



# 数字安全实用手册

防御大于技术



# 数字安全实用手册

一份用于敌对环境的实用数字安全指南

[practicaldigitalprotection.com](http://practicaldigitalprotection.com)



Copyright 2017

CC BY-NC 4.0

Creative Commons Attribution-NonCommercial 4.0 International License

[contact@practicaldigitalprotection.com](mailto:contact@practicaldigitalprotection.com)

# 目录

序言	4
简介	6
■ 第一部分: 风险	8
第1章: 了解你的威胁	9
基本保护行为	14
第2章: 电脑设置	18
关于密码的提示	31
■ 第二部分: 电脑安全	33
第3章: 主要规则	34
第4章: 获取信息	39
清空收件箱, 自动删除带来安全的一天	51
第5章: 存储信息	53
隐藏加密和文件修复	67
暗网	69
第6章: 分享信息	70
向正处于安全威胁的人发送信息	80
第7章: 删除信息	82
元数据, 分享发布, MICROSOFT OFFICE	92
元数据和JOHN MCAFFEE	96
■ 第三部分: 手机安全	97
第8章: 了解手机安全	98
第9章: 手机的使用	103
一部手机是如何几乎毁掉一切的	108
第10章: 手机设置	110
关于地理位置追踪的提醒	116
第11章: 可用的安全APP	117
工作日常流程	123
■ 第四部分: 预防性安全	125
第12章: 预防性保护	126

# 序言

如果你正在阅读这本手册，说明你很有可能已经对于基础信息安全的威胁有了意识。这份手册为专门找出信息安全的 key 问题以及如何预防的步骤而建立。它会说明为何信息安全如此重要，在实际案件中的正确操作能让你维持自由，而错误的操作可能会让你或他人进监狱。这不仅仅是一份信息安全手册，也是一份关于更安全的社交行为手册。

编写这份手册的目的之一是为在中国的记者、律师、NGO 工作者等提供一个基于信息安全的实用性解决办法。

## “你面临的大部分威胁更多是来自身体的，而非来自数字”

你应该有听说过 Edward Snowden 和他揭露的美国国家安全局的事件，另外可能在美国电影里也看见过电子监视或政府的特工和黑客攻破密码来盗取信息的对话。不幸的是，没有哪一个是和中国的人权捍卫者相关，甚至是整个世界。这里的关键问题是你要面对的不是美国或其他政府使用大量的资源来攻破你常在使用的邮箱和聊天软件的密码，而真正的问题是在当你被拘留或你的手机电脑被没收的情况下该怎么办。这份手册会将重点放在数字安全的行为方法上。

当说到信息安全，所面临的威胁在中国的体现相比通常意义下的信息安全有极大的不同。在中国面临的大部分威胁更多是来自身体的，而非来自数字。这份手册基于在中国的大量记者、NGO 工作者等的想法和建议，致力于提供一个能指导和对抗大部分的普遍威胁的指南来纠正对信息安全的误解。

你在网上或在可能参加过的其他培训中有接触过的大部分培训材料通常都汇集了大量的技术性解决方案，其中很多都是不必要的高阶。这通常都是因为缺乏深思熟虑的讨论，如何才能真正提升你的安全？不是来自高级的技术性解决方案（虽然有时候是需要的），而是在操作行为上作出轻微的改变。

另外，创建一份没有说明人们实际操作行为和规则的信息安全手册相当于是在浪费时间。如果一份手册只把焦点放在深奥的安全解决方案上，而没有解释它是如何影响我们的日常使用和效率，那它很有可能在一段时间后就被抛诸脑后，只是在初始会被使用，渐渐的就会被忽略，相比初始又减少了安全性。一个真正有用的手册应该是找到平衡点。

这份手册从以上几个问题出发，并展示步骤化、可单独学习的文字内容来让读者辨识和解决最可能面临的安全威胁。



# 简介

欢迎来到这本实用的自学信息安全手册。只需要拿出一天的时间它就能帮助你同时理解你自身的安全威胁以及提升你在使用电脑和手机时的安全性。我们建议你按顺序一章接一章的阅读这本手册，因为每一章节知识的介绍会基于前面章节的内容。

请带上你的电脑和手机阅读这本手册。在开始做任何改变前确保你已经建立了备份，或将你不能丢失的文档和数据都另行保存起来，你可以将它们转移到USB或另一个硬盘，或暂时性的放在你的云存储，后续我们在这份手册中也会教你如何保护你的便携式数据存储，比如USB。

所有章节的编写都基于电脑Win10和OSX系统。但很多的问题也同样适用于智能手机。有很多的App同时适用于iOS和安卓系统，关于智能手机的安全性内容会有专门的章节来介绍。

编写这本手册时有试图将文字写得具有可读性，而且大部分的章节格式都很类似。多个章节会以问题的基本说明或章节的概念为开端，接下来介绍操作习惯的改变减小安全威胁，最后以各种解决方案作为总结。大部分的情况都能在网上找到技术性的答案，所以只有在更复杂或重要的方面我们附上截屏来呈现每一个操作步骤。

手册的技术部分都是颜色标注的。在文字后面打上浅蓝色的背景部分是OSX系统(苹果Mac电脑)和iOS (iPhone)，文字后面打上浅紫色的背景部分是Win10电脑系统或安卓手机。

在章节之间是事例。这些事例来自被拘留过、绑架过或监禁过的NGO活动人士、记者和律师的真实经历，以此来说明信息安全问题对他们造成的影响，更具体来说，这些故事呈现出使用或不使用我们在此提供的建议是如何直接性的在刑讯中帮助或伤害到他们的。注：事例中的所有人名均为匿名或化名。

手册分为四个部分，再拆分为十二个章节。

第一部分 了解你的威胁，提供工具分析你自身的情况，了解什么是你最大威胁，同时也包含一些在你真正进入手册重点内容前的电脑操作步骤，比如改变一些基础的设置。

第二部分 电脑安全，也是手册的重点，内容包括第3章到第7章。每一个章节都把焦点放在某一个具体的问题。比如硬盘加密、安全浏览器、删除等。每个章节都由问题的介绍为开端。接着会有提出改变的提议，同时包括操作行为和技术性解决方案，以及在有必要的地方给予步骤化介绍。

第三部分 手机安全，我们从电脑章节学到的大部分知识都能用于手机和平板电脑，但是这一部分主要讨论那些具体与手机相关的威胁和解决方案。

第四部分 预防性安全。主要目的在于帮助你用实用性的、非信息安全相关的步骤来确保你的安全，如何为最坏的情况作好预备工作。

# 第一部分 风险

## 第1章

第1章了解你的威胁中将介绍存在的不同类型的威胁，引导你如何评估风险和需求，以此懂得如何将焦点放在最重要的威胁上。

## 第2章

第2章电脑设置中介绍如何做出通往更好的数字安全道路上的第一步，手把手教你操作电脑操作系统的基础设置，根据你的个人需求做出相应的更改。





# 第1章 了解你的威胁



通过阅读本章节能帮助你认识到有哪些对你不利的信息安全威胁，了解这些基本的信息能帮助你更好的理解和使用本手册后面的内容。

如果没有弄清所面临的威胁，那可以保障自己安全的操作步骤是寥寥无几的。这个章节简短的概括一些最常见的威胁。如果这里提到的某些威胁对你来说尤其重要或相关，请花时间在网上搜集更多的资讯。如果难以找到好的资源，问题并不清晰或是太技术化，请联系我们予以协助。

## 被强迫失去安全

这是建立这本手册背后最大的原因，因为那些在中国的人权工作者面临的信息安全威胁大大的多于被黑客。关键的威胁就在于被警方或其他人强迫失去安全，让你交出你的邮箱、云存储或加密数据存储的密码。这是整个手册的主线，也是手册把重点放在操作行为上而不是只注重技术的根本原因，因为这是解决这个威胁的唯一方式。当然，我们也会讨论技术性的威胁并提供解决方案。

## 后门通道

你一定不会花掉一个月的薪水买一个新的功能强大的门然后忘了买把锁对吧？或是安装了一个安全的大门和锁，但将后门大大的开着？不幸的是，当说到信息安全，这就是很多人在做的事。他们会设置非常高阶的密码，也会清除浏览器的痕迹，但在手机里会允许App不需要输入密码就能接入同样的服务，或是用手机浏览器使用同样的服务（比如连接工作邮箱），这就是将大门打开让任何获得你的手机或进入手机的人都能查看你的信息。最有效的安全意味着你必须分析自己的情形，如何切实的使用各种

服务和功能，这样，才能避免漏洞。

## 地理位置追踪

当今智能手机如电脑，电脑如智能手机。通过GPS、网络连接和手机无线电信号都能轻易的追溯到你的手机和电脑行踪。如果不设防，他人可以轻易的追踪到你，而且追踪设备的需求并不昂贵。并不需要政府才能实施这些追踪，你的手机从没停止过发送地理位置信号，甚至在没有SIM卡的情况下。已被安装的应用程序也通常会要求连接地理位置，也为别人能追踪到你开启另一扇大门。

## 拦截短信，电话，聊天和邮件

如果没有加密聊天信息、邮件、通话和短信，这些内容就会以纯文字的形式发出去，不仅仅只有服务商能读取，任何在你的网络连接下的人都能读取。幸运的是当今大部分的服务商都有加密功能，但前提是你得远离中国服务商，这些公司很可能在中国政府需要时而交出这些信息。还是那句话，主要的问题不是你发送邮件或短信，而是当你的手机或电脑在被没收后，你被迫交出你的登录密码。

## 安全设置

大部分的电脑操作系统的自带设置都是以使用方便为主，而不是安全。所以，第一步总是应该查阅所有的设置，做出提升安全性的设置。

## 破解密码

通过运行一个密码解读器能分分钟解出密码。使用BF算法（一分钟能尝试千万种可能）能在一小时内破解出4-6位数的密码。在设置和你的安全息息相关的服务密码时，比如你的工作邮箱或加密存储，想一想密码有多容易被破解。一个简短的密码也许能难住街上捡到你的手机的人，但在当你成为警方的目标时却没有任何作用。设置密码，一个长的随机密码是必须的。

