其他隐私信息，都可以进行限制。您应打开电脑搜索引擎中的所有过滤和安全功能（例如谷歌安全搜索™功能），以防幼儿在做家庭作业时无意中进入成人站点或其他不良站点。一定要向孩子演示如何关闭浏览器窗口，并告诉他们：如果出现什么奇奇怪怪或让人心烦的画面，完全可以关闭站点。告诉他们，除非您在场，否则千万不要在这些站点进行聊天、键入消息或向任何人透露信息。

热心提示：要告诫最小的孩子千万不要透露密码，哪怕是向他们最亲密的小朋友也不能透露！ 对于发生在幼儿园小朋友身上的帐户盗用（初级版的身份盗用）事件，我们已经屡见不鲜。

主要建议：

- 使用家长控制功能来限制网站和上网时长。
- 设置浏览器、会员和社交网站的高安全性和隐私设置。
- 在所有设备上均安装并维护互联网安全软件。
- 监控孩子的屏幕使用情况，当他们在线时，尽可能多地坐在一旁监视。
- 告诉他们要保护隐私信息（姓名、电话号码等），千万不要向朋友泄露密码。
- 开始在平时为孩子“返校”做准备的过程中进行“光说不干”交流（见第 15 页）。

介于童年中期与青少年期之间的儿童（8-12 岁）

介于童年中期与青少年期之间的儿童在电脑使用方面远比前一个年龄段的儿童更具社交性和冒险性。他们会与学校里的同龄人进行交流，从而了解到最新潮、“最炫酷”的站点。他们会注册自己的第一个电子邮件和即时消息帐户。请向自己的孩子询问这些帐户的情况以及密码是什么，以便您可以监控他们的活动，并了解他们目前都与哪些人进行交流。这个年龄段的儿童可能也开始光顾年龄大一些的青少年以及成年人所青睐的社交网站。美国《消费者报告》所开展的一项研究估计，有 560 万未成年孩子在使用 Facebook。[2] 这个年龄段的大多数儿童都到稍微年长一些时才会创建帐户（可以开始创建帐户的法定年龄通常为 13 岁），但他们会访问有自己的页面和个人资料的朋友、哥哥姐姐及其他亲属的页面和帖子。如果您的少儿还未到批准年龄就创建了一个社交网络，那么相应公司发现后会将他们的帐户删除。

这个年龄段的有些儿童会使用照片共享和博客网站，作为一种初级版的社交网络。您可能并未意识到他们可以使用这些应用程序发帖、发表评论并在好友圈中进行分享。对您的孩子访问的所有站点都要多加留意，特别是那些占用了他们大部分时间的站点。不可想当然地认为在他们泡在照片共享站点上仅仅是因为萌生了对数码摄影的兴趣！

2. http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm#How_children_fare_on_Facebook

热心提示：使用 Norton™ Family 监控创建和使用社交网络帐户的行为。您甚至可以看到孩子宣称自己有多大。

介于童年中期与青少年期之间的儿童还对音乐感兴趣，而通过互联网则可以轻松地收听、找到和下载新的曲目，还可以结识在音乐方面兴趣相投的其他人。他们可能会访问自己钟爱的乐团或明星的博客或网站，从而关注这些人的新闻；光顾不同的站点了解最新的八卦并获得可供下载的照片；抑或加入 Twitter 订阅。

在线视频站点目前极为流行。有些视频包含粗野的脏话或暴力内容，因此您需要仔细监控这个年龄段孩子的访问情况。还要提醒他们不要单击视频评论中的链接，否则可能会打开有危险或不良的站点。这个年龄段创造力较好的儿童则可以学会如何拍摄自己的数码照片、编辑视频并与朋友和家人分享自己的得意之作。在您或更有经验的朋友的帮助下，他们也开始在线发布自己的作品。

热心提示：检查浏览器的历史记录，了解孩子们访问的网站以及访问这些网站的频繁程度。Norton Family 可以帮助您监控网络活动，并防止孩子试图从历史记录中删除访问记录。

主要建议：

- 在所有电脑和移动设备上都设置密码，特别是手机。
- 经常检查电脑的互联网历史记录（或家长控制软件的历史记录）以了解孩子们访问过的站点，并监控他们的电子邮件和即时消息 (IM) 帐户以了解他们在与哪些人交流。注意：如果您的孩子已经使用了手机、社交网络、照片共享服务或博客服务，那么他们可能会通过这些媒介而非传统的电子邮件进行交流。
- 制定有关在线通信、非法下载和网络欺凌的规则。
- 应让他们知道千万不要单击电子邮件或 IM 中的链接——这是人们感染病毒或向不法分子泄露隐私信息和有价值信息的常见方式。
- 讨论有关发布与共享隐私信息、视频和照片的风险和顾虑。
- 留意是否有对某些在线行为产生迷恋或上瘾的迹象（见第 47 页上的“在线打游戏和上瘾迹象”）。
- 将电脑和手机放在家中显眼的位置。
- 培养坦诚交流的习惯，鼓励孩子向您诉说网上是否有任何东西让他们感到不安。
- 开始进行“光说不干”交流（见第 15 页）。

青少年（13-17 岁）

进入青少年阶段，他们会形成更高的独立性，这在他们的在线生活中会体现出来。这种独立性也带来了更大的责任，包括要更加仔细地管控他们的在线生活。但如今大多数青少年都在社交网络上创建了至少一个甚至多个帐户。有些孩子很容易将自己的父母加为好友，而有些则极力抗拒与父母进行在线联系。还有一些青少年则创建“虚假”个人资料用来将父母和家人加为好友并与他们联系，同时使用另一个帐户来从事真实、更值得调查的行为。利用像 Norton Family 这样的程序，家长就可以识破这种花招。

那么社交网络以及青少年在网上感兴趣的其他一些方面究竟有怎样难以抗拒的诱惑呢？通过网名、成员身份、博客、个人资料以及他们日常访问的其他一些互联网内容，青少年们可以相互之间交流自己生活的点点滴滴。他们的所思所想，在网络上到处都可以留下数字痕迹。他们往往并不知道（或者已经忘了）自己在网络上发布的一切所有人都能看到，而且可能会无限期地存留在那里。五年、十年甚至二十年后，潜在室友、浪漫情人、高校招生办职员或潜在雇主只需在网络上搜索一下，您孩子的所有照片、观点和想法可能就会永远呈现在大家面前。越早开始管理您的数字声誉，对您就越有利（见第 38 页）。

我们需要教会我们的孩子如何在冒险的同时不会深陷麻烦。这跟他们要先上驾校学习、然后才能驾车上路是一个道理。在您所上的所有那些游泳课中，您必须坐在游泳池旁边耐心听讲，也是这个道理。对于互联网，也需要有同样谨慎的态度。诚然，当您试着向您的孩子解释上网时的“交通规则”时，这些青少年可能会不屑一顾。因此，您可能会改而与他们就读的学校商议通过很多愿意提供这方面培训的组织来引入互联网安全演讲。例如，当地 D.A.R.E. 官员、地方检察官办公室、iKeepSafe、i-SAFE 等便属于此类组织。青少年所获的一些最出色的在线安全教育可能来自于接受过正确培训的同龄人。因此，请鼓励您孩子就读的学校请高年级学生参与辅导低年级学生如何掌控自己的数字声誉、在网上善待他人以及其他一些关键课程。您可能会发现，同样的信息如果由家人以外的人员提供，孩子们实际上会更加关注。此外，不要忘了面向家长和教师也安排一次类似的演讲。我们都有太多需要学习的地方！

热心提示：在网络上搜索一下您的孩子们，然后让他们看看您找到的结果。或者以自己作为反面典型搜索一下您自己，并坦承面对您找到的任何不雅内容。毕竟，您的孩子可能已经在谷歌上搜索过您了！ 您也可以设置谷歌或雅虎警报。

热心提示：在社交网络上与孩子成为好友的家长，不应对自己孩子的帖子或新闻订阅发表评论。应保持私下交流。

主要建议：

- 强化关于保持适宜得体在线行为（语言、隐私信息和影像、网络道德规范、非法下载、限制使用小时数以及避开不良成人站点）的规则。
- 了解您孩子的在线生活（社交网站、照片、隐私信息、俱乐部和体育活动），不管是他们在自己站点上的活动，在好友站点上的举动还是在他们学校网页上的行为，都要了解。
- 检查您孩子访问的站点；不要害怕讨论令您不悦或让您担忧的站点，必要时可以限制这类站点。
- 需谨记，您的孩子会在家里、在学校、在朋友家里、在图书馆、通过手机甚至使用游戏机来访问互联网——因此需要与他们交流他们在所有这些情况下的活动。
- 与您的孩子讨论有关性短信的隐私问题（见第 30 页）。性短信是年龄较大的青少年在恋爱关系中最经常发生的行为，被很多年轻人视作一项正常活动。
- 要求他们在未经您许可的情况下不要下载文件（音乐、游戏、屏幕保护程序、手机铃声）或进行财务交易。
- 告诫他们千万不要透露密码，并且当使用共用或公共电脑或者他们认为可能不安全的电脑时在键入隐私信息方面要小心谨慎。他们应始终处于已从帐户注销状态，即使是在家里时也是如此。
- 告诫他们知道千万不要单击电子邮件或 IM 中的链接——这是人们感染病毒或向不法分子泄露隐私信息和有价值信息的常见方式。
- 只要有可能，就应将电脑和手机放在家里的公共区域，而不是放在您孩子的卧室内。至少应让您的孩子夜间在卧室外给手机充电，以免深夜他们禁不住诱惑使用手机，从而影响他们的睡眠。
- 培养坦诚交流的习惯，鼓励孩子在网上有东西让他们感到不安时向您诉说。请谨记，他们虽然已是青少年，但仍然只是孩子。
- 提醒您的孩子要负责使互联网安全软件始终得到维护并保持最新状态，从而达到可以保护他们以及您的地步。
- 进行“光说不干”交流，并且一定要让您的孩子教您一些有关互联网的新事物（见第 15 页）。

