



如何使用WordPress 与Tor进行匿名博客

文：埃森·朱克曼

介绍

在压迫人们保持沉默的强权之下，总有一部分人依然坚持表达自己的意见，而工作在“全球之声”的一个最大的乐趣便是有机会与这样一群人工作在一起。同我共事的许多作者表示，他们想要在网上发表一些关于政治或个人问题的文章，但前提是不会因此而泄露自己的真实身份。这些作者包括一些国家的人权积极分子，身处在专制国家中的援救工作者以及工作在公司或政府机关中的告发人。

几个月以前我在“全球之声”上发表了一篇关于如何写匿名博客的技术指导，在其中我罗列了几种不同的匿名博客的方法。此后，我开始在世界各地举行专题研讨会并欣然地向人们传授一套高度匿名的工具——一种将Tor、WordPress以及各种免费邮箱相结合使用的匿名手段。以下的说明并不会提供给你多余的选择，而只是详细地向你介绍一种方法。

如果你想要快速阅读这篇文章或者你是那种做事情不需要知道为什么的人，便可以忽略说明当中“为什么”的部分。在将来某个时间里，我希望能将这篇文章整理得更加精致点，特别是将“为什么”的部分变得更加短小精悍一些，这样便可以大大缩短整个文档的长度。

如果我在文章当中某些地方表述的不清楚或者有什么错误的地方，请您在评论当中告诉我。这是一篇未经斟酌的草稿，我希望在把它发表在“全球之声”之前能够再进行一些整理。如果你认为这篇文章是有帮助的并想要对其进一步传播，请随意——正如这个网站几乎所有的东西一样，这篇文章同样遵循创造共享2.5协议，这就意味着如果你认为有市场并且有钱可赚的话，大可以自由的将这篇文章印在咖啡杯上进行售卖。

免责声明

一些人通过技术手段，便可以利用你在网络上的文章追寻到你的真实身份——例如，通过政府或警察部门从互联网服务商那里获取你的上网记录。不过只要你准确遵循本文所介绍的匿名方法，就能大大减少这种风险的可能性。遗憾的是，我并不能保证我所说的这些方法能在全部情况下都适用，包括你所处的环境在内。同时，如果这些方法的使用或误用给你带来了法律，民事或个人的麻烦，我也不会接受任何与之相关的责任，刑事或民事问题。

此外，当面对其它技术手段时，诸如键盘记录器（一种安装在电脑上用来记录你个人键盘输入的程序）或者是传统的监视手段（使用照相机或望远镜来监视电脑屏幕），本文所介绍的匿名方法就没有任何用处可言了。事实上，大多数通过作者发表在网络上的文章追寻个人真实身份的手段毫无技术性可言：一些人发表在网络上的文章本身就透漏了他们自己的身份，或者一些人还会将自己的个人信息与某个并不值得信赖的人分享。对于这些情况，除了告诉你要小心机敏点以外我实在是无能为力。假如你想要了解更多关于“小心与机敏（careful and smart）”方面的事情，我向你推荐电子前言基金会（Electronic Frontier Foundation）的“怎样安全地撰写博客（How to Blog Safely）”。

切入 正题……

第一步：隐藏你的IP。

每一台接入因特网的电脑都拥有或共享一个IP地址。尽管这些地址与我们现实当中的具体地址并不相同，但却可以引导一个聪明的系统管理员追寻到你具体地址的位置。特别是，如果你在一家互联网服务商那里工作，你便能轻易地将一个IP地址与在某个特定时间请求这个IP地址上线的电话号码联系起来。所以，当我们以匿名方式在网络上做任何事情时，都需要首先隐藏我们的IP。