## 病毒、黑客、ROOTKITS和其他

这本手册不会把焦点放在黑客威胁上，因为发生的几率不大。总之，病毒和Rootkits（一种恶意的程序，隐藏在电脑内的病毒，能令他人进入你的电脑）是比较普遍的威胁。确保你有开启防火墙，有杀毒软件运行，而且设置了自动更新。定期更新可以确保你的设备具有识别最新威胁的能力，过期的杀毒软件基本上不能保障你的安全。

## 网络连接

如果某人并不打算将你拘留，或是没收你的设备，而是秘密的获取你的信息，你的网络连接自然就会成为攻击的入口。你是否有更换过家里路由器的用户名和密码？答案恐怕是与大多数人一样，No。路由器的登录密码在网上有公布，几乎所有的路由器都是同样的密码。如果有人能连接你的路由器，那么他们也就能进入你的电脑。另外



也很重要的是要留意公共WiFi，它们具有天生的弱点，在公共网络下做任何事都要越加的小心。

## 文件恢复

当你删除一个文件、清空回收站或从电脑转移一个文件到你的USB或其他外部硬盘时，原文件都没有被删除掉，一个都没有。它们全都停留在原来的地方而且可能会待很多年。一个有一点点IT经验的人就能轻易的找到它们，通过下载免费的软件，简单的点击一个按钮就能找到任何从你的电脑中删除的文件。关于删除文件部分也是本手册最重要的内容之一。

你是否明白这些基本的概念以及它们是如何带来问题的？如果没有，请在继续阅读之前上网搜集更多的信息。最关键的方面是了解电脑和手机的地理位置是如何允许他人追踪到的，以及一旦电脑落入他人手里，文件修复工具是如何给电脑带来最大的威胁的。

## 预估你的风险和需求

在继续阅读这份手册前，你需要明白它是如何运用到你自己和实际情况中的。手册中提供的律师、记者和NGO工作者们的事例应该能够让你有更加切身的理解，那些都是非常严重的威胁。甚至如果你的工作不太能置你于被控告或严重的迫害情形，你也可能会在某种情形下被监控，比如当你的朋友或同事出事时，你就可能被通知配合审问，调查或是没收监视你的电脑和手机。如果那时你还没有开始做好保护自己的步骤，这就很可能对你造成一个全新的安全问题。所以，不要因为对于安全问题的忽视而导致小问题变大问题。

### “完善的安全意识能让小问题更小”

#### 第一步：什么是你需要保护的？

你工作的信息是哪方面的，如果被交到警方手里，会如何影响到你。更重要的是，会如何影响到他人？如果你的整个硬盘都被没收，外人能从中获得你和工作的什么讯息？又能获得他人的什么讯息，比如资助人，同事或合伙人？要意识到忽视基本的安全考量会如何影响到你和他人。

## 第二步：哪一个设备有风险？

你是否只有一个手机？也许你还有另一个卖给了你的同事？你只用一个电脑吗，还是也在使用办公室的电脑？或许你有时候会用朋友的电脑查阅你的邮件？列出一个你在使用的或最近在工作中用过的设备清单。

## 第三步：你为什么会有威胁？

你是记者？一旦情况对你不利，他人是否很容易就能找到你的文件？你是NGO工作者？警方有可能做出对你不利的指控，针对你的工作内容以及谁提供的资助金？还是你是一个为当局并不希望被接收法律辩护人客户的律师？

## 第四步：你的威胁是谁？

是当地警方？还是国家安全局的警察？找出谁是最可能的迫害者，再来决定你的安全方案。也许你并不是目标，但你常常一起工作的报社（媒体）是目标。如果是，谁是这个陷害者，尽管你并不是一个重要的目标但你是怎么被卷进去的？

这些问题是在你继续阅读这本手册前需要思考的。这些问题也会在本手册的最后一章，第12章：预防性安全中继续讨论到。试着从现在开始考虑会使这本手册带给你更大的作用，也能令你更容易地理解每一个章节在你自身上的适用性。



## 基本保护行为

一旦被警察或国安带走，就几乎失去了保护自己的机会。特别是在像越南、中国、巴基斯坦这样的国家，执法人员几乎为所欲为的执法方式，更是留下极少的安全保障。他们会让你做任何他们要求你做的，不管是通过威胁你、同事或你重视的人，还是通过直接的身体或精神上的酷刑。在面临这种境况时唯一保护自己的方法就是在这之前你已经做好了保障自己安全的步骤。这些步骤其实都非常简单，而这些看似简单的步骤，你选择做或不做，对你个人的差别就相当于自由和坐牢，或是是否会将他人陷入危险困境。

对警方来说如果要用随机的方法获取你的信息，有太多的服务、邮箱、网络软件，很难让他们有效率的获取。他们需要有大致的方向，从何处下手。如果他们强迫你交出某个服务的登录密码，大部分情况下，他们需要先知道你在用什么服务。在中国，他们可能会估计你有微信账户，在越南，他们估计你会有Facebook账户。总之，除了这几个特别广泛的服务之外，大部分其他的服​​务他们需要先知道你在用的是哪一个。

大部分普遍问题的解决方案都已经在下面的手册内容中提供了。

## 减小可能因为第三方或他人所造成的伤害

首先，你的账户会被发现的原因可能因为他人的遭遇。你平常在通讯的伙伴、同事或其他人可能被带走，他们将你们之间联系的信息交了出去，或是他们有可能出卖了你。也就是说，对于敏感的工作来往，你需要考虑到的不仅仅是你该说什么，还有如何存储信息。这样你得先要有一个专门的邮件或聊天软件用于最敏感的工作，这个账户或邮箱不应该用于你的常规工作和聊天。

这种账号不要使用你的全名，也不要再在邮箱或邮件的内容、聊天会话中包括任何可能显示你的确切身份、地理位置的信息。这样就算是被第三方查出这个账号与另一个人的来往记录，另一个人供述出这个账号是你的情况下，你也还是有一些否定的空间。

这个问题是最大的顾虑之一，也是你自身最难以控制的，因为取决于他人。

要减少此类风险最安全的办法就是在最敏感的互动中使用有自动销毁和删除功能的邮箱和聊天软件。也就是在发件者和收件者双边的脚本和邮件会在被发件人设置的一定时间内被自动删除，比如说在发出邮件后一小时或一天后即自动删除。虽然邮箱发送者的用户名能够被看到，但是由于发送的信息或说“证据”再也无法被任何人打开了，包括你和那个收件人，因为邮件都会按照设定的时间自动销毁，也不可能被修复。



自动销毁邮件尤其是在当你与一个你不完全信任的人通讯时，或与某个非常缺乏IT操作技巧的人联系时很重要。使用方法也很简便，同样地也适用于某些聊天软件。

## 电脑痕迹和证据带来的损失

一旦你被带走或是你的电子设备被没收，当局很可能启动技术化的电脑分析。这是通常警方追踪到你所使用的账户的方式，再通过他们所掌握到的信息，更容易强迫你交出这些账户的密码。一旦他们成功，他们所找到的这些信息就很有可能用于对你或他人不利。这个问题的重要性不用多说，我们也有一些方法来应对。

比如浏览器，通常可以保存和存储大量的数据。最明显的类型是一个链接到邮箱服务的书签，或已访问的网站cookies和更进阶的数据，还有登录信息甚至是密码。

你可以将浏览器设置为自动删除此类信息，但是这意味着每次当你打开浏览器时都需要重新登录每一个网站，包括社交媒体，购物网站等。这样你也不会使用书签功能，这样会让整个使用电脑的过程非常低效，而且看起来也很可疑。

相反地，你应该做的第一件事情是使用双重浏览器策略。一个浏览器用于平日普通的浏览和使用，另一个浏览器用于最敏感的邮件收发和相对敏感的搜集工作。第二个浏览器应该设置关闭时自动清除痕迹，也需要添加特定的安全插件以协助浏览器的清除工作，以便更彻底的移除掉更多的痕迹。

## 操作系统痕迹和证据

与浏览器一样，操作系统也总是在收集你使用电脑的痕迹。这包括网站访问、Word文档的打开和编辑、临时数据和文档的复制等几乎所有动作的脚本。要获得这些信息本身需要更高级的技术手段分析你的浏览器，但是对于拥有大量资源的警方和政府来说这些并不难。

要应对这个问题，你需要用到一个专门清除这些痕迹和电脑内临时数据的软件，幸运的是它用起来也并不难。

## “删除的”资料

一个被误解的最深的概念是从电脑中彻底删除信息，警方了解并利用着人们的这个误解。也就是说，当你“删除”某个资料时，或是清空垃圾箱时，它们都没有被真正的删除。唯一的区别在于电脑或手机将这个“删除”的区域标注成了“可用空间”，后续可以被新的数据覆写。但被删除的数据还在那儿，大



部分时候它们也许可以存在好多年，也有一些情况是“被删除”的一部分数据被新的音乐、视频或其他文件所覆写，但剩下的部分仍然在那儿。

虽然你并不能肉眼浏览或看到它，但是有很简便的免费软件就能轻易辨识这些数据，用于读取和存储这些数据，就像这些数据从来没有被“删除”过。这类的软件使用起来非常容易，实际上甚至不需要懂电脑技术的人都会使用，只需要5分钟就能搞定。一旦你被拘留，这类数据读取的方式会用到你的USB、手机、电脑和其他电子设备中，要记住。

## 你的数据

当然最关键的问题就是你的所有文件了，不管你是存储在USB、手机、外部硬盘或电脑内的文档、视频，或照片，保护这些信息的唯一路径就是将它们存储在一个具有高级安全系数的地方，那就得是在电脑内的一个加密的、非常隐蔽的硬盘内。

也就是说，如果只是基础加密，警方可以通过直接或数据分析的方式就能找出，所以，要真正的保护好你的信息，就需要使用到“隐藏的”加密空间，让他们根本不知道你有加密的信息存在，这样他们也就无法通过威胁或酷刑让你交出他们根本不知道是否存在的空间密码。

而且，这个步骤的操作比听起来简单多了。

你也应该将存储简单化，意思是说不要将所有的工作文档都存进这个空间，而是仅存储那些有必要的。大概浏览一下你的旧文件，很有可能大部分的文件你都不会再需要了，草稿、以使用过的文件、内容已经被加入到主要文档的协助文件等等，这些都应该被删除。仅存储那些真正有需要的文件。