大学及更高年龄段子女

随着青少年逐渐长大并出去闯荡，不管是外出求学还是工作，他们都将需要了解在网上世界需要承担起的更多成年人责任。这包括保护他们的隐私，特别是他们的社会安全号 (SSN) 和财务信息；防范身份盗用；以及与他们的信用记录相关的风险，这对于一个年轻人来说尤为重要。如果您的孩子在大学或新的工作中使用笔记本电脑，需确保他们了解使用无线连接所带来的额外风险，并确保他们购买了包括可靠备份解决方案在内的必要安全软件。他们可能想要省去这些选配件，但事关他们笔记本电脑的安全，因此最好坚决要求他们保持警惕。

热心提示：检查您的诺顿帐户 (www.mynortonaccount.com/amsweb/changeLang.do?langCode=CS)，了解您家里的安全软件能否安装到其他电脑上。其中一些诺顿安全套件允许在同一个家庭内的电脑及其他设备上安装多次。

如果您的孩子是要外出去上大学，需了解这所大学里采取的具体电脑政策。有些学校要求新生采用特定的操作系统或软件配置，因此最好先了解清楚这些信息，再去电脑商店购买电脑。有些教室和学生宿舍配置了无线技术（通常称作 WiFi），因此您将需要确保您购买了合适的 WiFi 卡，以便您的准大学生子女将能够享用这些服务。

热心提示：可以通过语音 IP 电话 (VOIP) 与您已长大成人的孩子们保持联络。可使用由 Skype 提供的或您最喜欢的社交网络内的免费语音和视频聊天服务。

进行“光说不干”交流

“不知者不受害。” 就您的孩子以及他们在网上的所做作为而言，您实际上并不信奉这一信条。但我们当中的很多人却表现得像对互联网上存在的种种危险视而不见一样。如果您跟大多数家长一样，不是互联网专家，甚至还不如您的孩子们上网熟练， 这也没有关系。事实上，不需要成为专家也可帮助您的孩子们安全享用互联网。您只需要与您的孩子讨论他们在互联网上都做些什么，并解释您的家庭使用规则即可。然后不厌其烦地反复讨论这一话题，直到您认为已足以让他们明白您告诉他们的这些规则的重要性为止。

我就直截了当地说吧：想让您的孩子坦诚告诉您他们的互联网体验，并非易事。全球有五分之一的儿童承认他们在互联网上的活动是他们的家长不会同意的。但是，全球有 62% 的孩子们已经有了负面的在线体验。[3] 如果您不问，您的孩子可能就不会告诉您实情——所以现在问，正当时！

3. 根据诺顿家庭报告：http://us.norton.com/norton-online-family-report/promo

虽然所有家长中有一半的家长称他们就互联网安全与自己的孩子进行了交流，但通常都只是交流一次就了事，而在交流过程中也只是提供了以下两点意见：“网上的人不一定就是他们所标榜的自己”以及“要远离网上的陌生人”。孩子们担心，如果他们告诉您自己在上网时犯下的错误，家长的反应将是没收他们的电脑、断开他们的互联网连接、不再让他们与朋友们接触，以及不再让他们与外面的世界联系。他们认为爸爸妈妈对网上的世界根本就不“明白”。

不过，在诺顿，我们通过在全球范围内对家长和孩子们进行调研已得出结论：孩子们希望自己的家长对互联网有更多的了解。他们也极为愿意与自己的家长讨论网络。这令人十分欣慰。

那么现在您已经知道您的孩子们愿意与您进行交流，您也意识到自己需要更多地了解他们在做些什么，您该如何着手呢？您如何与孩子们联系才能使他们与您坦诚相见？您如何避免对您可能听到的事情指手画脚、反应过激或惊慌失措？您如何营造一个交流式、非对抗性的讨论氛围，使你们之间的讨论极富成效，以便您可以反复开展这项活动，而不会导致孩子们捂着耳朵全然不听？

我想介绍一个老词新解式的概念：“光说不干”。我建议立即与您的孩子讨论他们的在线活动，然后定期反复讨论。您孩子的在线活动会不断地变化。随着他们逐渐长大，他们会访问不同的网站，尝试新的活动，并创建新的社交网络帐户。比如，不久前所有人还都在讨论电子邮件； 而如今，他们都在自己的社交网络中使用内置的消息传送工具或者在自己的手机上使用文本消息来进行沟通。随着孩子们越长越大，他们对隐私保护的需求将与日俱增，同时他们所冒的在线风险可能也会增加。青少年在正常的成熟过程中，会不可避免地冒些风险。但身为家长，您有责任设定好界限，以便这些风险不会破坏您孩子的声誉或他们的未来。您须知道，这些界限可能也会时不时地被触碰或越过。

对于“光说不干”交流，需要重点探讨五个问题。这些问题应该对所有年龄段的孩子都适用，不过您将需要对内容进行调整以适合具体的年龄段。一定要给您的孩子留出一定的空间（既包括物理空间又包括时间余地）来问答您提出的这些问题。就我个人而言，我喜欢在车里与我的孩子们进行这些讨论（由于某种原因，当所有人都在看着前方的路时，孩子们似乎更容易向他们的父母敞开心扉）。

1. **你的朋友们在网上都做些什么啊？**这个问题会将注意力从您孩子的身上转移到他/她的圈子一般进行的在线活动。最好以中立、无针对性的原则开始讨论并在讨论过程中坚持这种原则。如果希望自己的子女坦诚地向您反映情况，您就必须让他们确信您在听到他们的回答后不会惩罚他们。您将开始听到诸如打游戏、聊天、建立社交网络等活动，甚至还会听到家庭作业和调研活动。

2. **现在有哪些最酷或最新潮的网站和应用程序？**让您的孩子告诉您为什么这些站点和程序很酷。您也可以问问哪些网站和程序不再流行以及原因是什么。

3. **能不能给我看看你最喜欢的东西？**没错，我希望您从异常繁忙的生活中抽出 20 分钟时间看看从雪山上滑下的企鹅，或您孩子心目中挥舞着剑、有着榔头发型的武士阿凡达。问一问他们如何设置安全或隐私设置（在屏幕顶端和底端找一下相应站点的这些区域）。或许您也禁不住诱惑与他们一起玩，并建立您自己的帐户。（如果您这样做了，一定要让孩子知道）。问问孩子他们如何使用这个站点以及为什么这类站点比其他站点更受青睐。

4. **你有没有听过“网络欺凌”，你在上网时是否曾遇到过？**您的孩子可能并不知道“网络欺凌”这个术语，但他或她知道这是怎么回事并有所体会。有些孩子将网络欺凌称作“戏剧性事件”或“开个玩笑而已”。讲一件您通过新闻报道读到或看到的下流电子邮件、尴尬照片或向其他孩子们透露或传遍的个人信息。问问他们虚假社交网络个人资料的情况。了解您的孩子是否曾听说过有这种行为发生。确保您的孩子明白网络欺凌十分常见，如果他们未曾见到过，那非常好。确保他们了解当网络欺凌确实发生时该如何反应（他们不应该回复任何包含网络欺凌的电子邮件或 IM；他们应设法将其保存下来或打印出来以便可以向别人出示；如果他们知道如何阻止，那么应该将其阻止；最重要的是，他们务必要将其报告给爸爸/妈妈或其他值得信赖的成年人。）

5. **网上是否有任何内容曾让你感到奇怪、难过、害怕或不安？**可以趁此机会讨论网络欺凌、在浏览过程中的无意发现（例如色情站点或种族主义站点），甚至是涉及到附近某位朋友或同龄人的怪事。目的是确保您的孩子知道，当他们在网上看到一些异常或不好的事情发生时，可以向您求助并且不会受到惩罚。当您的孩子经常使用互联网时，遇到不好的事情几乎不可避免。确保您的孩子知道，他们可以向您求助并且您不会反应过激。

针对孩子年龄较大的家庭的额外提示或问题：

- 你真的认识你“好友”名单里的每一个人吗？
- 你知不知道如何使用和设定隐私与安全设置？能给我演示一下吗？
- 你是否收到过陌生人发来的消息？如果收到过，你是如何处理它们的？
- 你是否知道有人打算与他们在网上聊天的网友进行线下会面？
- 你好友群里的人是否曾在网上或电话里相互谩骂过？如果发生过这种事情，他们都说了些什么？有没有人谩骂过你？如果有的话，你会不会跟我说？
- 有时孩子们会弄到一些裸照或性感照片并相互传看。你学校里或你认识的人是否有过这种事情？

就这么简单。这就是“光说不干”。它并不难，也不需要技术，是完全可以做得到的，我希望您试一试。如果您是位教师，您可以在与全班同学讨论的过程中试试这种方法。

基础知识

在我们讨论互联网风险的过程中，您会发现它其实可以分为三类：网络犯罪、人际问题和声誉/隐私问题。在本指南的其余部分中，我们将讨论每个领域内促成风险的各种问题；不过您可能会发现，如果将在线问题视作是由“未知的不良分子”、“我认识的人”和“我自己的错误”导致的，则会很有助益。

网络犯罪是实实在在的犯罪

网络犯罪是一种实实在在、全球性且日渐猖獗的现象。诺顿已开展了多项全球性研究，采访过全球数以千计的成年人和孩子。在 2012 年度的诺顿网络犯罪报告中，我们发现全球有 2/3 的成年人曾经是某种形式网络犯罪的受害者。[4] 他们所遭遇的网络犯罪可能是病毒、蠕虫、特洛伊木马或其他恶意软件，但也可能包括在线欺诈、遭劫持的社交网络以及电子邮件帐户和网上猥亵。虽然诺顿有很多工具可帮助您抵御网络犯罪，但您可以采取的最重要的步骤则是在上网前先在您的所有电脑和移动设备上安装优秀的互联网安全软件。