如果你想要通过家庭或工作的电脑撰写博客，那么你需要做的是：

a) **安装Firefox**。从Mozilla（谋智）的网站上下载Firefox并将其安装在你撰写博客的电脑主机上。

所以，当我们以匿名方式在网络上做任何事情时，都需要首先隐藏我们的IP。



为什么？

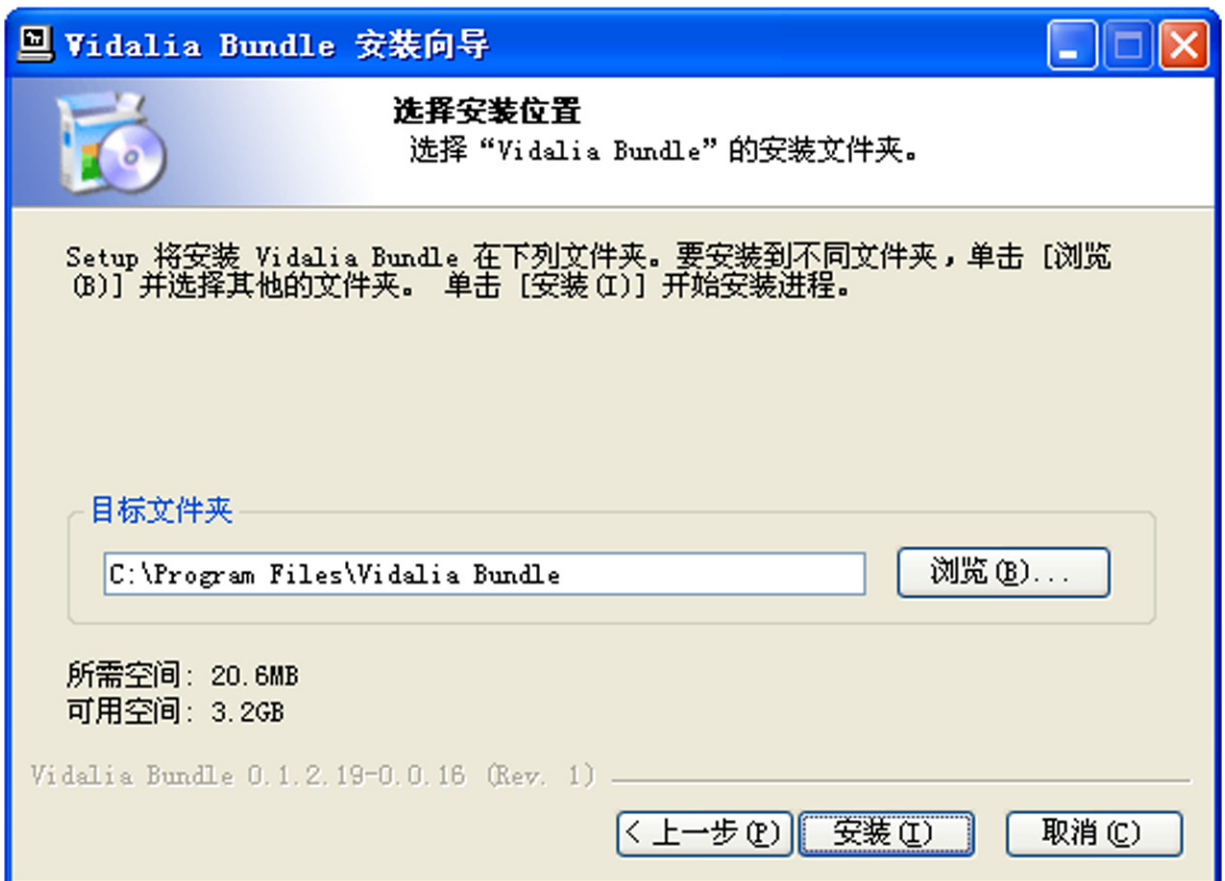
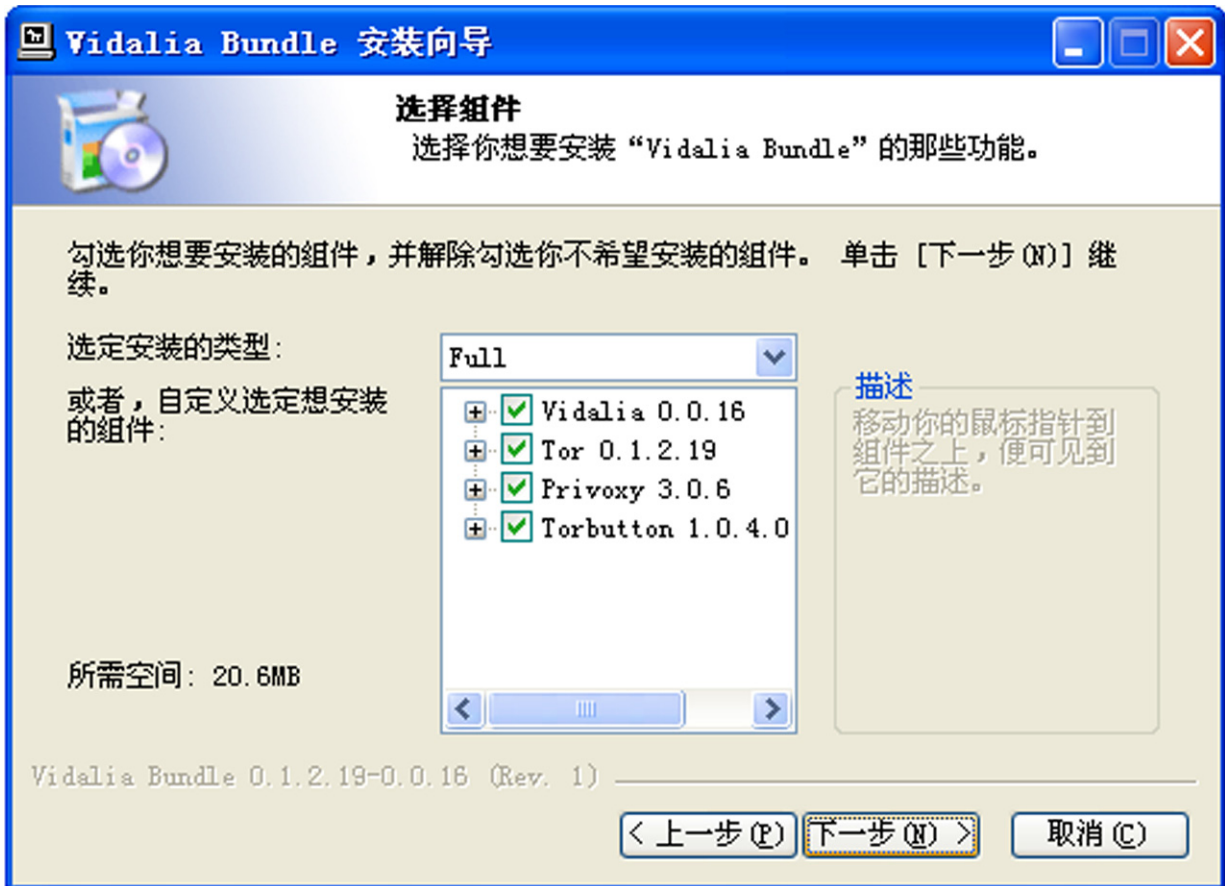
IE浏览器的一些严重的安全漏洞会危及到你的网络安全。与其他浏览器相比，这些在IE中的漏洞长期没能得以修复。（不相信我么？去问问Bruce Schneier吧）而对于那些你不小心从某个网站下载的间谍软件来说，这种漏洞是浏览器最大的弱点。此外，许多个人发布的工具都是专门为Firefox设计使用的，其中就包括Torbutton 在内，在下面的步骤当中我们便会用到它。

IE浏览器的一些严重的安全漏洞会危及到你的网络安全。

b) **安装Tor**。从Tor的网站下载安装程序。如果在你的国家里Tor的主站被封掉了，你同样可以去它的一些镜像网站下载到安装程序。为你的系统选择“最新发行的稳定版本”并将其下载到你的桌面上。遵循你所下载版本右边的相关说明。你将安装两个软件包并需要对Firefox中的新功能进行一些修改与配置。

平台	软件包
Windows 安装和配置指导	Tor & Privoxy & Vidalia & Torbutton bundle: 0.1.2.19 (sig)
Mac OS X 安装和配置指导	Tor & Privoxy & Vidalia & Torbutton bundle: Universal Binary (OSX 10.4 & 10.5): 0.1.2.19 (sig) 10.3 (Panther): 0.1.2.19 (sig)
Linux/Unix 软件包	Linux/Unix 下载页面







为什么？

Tor 是一种非常精密复杂的代理服务器系统。代理服务器会代表你请求网页链接，这就意味着网络服务商无法看到请求网页的那台电脑的IP地址。当你启动 Tor 时，你将会使用三个不同的代理服务器来接收每一个网页信息。网页在不同的服务器之间进行加密传送，即使链条中的一两台服务器受到了追查，也很难看到你正在接收什么网页或在什么网页上发布帖子。

Tor 会安装另外一种名为Privoxy的软件，它会阻止cookies和其他的追踪软件，以提高你浏览器的安全性。而且方便的是他还会阻挡你在浏览网页时遇到的许多广告。

当你启动 Tor 时，你将会使用三个不同的代理服务器来接收每一个网页信息。

确定Vidalia和Privoxy 已经开通了

Vidalia的图标

Privoxy 的图标



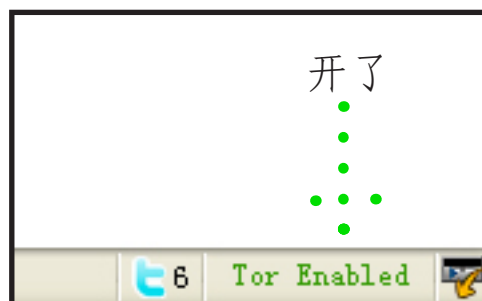
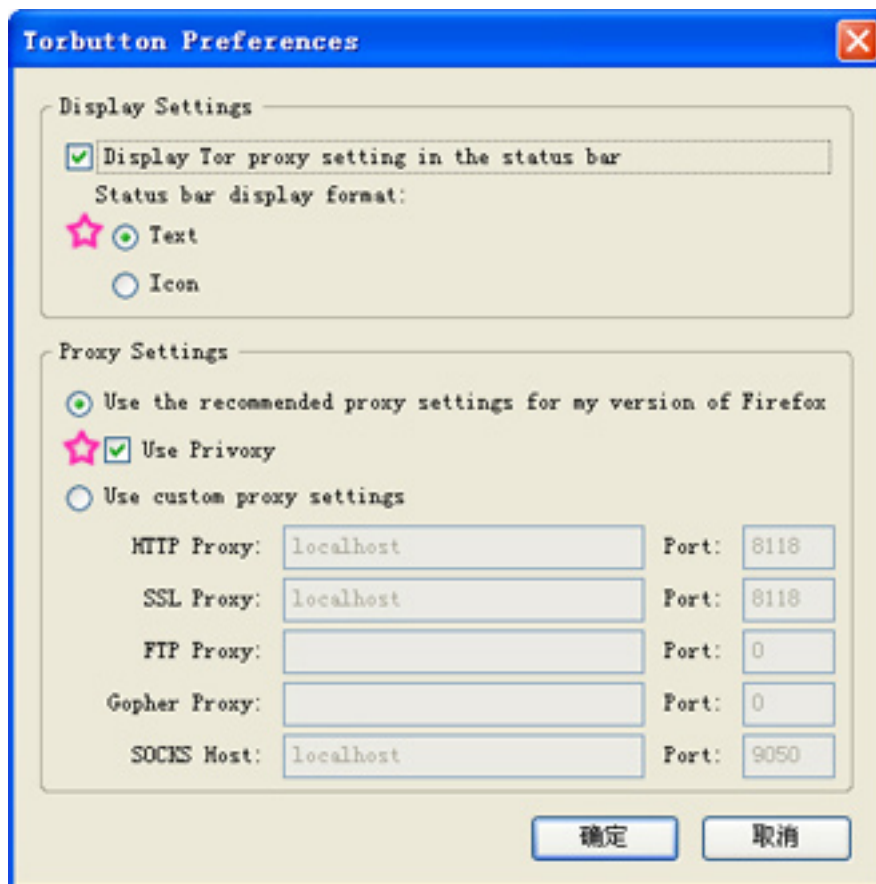
c) 安装 Torbutton。按照安装页面的指示，阅读相关信息然后进行安装。你只需要使用Firefox进行简单的安装——Firefox将会从上面提到的页面上直接请求你的许可进行自动安装。