你也可以将需要保留但可能不会用到的旧文件转移到一个安全的云存储。你需要使用一个安全度高，在中国没有服务器的云存储服务。另外你也需要留意浏览器中的信息，要确保警方无法发现你所使用的云存储并获取登录方式。

## 手机，PAD和APP

在工作中要将电脑和手机的使用分开，这两者之间不要有重叠。所做的安全步骤都有可能因为疏忽的使用手机而毁于一旦。自动销毁脚本文件，保持清除浏览器痕迹的动作都有什么用呢？既然警方都能在你的手机上轻易的找到这些信息的话？

人们通过手机内的App进入账号和服务，使用手机App不仅相当于给予警方直接的（虽然有限）进入你的账户的通道。比如邮箱，就算是你为手机的App



额外设置了密码保护，但这样还是暴露了你在使用的服务，这样他们还是可以强迫你交出密码。手机可以让你所做的电脑安全设置功亏一篑，这样的事件发生过很多次。

务必仔细研究手机的使用方式，务必避免在手机中使用工作相关或能被察觉到你在使用的服务App。此外，不要用手机内的浏览器进入工作（敏感的）网络邮箱，因为手机内的痕迹是几乎不可能清除掉的。而且，在手机内彻底的删除也非常难，坚决不要用手机存储任何工作文件，也不要临时下载任何工作文件再转移到电脑。

## 你自己

最后，你是你自己和他人最大的威胁。要保护好你自己的信息、文件和数据需要你做好充分的计划。除了做出必要的风险评估之外，你也需要做好计划，如果在被带走的情况下你会做出哪些反应。而且还要将你的计划告知几个你信任而且不太可能会被带走的朋友。一旦被审问，什么样的信息是你该说的（因为你一旦进去，你总是得要说一些东西，否则很明显他们知道你在隐瞒），什么样的信息是你一定要保护的？同样地，如果你有同事，你们需要一起讨论出一个每个人都同意的应对方案。你也需要考虑到他人最有可能会放弃保护的信息是什么。

在政治领域有一句话是这样说的：绝不要撒公众能够发现的谎。对你来说，则是不要撒警方能够发现的谎。关于这点我们并没有技术性的解决方案，只能靠你自己的谨慎和智慧了。

## 但是

现今，在像泰国、越南、中国等国家要不提供身份证明注册一个SIM电话卡可以说是很难。这也就意味着当所有的互联网服务供应商（ISP）要求你的ID设置网络连接时，也就产生了问题。在中国和越南，警方可以任意要求连接到通信公司和网络公司的运作记录。这些公司通常都有将客户使用服务的记录存储起来，比如他们会记录下你使用手机的情况，包括你的地理位置，网络使用情况等等。

也就是说因为上面提到的这些情况，你在手机内所做的为了保护数据、隐藏使用的服务（比如邮箱）等步骤都可能变得徒劳。幸运的是，你可以通过使用VPN或TOR对互联网服务供应商隐藏上面提到的大部分信息。

手机的安全问题并不是那么好解决，所以，针对工作，我们还是建议你使用电脑，而不是手机。



## 第2章 电脑设置





本章节会教你在PC和MAC上作出一些必要的设置。通过阅读本章节的内容，你会更加理解电脑的基础设置，如何的调整和控制你的电脑。

作为本手册一个提示，对于技术操作介绍的部分我们会在Win10和OSX中用到搜索功能。也就是当要做一些技术性的设置时，我们会提供搜索词以找到具体的设置位置，也许你已经非常熟悉搜索功能，但是这里我们还是截屏展示一下搜索区域在Win10和OSX中分别所在的位置。（如图Win10·01和OSX·02）

因为不能确定你的电脑用的是哪种语言，搜索的关键词我们会提供中文和英文，搜索词会以加下横线的方式显示，比如：搜索词。

在所有针对技术问题的介绍中，只要有使用截图（图片），这些图片都会被命名，标注相应的序号和参考名。这些截图名要么根据特定的操作系统，比如用WIN10或OSX命名，要么是在这两个系统都适用的软件截图，则用WIN10+OSX命名。同样的方



式在第三部分手机安全的介绍中也一样，手机部分截图则用Android和iOS来代替。

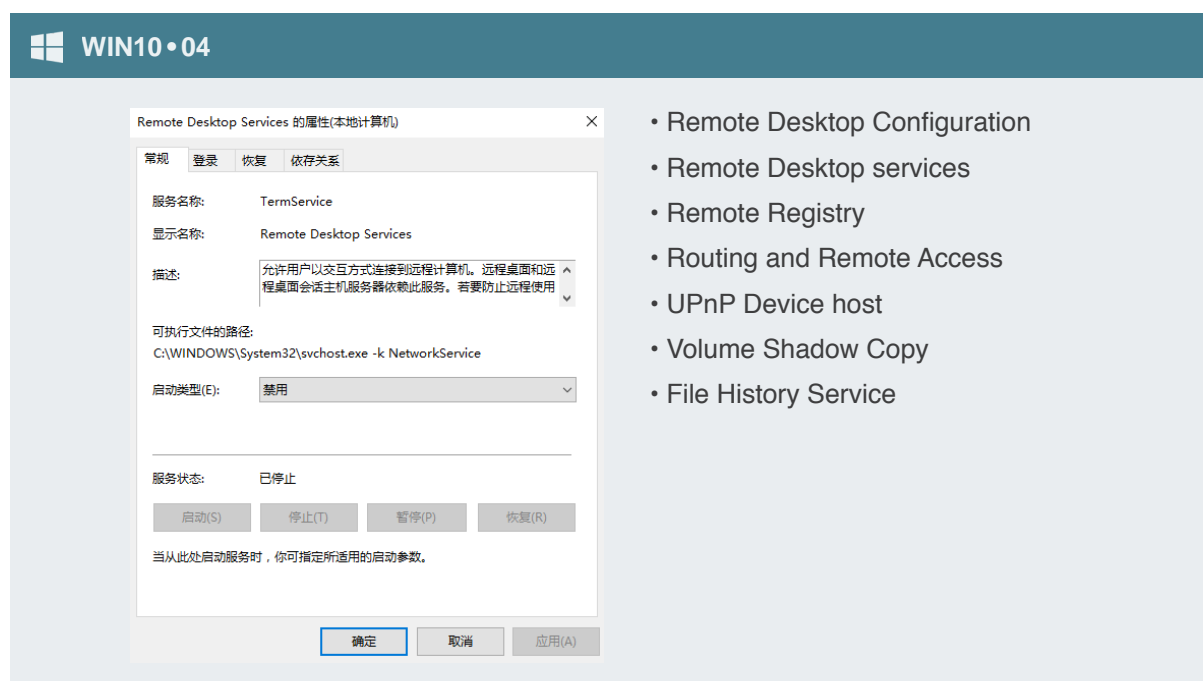
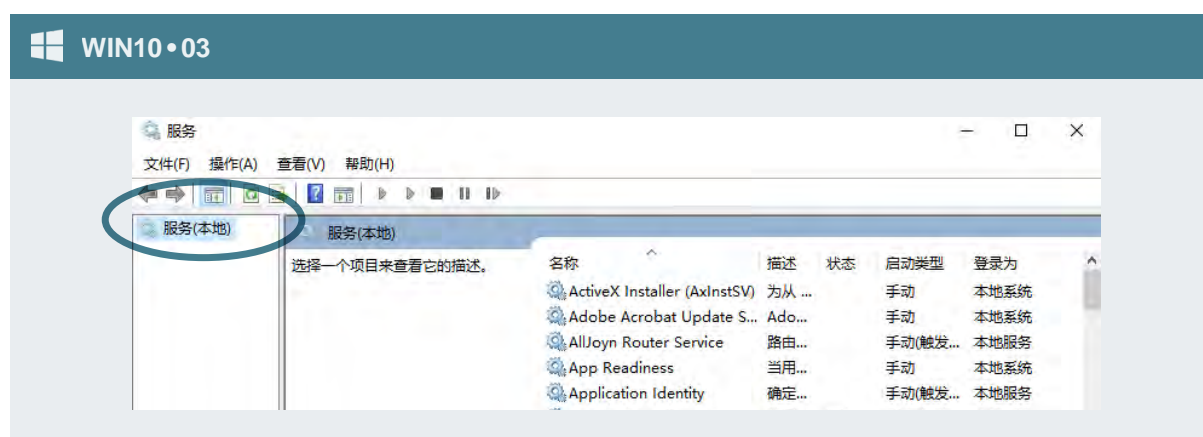
针对Win10的系统，我们在进入到手册最重要的部分前，需要注意的问题主要分为三个区域：服务、本地安全策略、和设置。

## 服务 (英文：SERVICES 中文：服务)

在电脑的后台运行的服务决定你的电脑能够做些什么。比如，要拒绝远程登录到你的电脑，在服务项内的远程功能就应该被禁用。我们会列举出几个关键的需要被关闭（禁用）的服务以提升安全性。