病毒、蠕虫和间谍软件

计算机病毒已经问世了超过 25 年，其具体形式千变万化。但直到人们普遍在互联网上交换电子邮件和文件，这些威胁的分布才真正铺开！ 那些制作病毒及其他形式恶意代码或“恶意软件”的人过去经常实施各自的毁灭计划，以此证明自己的软件技能或相互炫耀。我将病毒编写时代早期的这段时间称为“沽名钓誉期”。但如今，所下的赌注已远非以前可比，很多不良分子受其非法活动所带来的经济收益驱使，已成为国际性的网络罪犯。因此，我们现在所处的病毒编写时代已进入“谋财期”。有些安全分析师估计，一名网络罪犯每年可通过网络犯罪活动牟取数十万美元。在诺顿，我们每天都会发现超过一百万种新型恶意软件！ [5]

4. 资料来源：诺顿网络犯罪报告，www.norton.com/2012cybercrimereport
5. 资料来源：2011 年度赛门铁克互联网安全威胁报告

2010 年，我们观察到出现了一种可通过危害我们的物理基础架构来制造麻烦的新型恶意软件。这意味着，当 Stuxnet（震网）恶意软件瓦解了伊朗的一处核设施时，这也为我们提供了首起意图危害制造和工业系统的有组织、有条理网络攻击的证据。这着实让互联网安全领域的很多从业人员为之一惊！

就您现在不得不担心的问题而言，诸如间谍软件、击键记录程序和 Bot 等恶意软件可能会给您带来无尽的麻烦。间谍软件和击键记录程序会监视您的正常计算机活动，然后通过互联网将您的隐私数据报告给外部的罪犯。电子邮件、即时消息或社交网络中的危险链接可以悄无声息地在您的电脑上安装恶意软件，或者导致您访问承载有恶意软件的网站。可以在您家庭的电脑上安装互联网安全软件并确保它采用最新的防护文件进行了更新，以此方式帮助保护孩子们及电脑的安全。告诉您的孩子们不要关闭病毒扫描程序或防火墙，即使他们认为关闭后可能会加快游戏运行速度，也不例外。这根本就不是可以冒的安全风险！

欺诈软件

欺诈软件、假冒防病毒软件或虚假防病毒软件是一种可以危害您的电脑并让您蒙受经济损失的恶意软件威胁。通常，这种问题开始于无辜的网上冲浪人员遇到奇怪的弹出式广告时。这种广告伪装成一条操作系统消息或一则由电脑发出的病毒警报。这条消息会告知您，您的电脑“感染了一个病毒”，并指示您运行扫描程序来找到该病毒。很多人都会相信这条警报是真实的，因而会遵照这种指示操作。儿童尤其容易受到这种威胁的攻击，因为他们常常认为自己可以通过“清理病毒”来给父母帮上忙。

接下来发生的就是纯粹意义上的邪恶网络犯罪。所谓的“扫描”会向您显示您的电脑感染了很多问题，并告知您购买清理工具。很多人都会落入这个圈套，不但下载了包含更多恶意软件的危险文件，还向骗子透露了自己的信用卡信息。这种欺诈软件或假冒防病毒软件随后会劫持您的电脑，从而阻碍您的安全软件运行并防止您通过互联网寻求帮助。而且，您的信用卡现在也很有可能已被拿到国际黑市上交易。

请确保您和您的孩子们清楚不要落入这些危险的欺诈陷阱。如果您的电脑受到了感染，诺顿可以提供帮助。我们有一款名为 Norton Power Eraser 的免费工具就是专为根除这些恶意代码段而设计的。如果您的电脑遭到这种侵入并导致您无法访问互联网，那么您必须从另一台电脑（请朋友帮忙）下载这款工具，并将这款程序放到一个磁盘或 U 盘上。也可以通过 NortonLive (www.norton.com/nortonlive) 请我们的技术人员（收费）为您完成这项工作并删除病毒。

点击劫持

在社交网络中，诈骗者们会尝试通过多种不同的伎俩来诱使您单击并下载他们的恶意软件或透露您的隐私信息。精心设计了标题（“天哪！ 你不会相信这姑娘都干了啥！”）的搞笑视频或可向您显示谁在查看您个人资料的虚假应用程序可能就非常具有诱惑力。

Bot 真来了...

您是否曾听说过机器人接管全球计算机的故事？这绝非笑谈。Bot 和“僵尸网络”现在已成为影响我们在线安全的主要威胁。Bot（机器人的简写形式）是一种隐秘软件，可以悄悄潜入您的电脑，并导致它向他人发送垃圾邮件和网页仿冒电子邮件。

很多非法企业现在都仰仗这些可以像野火一样蔓延的 Bot 发展壮大，它们利用数十万没有戒备的个人电脑的计算能力， 一门心思为了窃取您的个人信息并骗取您辛苦赚来的金钱。

它们是如何做到的？Bot 是一种由网络罪犯偷偷植入您电脑中的恶意软件，从而使攻击者能够控制您的受感染电脑。这些“网络机器人”通常加入到了由用来执行各种自动任务（包括传播病毒、间谍软件、垃圾邮件及其他恶意代码）的受感染计算机所组成的网络。更糟的是，Bot 还用来窃取您的个人信息，并且可通过未经授权使用您的信用卡和银行账户来严重损害您的信用。Bot 还可以显示假冒网站，这些网站伪装成合法网站，骗您进行资金转账并提供自己的用户名和密码以用来实施更多非法活动。

抵御这些恐怖的小 Bot 的最佳方式就是安装一流的安全软件，并确保将您软件的设置设为自动更新，以便您确信自己获得的是最新防护。专家还建议千万不要单击电子邮件中的附件或链接，除非您可以确认其来源；您需要教孩子们学会这一点。一旦感染了 Bot，这些阴险的程序便会设法隐藏起来以免被您的安全软件发现，因此您可能需要访问诺顿网站来下载专用的免费工具来删除它们。

隐私信息和身份盗用

您的孩子并不会自然而然就明白何谓“隐私”信息，因此您需要解释这一概念：它是指可被陌生人用来访问个人或财务信息的任何信息。隐私信息包括您的姓名、电话号码、地址、您母亲的娘家姓、您参与的体育俱乐部、您就读的学校甚至是您私人医生的姓名等真实数据。不良分子可以将一条不起眼的线索变成一条有关孩子和家长的完整记录，然后他们就可以通过交易和出售这些隐私数据来牟利。不良分子可以轻易地以您的名义申请赊购，从而获得实实在在的商品和金钱， 同时也葬送了孩子的（或您的）信用评级及良好声誉。

如果您怀疑您或您的孩子已成为身份盗用的受害者，您将需要监视自己的信用报告，看看是否有新开帐户或新增贷款的证据。您有权每年从以下三家信用报告服务机构中的每一家免费获得一次报告：Equifax®、Experian® 和 TransUnion®。明智的做法是，每隔四个月轮换着向这三家机构索要报告，这只是为确保您的身份和信用是安全的。一旦您发现身份盗用证据，您便需要向执法机构报告，首先要向您当地的派出所报案。当您与所涉及的其他站点和公司交涉时，警方出具的这种报告将会使形势对您有利。您可能还能够对您的信用报告进行“冻结”。有关详细信息，请访问 www.ftc.gov。另一项有用的资源为身份盗用资源中心，其网址为 www.idtheftcenter.org。

人际问题

互联网在人与人之间建立了我们几年前可能都难以想象的联系。而利用所有这些联系和沟通形式，少数不法分子可能会给我们其余的人带来非常不安或痛苦的经历。正是互联网的匿名性实现了常常跨越了雷池的言论自由，从而给他人带来了痛苦和磨难。幸而，大多数年轻人都希望在线上和线下都举止得体。通过一些互联网安全教育，我们可以帮助我们的孩子们学会正确、善意的互联网导航方式以及在他人不友善时如何应对。互联网上有哪些“人际”问题？这包括诸如网络欺凌、密码盗用和性短信等问题。

网络欺凌和网络盯梢

得益于技术，我们的孩子们有比以往更多的方式来进行联络、社交和发挥创造力。遗憾的是，有些孩子却使用电子邮件、即时消息、手机照片、社交网络以及文本消息来为难或欺凌其他孩子。此外，孩子们的数字消息也可能会遭到编辑而更改了原意，然后再被转发给其他孩子，从而达到为难、胁迫或侮辱的目的。孩子们并不会充分报告自己的网络欺凌经历，因此难以掌握有关这个问题的准确统计信息。大多数研究就这个问题得出的结论是，有大约五分之一的孩子们遭受过网络欺凌，但美国国家犯罪预防中心的研究结果则表明这一比例高达 43%。[6]

请确保您的孩子们明白，他们必须保护哪怕是最为平常的文本消息，密切注意自己所编辑的话语。他们绝不能对别人实施网络欺凌，并在自己受到网络欺凌时一定要告诉您。为手机设置密码可以防止私人电子邮件、照片和消息遭到不希望的偷窥。

热心提示：如果您或您的孩子受到网络欺凌：不要回应。作出回应便正中欺凌者下怀。保持沉默可以使他们困惑。如果有人问您的孩子“你看到那个帖子或消息了吗？”，应教他回答未看到，甚至可以回答“昨晚我妈妈用我的电脑工作。可能她看到了吧。”

6. http://www.ncpc.org/resources/files/pdf/bullying/Teens%20and%20Cyberbullying%20Research%20Study.pdf