为什么？

手动打开Tor意味着你需要改变浏览器的偏好设置来使用代理服务器。由于步骤繁琐，人们有时便会忘记。Torbutton的有用之处便在于将所有的步骤简化为一个按钮并且能够随时提醒你是否在使用Tor。

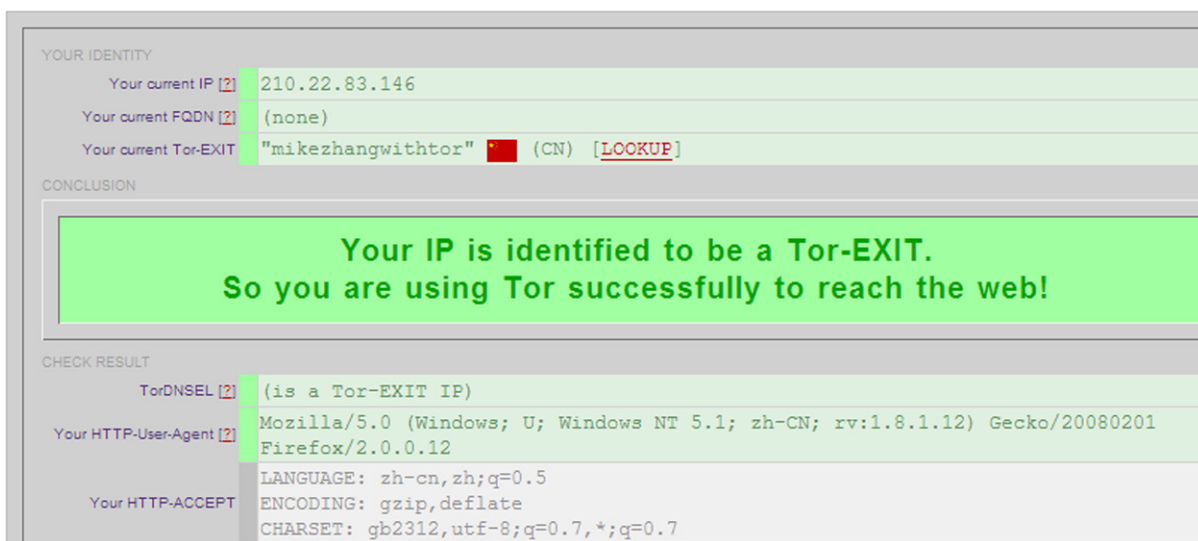
你也许会发现Tor减慢了你的网速——这是因为Tor在请求网页链接时需要通过三个代理才能到达你所想要浏览的的网站。一些人，包括我在内，只有在非常有必要隐藏自己身份的情况下才会打开Tor，而在其它时间则会关掉——Torbutton使这一切变得非常简单。



d) 在Firefox中开启并检验Tor。打开Tor，访问这个URL (<https://torcheck.xenobite.eu/>)。点击后，你会看到一个安全警告对话框——无法证明xenobite.eu是一个可信赖网站。点击OK，接受该网站的证书。



点击后，如果你得到的信息是：“Your IP is identified to be a Tor-EXIT. So you are using Tor successfully to reach the web.”，就证明你已经正确安装了所有的程序并为下一步做好了准备。



相反，如果你没能正确安装Tor则会得到这样的信息：“Your IP is NOT identified to be a Tor-EXIT. So you are not using Tor to reach the web”



CODE VERSION: 2007-11-08 00:18:24 GMT/UTC CURRENT TIME: 2008-03-11 17:13:49 GMT/UTC

YOUR IDENTITY
 Your current IP [?] XXX.XX.XX.XXX (probably your Home-IP)
 Your current FQDN [?] XXX.XX.XX.XXX.dsl.velcom.ca (Lookup/reverse correct)

CONCLUSION
**Your IP is NOT identified to be a Tor-EXIT.
 So you are NOT using Tor to reach the web!**

CHECK RESULT

TorDNSSEL [?]	(NOT a Tor-Exit OR service unreachable)
Hidden Services [?]	(unknown yet)
JavaScript-Support [?]	(unknown yet)
ActiveX-Support [?]	(unknown yet)
Java-Support [?]	(unknown yet)
Cookies-Support [?]	(unknown yet)
Your HTTP-Referer [?]	(unknown yet)
Your HTTP-VIA	(none)
Your HTTP-User-Agent [?]	Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12
Your HTTP-ACCEPT	LANGUAGE: en-us,en;q=0.5 ENCODING: gzip,deflate CHARSET: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Your HTTP-CONNECTION	keep-alive

SAFETY CHECK
 Klick 'START' for some safety checks!

THIS INFORMATION IS PROVIDED WITHOUT ANY WARRANTY CODE: [INDEX.PHP] | [JAVA.APPLET] | COUNTER: 1200620 | [STATS] | EMAIL: BLUESTAR88@XENOBITE.DOT.EU

GETTING HELP ON NON-WORKING TOR
 • [Here](#) you can find some hints.

REMARK(S) ABOUT THIS TOR USAGE CONCLUSION
 • This conclusion is valid only for your current webbrowser connections and not general for all other applications, because they each depend on an individual configuration which cannot be checked here!
 • This statement could be false, if my database AND the TorDNSSEL-database are not knowing your current Tor-EXIT server node yet
 • Is this NOT your Home-IP? Then you're probably using Tor to reach the web!