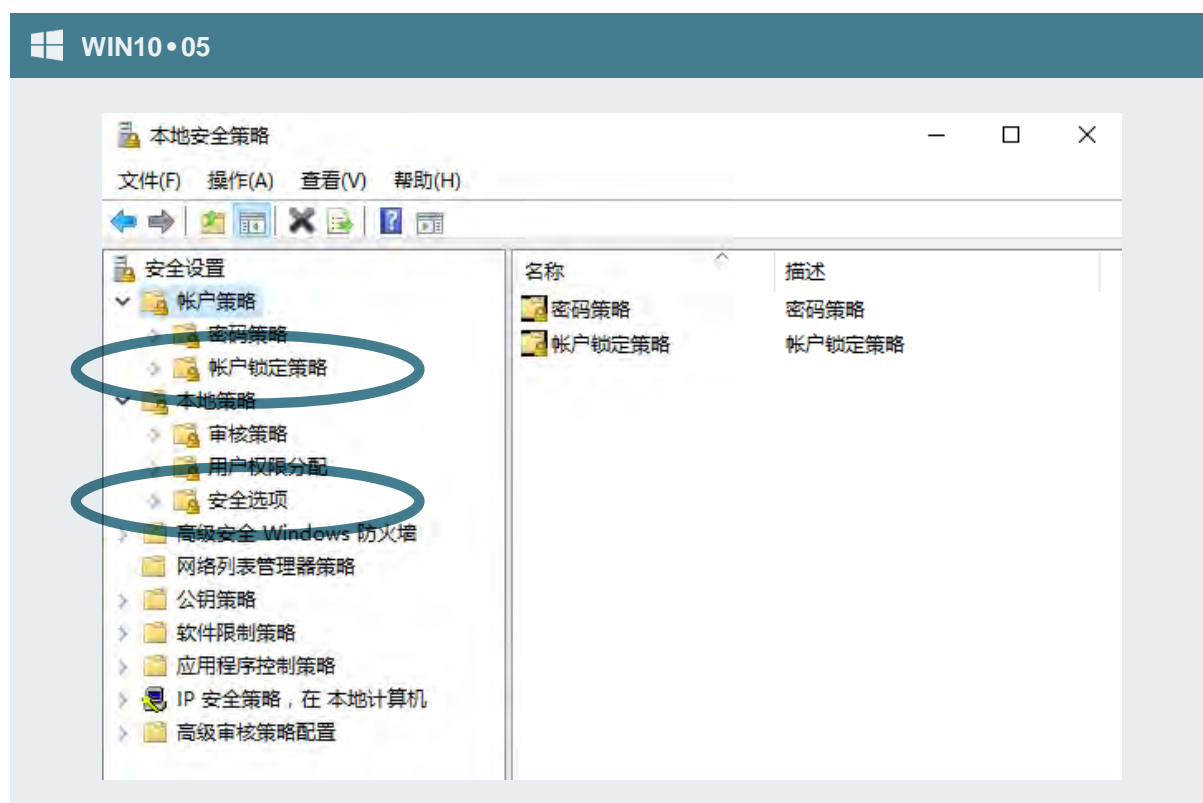
在Win10系统，在搜索栏键入服务即可打开服务的设置窗口，在打开的窗口（WIN10·03）中找到各项服务的列表，在各栏双击进入设置。

双击后跳出的小窗口，找到启动类型，点选禁用，再点确认即可。

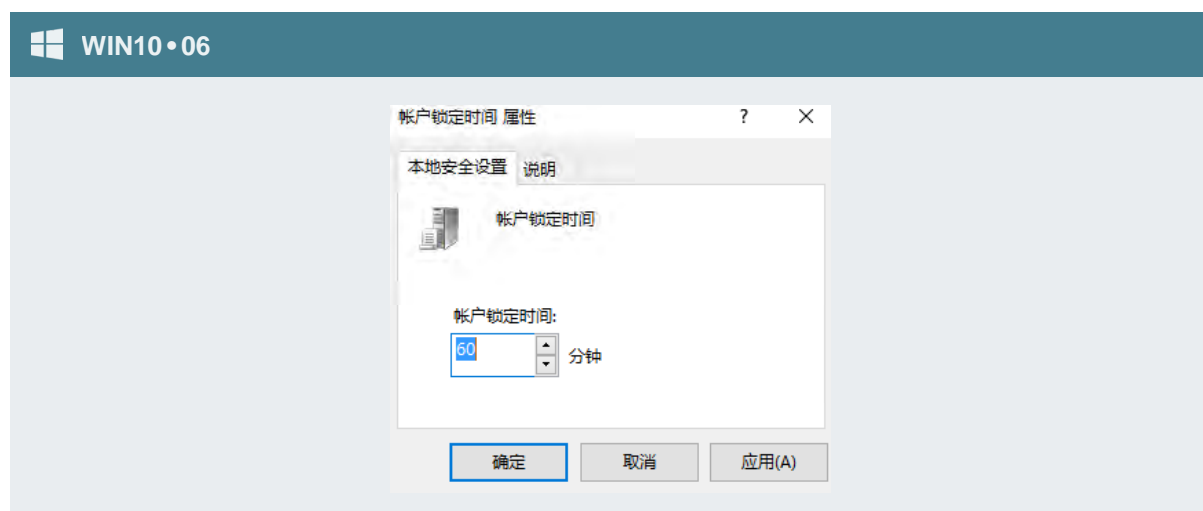


## 安全策略 (英文: LOCAL SECURITY POLICY 中文: 本地安全策略)

安全策略区域允许你为安全相关的问题设置策略。比如说, 你可以设置如果有人连续用错误的密码尝试进入你的操作系统5次, 电脑就会冻结1小时。关于一些必要的安全策略设置我们会一一介绍。在搜索栏键入本地安全策略就能打开设置窗口 (WIN10·05)。

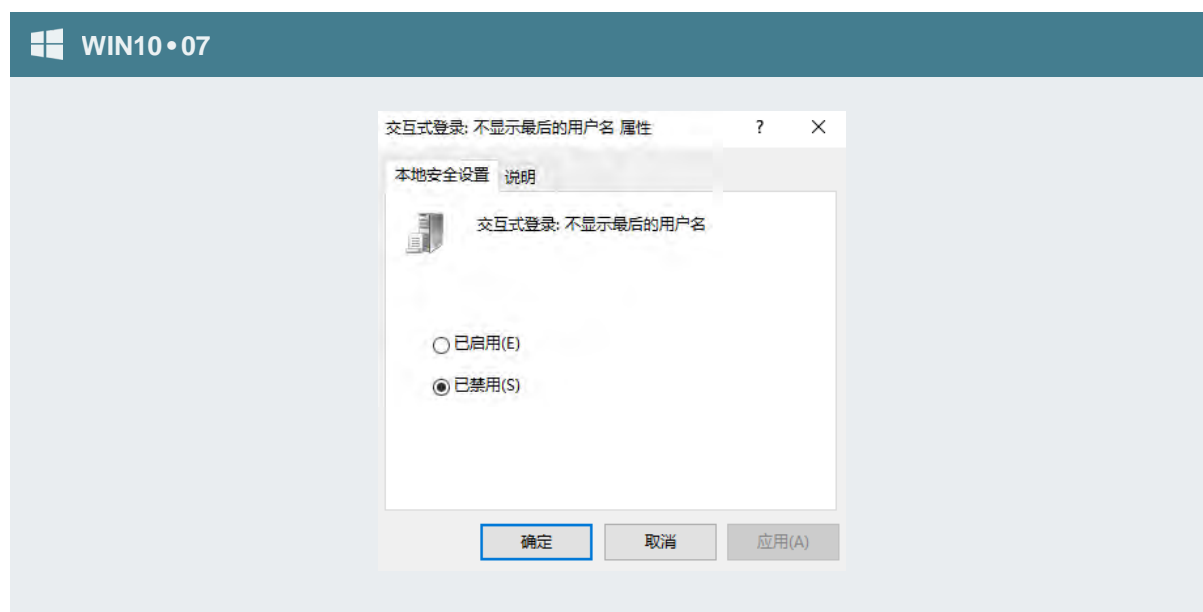


点击帐户策略, 然后再点帐户锁定策略, 双击右边窗口的帐户锁定时间, 在跳出的窗口中选择时间, 可以输入60分钟再点击确定 (WIN·06)。然后再双击帐户锁定阈值, 键入3或5, 意思是如果连续输入3-5次错误的密码, 电脑会按照你设置的锁定时间冻结。



注意: 在进入下一步之前, 先确保你知道你的Win10系统的邮箱和密码, 在下面的这一步设置后你需要用到账户登录。

点击本地策略, 再点安全选项, 双击右边窗口的交互式登录: 不显示最后的用户名, 点选禁用并确定。双击交互式登录: 锁定会话时显示用户信息, 点击下拉菜单选择不显示用户信息并确定。(WIN10·07)



最后, 很重要的步骤, 位于本地安全策略窗口下的本地策略>安全选项栏下, 找到关机: 清除虚拟内存页面文件并双击, 选择启用再确定。关于这个问题在第7章: 删除信息中有更详细的介绍。

## 设置 (英文: SETTINGS 中文: 设置)

这一项包括一些基本的设置, 比如允许App和程序使用地理位置服务或允许使用照相机和麦克风等。也包括一些能提升安全性的设置。

更新 (英文: Advanced Windows Update settings 中文: 高级Windows更新选项)。点选自动的更新方式, 在更新Windows时提供其他Microsoft产品的更新前打勾。

Windows Defender (英文: Windows Defender settings 中文: Windows Defender设置)。开启实时保护和基于云的保护。

备份 (英文: File History settings 中文: 文件历史记录设置)。确保这个选项没有选择和添加任何的备份驱动器。

位置 (英文: Location privacy settings 中文: 位置隐私设置)。确保定位是关闭状态, 然后再点击下面的清除这台设备上的历史记录清除。与智能手机不一样, 在电脑上从来都不需要使用到定位。

摄像头 (英文: Webcam privacy settings 中文: 摄像头隐私设置)。如果你很少使用摄像头的功能, 直接点选关闭。如果经常使用, 可以将此项开启, 不过要到下面的具体的可允许使用摄像头功能的应用中, 一个个的点选, 将那些不需要使用到摄像头功能的应用全部点关闭, 仅在你会用到摄像头功能的应用后点开启 (比如Skype)(WIN10·09)。在设置区域的其他一些项目, 比如麦克风和联系人等, 都是与摄像头一样的设置方法, 要么直接关闭服务, 如果开启的话则个性化的选取那些可允许的应用。