应使用键盘上的 Print Screen 键或智能手机上摄像头功能保留任何欺凌消息的一份副本， 因为您无从得知校方领导或执法机构何时将需要完整的事件记录。

如果合适，可以向相应网站或提供商、学校等方面举报网络欺凌行为。如果网络欺凌行为涉及在校的孩子（大多数被欺凌的对象都知道涉及到谁或谁有很大嫌疑），那么您可以向校长、老师、法律顾问或驻校治安警举报。几乎所有学校现在都制定了具体规定了将如何处理这种情况的网络欺凌政策。请确保您留有完善的书面记录并要求校方以书面形式向您提供他们的行动方案。如果任何欺凌行为涉及到关于进一步采取措施的威胁或暴力威胁，您可能需要通知警方。通常，警方可以帮助您联系网站所有者来撤除冒犯性的内容，但您必须积极推动事态的持续进展。

学校目前都纷纷制定政策和保证声明来解决这种问题，以此方式响应人们不断提升的网络欺凌防范意识。通常，根据州法律，它们需出台政策并开展全校范围内的培训。美国青少年 Megan Meier 的自杀悲剧在一定程序上是由于（还有其他因素）网络欺凌已经成为一种盲目跟风。更近时期与网络欺凌和青少年自杀关联的报道包括 Phoebe Prince 和 Tyler Clementi。务必要谨记的是，不管网络欺凌情况有多么严重，自杀都很少是由于单一原因或单起事件而导致的。如果您看到一条网上留言称发帖人正考虑自杀，一定要当真并向执法机构、相应网站或服务的主人或者美国防自杀生命热线 1-800-273-8255 报告。

不论在何处发生在线欺凌以及遭受欺凌的对象位于何处，都会有目击骚扰过程但却保持缄默的旁观者们，这些旁观者们由于充当了观众，因而让欺凌行为更加肆无忌惮。请确保您的孩子们明白，他们绝不能参与网络欺凌行为，即使是要求他们做的只是访问某个站点、打开一封电子邮件、将一条残酷的消息传递下去或者向一个卑鄙的社交网络页面添加自己的评论，也不例外。向您的孩子培训如何向遭欺凌的对象/受害者回以善意、支持和友好。给遭受网络欺凌的人打个电话，只是为了说声“我看到了他们的所作所为。这是不厚道的做法，我也很难过。”将会给其带来莫大的安慰和鼓舞。

网络盯梢是网络欺凌的一种十分危险的延伸，那些参与跟踪真实或“线下”生活的人可能会采用这种手段。据美国司法部透露，有十二分之一的美国女性在一生当中曾成为盯梢行为的受害者。[7] 18 至 24 岁的女性在线下和线上被盯梢的风险都是最高的。随着人们意识到这个问题，我们的年龄较长的青少年们可以学会保护自己，家长们也应了解如何给予帮助。盯梢者可能会劫持电子邮件帐户，并伪装成被劫持了电子邮件的人员。攻击者可能会丑化一个社交网络页面或向受害人的好友发送令人憎恶的消息，进行赤裸裸的身份盗用，或企图使某人的信用和声誉毁于一旦。

网络盯梢可能十分危险，因而应向执法机构、Internet 服务提供商和网站主人报告。应将网络盯梢和网络欺凌的所有证据都保留下来。

保护您的密码

我在学校与孩子们交流时，常常会问有没有人的密码在未经自己同意的情况下曾被别人使用或更改过。即使是向只有五岁（幼儿园阶段）的儿童们问这个问题时，也有大约 ¼ 的人举手。孩子们常常以这种方式滥用别人对自己的信任，哪怕对方是好朋友或兄弟姐妹也是如此。尽管这种滥用行为的初衷可能只是开个玩笑，但却会将孩子置于帐户管理不当、隐私信息遭泄露、社交网络被用来制造麻烦的境地。注销是另一种可确保无人能访问您帐户的绝佳方式。我儿子在付出了惨痛的代价后才明白这个道理：当时他在一位朋友家里忘了从自己的社交网络注销，结果那个男孩在他的页面上发布了一些粗俗的评论！

应引导您的孩子使用仅向您透露的密码。确保他们将电子邮件和社交网络的密码排定为需要确保复杂性和唯一性的最重要密码。应避免使用您的孩子或互联网黑客可能能够破解出来的易猜密码（例如词典里的词、名字或日期）。

下面介绍了管理密码的一种好方法。选用一个您将能够记住的主密码，然后针对不同的网站对该密码进行定制。第一步是选用一个包含超过六个字符并对字母与数字进行了某种组合 （而不是使用实际单词）的合格主密码。

7. http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspxnz?DocumentID=40616

在本例中，我们姑且使用“I want to go to Paris”这个短语。将这个短语缩减为仅剩每个单词的首字母，然后使用数字“2”来代替单词“to”，这样您最终得到的就是“Iw2g2P”。然后将相应网站的第一个和最后一个字母再加到这个密码上（Symantec.com 网站的密码将为：“SIw2g2Pc”）。这个小技巧有助于我记住所有那些各种各样的密码，同时又能让密码保持足够复杂，从而使计算机黑客难以破解它。这个序列很适合我，但对任何其他人则并不适合。它还有助于我对不同的帐户采用不同的密码。如果一个帐户的一个密码遭到破解，其余密码依然安全。

即使有了复杂且唯一的密码，但由于每天都需要多次输入它们，因此依然很容易乱成一团。有些电脑应用程序可以管理密码，有些浏览器现在也具有了存储多个密码的功能。将密码记录在电脑上存储的列表中、记在电脑旁所贴的便条上，诸如此类，都是非常不安全的做法。我采用的是 Norton 360 和诺顿网络安全特警软件程序中内置 的诺顿在线身份安全这项密码管理功能。

我在前面提到，电子邮件和社交网络应优先采用唯一且复杂的密码，但您是否知道原因是什么？如果黑客控制了您的电子邮件，他们就可以通过单击其他网站上的“忘了密码”链接来更改您的所有其他密码。而如果他们得以掌控您的社交网络，他们就可以对您的所有联系人实施欺诈或向他们发送危险链接。

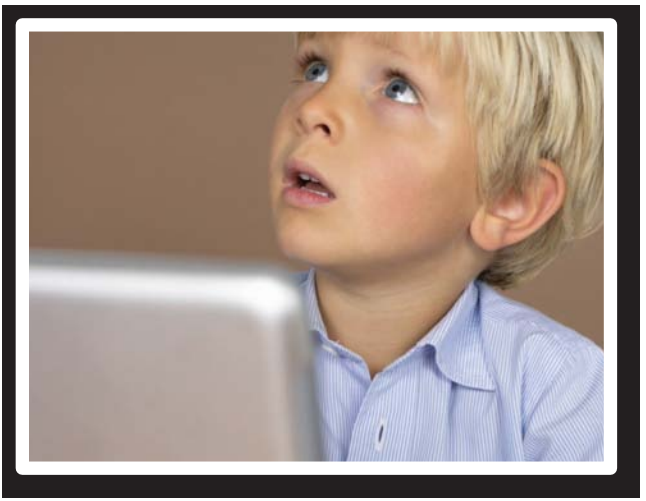
家长注意事项：务必要掌握您孩子的电子邮件、IM、社交网站及他们各种设备的密码。这是明智的做法，这样您就可以了解哪些人在与您的孩子交流，并且在出现麻烦的情况下，您也将拥有重要的访问权限。如果您的孩子忘了他们的音乐播放器或手机等移动设备的密码，可能将无法找回。因此，请与家人一起共同制定您家的密码策略。

互联网猥亵者

统计表明，儿童在网上被性猥亵者接近的几率很低，但这依然是家长们心头最大的顾虑。每当我与家长团体交流时，他们都希望听听在使孩子远离网上陌生人方面我有什么建议。美国国家失踪与受虐儿童援助中心在 2006 年开展的一项研究表明，有七分之一的儿童在网上曾被提出过性要求，但这些联系人大都是同龄人而非陌生人，并且这些联系人也不会给儿童带来不安。

要确保您的孩子明白，他们绝不能与陌生人进行电子邮件往来、聊天或文本消息交流，在现实生活中与陌生人见面也是绝对不行的。确保他们明白，他们在网上看到或认识的人仍然是陌生人，不管在网上见到了他们多少次，都是如此。

尤其令人担心的是有的孩子会在网上与陌生人讨论性话题——事实证明，这会导致更多的线下会面。如果有陌生人在网上接近您的孩子来讨论性话题，请访问 www.missingkids.com（美国国家失踪与受虐儿童援助中心建立的一个站点）并向他们的检举热线举报。要教会您的孩子将任何要求告知“A/S/L”（代表“年龄、性别和地点”）或任何类似信息的情况报告给您或其他可以信赖的成年人。



性短信

“性短信”是指以电子方式发送性方面的图像或视频的行为。这类图像常常是使用手机上的内置相机或视频摄像头拍摄的，然后以多媒体消息传送服务 (MMS) 消息的形式发送给他人。据 Pew Research 报告，在拥有手机的青少年中有 4% 的人发送过性短信，有 15% 的人收到过性短信。来自 Pew 的 Amanda Lenhart 将这类性影像的目的描述为一种用来建立亲密性、暗示自己有空或制造浪漫情缘的“关系媒介”。Pew 的研究成果将性短信情况划分为以下三类：

1. 完全在两个恋人之间交换图片；
2. 在恋人之间交换这类图片后，随后将图片传给了这种关系以外的人；
3. 在尚未建立恋人关系但通常有一方期望建立这种关系的人之间交换这类图片。

您可以想象一下，当一群受欢迎的孩子瞄上另一群略不占优势的青少年来诱使他们提供性图片时，有哪些强大的力量在起作用。这些略不占优势的青少年可能会屈服，以此作为得以接触某个男孩、进入某个圈子或获得某种社会地位的策略。