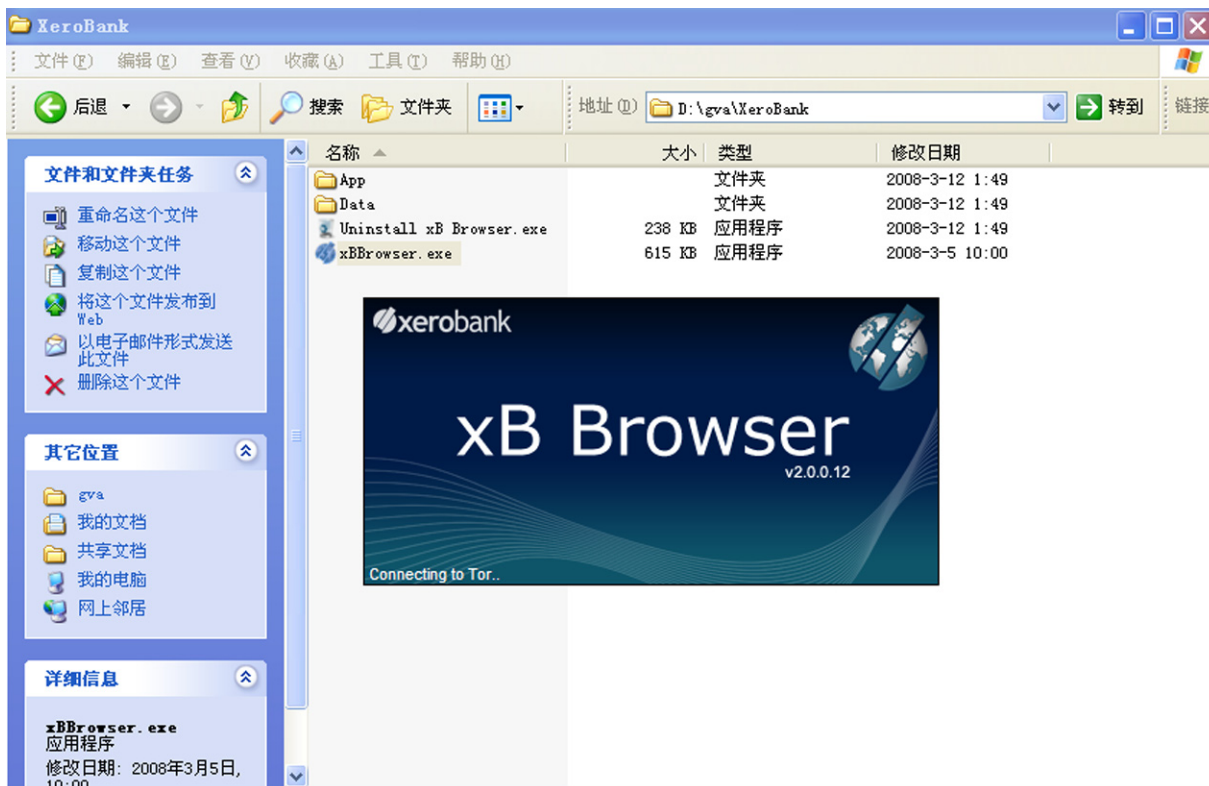
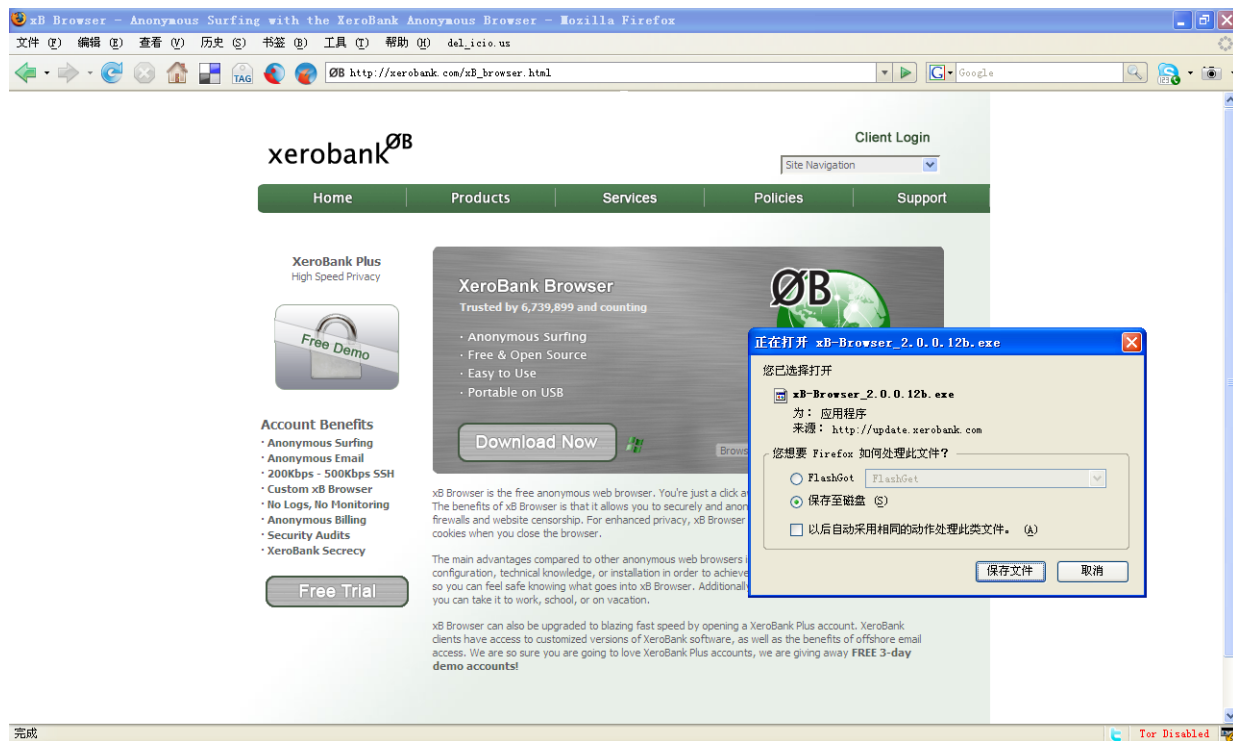
WARNING
**Do you have done some safety checks on your browser already?
 Klick 'START' to do some on here.**