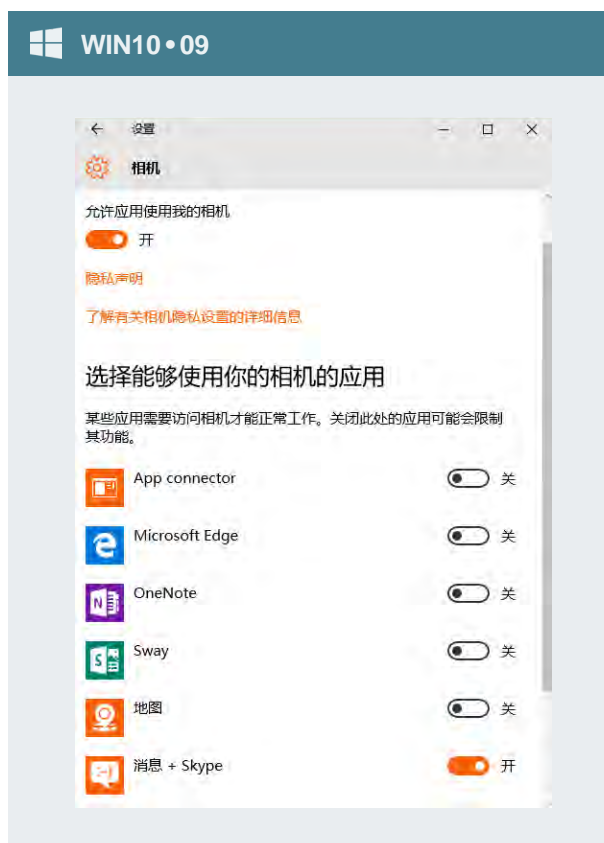
麦克风 (英文: Microphone privacy settings 中文: 麦克风隐私设置)。如果你很少使用麦克风, 则直接关闭。如果经常使用, 则开启, 不过需要一个个浏览下方的应用, 仅开启会使用到麦克风的程序 (比如Skype), 其他的则关闭。

Cortana (英文: Cortana & Search settings 中文: Cortana和搜索设置)。关闭所有的选项, 这是Win10的一个搜索功能, 擅于收集你的上网活动信息, 因此, 最好关闭这个功能。

账户 (搜索Privacy或隐私设置, 进入账户信息)。关闭账户信息。

联系人 (英文: Contacts privacy settings 中文: 联系人隐私设置)。查看所有能够连接到你的联系人的应用, 将不必要或没有使用的应用关闭。

在隐私标签下 (英文: Privacy settings 中文: 隐私设置) 进入常规、日历、通话记录、电子邮件、消息传送、无线电收发器和其他设备, 将每一个都设为关闭。除了你确定要允许某个功能的连接的情况下, 不过应该不太可能。





在反馈和诊断选项内（英文：feedback settings 中文：反馈设置），在Windows应该询问我的意见栏下点选永不，在向Microsoft发送你的设备数据栏点选基本。

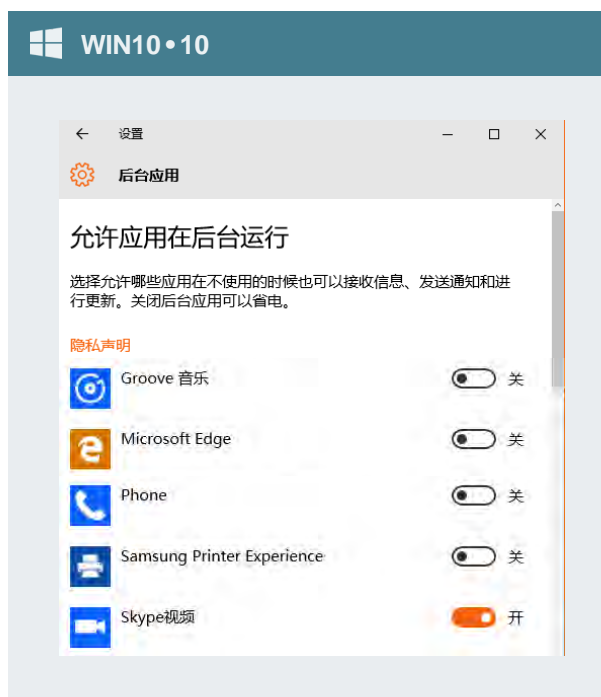
查看你的登录选项栏（英文：sign-in options 中文：登录选项）。确保在电脑进入睡眠后需要密码才能恢复。

查看你的开始设置（英文：start settings 中文：开始屏幕设置）并在以下的选项前设置为关闭，包括显示最常用的应用、显示最近添加的应用、在“开始”屏幕或任务栏的跳转列表中显示最近打开的项。

打开蓝牙设置（英文：Bluetooth settings 中文：蓝牙设置）并关闭蓝牙服务，仅在需要使用时才打开。如果有时候你会使用到蓝牙服务，则点击进入更多蓝牙选项，在新跳出的窗口中，不点选允许蓝牙设备查找这台电脑，而是在新Bluetooth设备要连接时通知我前打勾。

搜索（英文：Allow remote access to your computer 中文：允许远程访问你的计算机），确保远程协助和远程桌面都是不允许的。

最后，在隐私栏最下方的后台应用（WIN10·10），一个个查看哪些应用有被允许在后台运行，将所有你不需要在后台运行的程序都移除掉。如果有在电脑中使用聊天应用的话，



那它们就应该被允许在后台运行。（但是最好还是避免在电脑上使用聊天软件）。

针对OSX系统的设置会相对比较容易，所有的设置通过系统偏好设置栏管理，一旦打开，不需要使用搜索关键字就能轻易的作出更改。通过点击苹果菜单找到系统偏好设置后 (OSX·11)。偏好设置窗口(OSX·12)下需要更改的选项在下图中做出了标记。

## 安全

在安全选项下，你可以做出多种类型的安全设置。进入安全后（在有些OSX系统版本叫做安全性与隐私），从第一个通用标签入手(OSX·13)，启用进入睡眠或开始屏幕保护程序X分钟后输入密码，在框中填入比较小的数字，比如1-5分钟。往下再勾选停用自动登陆。在做任何系统偏好的更改设置前，你需要先点击窗口左下角一个锁的图标(OSX·13)，输入用户名和密码后才能成功的更改任何设置。第一个标签FileVault可以暂时忽略，因为后续我们会在加密硬盘的章节中介绍到。



第三个标签防火墙，点击打开以激活防火墙 (OSX·14)。



在新版本的系统中，你会看到有第四个标签隐私（OSX·15）。在这里你可以控制应用程序的权限，比如定位服务和通讯录等，确保将定位服务关闭，再浏览一遍各个应用程序都有什么权限。

点击高级按钮，点击启用隐身模式（OSX·16），现在安全的设置就已经完成了，可以再回到系统偏好设置的屏幕。



## 蓝牙

在蓝牙选项下，你需要保持蓝牙是处于关闭状态，只有在你需要使用的时候再手动打开。

然后点击高级按钮，确保不要选中允许蓝牙设备唤醒这台电脑。（OSX·17）



## 共享

在共享选项，在服务标签下（OSX·18），要确保电脑的名称与你的实名没有任何关联，另外也不要允许其他的账户进入你的电脑。在左边的服务下的所有框前都不要打勾。



## TIME MACHINE

在Time Machine选项下，确保Time Machine处于关闭 (OSX•19)，这是一个自动的备份功能，你不会希望被后台建立备份文件，因为这会带来安全威胁，更多关于备份的介绍也会在后续的章节中讨论。



## ICLOUD / MOBILEME

只有少数的OSX新版本在系统偏好设置内显示iCloud。iCloud是一个自动的、基于云备份以及同步的功能。与Time Machine一样，都会对安全造成一定的威胁，最好

不要使用为好。如果你有启用过(可能早期有要求你手动设置开启过), 关闭它。如果你从来没有使用过, 则点击这个图标, 确保是未被启用的。(OSX·20)

有一些版本还有MobileMe, 与 iCloud的情况一样, 如果你的版本有这个选项, 则点进去, 选择禁用。



## 通用

在通用选项下, 确保在最近使用的项目栏下将数字设置为0。这个选择能确保如果他人打开你的应用程序或文档, 电脑不会显示你之前有操作过的文件和程序。(OSX·21)



## 用户与群组

用户与群组, 在有的版本中叫做账户, 确保你不允许客人用户进入你的电脑, 客人用户应该被禁用 (OSX·22)。

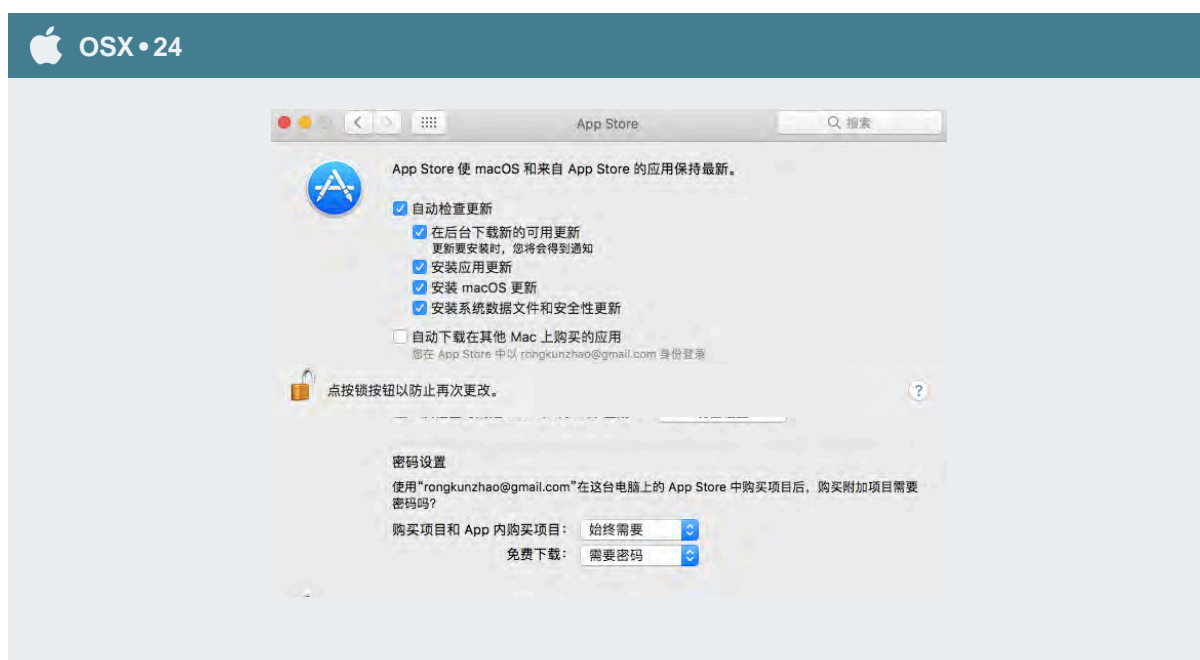
接下来, 点击登录选项 (OSX·23), 确保自动登录设置为关闭, 然后将登陆窗口显示为名称和密码, 这样每当你进入电脑时会要求你输入用户名和密码, 而不是只有密码。在做出这个选项前请先确保你记得你的用户名, 不要点选显示密码提示。