让事情变得特别可怕的情况是，这类图片可能会被视作一种儿童色情作品，从而使拍摄者和接收者都陷入水深火热的法律调查中。这类照片一旦从电脑或手机发送出去，就覆水难收了。已经出现过在某种欺侮事件中一些小女孩在学校里迫于年龄稍长一些的男孩子的压力而拍摄这些照片的情况。在新西兰，一名 12 岁的女孩子曾被在网上游戏世界中清除了她帐户的人员要挟拍摄这类图片。执法机构非常清楚这种趋势，但在接下来如何行动方面多少处于两难境地。他们的职责是停止拍摄儿童色情作品的行为，担当拍摄者是儿童并且还可能是受害者时，接下来该如何处置可能就很难断。我们开始注意到法律体系采取了一种更加平衡的方法来处理这类情况，判罚相关儿童接受咨询并从事社区服务， 而同样的情况仅仅在几个月前还可能会招致监禁或被列入性犯罪者登记库。

安全浏览

确保您的浏览器设置为向您提供内置的安全保护和安全功能。例如，Microsoft® Internet Explorer 提供了安全和隐私设置。可在“工具”>“Internet 选项”下找到这些设置。诸如谷歌等常用搜索引擎也提供了安全功能。例如，谷歌的安全搜索便用来筛查包含露骨性内容的站点并将它们从您的搜索结果中删除。虽然没有一款过滤器是 100% 准确的，但安全搜索可帮助您避开您可能不希望看到或者希望您的孩子不会偶然看到的内容。

默认情况下，开启的是“中等”安全搜索，这有助于将露骨图像排除在搜索结果的范围之外。如果您愿意，可以将设置更改为“严格”过滤，以便有助于过滤掉露骨文字及图片。可以通过单击谷歌主页右上侧的“搜索设置”来修改您电脑的安全搜索设置。Norton Family 则可以帮助您设定并锁定这些安全搜索设置。

保护无线网络

家庭无线网络可能会带来其他一些安全问题，因此您需要采取很多措施来确保它们受到保护以免遭不明入侵者侵入，这些入侵者可能会占用您的带宽，更有甚者，还会从您的系统传播他们的垃圾邮件并发动其他攻击。此外，借助笔记本电脑、智能手机或平板电脑以及一个无线网络，您的孩子们可以从家里的每一个角落访问互联网，从而大大增加了您监控他们活动情况的难度。

如果您家里配备了无线网络（称作“WiFi”），请确保您采取一切可能的措施来保障它的安全：将路由器密码重设为符合良好密码规则且不易猜到的密码；启用无线加密以防陌生人从互联网发现您的网络；限制您的系统在网络上共享的访问权限，并确保您的互联网安全软件保持最新状态。在我家，我们有时会在就寝时间使用路由器的控制功能关断我们孩子的笔记本电脑、游戏机及可联网的音乐播放器对网络的访问。这有助于我们的孩子克制在深夜聊天和发帖的冲动。

有些家长甚至会在晚上断开路由器连接并将路由器拿到自己的卧室内，还有一些家长则每天更改一次 WiFi 密码——只要是适合您的措施，都可以采取。

家长控制软件

借助家长控制软件，您可以选择允许孩子在何处、何时上网，并可确保他们不会查看不良内容。家长控制功能因提供这种功能的应用程序而异。通常，您可以根据要保护的孩子的情况，对这种程序进行多种级别的自定义。例如，对于五岁的孩子，您可以创建一个“白名单”，然后将事先选好、经家长批准可允许孩子访问的网站列入此名单。

您也可以设置要求提供家长的登录凭据才能允许孩子上网冲浪的帐户，或者设定时间限制。您可以赋予较大的儿童或青少年更高的访问权限和灵活性。可以按程序库中的站点类别来限制网络访问，以防他们接触到种族主义、色情或其他有害内容。值得一试的是我们的免费程序 **Norton™ Family**（也提供收费的 高级版本。）

Norton Family 是一项屡获殊荣的家庭安全服务，在 PC、Mac® 和 Android™ 设备上均可运行。您可以用它支持的 25 种语言中的任意一种语言使用它。它最让我喜欢的方面是十分易用。它在设计上确实充分考虑到了普通大众的需要。您可以在家里的所有电脑上安装它，然后便可从任意位置登录它，甚至可以从可联网的智能手机登录。可以限制每个孩子能够访问的站点类型，为每个孩子专门制定时间限制，监控社交网络搜索活动并查看他们的网络历史记录。由于这些信息存储“在云中”，因此您的孩子无法通过删除他们的历史记录来掩盖他们执行的活动。

我们的专家顾问委员会不乏儿童培养、执法以及在线安全方面的专家，甚至还包含“青少年学家”。他们与我们的 **Norton Family** 团队协力设计灵活但功能强大的程序。该团队以鼓励家长/孩子沟通原则为指导。您无法使用该程序来暗中监视孩子的举动，因为孩子始终都可以看到它，每次启动电脑后它都会以一个图标的形式显示在工具托盘中。我们希望家长耐心向孩子们解释它的工作机制是什么、他们可以看到什么并共同商定家庭使用规则。既然 Norton Family 免费提供，何不尝试一下呢？

要创建帐户，请直接访问 www.onlinefamily.norton.com 开始 创建。但请谨记，没有一款软件可以完美无瑕地防范每一种可能的互联网风险。不管孩子有多大，家长们都需结合运用软件、教育、监督和沟通等方法来保护他们。网络蕴藏着丰富的资源，如果完全封锁它，那就事与愿违了。家长需要与孩子进行沟通，以确保孩子在上网时能够秉持他们的信条、道德观和价值观。

风险

剽窃与作弊

轻而易举就能找到针对所有常用学校教材的在线家庭作业指导书，并且很多网站也在兜售申论答案和论文！ 作弊从未像现在这么简单、随处可见并诱惑着我们的孩子们。要提醒您的孩子，务必要仅将互联网用作调研之用。向您的孩子解释，为什么说由用户制作的内容（例如维基百科上的那些内容）可能并不是完全可靠的。教会您的孩子使用此类在线资源作为一个起点，并向他们演示如何查找最可信、最可靠的在线调研站点。

文件共享、音乐和视频下载

孩子们很快就会懂得相互之间分享音乐的乐趣。通常，当他们介于童年中期与青少年期之间时，就会从别人那里了解到文件共享站点，特别是免费的站点。要让您的孩子意识到文件共享站点和程序的危险性，从定义上就可以看出，它们会使陌生人得以访问您电脑的某一部分。使用文件共享站点可能会使您的电脑和信息面临 Bot 软件、间谍软件、击键记录程序、病毒及其他危险恶意代码的威胁。

我曾经参与过一个执法研讨会，在会上相关人员演示了通过流行的文件共享站点可以多么快地找到敏感的财务文档，只需运行一次搜索即可达到目的。那位官员打开了其中一款程序，键入“tax return”（纳税申报单），然后在几秒钟之内就出现了数以百计的实际纳税申报单。他双击了其中一份申报单，我们便可以看到这个无辜的家伙在不知不觉中就透露了自己的隐私信息及有价值的财务信息。此外，下载免费的音乐或视频常常也是不合法的。应向您的孩子演示可以在何处合法地下载音乐和视频，例如可从 iTunes® 和亚马逊等站点下载。

社交网站

无论是对孩子们来说还是对成年人来说，社交网站都是互联网上增长最快的现象，但真正推动它们增长的是从童年中期到青少年期这个年龄段的孩子（需谨记，按照法律要求，用户需年满 13 岁才能使用社交网络）。Facebook 作为最流行的站点，现在自称其站点上的成员数已有十亿，真是让人难以置信。所有社交网络都为孩子们提供了一个在网上与新老朋友相聚的场所。若谨慎使用，这些站点是我们大家交流和分享体验的绝佳方式。但如果使用时粗心大意，社交网站就会像所有其他站点一样，可能会使您的朋友、家人和网络面临恶意软件、网络罪犯甚至身份盗用的威胁。

网络罪犯可能会在我们最喜欢的社交网络中传播恶意软件，为此，他们会骗我们单击某个视频链接、下载某款程序或重新登录到伪装成该社交网络的某个假冒页面。他们的目的是窃取您的帐户登录凭据、向您的好友圈子传播恶意软件、使您的电脑感染恶意软件或诱使您访问以偷渡式下载来迎接您的受感染站点。请告诫您的孩子避开这些狡猾的伎俩；如果他们落入圈套，请删除您帐户中的所有欺骗性帖子、更改您的密码并向社交网络安全团队报告。

请告诫您的孩子不要发布隐私信息或不良或误导性的图片。这些信息一旦发布，就会成为公开信息，从而可能会存储在他人的 PC 和互联网历史记录文件中。即使您删除了此类信息或照片，它们可能仍存在于互联网上，并掌握在可能会使用和滥用它们的人的手中。如果有关人员要求您或您的孩子“取消标识”某个人或者删除某项评论或发布的其他内容，要确保你们都表现出良好的在线礼仪并立即予以遵守。

甚至是我们对社交网络的定义也需要更新。有些未到法定年龄、介于童年中期与青少年期之间的儿童已经开始使用照片共享站点和博客服务作为社交网络。只需发布一张载明大家聚会地点信息的纸的照片，您所有的“关注者”便都开始对这个计划发表评论并更新该计划。而这完全发生在家长的视线范围之外，因为“按照定义”这种照片共享站点并不是社交网络。因此请留意您孩子使用的所有站点。

利用社交网络，孩子们可以形成好友圈子，圈子里的人相互之间可以自由交流。请确保您的孩子不允许他们不认识的人加入他们的圈子。他们应将相应的页面设为私有，以便只有受到邀请的好友才能在站点上找到他们。应与他们一起了解帐户的隐私和安全设置。