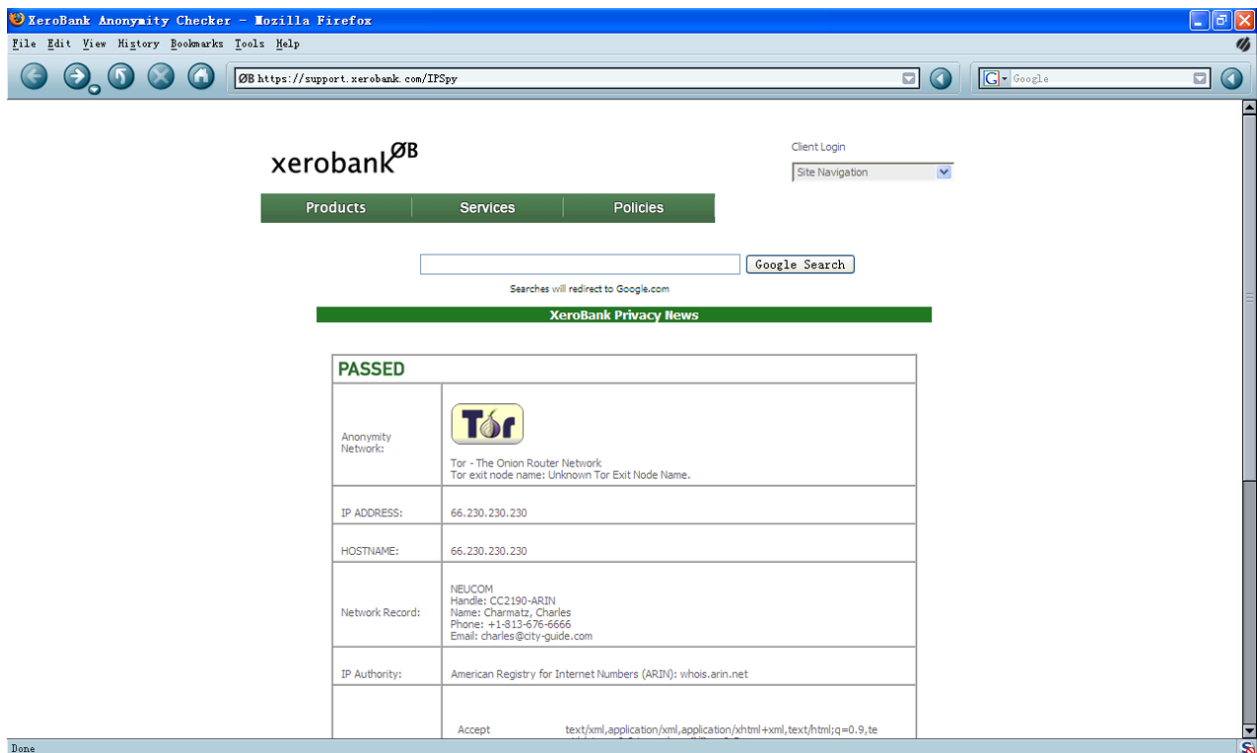
为什么？

经常检验一下你所安装的软件是否运行正常是非常有必要的，特别像Tor一类的重要软件更是如此。你所进入的这个网页会检测你的请求来自于什么样的IP地址。如果是来自于一个已知的Tor的节点，就证明Tor运转正常而你的IP也已经隐藏起来了；如果不是，就证明哪里出了问题，你就需要搞清楚Tor为什么无法正常运转了。

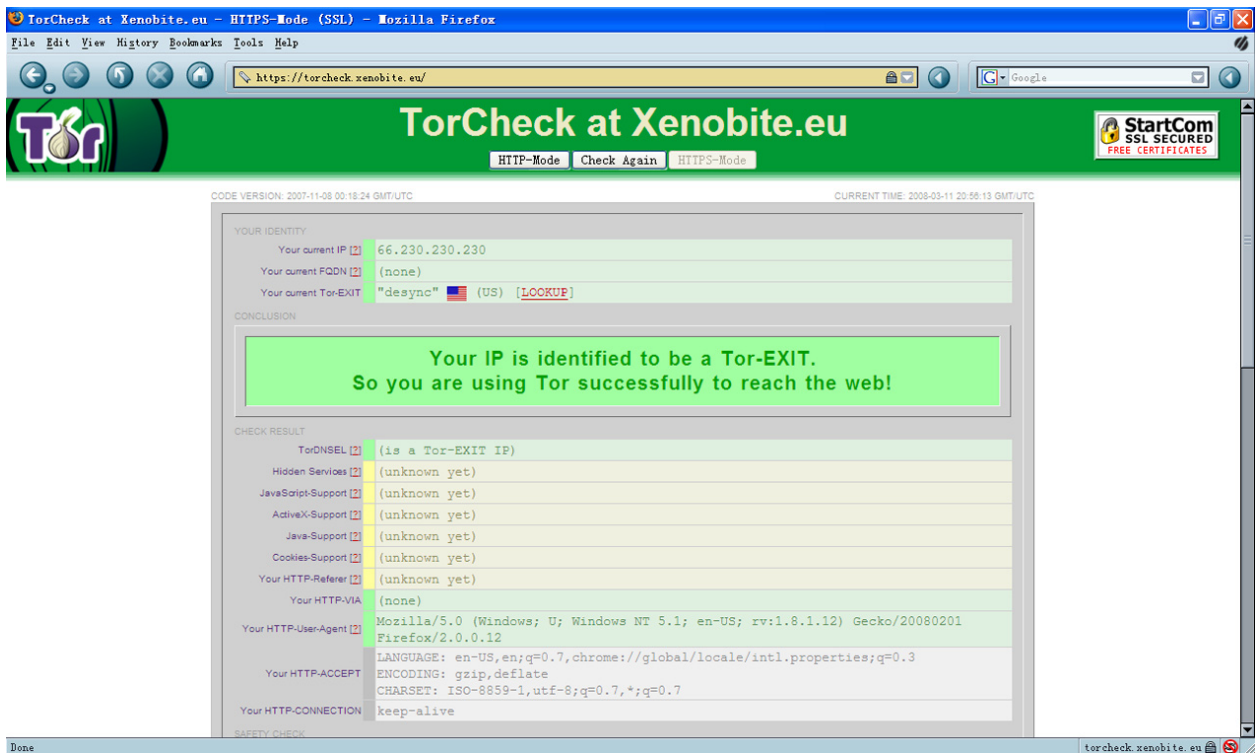
补充方法：如果你准备在一台与别人共享的电脑上写作（比如在网吧里）或者你无法在你使用的电脑上安装软件。

a) **下载XeroBank Browser (xB Browser)**或者**Tor on a Stick (ToaSt)**. 选择一台你可以存储文件的电脑，从xB Browser的网站上下载软件包。然后插入你的U盘并将xB-Browser.exe文件拷入U盘中。如此一来，在任何一台装有Windows系统并且可以使用U盘的电脑上，你都可以使用这个由Tor保护的浏览器了。当你使用共享电脑时，要先退出系统自身的网页浏览器，然后插入U盘，找到U盘的系统文件夹，接着双击xB-Browser_latest.exe。这样你便能启动一个新的浏览器，并通过Tor来上网了。





b) 使用已经绑定Tor的浏览器访问验证Tor的站点，以检测XeroBank Browser是否运行正常。一定要确定得到的信息是：“Your IP is identified to be a Tor-EXIT”。



为什么？

XeroBank是一款高度定制，并已经安装了Tor与Privoxy的Firefox浏览器。它被设计成为一个可以存储在U盘中使用的程序，从而使你能够在不允许安装软件的共享电脑上启用Tor。我推荐XeroBank，而且我在旅行当中也经常使用它，然而与此同时，Tor的工作人员并没有正式支持这款软件——因为令他们不满的是这个程序的早期版本并未连同源代码一起发布，这样一来就无法准确知道XeroBank究竟是怎样工作的而且又是如何利用Tor的源代码的。不过这款软件的一个新近版本已经包含了源代码——不知道Tor的程序员们是否会对这个版本表示他们的赞许。Tor的领导者Roger Dingledine也已经表示他与他的同事们正在计划开发一款开放源代码并嵌有Tor的便携浏览器，但是有关这项新工程的时间表并未公布。

第二步：创建一个新的，难以追查的电子邮箱帐户。

大多数网络服务，包括博客托管服务在内，都要求有一个电子邮箱地址以方便他们联系自己的用户。对于我们来说，这个邮箱地址不可以与我们的身份信息有任何关联，其中就包括我们注册服务时所使用的IP地址。这就是说我们需要使用Tor来注册一个新的帐户，而且要确定我们所使用的资料如名字、地址等等，不会与我们自身有任何关系。绝对不可以使用一个已经存在的邮箱帐户，因为你很有可能是在未隐藏IP地址的情况下注册的，而大多数webmail的服务商都会记录你在注册时的IP地址。

绝对不可以使用一个已经存在的邮箱帐户

a) 选择一个webmail 服务商——我们推荐Hushmail, Vaultletsof 和 Gmail, 不过只要使用Tor, 你也可以选择Yahoo 或者 Hotmail。同样, 你也可以在fastmail.fm. 上轻松快速的注册一个webmail的帐户。