## 系统更新/APP STORE

在应用更新下你的电脑会每日自动查看或下载更新，在新版本的OSX中更新的选项在App store下，当你收到一个提示消息告诉你系统有新的更新，可以选择安装。也要确保你的电脑有设置自动检查更新以及自动安装应用更新 (OSX·24)。虽然你一般会收到有可用更新的通知，但是在设置中勾选了自动检查和安装应用更新能确保一旦有可用的更新即可第一时间收到通知并安装。



## 节能

在节能选项下 (OSX·25)，确保禁用唤醒以供Wifi网络访问。

恭喜你！手册最无枯燥的章节已经完成了，现在我们移步到手册的最主要部分：第二部分。





## 关于密码的提示

我们由不直接讨论密码来展开这个部分，如果警方得以进入你的账户，对你大的保障是让他们无从问起。这也是为何你的工作浏览器必须是在每一次关闭时都要删除痕迹（第4章：获取信息）的原因，也是为何你应该将工作文件（第5章：存储信息）隐藏在加密空间，为何在关闭电脑时用CCleaner擦除所有的工作痕迹（第7章：删除信息）的原因。

简单来说，就是如果他们不知道你在使用的服务有哪些，那他们也就无从问起你的密码，这是你保护自己的方式，也是任何安全行为的最关键，确保他人找不到你在使用的服务，也就无从强迫你交出密码。

密码通常称作password，有时候也叫passphrases，前者的字面意思是单词，后者为句子，这两者的说法与现实情况都相违背，为什么呢？看下面三个方法是怎么破解密码的。

第一种形式是 社交工程法，就是基于你是个什么人以及你的背景来分析出你的密码，比如用你父母的生日数字结合你宠物的名字，或是你最喜欢的运动等等。

要避免社交工程法的分析破解，就要记住不要用名字，自己、家人和朋友的生日数字等等用作密码。

第二种形式是字典式攻击法，就是电脑可以在几分钟内过滤所有的字典，同时也会结合单词，甚至是长句子，能够很快就被破解，大概几小时内就能完成。

要从字典式攻击中保障自己的安全，就千万不要只设置包含字母的密码，就算是长句子或俚语，特别是要避免中文和英文的单词。

第三种形式是暴力破解法，用电脑以每分钟分析千万种的字符结合，一次暴力破解能很快解出一个简短的密码，就算这个密码是随机的，特别是仅使用4-6位数字的密码。

防范的方法是不要使用太短的密码，应该包含所有四种类型的字符，这样才能让暴力破解更难以破解出任何密码。

键盘是由四种不同的字符组成的，有大写字母（ABC），小写字母（abc），数字（123）和特殊字符（?!@）。

一个好的密码应该是在每一组里面包括至少一个字符，最少长达10个字符，如果是敏感账户，切记跟随上面提到的所有规则，设置一个更高级的密码。





可以试试网上测试密码强度的服务，比如How Secure is My Password。别用真实的密码测试，可以随机键入密码试试。这个网站会根据你的密码长度得出你的安全程度，并且计算出破解它要花多少时间，有的只需几秒钟，有的则长达几百万年。(https://howsecureismypassword.net/ 占)

也要确保用于工作的密码不要与私人使用的服务密码相关联。工作相关密码不要和网上购物账号等私人服务密码有任何类似的地方。比如，你的私人密码使用的是Innoj-A7?，则工作密码就不要使用InnojH\*ASH-B7?，这两者间太相似。确保这两个密码间不要在结构和类型上有任何相似的地方。

我们也不建议你使用密码管理软件，比如KeePass，除非将这个软件存入一个隐秘的加密USB中。如果将密码管理软件安装在电脑中，只需要一个粗略的浏览就能知道你在使用，那警方就能轻易的通过这个软件中存入的各个服务密码，一个个的登录你的账户。另外我们也不建议你将密码管理软件存储在隐藏加密硬盘内（关于加密硬盘的内容在第5章：存储信息），不建议的原因是如果你的隐藏空间被找到，他们也就能找到你的密码清单，那也就表示所有存储的密码都会一一被攻克，所有的邮箱和其他服务密码都会被找到，而这些也正好是你本身最需要隐藏的信息。

## 视网膜和指纹识别

千万不要使用视网膜识别、指纹识别或其他生物识别信息服务，它听起来似乎是高端的技术，但是远远比不上一个强度高的密码来的安全。鉴于我们上面提到的步骤，一旦这些生物识别信息被泄露，与密码不一样的是，它们是无法改变的。如果你的密码被泄露你能轻易的再建一个新的，但你却不能再建一个新的眼睛和指纹。

也就是说，如果你设置了视网膜识别和指纹识别用于进入手机或解密文件，一旦你被拘留，警方甚至不需要给你施压以获得你的密码，他们只需要将手机拿到你的面前，对着你的脸部或抓住你的手指按住屏幕就可。你是不是处在清醒状态都不重要。所以，千万不要使用。



# 第二部分 电脑安全

第二部分是关于电脑的内容，包括五个章节，随附一些简短的插页。

## 第3章

主要规则，手册中最重要的章节，因为介绍了基本的使用习惯和规则能大大的多过技术解决方案带来的安全保障。

## 第4章

获取信息，介绍网络连接，如何在浏览网页时隐藏你的IP地址，浏览器的使用以及如何获取信息。

## 第5章

存储信息，如何安全的存储数据和文件。

## 第6章

分享信息，包括安全邮箱，云存储，与他人分享信息和安全会话有关的使用方法。

## 第7章

删除信息，介绍在IT安全中的关于删除信息的误解，教你如何完全的删除。



数字安全实用手册

## 第3章 主要规则



通过阅读本章节的内容会帮助你了解到存在的数字安全威胁，了解这些基本的威胁得以帮助你更好的理解本手册接下来的内容。

很多网络安全的因素都不在于技术，而在于使用习惯。鉴于此，以下会介绍一些重要的使用规则。如果无法马上将这些方法贯彻到操作习惯上也不必担心，因为我们后续会在相关的章节中详细讨论这些问题。总之，这些规则能令你在个人安全、使用电脑和手机的安全道路上走得更远。所以请用心阅读这个简短的章节，这样在学习这个手册的不知不觉中就掌握了这些关键。

在阅读完每一个主要规则的说明后，先暂停，问自己如何将它们贯彻到你的使用习惯和日常上。这些规则并不复杂，但需要一些时间来仔细的思考每一个主要规则，这会令你掌握它们之间的关系并贯彻到你的日常中。看是否已经理解了这些线上和线下的习惯建议？如果还没有的话，想想为了达到安全，你需要做出哪些改变？如果有问题或疑问，圈出它们或写下来，它们很有可能会出现在手册接下来的章节，如果没有，我们也会附上额外信息的来源。

## 了解你的威胁

要在无处不在的威胁中全面保卫自己是不太可能的，就算把它当成全职工作来做也不一定能100%保障安全。现实点来说应该把焦点放在主要的威胁上。因为在中国的NGO工作者、人权捍卫者、记者、律师们面临的多种本质威胁，我们将范围缩小到那些主要的威胁，也是作为这本手册的基础。总之，要了解到对你不利的各种方法和技术是一条漫长的路，这也是为什么阅读和理解第一章了解你的威胁很重要。坐下来

分析你自己的情况，确定个人倾注的焦点是什么，了解你面临的威胁的前因后果，它们来自哪里，如何让它们远离或是让它们变得没有那么严重，这些都很重要。在第12章的预防性保护中能根据我们提供的要点一个个划出你面临的主要威胁和可能性。

## 简单化 简单化 简单化

即使是专家也会觉得管理多个程序的安全维护要比仅几个程序的安全维护困难得多。多一个程序就多一份安全威胁。你要做的第一件事情是查看电脑和手机里的所有程序，看是否都在使用它们？如果没有的话，删除它。它们是否是必要的？如果不是，删除他们。现今，一部手机能很快的被各种聊天软件填满，但是不一定真正有必要的使用它们，如果多半都不能用到的话，删除它们。这也是一个为手机和电脑腾出空间和加快速度的加分项。

## 避免中国公司和中国程序

不像外国或至少西方国家的公司、服务和程序，中国程序没有强大的加密功能。中国程序收集到的用户信息不受法庭保护，而是随时开放给政府和警方在他们需要的情况下浏览的。因为对加密的缺失，数据也较容易被他人获取。中国的程序被证实相对类似的外国公司要获取更多的用户信息（QQ大概是中国公司里面最糟糕的）。他们有可能在安装时顺带建立“后门”，给政府直接的通道连接到你的电脑和手机，甚至是在你不知情的情况下。只要一个程序，比如微信，就能造成你整个手机和电脑的安全威胁，要当心！

## 零收件箱策略

邮箱面对的最大威胁不是被高级的黑客入侵，而是当你被拘留时，警方强迫你交出你的邮箱密码。如果被拘留，警方就有机会获取你的邮箱登录密码，要么你交出你的密码，就算你不交出，你的同事或朋友有可能交出他们的密码给警方，这样你和他们所有的通讯记录都会被警方看到，这也是为何零收件箱策略能带来便利，是为你带来安全的重要工具之一。

设想在你被带走后你交出了邮箱密码，这个零收件箱策略则能保证没有任何内容可以被看到，简单来说就是保持你的收件箱（和其他的文件夹）为空。同样地，让你的同事和朋友也如此操作。这也会在后续的第6章：分享信息中继续讨论到。

我们也会给你介绍一个安全的、有自动销毁和高级加密功能的网络邮箱服务，类似聊天软件Telegram和信息软件Signal，这样你就不用再担心邮件的问题了。

## 无回复约定

无回复约定是零收件箱策略的延伸版。如果你的邮箱确实被人登录了，他们只需要稍微等一等就能了解你的大量信息，因为我们一般在使用邮件的方式。当我们通信时，我们通常都是在当前的邮件下点击“回复”，而不是重新写一封。鉴于此，早前的通