您和您家人在接受加为好友申请时务必要多加小心，千万不要接受你们不认识的人发出的申请。据 2012 年度诺顿网络犯罪报告，35% 的在线成年人曾将他们不认识的人加为他们社交网络中的好友。这些陌生人一旦加入到您的圈子，就可能会使您和您的好友面临恶意软件和网络犯罪的威胁。请确保您的孩子正确地设置了隐私设置功能，以便他们可以限制能够访问他们的页面来查看照片或观看视频的人员。为帮助完成这种设置，我推荐参考 ConnectSafely 发布的“A Parents’ Guide to Facebook”《Facebook 家长使用指南》(www.fbparents.org)；如需了解有关社交网络安全所有方面的一些精彩提示（适用于任何设备），请单击 ConnectSafely.org 的 Tips & Advice （提示和建议）页面 (www.connectsafely.org/tips)。Facebook 也提供了很多有价值的安全提示，例如向同一帐户注册多个电子邮件地址或启用用来提醒出现新登录名的警报。如需更详细了解用来保持帐户安全的最新方法，请访问 www.facebook.com/security。

在社交网络领域存在一项主要顾虑就是垃圾邮件和网页仿冒攻击。我们需要在答复陌生人发来的消息或单击社交网站内的链接方面保持警惕和谨慎。在大多数情况下，您的安全软件都可以阻止您可能链接到的绝大多数有害站点，或者阻止下载间谍软件、击键记录程序或其他恶意代码。但如果黑客掌控了您的社交网络，他们就可以诱骗缺乏保护的好友单击恶意链接或访问危险站点。常见的在线骗局都是骗子冒充您向您的圈子骗钱，它们之所以日益猖獗，就是因为能屡屡得手。如果您在您的订阅中看到垃圾邮件链接，一定要迅速将它们删除并将它们标记为垃圾邮件，以便有助于保护在线的其他人员。诺顿网页安全是一款免费供 Facebook 上的所有用户使用的工具。它可以扫描在您的 Facebook 页面上找到的所有链接，以检查是否存在任何可能有危险的内容。

色情、赌博、种族主义、厌食和仇恨站点

互联网世界最黑暗的角落包含一些危险和非法的要素。研究表明，很多儿童在 11 岁前都已经看到过在线的色情作品。[8] 如果不使用家长控制软件或浏览器过滤器，您的孩子几乎不可避免地会遇到一些让您和他/她都会感到心烦意乱的内容。请确保您的孩子明白在遇到这类内容时要告诉您，并使他们确信告诉您后您不会生气。最重要的是，要解决这种问题，并防止其以后再度发生。

有些儿童和青少年可能会对传播种族主义或仇恨内容或者提倡铤而走险和伤害行为（例如厌食和自残）的站点感到好奇。只有定期检查您电脑的浏览器历史记录或查看您的 Norton Family 数据，您才能发现这种情况。哪怕孩子只访问过一次这类网站，您也应就此事与孩子交流。不要想当然地认为这只是出于无聊而好奇的行为。应解释您针对这类站点的家庭使用规则，并询问您的孩子他们是出于什么动机访问的。在你们交流过程中，如果孩子暴露出一些问题（例如沮丧或自我憎恨），应毫不迟疑地求助于治疗机构内的儿童专家或请其他训练有素的专业人士来处理此类问题。

8. http://news.cnet.com/8301-17852_3-20006703-71.html

数字声誉

您的数字声誉是别人通过搜索引擎结果审视您的人生时所得出的印象。孩子将一些东西放到网上后造成了学业、经济或感情方面的损害，这方面的新闻报道已经层出不穷。一名高中生曾因为发布了他们一群人拿着一个啤酒瓶的照片，而被取消了奖学金资格。一名员工曾因为在社交网络上发布了对他们老板的评论，而被随后解雇。即使您的孩子在他们所发布的内容方面十分谨慎，也务必要了解他们的在线活动，以确定他们所说的、上传的或评论的任何内容是否可能导致他们将来为此付出代价。调整社交网络隐私设置或者删除在陌生人看来具有冒犯性、幼稚或愚蠢可笑的评论、照片、视频和帖子，永远都不算晚。

要从站点上取下一些内容或者防止它们再度出现在搜索引擎结果中，可能绝非易事。但了解您的数字声誉情况并采取措施来确保它的准确性，依然值得一做。如果您在体育方面出类拔萃，应确保您的成绩能够在线查到。您曾赢得过辩论赛？那么可以在视频共享站点上发布一段视频，并标上您的姓名。曾经参加徒步行走募捐活动来筹措善款？这是光荣之举，应确保慈善机构的网站正确拼写了您的姓名。这样，您就可以确保在查找您时最先显示的结果都是正面的，从而将任何负面的信息远远推到结果中的后面部分。

热心提示：以您的姓名和您孩子的姓名设置一个 Web 提醒，并讨论所显示的结果。

青少年在线隐私保护

应向您处于青少年阶段的孩子提供关于互联网的教育。成长到这个阶段，他们已经（或者应该）历练得足够精明，能够认识到网上的人员并不一定就是他们所宣称的自己。可以很容易在年龄、性别和地点方面撒谎；因此很多人出于天真和“并不那么天真”的原因在这方面信口雌黄。应不断提醒您处于青少年阶段的孩子，他们在网上不能再像面对面接触时那样相信陌生人。他们绝不应允许陌生人加入好友名单或者加入聊天或 IM 对话。他们也绝不应接受陌生人提供的免费软件、铃声或屏幕保护程序。

应提醒这个年龄段的孩子，电子邮件地址、用户帐户名以及 IM 签名不应采用他们的真实姓名、他们学校的名称或这二者的某种组合；他们不应具有挑衅性或以其他方式招来猥亵者。他们应尽可能匿名。此外，他们也绝不应向别人透露密码，哪怕是好友也不例外。这听起来可能是再明显不过的事情，但年龄较大的青少年往往会以透露密码作为考验“友情”的方式。这绝非明智之举！

确保您孩子所就读学校的网站采用了密码保护机制或者要求登录才能提供泛泛的公开信息以外的内容。例如，我家乡的一所学校曾在其网站上发布了一个运动队旅游行程，行程中注明了航班信息和参与旅游的学生姓名。其他可能存在的问题包括，在该网站上还发布了班级名、学生地址和家庭电话的列表。

电子邮件

不论是孩子还是成年人，对于不同的用途都应设有不同的电子邮件地址。例如，可取的做法是：设一个地址用于在线购物，再设一个地址用于网上银行交易，另外设一个地址用于与朋友和家人通信。这样做好处多多；例如，如果您在家庭电子邮件邮箱中收到银行通知，您就会知道这是恶意垃圾邮件，应予以删除。

确保为您孩子的电子邮件帐户启用了最高级别的垃圾邮件过滤。根据诺顿开展的一项调查研究，有 80% 的儿童的反映他们每天都会收到不良垃圾邮件。诺顿网络犯罪指数是一款用来跟踪并向电脑用户警告全球范围内每日网络犯罪风险的免费工具，据该工具报告，垃圾邮件数量在全球电子邮件数量中所占的比例经常达到 80% 左右。如果您的孩子因太小而不懂得忽略或删除垃圾邮件（其中有些邮件可能包含极具冒犯性的图像和内容），那么请勿允许他们自行管理帐户。应避免在线发布您的电子邮件地址，以防“屏幕抓字软件”将您添加到它们的垃圾邮件目标名单中。应以“名字 at isp dot com”格式将您的地址键入到网上。例如，对于我的电子邮件，应这样键入：“marian at Norton dot com”。

在为孩子创建电子邮件帐户时应小心谨慎。请选择不会使陌生人能顺藤摸瓜找到他们的名称。它们不应采用名字与姓氏的组合。它们也不应采用具有暗示性的网名或地址，例如“性感的小莱”或“疯狂云雨”，尽管用这样的名字看似很“酷”。确保他们使用强密码，并且绝不会向他们家长以外的任何人透露这些密码。您应知道您孩子的电子邮件帐户密码，以便您可以经常监控他们的活动。应了解他们都在跟谁发送电子邮件以及收到的都是谁发来的电子邮件。这些人您是否都认识？还要让您的孩子知道，您之所以这样做，是为了帮助保护他们的安全，而并非因为您不相信他们。

即时消息

即时消息 (IM) 并不是新出现的功能，但已经给家长们带来了更大的挑战，因为它现在包含在社交网络中，不太容易看到，因而也不易监控。它也已经成为手机上常用的服务。您可能无法轻而易举地跟踪它， 但您应研究像 Norton Family 这样的一些服务或您的手机提供商提供的一些服务。

下面提供了消息传送领域一些常见的缩写词及它们所指的含义。

- POS/P911/PAW/PAL - 家长警报
- BFF - 永远最好的朋友
- BRB - 马上回来
- G2G、GTG - 我得走了
- L8R - 回见
- LOL - 大声笑
- NM JC - 没什么，只是让人不寒而栗
- TTYL - 等会儿再说
- TY/TX - 谢谢
- YW - 别客气
- 如需更加详尽的列表，请访问：
  http://en.wiktionary.org /wiki/Appendix:Internet_slang

主要建议：

- 告诫孩子不要单击他们所收到的电子邮件内的链接，因为这些链接打开的可能是虚假网站。千万不可通过 IM 接受链接或下载文件。
- 禁用电子邮件中的预览功能。这样可防止邮件中的潜在恶意代码执行。
- 孩子不应回复不认识的人发来的电子邮件或意外即时消息。
- 他们不应公开自己的即时消息个人资料或社交网络页面。
- 将即时消息首选项设置为阻止陌生人联系。
- 他们不应允许站点显示他们的联机状态或者在他们访问的页面上显示他们的 ID 或隐私信息。
- 他们在不使用 IM 时或者在编辑他们的社交网络页面时务必要注销，以确保他们的隐私得到保护。