为什么？

使用Webmail是创建“一次性”邮箱地址的最好方法，一来你可以使用它注册其他的网络服务，二来你也可以随意的忽略它。不过许多用户也将webmail当作他们的主要邮箱来使用。如果你想要这么做的话，了解一下不同邮件服务商的长处与短处就显得十分有必要了。

Hotmail与Yahoo的“安全特性”都让隐私保护者们感到非常不快。两者都会记录发送邮件的电脑IP地址。当然，当你通过Tor来使用这些服务时也就不必担心这些事情了，因为他们所记录的IP地址将仅仅是Tor的IP地址，而并非你的IP地址。同时，Hotmail与Yahoo都不为他们的webmail提供安全的HTTP（https）接口——这也没什么关系，只要你每次都使用Tor来登录这些邮箱服务就可以了。然而，许多用户都需要在一些没有安装Tor的环境下检查自己的邮件，所以对于你主要的webmail帐户来说，选择一家为邮箱提供https接口的服务商还是很有必要的。

Hushmail为它的webmail提供了相当高的安全保障。他们支持PGP加密系统——如果与你通信的人同样使用PGP，那么这将是非常有用的。他们使用https接口进入webmail并且在发送邮件时不记录发送者的IP。不过他们提供的是一种营利性服务，而且只提供有限的服务给非付费用户。如果你注册的是一个免费帐户，还将不得不每几周就要登录一次，以确保系统不会删除你的帐户。因为他们会极力将免费用户转化为付费用户，而且他们的系统中使用了大量的Java小应用程序，所以一些人发现Hushmail对于他们来讲并不是一个好的选择。

Gmail，尽管并未把自己宣传为一种安全可靠的电子邮件服务，它却拥有一些很好的内置安全特性。如果你访问这个特殊的URL，你与Gmail的整个会话都会通过https进行加密。（我推荐你收藏这个URL并在以后都使用它来登录Gmail）Gmail不会将源头的IP地址加入邮件的报头，而且你还可以使用FreeEnigma和与其配套的一个Firefox的扩展为你的Gmail添加强大的加密程序（这同样也适用于其它邮箱服务），从而使你的Gmail具有支持PGP的功能。

针对所有webmail帐户的一个警告——你信任着处理你所有电子邮件的这家服务公司。而如果这家公司被黑客侵扰，或者他们受到了其他政府的施压而透漏了信息，他们可是有权得到你收发的所有邮件文本的。解决这个问题的唯一方法是在文本编辑器中编写你的邮件，并在你自己的电脑上使用PGP对其进行加密，而且收信人同样也要使用PGP。虽然这种方法已经远远超出了我们所想要和需要的保密程度，但重要的是要记住你所信任的这家公司也许是，也许并不是真正在维护你的最高利益。特别是像yahoo这样的公司有着将信息转交给中国政府的陋习——中国的异议人士控告yahoo公司非法泄露用户信息。所以当决定信任谁时，最好是三思而后行。

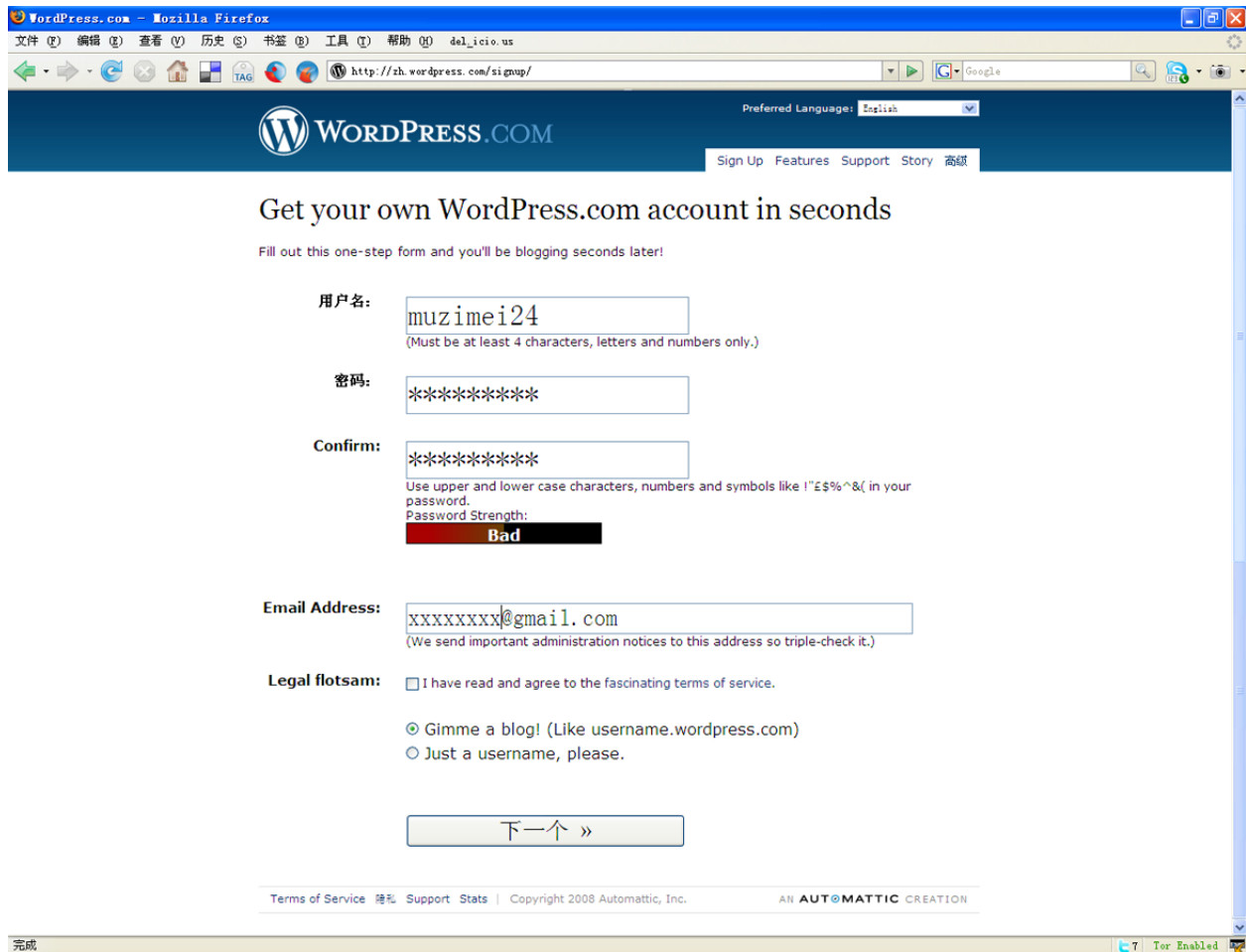
为帐户设置一个强大的密码（至少八个字母，包括至少一个数字或一个特殊字）。

b) **打开浏览器中Tor，或者启动XeroBank。**访问你所选择的邮件服务网站并注册一个新的帐户。不要使用任何有关个人身份的信息——可以考虑起一个不起眼的名字，将自己伪装成一个美国人或英国人，因为在这类国家中存在着大量的网络用户。为帐户设置一个强大的密码（至少八个字母，包括至少一个数字或一个特殊字）并选择一个与你的博客名近似的用户名。

c) 确定你可以在Tor开启的情况下登录邮箱和发送邮件。因为Tor似乎每十分钟便会改变自己的电路，从而会打断你在webmail上的操作，所以你最好考虑一下把写一封新邮件的时间缩短到十分钟之内。