信内容会包含在同一封邮件内，通常这样来来回回的回复可以持续很长一段时间，也因为这样，一个简短的新邮件会包含一段更长的早期邮件内容。也就是说，如果你的邮箱被控制了，控制的人只要等人用回复功能回复你的邮件，就能读到你们先前的通信内容。

所以，当你用邮件回复你的同事或朋友时，避免使用邮箱的回复功能，换句话说如果要用的话，确保删除原先的邮件文字。这能确保在被拘留的情况下，如果警方在查看你的邮件，一封新的邮件到来时，也只会包含尽可能少的资讯，而且他们也无法仅从收到的任何使用回复功能邮件中就能应对你的零收件箱策略。更多的关于个人邮件和安全邮件习惯的内容都到会在第6章：分享信息中有更详细的介绍。

请告知你最常通信的朋友或同事避免使用回复功能。

## 保障基础设置

你不会花10000人民币买一个高级的安全门和锁，但不关家里的窗户对吧？对你的电脑和手机来说是同样的道理，不幸的是，电脑和手机通常自带很多的设置，其中大部分的设置并不安全，所以，在开始为它们加入更技术化的解决方案和提升操作习惯来提升你的设备安全性前，需要先确保这些基础的安全。这听起来比较无聊，都是针对各种小问题的操作步骤介绍。但是，这会让你自身和电子设备更加安全。关于这些基础设置的各种问题会出现在第3章：电脑设置和第10章：手机设置中，我们也建议你在读完这个章节后就马上动手操作。

## 更新 更新 更新

定期更新的重要性提多少遍都不算多。而且是最容易被人忽略的安全缺口，千万别犯这个错误。务必将操作系统（OS）设置为自动更新，确保你的浏览器设置为自动更新，对于其他任何工作相关的程序都是一样的道理。也许你会因为时有的更新而暂停手边的工作而气恼，但这是保护你的电脑和手机安全的关键。宁愿多花几分钟更新程序，而不是花几个月时间待在看守所吧？程序、OS和各种服务因为新的“漏洞安全”被堵住变得更安全，新的威胁都被找到并且应对，只有允许了自动更新才会让你从中获得安全。已过期的程序通常都很容易受恶意软件所攻击，定期更新能令你避免陷入此类不必要的威胁中。

## 紧急计划

在你的同事或朋友被警方带走时，他们的电脑已经被警方没收的时候，一切都已经太迟了。也就是说如果你等到那时候才与工作相关的同事或朋友讨论如何删除敏感的材料，这可能会让你陷入被认为尝试销毁证据的罪名的局面。你必须在这些情形发生之前先准备好，必须知道在事情发生之前、之中、之后分别要怎么做。当然，也必须知道你的朋友和同事会怎么做。你需要有一个计划。唯一的方式就是提前讨论，协商好如果在其中某人被带走或电脑被没收的情形下你或其他人应该如何应对。是否所有人

都将手机原厂设置呢？还是再三确定收件箱是否为空？还是你们所有人都重设密码，将电脑格式化？不管你们怎么决定，最重要的是所有人都做同样的操作，并且知道对方会怎么做。

这个叫做制定并遵循“安全协定”。如果就你自己做了很多事情并且处于安全状态，但有一个同事没有做，这会让你的尝试和努力变得毫无意义并且也会为其他人带来风险。和你的同事坐下来谈论这件事情，记住，如果你的工作网络包括多个团体或同事，或针对不同问题的人权工作者，他们不一定都知道对方，有的人比其他人做的事情更加敏感，你可以和不同的团体建立不同的紧急计划，这一点很重要，建立一个紧急计划就是建立“安全协定”。这样每一个人都知道，而且也很容易遵循，不是什么难以达到的难事。相关的更多讨论会出现在第12章：预防性保护。

在进入下一个章节之前，确保你已经执行了我们在第2章：电脑设置中所建议的操作，保障基础的设置能够为后续更高阶的技术和操作行为安全步骤带来大大的帮助。

## 本章问题

- 什么是零收件箱策略，它为什么重要？
- 为何坚持“无回复约定”的习惯很重要？
- 没有定期更新的软件会面临什么样的威胁？
- 紧急计划是指什么？
- 设计一个紧急计划需要的步骤是什么？
- 为何要减少和简单化所使用的程序数量？



## 第4章

# 获取信息



这一章节中会教你如何安全的获取信息。包括查找和获取信息、使用浏览器以及在使用浏览器时所用的网络连接方法。为安全起见，不仅要留意浏览器本身，也要留意获取信息的网络连接。在保障网络连接的同时也能顺便解决审查制度的限制。

## 总结和行为

这个章节涉及的内容包括网络连接和浏览器的使用。后续的手机章节中会讨论应用程序。章节的第一部分是关于设置浏览器和使用浏览器的操作习惯的实用方法，第二部分是关于网络连接的概念，主要是了解网络连接的工作原理，以及如何以安全的方式连接上网。

我们的眼和鼻好比互联网中的浏览器。很多人也都在使用浏览器发送邮件，很多工作相关的使用都关系到浏览器，所以浏览器的安全问题就变得很重要。

当使用浏览器的时候，有两件事情会发生，一个是你访问的网页会收集你的信息，同时电脑也会收集你使用浏览器的记录，这些信息包括收集Cookies, LSO虚拟数据，键入的密码，浏览器的历史记录等等。便于运行正常，大部分的网页都是用一种JavaScript编程，这样浏览器和电脑都很容易获取网页Bug和病毒，再通过浏览器感染整个电脑，这两个方面都需要注意。幸运的是，我们有办法能够解决这个问题，而且第一步只需要改变操作习惯就能解决。

## 双重浏览器策略

原则上来说我们建议仅使用一个浏览器，并设置为在关闭时自动删除所有数据。但取决于你的个人目的的浏览器使用需求量，如果在使用每个服务时都需要重新登录一次密码，使用起来很没有效率，也非常不方便。所以我们给你推荐双重浏览器策略。选一个浏览器用于个人上网，再选一个用于工作。工作浏览器只用火狐（Firefox），

它并不是最快的浏览器，但是允许重要的安全附加组件和扩展的设置，如果你还没有安装Firefox，请即从官网 <http://www.firefox.com.cn/> 下载和安装。

个人上网我们推荐使用Chrome或Opera。双重浏览器意味着用于个人上网的浏览器你可以维持以前的上网习惯，也不用被附加组件和扩展耽搁太多时间，但是工作相关的上网习惯虽然麻烦却能明显的提升你的安全性。

一旦做好决定，就持续下去。Firefox用于工作中的搜索、邮件和任何其他使用，另一个浏览器用于个人上网，不要安装两个以上浏览器，仅选择两个浏览器并持续使用下去。


要能安全的使用工作浏览器，这里需要安装一些附加组件和扩展程序。


## 附加组件/扩展程序

打开火狐浏览器，点击右上角设置就能找到附加组件的区域（WIN10+OSX·26），点选附加组件，在这里能让你搜集和添加附加组件，在扩展标签下能显示所有已安装的附加组件。

找到并安装以下四个附加组件：RefControl, NoScript, BetterPrivacy和 HTTPS Everywhere。

 **Refcontrol.** 在访问某个网页时，网站能追踪到你是从哪进入的，比如说你本来在用Google，接下来又打开了Facebook，Facebook就会被告知你是从Google进入到Facebook页面的。这个数据作为引用，通常被用作分析人们通常在网页上做些什么。安装RefControl 并作几个简单的设置就能防止被分析。安装后，点击选项，在最下方的将未列出的站点设置为屏蔽或伪装。

 **NoScript.** 这个程序能在使用浏览器时自动屏蔽Javascript。这非常重要，因为很多的病毒和未知的传输都是通过被感染的script（脚本）。这样就禁用了动态图形、自动视频回放等等功能。在浏览器上会显示一个小图标，如果你完全的信任那个网站，则只需要点击那个小图标，允许运行即可。如果你进入的所信任的网站无法完整的显示，则是因为一些脚本被禁用了，在这种情况下只需要允许即可。除此以外在这个插件上就无需再做其他的设置了。

 **BetterPrivacy.** 通过安装这个附加组件有关闭浏览器时自动删除数据功能选项。只要安装了这个组件，你才能彻底的删除LSOS — 一种难以清除的新型Cookie，也叫Flash Cookie。安装后，点击选项，选择选项&帮助列表，点选当Firefox退出时删除Flash cookies，点选同时删除Flashplayer默认Cookie，以及点选删除Cookie时同时删除空的Cookie文件夹。





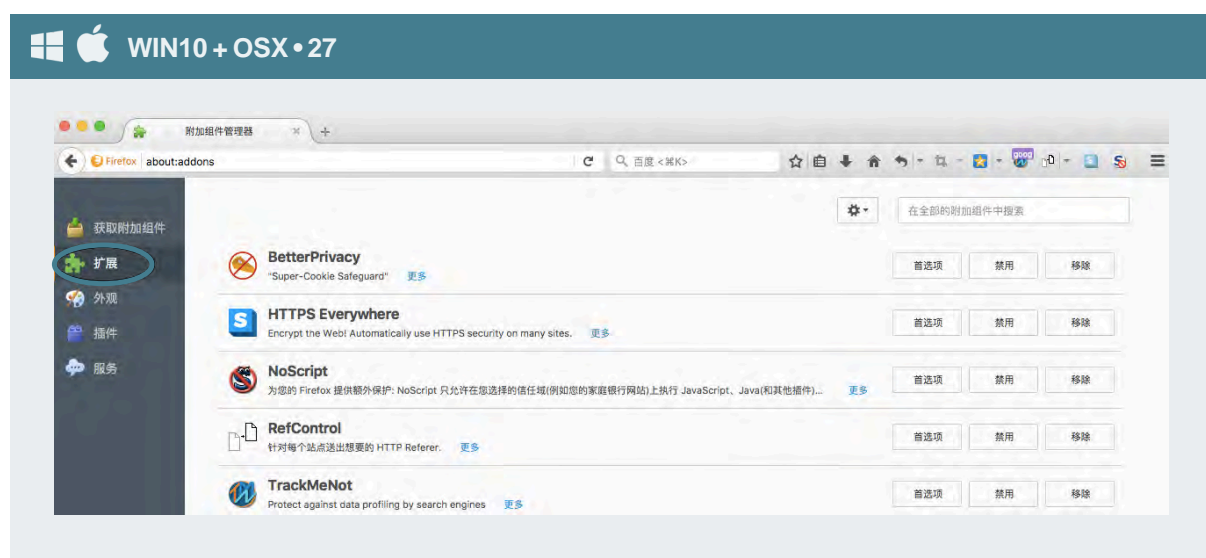
**S HTTPS Everywhere.** 有些网站支持电脑和网站间的连接加密，比如银行、邮件服务商、社交媒体等等。这样能多一层安全。虽然提供HTTPS功能的网站并不普遍，而且有的网站提供但却不自动启动。这个附加组件能自动开启那些支持此功能的HTTPS加密。下载后能在Firefox的工具栏看到这个图标，点击启用就能自动运行此功能了。