手机安全

随着您的孩子升入中学和高中，他们会索要（需要？）一部手机。Pew 最近开展的一项研究表明，年龄为 12-17 岁的孩子中有 75% 的人拥有手机。6-9 岁孩子也有手机的情况也已经屡见不鲜，通常都是他们的哥哥姐姐或父母用旧后给他们的。手机类型和服务套餐如此多种多样，因此您在选择前需要做好功课。并不是您 12 岁的孩子想要一部手机就意味着他们需要不受限制地发短信或访问网络。

您的孩子拥有一部手机后，您将不得不学习如何发送短信。Pew 研究还发现，54% 的青少年每天都会发送短信。有一半的青少年每天发送不低于 50 条短信；而对于这个年龄段的女孩子来说，每天的平均短信量超过 100 条！ 从童年中期到青少年期这个年龄段的孩子早已摒弃了电子邮件通信方式，改而喜欢发短信和使用他们喜爱的社交网络内置的消息传送工具。孩子只有在跟父母联系时才用他们的手机打电话。有些孩子仍然使用他们电脑上的即时消息和视频聊天工具。但即使是这些服务，也会日渐成为他们喜欢的社交网络的一部分而已，从而不再作为一项独立活动出现。

如果您孩子的手机可以访问网络，则应考虑为它增加安全保护。您可以阻止任何人向该手机添加间谍软件或植入全球定位系统 (GPS) 功能来跟踪他们的物理位置。您还可以设置远程锁定和擦除功能，以防手机丢失或失窃。诺顿针对智能手机推出了多款安全产品，您可以访问我们的 www.norton.com 网站了解它们。

主要建议：

- 为手机/设备设置密码以防遭到不受欢迎的访问。
- 在手机背面贴上联系电话号码，以防丢失。
- 安装安全软件以便在发生丢失或失窃时保护手机及数据。
- 夜间将设备拿到厨房充电，以便最大限度地减少夜间发短信和使用手机摄像头拍摄不良照片的情况。
- 研究提供商提供的服务，例如网络过滤器、时间限制、号码阻止及其他家长控制功能。

移动设备的安全

最近发布的诺顿网络犯罪报告显示，35% 的在线成年人发生过移动设备丢失或被盗事件。我们通过赛门铁克在 2012 年开展的 Honey Stick 项目了解到，当智能手机丢失后，只有一半捡到者会设法送还。并且，几乎所有的捡到者都会先访问手机的数据。请通过为设备设置一个密码来防止别人查看您的私人消息、联系人和图片。然后，在手机背面贴上一个写有联系号码（例如您家里的号码或办公号码）的胶带（没错，是个土方法！），以便捡到它的好心人能够将它送还您。

除了手机外，我们的孩子还时刻随身携带着功能强大的电脑。想一想还有很多提供网络浏览器的流行游戏机或诸如 Apple® iPad™ 之类的平板电脑。这些设备提供的功能非常精彩，但我们确实需要考虑安全威胁和在线安全风险，即使是我们主要用来阅读电子读物和打游戏的设备，也不例外。

请为所有移动设备设置密码。这可以防止他人安装间谍软件或未经许可购买应用程序。可以设置过滤器和家长控制功能，可以在设备上进行设置，也可使用家里的 WiFi 网络来设置。可安装安全软件以检测间谍软件或阻止未经授权进行的访问。路由器提供了众多用来控制这些设备如何使用家庭网络的方式。通过调整路由器设置可以设置时间限制、按类别过滤网站甚至拒绝未经授权的用户进行访问。

值得关注的一个趋势是将能够通过我们的移动设备进行购物。利用一种称作“近场通信”的新技术，可以在手机和移动设备上通过发送授权信号进行购物。众多提供商都已开发出了应用程序来帮助人们购买咖啡、进行个人间支付、开展网上银行交易——所有这些都通过移动设备的电磁波实现。我们可以确信的是，网络罪犯定然会开发出相应的漏洞利用工具，因此要小心使用移动支付并仔细监控您的帐户。

博客

博客是一种在线日志或日记。您可以访问 www.norton.com/askmarian 来阅读我的博客。 有些博客是主题性博客，专门围绕特定主题撰写。青少年的博客往往更像是传统的私人日记（只不过这些日记是发布在青少年自己的网站或社交网站上，对互联网上的所有人开放），相当于将他们的日记放到网上，让全世界的人都能看到。您的孩子应先确定他们撰写博客的目的何在，然后再开始撰写。搜索引擎通常可以提取所发布的这些信息，从而使您为保护您的隐私而付出的所有努力功亏一篑。如果您在自己的博客上发布照片或指向私人网站的链接，也会削弱您的隐私保护。

此外，诸如潜在雇主或学校招生办职员等人可能也会阅读您的博客，并且这种曝光可能还会影响您生活的其他方面。例如，已经有一些参加求职面试的人因为他们个人博客或提到他们的朋友及家人博客中的内容而被拒绝。务必要在网上搜索一下您自己及家人。如果您反对他人发布的某些内容，您可以请求他们将其删除，并且您也应该这样做。如果他们拒绝删除，您可以向网站主人进行举报。如果这些内容涉及诽谤或者违法，您也可以请执法部门参与进来。

数码照片与隐私

很多孩子都有带照相功能的手机，并且很多孩子还有自己的数码相机。告诉你的孩子为什么上网时不能将照片发送给
陌生人或可能会滥用照片的伙伴。你可以跟踪从手机发送数码照片的情况，只需检查你的在线或纸质帐单即可。确保你的孩子让你查看其手机上的照片，这样你才可以向他们提出您认为无聊或不适宜共享方面的建议。如果你有使用照片共享站点，请确保你禁止其他人使用你的照片，尤其是人物照片。未经当事人允许便使用照片共享站点上的照片，这样的案例又不是没有发生过。

许多手机和数码相机都会在照片上添加地理定位信息标签。这使得你很容易弄明白照片的拍摄地点，以及制作一张照片地图描绘你开车去过的全国各个地方或徒步游览过的一条偏远瀑布。不过一般情况下，实在没必要在每一张照片上都显示你所在的位置。检查相机或手机的设置，关闭在照片中添加地理定位标签的功能。此外，如果你的孩子在使用社交媒体主导的地理定位服务，或在社交网络上显示其所在位置，请告诉他们这可能会引发的隐私问题。

主要建议：

- 关掉相机或手机照片上的地理定位标签。
- 不要公开隐私相册。
- 要求照片共享站点的访问者使用密码。
- 利用备份软件对照片进行备份，因为电脑死机、断电、建筑物火灾或自然灾害很容易让你的照片和其他的电脑文件瞬间消失不见。
- 仅使用提供了安全保护的在线照片服务。
- 若某项在线照片服务为你提供了通过其服务发送电子邮件的选项，那么为了保护你朋友的隐私，请向朋友发送指向该站点的链接。

网上购物

互联网是购物者的天堂，对于有信用卡或预付费礼品卡（或可使用你的卡）的青少年来说尤其如此。不过，若想安全地购物，他们应遵循一些规则。在开启任何网上购物会话之前，确保你的安全软件处于开启状态且已经过更新。仅在了解且信誉良好的站点购物，因为在未知网站上购物有风险。确保你输入个人数据（如地址或信用卡号）的任何网页都采用了加密技术，这是增加安全性的途径之一。你可通过网址判断网页是否采用了加密技术，若网址以 https 开头，则说明采用了加密 技术。此外，还需要查看浏览器框架的底部是否有锁图标，若有锁图标，则说明你正在访问的网站采用了加密技术来保护你的通信安全。

在信誉良好的站点上购物只是成为安全在线购物者的第一步。不要通过点击电子邮件中的链接来访问喜欢的商店或商品， 而应该在浏览器窗口中输入商店的网址。这样操作有助于你幸免成为网络钓鱼攻击的受害者，否则你会转到一个假冒你所喜欢商店的站点， 这样一来，网络钓鱼者便可盗窃你的密码、登录名、存储的信用卡信息，甚至更糟。

尽量经常检查信用卡帐单，至少每个月检查一次。这是了解谁在使用该信用卡及在问题变得难以解决之前发现问题的最佳途径。信用卡发行公司会向消费者提供保护，并且将与你一道解决任何有争议或未经授权的费用。不要在线使用借记卡。信用卡也会提供保护，包括查询非正常费用的功能。而使用借记卡消费，钱会直接从银行帐户转出，在每月的帐单出来前，任何人都不会意识到这一点。要让转出的钱重新回到帐户绝非易事，这个过程需要一定的时间才能完成。

网上和移动银行业务与帐单支付

越来越多的人完全接受网上银行业务。将工资直接存到你的银行帐户是最安全的途径，这可以防止其他人从你的信箱中窃取你的支票，并且这种途径使你可以更快速地拿到资金。这同样也可以为老板节约成本。网上报税不久后将在美国成为标准方法。

美国银行的最新趋势是移动银行业务。各大金融机构均提供了许多适用于苹果和安桌设备的应用，这使得存现支票就像拍摄并发送一张手机照片一样简单。当然，最初接受这种技术的人是年轻人，不过随着不断实践，我相信我们中的大多数人也会去试一试。

网络犯罪早已做好利用这些工具的准备。我们已经发现了诸如ZeusTrojan 等大量恶意软件，这些软件到处寻找网上银行业务凭据并且已从受害者那里偷走了数百万美元。有些恶意软件将目标锁定在管理小型企业和慈善机构的人身上，它们从网站获取信息，然后发送有针对性的“鱼叉式网络钓鱼”消息。