第三步：注册你新的匿名博客

a) 打开浏览器中的Tor，或者启动XeroBank。访问WordPress.com，点击“Get a New WordPress Blog”的链接，创建一个新的帐户。使用你刚刚创建的电子邮箱地址，并创立自己的用户名。用户名将会成为你博客地址的一部分：[比如木子美]：muzimei.wordpress.com。



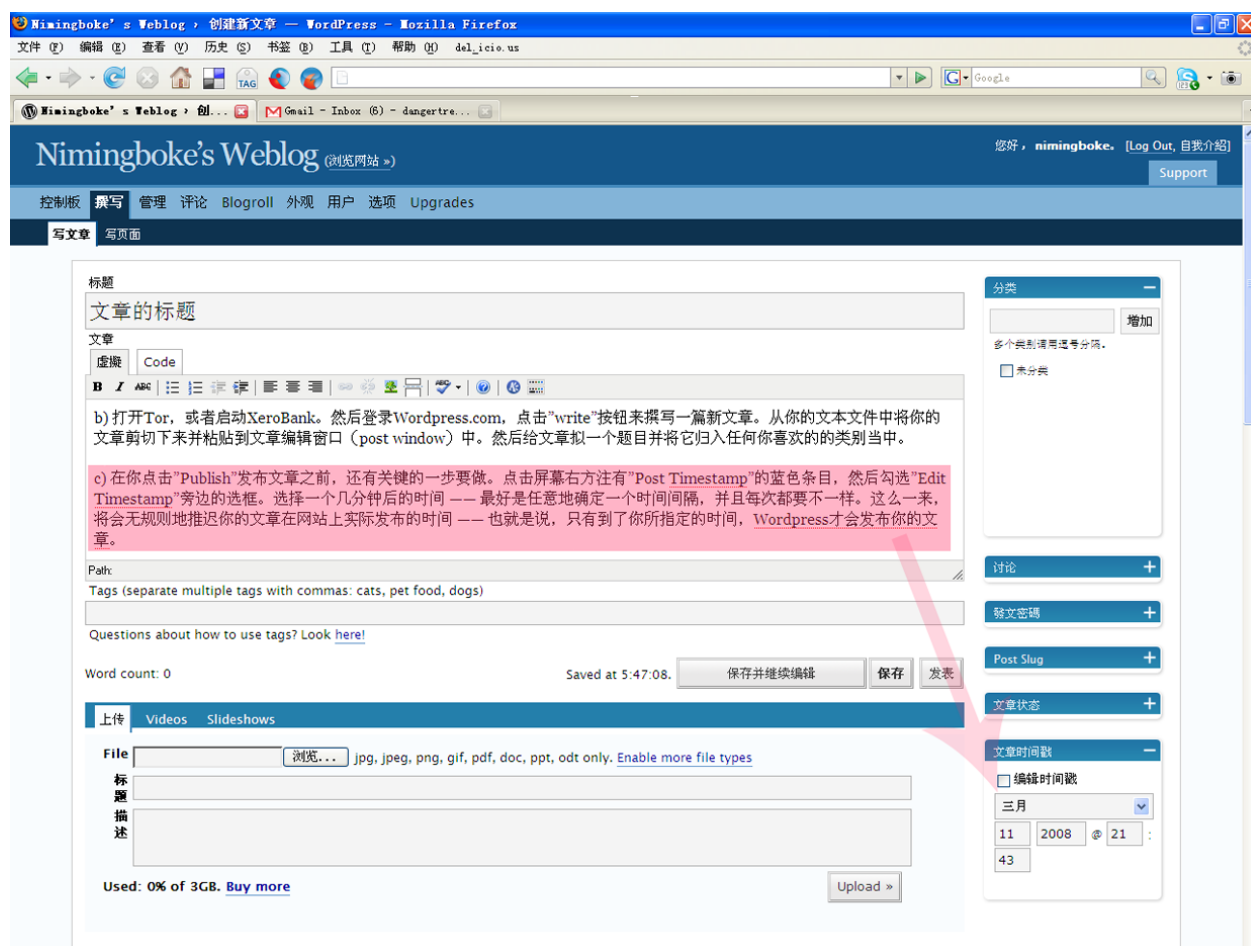
b) Wordpress将会向你的webmail的帐户中发送一个激活用的链接。使用开启Tor功能的浏览器接收邮件并按照激活链接的指示继续。如此一来Wordpress便能确定你正在使用一个可用的电子邮件帐户，从而使他们可以将更新的服务信息发送给你。最后，他们将会公开发布你的博客并将你的密码发送给你。你将需要再次检查你的webmail来接收密码。

c) 继续使用Tor，利用你的用户名与密码登录你的新博客。首先点击“My Dashboard”，然后进入“Update your profile or change your password.” 将你的密码更新为一个你能记住的强大密码。当然你也可以随意向你的简介中添加一些信息……只是要保证信息的任何一个部分都不会联系到你的真实身份。

第四步：在你的博客中发表文章

- a) **离线撰写你的博客。**这种方法不仅避免了因浏览器故障或网络中断而造成的文件丢失的情况，也同时允许你可以在一个比网吧更为私人的地方编写你的文章。而且，我们只需要使用像写字板这样Windows自身所配备的简单编辑器，就可以很好的进行编写工作了。最后要将你的文章保存为文本文件（撰写完博客以后，一定要记住将这些文件从你的机器上彻底删除。推荐使用Eraser或Ccleaner一类的软件，它们不仅提供了各种的语言版本，并且可以自动清除电脑中所有浏览器以及其他应用程序中的临时文件）。
- b) **打开Tor，或者启动XeroBank。**然后登录Wordpress.com，点击“write”按钮来撰写一篇新文章。从你的文本文件中将你的文章剪切下来并粘贴到文章编辑窗口（post window）中。然后给文章拟一个题目并将它归入任何你喜欢的的类别当中。
- c) 在你点击“Publish”**发布文章之前**，还有关键的一步要做。点击屏幕右方注有“Post Timestamp”的蓝色条目，然后勾选“Edit Timestamp”旁边的选框。选择一个几分钟后的时间——最好是任意地确定一个时间间隔，并且每次都要不一样。这么一来，将会无规则地推迟你的文章在网站上实际发布的时间——也就是说，只有到了你所指定的时间，Wordpress才会发布你的文章。

离线撰写你的博客。撰写完博客以后，一定要记住将这些文件从你的机器上彻底删除。推荐使用Eraser 或 Ccleaner；这两个软件不止有各种的语言版本，还可以自动清除电脑中所有浏览器以及其他应用程序中的临时文件。



为什么？

通过编辑timestamp，我们可以有效地防止某些人利用技术手段来确定我们的身份。比如说，你正在撰写一个名为“打到埃塞俄比亚电信公司！”的博客。而这家公司的某个人可能已经开始密切监视这个博客了，并在试图弄清楚是否是他们的某个客户在撰写这个博客。它们开始记录你的博客每次发布文章的时间，并将这些文章的发布时间（timestamp）与他们自己的信息记录进行比对。结果他们发现在一个月当中，每次这个博客发布文章前的几秒钟，他们的一个客户都会接入Tor的某个网点。因此他们推断正是他们的这个客户在使用Tor来撰写博客，并将这件事的相关信息提交给了警察。