就像信用卡一样，时时关注所有电子银行业务活动。定期访问你的帐户以检查交易情况。确保及时、准确地支付帐单。以与常规互联网安全一样的方式保护你的电脑，防止其他人窃取你的密码或银行业务信息。此外，不要从公共电脑、自助上网点或不安全的无线连接访问你的帐户。总是在网络浏览器中输入银行的网址，不要点击电子邮件中的链接。完成操作后，务必注销帐户。不要在浏览器中存储帐户登录信息。

在线打游戏和上瘾迹象

MMORPG - 什么是 MMORPG？它代表着越来越受欢迎的且容易让人上瘾的“大型多人在线角色扮演游戏”。一些青少年，尤其是男孩特别容易沉浸其中，从而远离现实生活。与你的孩子就以下方面立下规矩：可花在这些站点上的时间、他们能否得到钱用来成为会员或在现实生活中（如在线拍卖站点）或在游戏中购买游戏配件，以及任何其他你可能会有的担心。

据哈佛大学附属麦克莱恩医院电脑上瘾服务部门 (www.computeraddiction.com) 研究，以下是一些心理和身体上瘾的症状：

- 无法停止活动。
- 忽略家人和朋友。
- 对老板和家人掩饰种种活动。
- 学业和工作上出现问题。
- 腕管综合征。
- 眼睛干涩。
- 不注意个人卫生。
- 睡眠障碍或睡眠发生改变。

停下，思考，连接。

国家互联网安全联盟 (www.staysafeonline.org) 向消费者提供了有关如何保护自己以及为大家维护网络安全的指导。其“停下，思考，连接”活动旨在让我们在采取操作（如点击未知链接、 打开电子邮件附件或访问新网站）之前进一步了解网上风险。

重要提示

对成年人的重要提示

- 在所有电脑和移动设备上使用互联网安全软件。
- 在所有电脑和移动设备上设置密码。
- 请勿打开可疑电子邮件或点击未知链接。记住“停下，思考，连接”原则。
- 避免使用文件共享软件程序。
- 在使用公共电脑或 WiFi 网络时保持警惕。
- 备份你的电脑 - 在 Norton™ Online Backup - 的保护下上网
- 为你的家庭就你将如何使用技术定下家规并设置限制。
- 了解社交网络 - 加入并使用隐私和安全设置
- 帮助你的孩子管理其数字声誉。为每个家庭成员设置搜索警报。
- 发帖以永久保存。切勿与陌生人“交友”，并限制可看到你所发帖子的人。
- 使用父母控制软件并经常检查你电脑的互联网历史记录。
- 和你的孩子一块上网，并定期“谈心”。
- 告诉你的孩子当他们在电脑上看到任何令人不安的东西时要告诉父母、老师或者受信任的成年人。
- 为所有帐户使用复杂且唯一的密码。利用密码管理程序可轻松搞定这一点。
- 定期检查银行业务的网上帐单和帐户、信用卡、手机和其他服务是否存在可疑活动。
- 仅安装知名和广受好评的软件和移动应用。
- 文明上网。通过你的在线活动为他人树立典范。

对孩子的重要提示

- 在点击电子邮件中的链接、即时消息和社交网络时多加警惕。
- 为所有帐户使用复杂且唯一的密码。利用密码管理程序可轻松搞定这一点。记住，不要将密码告诉他人。
- 为你的智能手机设置密码，阻止未经授权的用户查看你的信息。
- 在完成操作后注销帐户，防止其他人访问你的帐户。
- 如果事先没有征求家长的意见，请勿下载、在线购买、安装软件或应用。
- 遵守你使用的所有在线服务制定的规则。在你年满 13 岁且得到父母允许之前，请勿加入社交网络。将你的父母加为好友。
- 合理地限制你在网上分享的内容并使用隐私和安全设置。请勿在公共上网场所列出隐私信息，且仅发布父母会同意的照片和视频。
- 文明上网。通过你的在线活动为他人树立典范。应其他人的要求删除相应内容。报告网络暴力。
- 如果你在网上或移动设备上看到的东西让你不安，请告诉你的父母或其他你信任的成年人。
- 务必在你的所有电脑和移动设备上使用安全软件。

结束语

互联网是一个精彩的资源密集地，里面的内容经常让人感觉它像一座实际的城市。通过互联网，我们不仅可了解世界各地的教育和娱乐新闻，并且可访问诸如聊天、电子邮件、网上购物等大量服务，大大方便了我们的生活。通过了解和认识网上存在的风险和威胁以及使用最新的互联网安全软件，你可以帮助正处于成长阶段的孩子更具独立性地在这座神奇的网络城市中行走。通过了解新技术和在线问题，继续自我学习。务必从自身做起，让上网行为符合安全互联网实践，为你的孩子树立行为榜样。非常感谢！

资源

是否希望获取学校、教堂或者其他当地组织提供的家长或学生互联网安全演示？现在，很多个人和组织提供了免费或者价格低廉的互联网安全演示，但是有时这些演示初次使用起来很复杂。

以下是有关如何联系相应组织的建议。此外，最好问一下您的朋友和邻居，了解您的当地社区可以提供哪些相关的服务。

- D.A.R.E. 或当地公安局负责网络犯罪的干警
- 地方检察官办公室
- 学校的 PTO 或 PTA 组织
- AntiDefamation League (ADL)
- iKeepSafe
- i-SAFE
- 国家互联网安全联盟

面向家长的出色资源网站

- Ask The Mediatrician: http://cmch.typepad.com/mediatrician
- Lady Gaga 的“Born This Way”基金会：www.bornthiswayfoundation.org
- Connect Safely：www.connectsafely.org
- Stop Bullying：www.stopbullying.gov

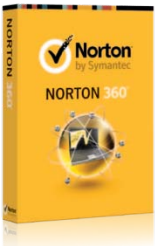
其他务必了解的互联网安全资源

- 诺顿家庭资源网站：www.norton.com/familyresource （文章、新闻快讯、博客、视频）
- 诺顿网络家庭安全设备：www.onlinefamily.norton.com
- 诺顿网络犯罪索引，为您提供全球最新网络犯罪威胁情报的免费资源网站：www.nortoncybercrimeindex.com
- 联邦贸易委员会提供了多种有用的资源：www.ftc.gov
- www.annualcreditreport.com （至少每年订购一次真实且免费的信用报告）
- www.staysafeonline.org

诺顿安全产品

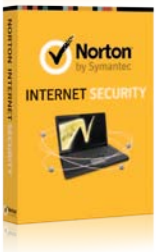
Norton One™

这一成员资格让您可比以前更为轻松地保护多台电脑和设备。利用您所偏好的诺顿安全产品，保护任意多个 Mac、PC、iPhone、iPad 和 Android 设备。此外，利用防窃功能，增添额外的防护层。如果您需要帮助，有专门的专家为您提供全天候服务，平均等候时间不到 2 分钟。



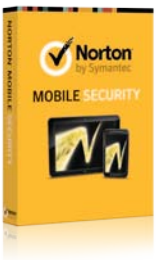
Norton 360™

Norton 360 提供全面、易于使用的保护，可为您、您的电脑和文件防范任何威胁。PC Tuneup 可优化您的电脑，自动备份则让您的数码照片和其他重要文件安全无虞。



诺顿™网络安全特警

让您在网上冲浪、购物、办理银行业务和进行社交活动时，不用担心病毒和网络犯罪攻击。诺顿安全特警可为您提供快速且耗用资源低的保护，不仅可以阻止威胁和保护您的身份，而且不会导致电脑速度变慢。



诺顿™手机安全软件

诺顿手机安全软件 — 简单却功能强大的基于 Web 服务，让您的智能手机和平板电脑远离在线威胁和手机垃圾邮件。它还可帮助您恢复丢失或失窃设备中的数据，防止陌生人访问这些设备上的隐私信息。

诺顿™ 网络家庭防护

一种确保孩子上网安全的明智方法。诺顿家庭防护为您提供了多种工具，让您可以管理孩子上网时访问的地址、上网时间、网上交流对象，以及他们与别人共享的信息。最重要的一点是，它让您可与孩子进行积极的交流，帮助他们养成良好的上网习惯。

用于 Facebook 的诺顿™ 网页安全

用于 Facebook 的诺顿网页安全可以通过扫描 Facebook 馈送来为您过滤恶意的 URL。此外，它还可通过告知您的朋友您馈送中可能包含的恶意 URL，来为他们提供保护。

Norton™ Hotspot Privacy

Norton Hotspot Privacy 可在您使用公共 WiFi 热点时，为您创建私密的安全连接。您可放心地随时随地保持联网，确信自己的用户名、密码和在线活动将远离黑客和窃听程序的攻击。

诺顿™ 在线身份安全

诺顿在线身份安全是一款免费的应用程序，它可跨 PC、移动设备和浏览器存储并同步您的用户名和密码，让您随时随地均可轻松安全地进行在线访问。

Marian Merritt

Marian Merritt

Marian 是赛门铁克公司的诺顿互联网安全宣讲师。她致力于向大众提供有关家庭网络安全的技术问题的信息。Marian 善于用大众容易理解的语言阐述复杂的技术问题。她定期与教师、家长和孩子进行交流，确保公司“获取”了当今互联网世界的最新趋势， 家庭和学校“获取”了培养智慧且安全的技术用户所需的信息。

担任宣讲师之前，Marian 曾担任赛门铁克的多个消费产品管理职位。她现在与先生和三个孩子居住在美国加利福尼亚州的洛杉矶。

访问 www.norton.com/familyresource 和 us.norton.com/security-center

- 如果您想获取更多的培训和教育资料
- 如果您已遭受互联网犯罪的攻击
- 如果您希望获取有关互联网威胁演变的最新信息

您可以访问 www.norton.com/askmarian 阅读 Marian 的博客。 您还可发送电子邮件至 marian@norton.com 向 Marian 提出您的问题。

家庭在线安全指南

作者：Marian Merritt