通过编辑timestamp，我们可以有效地防止某些人利用技术手段来确定我们的身份。

第五步：销毁你的踪迹

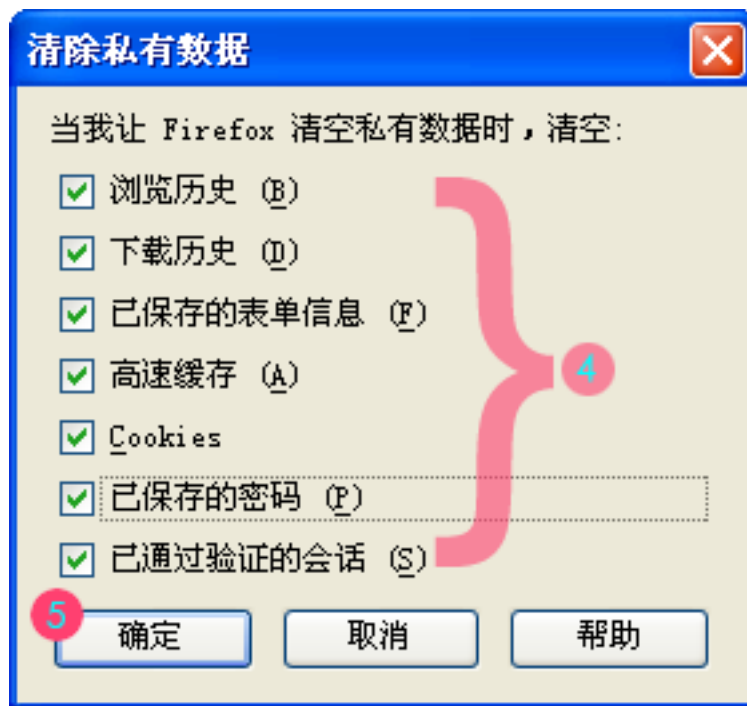
a) 将你的文章草稿从你的笔记本电脑或家用电脑中**彻底删除**。如果你使用U盘将文章带到了网吧，则同样需要删除其中的草稿文件。仅仅是将文件删除到回收站并清空回收站是不够的——你需要使用像Eraser 或Ccleaner这样的专业删除工具，它们会使用数据重新复写旧文件所在的硬盘区域从而使得删除的文件无法得以恢复。在Macintosh的系统中已经建立了这种删除功能——将文件放入回收站并从菜单中选择“安全清倒废纸篓（Secure Empty Trash）”。

b) 在Firefox中**清除你浏览历史**，cookies和已保存的密码。在工具（Tools）菜单中，选择“清除隐私数据（Clear Private Data）”。选择所有的项目然后点击“okay”。你或许想要Firefox在退出时自动清除你的隐私数据——操作过程是“Firefox ->选项（Preferences）->隐私（Privacy）->设置（Settings）”。在注有“退出Firefox前自动清除我的隐私数据（Clear private data when closing Firefox）”的选项前打勾。如果你无法在你使用的电脑上安装程序的话，可以从U盘上运行IE Privacy Cleaner来清除浏览器的临时文件。

为什么？

通过检查你的浏览历史可以非常容易的看到你浏览过的网页。因为在高速缓冲区中储存有电脑浏览过的网页数据，所以更多狡猾的跟踪者还会检查你的高速缓存文件以得到你的浏览历史。我们需要将共享电脑中所有的这类历史信息通通删除以防止这台机器的下一个用户找到它们。我们同样要将这类信息从我们的个人电脑中彻底清除掉，从而确保当我们的电脑丢失、被盗或被扣押时，我们不会与我们曾经编写发布的文章有任何连系。





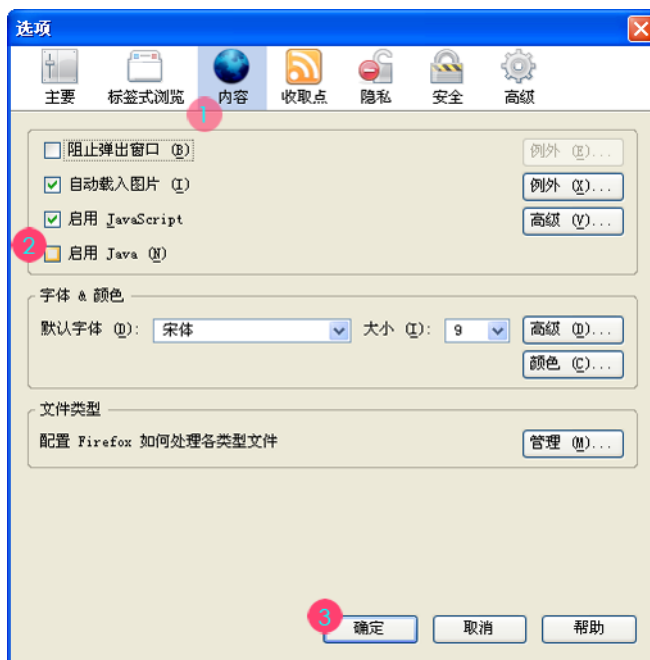
结语：

—— 仅仅是在编写自己的博客时保护自己是不够的。如果你还想要在登录自己博客的情况下在别人的博客上发表评论，你同样要使用Tor来发表。因为大多数博客系统都会记录评论来源的IP——如果你不使用Tor，就等于在邀请经营这家网站的任何人通过你的IP地址追踪到你的电脑。Tor就像是避孕套——千万不要在没有安全保障的情况下博客。

—— 匿名并不代表着你不应该好好地装饰一下你的博客。Wordpress中的“Presentation”选项为你提供了许多选择——你可以挑选不同的模板，甚至还可以上传照片来装点它们。但是一定要非常非常小心地使用你自己的照片——发布一张照片会透漏你的许多信息（比如，如果照片是在赞比亚拍摄的，那就证明了你住在赞比亚或曾经去过那里）。

—— 如果你对自身的安全非常担心，你或许需要更进一步的设置你的Firefox浏览器，并关掉Java。在Java最新发表的版本中有一个致命的安全漏洞，它会允一种许恶意脚本的作者推算出你的电脑IP地址，而且**即使你使用了Tor也无济于事**。我们对此并不十分担心因为我们不认为Wordpress.com或者Google会使用这些恶意脚本……不过，如果你使用Tor有其它用途的话你就需要好好考虑这个问题了。关闭Java的步骤是：打开“Firefox ->选项 (Preferences) -> 内容 (Content)”，然后取消“启用Java (Enable Java)”的选项。

—— 如果你是你们国家中唯一使用Tor的人，事情就变得非常明显了——总是同样一个用户在使用Tor网点的IP地址。如果你想要使用Tor而又担心网络服务商会追查Tor的使用者，你或许可以鼓励你其他的朋友们也一起使用Tor——这样一来，就形成了密码研究者们所说的“覆盖流量(cover traffic)”。除了编写博客，你也许还想要使用Tor来浏览不同的网站。然而无论是哪种情况，都说明Tor已经不仅仅只能用于编写你的匿名博客了，而这也意味着当网络服务商从他们的记录中看到有用户在使用Tor时，并不会自然而然地以为有什么坏事情发生了。



最后一点关于匿名意见：如果你真的不怎么需要匿名的话，你最好不要这么做。毕竟，当你使用自己的真实身份编写博客时，人们可能会把你的话更当回事。但是一些人确实有着匿名的需要，而这也是这篇指导文章存在的原因。请您一定要在真正需要匿名的情况下再使用这些技术。