与上面的附加组件不一样的是，下面这个组件不能在附加组件区域安装，而需要到download.com 下载，先搜索KeyScrambler，选择下载并像普通程序一样安装，电脑就能在重启之后运行这个程序了。

**K KeyScrambler** 是加密浏览器中输入用户名和密码时的按键的小程序。高阶的黑客能通过在你的电脑装一个键盘记录程序，获取你键入的所有记录，以此得到你键入过的所有账户信息，包括用户名和密码。通过对登录用户名和密码按键的自动加密，这个小程序能够让你在此类攻击中获得安全保障。

在安装了这几个组件后（WIN10+OSX·27），再花一些时间看看获取附加组件的页面，熟悉一下还有哪些组件，有可能发现其他对你的安全或工作效率有用的组件。也可以搜索最好的firefox附加组件，看看有哪些其他适合你的附加组件。

现在你已经完成了工作浏览器安全设置的一半，接下来还需要做一些其他的更改。



## 设置和选项

安装完Firefox的附加组件后，接下来是时候做浏览器的设置了。

点击浏览器右上角的设置按钮，再点选项。在选项下有好几个标签，每一个标签我们都会在下面提到，需要做一些必要的设置。

## 常规

点选总是询问保存文件的位置 (WIN10+OSX·28).



## 搜索

确保提供搜索建议没有被选中 (WIN10+OSX·29).





## 隐私

允许在隐私浏览窗口中使用跟踪保护，在历史纪录下，点选不记录历史，在地址栏的选项中确保每一项都没有被选中。(WIN10+OSX·30)



## 安全

在安全标签下，(WIN10+OSX·31) 勾选常规下的所有四个选项，确保未勾选登录信息下的两个选项（记住网站登录信息以及使用主密码），在这个页面也顺势点进已保存的登录信息内看是否有任何登录信息是有被保存的，如果有的话，请删掉。



## 同步

不要使用同步功能，也不要将Firefox与其他的邮箱账户等绑定，不要用邮箱登入Firefox浏览器。

## 高级

在数据反馈栏下，确保所有框前都没有打勾，网络栏下点选无视自动缓存管理，以及在下方的空格里键入50。最后，在更新栏下点选自动安装更新，并确保有点选自动更新搜索引擎。（WIN10+OSX·32）



## 为何要选下载时总是询问保存文件的位置？

现在你已经完成了上面的设置和选项，你需要明白这么做的原因。系统默认的浏览器下载储存文件夹是安全的一大威胁。

如果没有做任何设置，你从浏览器下载的文档都会存储在操作系统的硬盘内，当你删除或移除文档，从回收站清空时，原本的文件并没有被删除掉。这听起来很遗憾，那是因为通常意义下的删除并不意味着真正的删除。安全的删除很重要，我们有一个专门的章节介绍这个问题，在第7章：删除信息。现在，请确保你有点选总是询问保存文件的位置，每下载一个新的文件时被问到存储文件的位置时，必须确保所有的工作文档都被存储在加密硬盘或空间（如USB, SD卡）。在下面的章节中我们会详细讲解设置的步骤。

另外，也不要将路径设置为自动存储到加密空间，因为如果不小心在手动打开加密空间之前就点了下载，Firefox会在不询问的情况下自动改变下载路径到系统自带的路径，这是为何有必要点选总是询问保存文件的位置的原因。

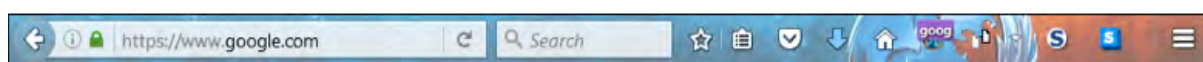
完成以上设置后，我们算是完成了工作浏览器的设置。正如我们说的Firefox是你工作的最好搭档，相较于那些速度重于安全的个人上网浏览器，如Google, Opera等等，Firefox能提供最大化的安全系数。我们也建议你打开个人上网浏览器的设置和选项，依个人情况看能做出哪些必要性的设置和更改，至少可以了解有哪些可以作出修改的功能。

## 网络连接, VPNS 和TOR

### HTTP VS HTTPS

现在有很多的服务都提供登录加密服务, 比如Facebook, Gmail, 银行官网等。但此功能在中国服务中并不普遍。就算有这个功能也不可靠, 因为这些公司会记录下你的信息并在政府需要的时候交出去。如果要知道上的网站是否有提供加密功能, 通过很简单的方式就能辨别。只需要看浏览器的地址栏就知道。

未被加密的连接在网页的开头显示HTTP (http://www...), 有加密的连接显示HTTPS (https://www...)。上Twitter, Facebook和Gmail试试看就知道了。通过Firefox中的Everywhere组件的使用, 浏览器就会自动使用https加密上网。



### 你的网络: 路由器

现在大部分的上网方式都是无线连接, 无论是在家里, 办公室还是在咖啡店工作时。鉴于此, 你需要了解无线路由器的基本运行原理, 也需要了解VPN和TOR是如何运行的, 如何能在审查制度下无限制上网, 以及如何隐藏IP地址。

在使用无线上网时要考虑到的第一件事是信号必须被加密, 否则所有的传输都能被周边的任何人读取。用于Wi-Fi路由器的标准加密通常被叫做WPA2, 只有需要输入密码连接的无线网络才是加密的, 不用密码就意味着没有加密。

这个密码是用于上网连接的(无线上网信号), 每次要连接Wi-Fi网络时输入密码即可。通常在买路由器都会自带一个标准的登录账号, 比如“admin”为用户名, “password”为密码, 很多人从来都没有留意过这个, 也不会去登录路由器改掉它。这样就很容易让那些打算追踪你的人轻易获取你的路由器连接并监视你等等。所以路由器的登录账号一定要更换。只有一个Wi-Fi密码保障你的无线上网, 但没有保障负责网络连接的路由器, 这样是远远不够的, 也给你自己带来了风险。

### 你的网络: ISP, IP地址和MAC地址

当连接上网时, 路由器会使用 and 通过网络服务提供商 (ISP) 将你与更广的网络相连接。比如中国联通就是ISP的例子, 也就是那个你购买互联网服务的公司。这个ISP通常能收集你的网络使用信息, 以及你去过的地方等等。也就是说, 你家里的路由器连网时首先都要先通过ISP的服务, 从那儿再连接到更广的网络。这样审查制度也就存在了, 因为他们会封锁一些网站和网页内容。

而你上网的足迹, 不管是由ISP所掌控的你的连接, 还是你访问的网站或你的手机连接的服务, 都是通过你的IP地址和MAC地址来追踪的。

IP地址就是你的上网连接地址, 通常很容易被辨认和追踪。如果通过无线连接上

网，你的IP会改变(为动态)，但是你的ISP总会知道所使用的网路连接是与哪一个IP地址相联的。

你的设备也会有一个MAC地址，每一个有联网的设备都会有一个MAC地址，这个独特的MAC地址是专门为实质的硬件生成的。一旦硬件被产出，MAC地址会随机而生。MAC看起来是这样的：00:0a:95:9d:68:16。在网上时MAC地址倒是不会分享出去，所以不用为此伤脑筋，但是IP地址是可能对你造成问题的。

在Win10中有开启随机硬件地址的设置选项，如果你找到这个选项，启用它。

(WIN10+OSX·33) 如果在启用期间发现你的网络连接有异常，请重启电脑，如果问题仍然存在，则关闭。

幸运的是，这里有一些非常简单的方法避免被ISP监视你的上网活动，或被网站追踪你的IP地址，这些解决方法被称作VPN和TOR。



## VPN

使用VPN(虚拟私人网络)不仅仅意味着避免ISP轻易获取你的信息，因为VPN能对连接和传输加密，而且也能规避ISP的审查制度。访问的网站也很难记录下你的真实IP地址。总而言之，建议你总是在电脑中使用VPN，将它设置为在电脑启动后自动开启。几乎找不到不使用VPN的理由，有的VPN自带切断开关功能，意思是在你的VPN掉线的情况下能自动关闭上网（以此预防在VPN掉线时你的真实IP被网站或使用过的服务商记录下来）。

VPN的使用能让你的电脑和路由器直接连接到国外的服务，通过ISP建立一个叫“隧道”的入口，访问的网站所能看到的是你连接的服务的IP地址（VPN的服务），并不是你电脑本身的IP地址。另外，你的ISP无法将你带到网络流量中，也就无法记录你的行踪，或阻止你要上的网站。VPN意味着跳脱了ISP。尽管你身在中国，但你的电脑就好比在美国或澳大利亚等其他国家一样，可以畅通的进入那些在中国被禁止的网页或上网活动。

因为用VPN时是来自香港、北美或他国的网络服务，所以当连接国内的网站和服务时速度会慢一些，倒是不会影响上国外网站的速度。不过如果你购买了价格不低的VPN服务，通常可以设置哪些部分使用VPN（比如Firefox），哪些部分不使用VPN（比如你的私人上网浏览器）。这样就能解决上国内视频网站等网速慢的问题了。

Astrill.com 是一个非常安全强大的VPN提供商，它的服务遍及全世界。GetAstrill.com 是没有被封锁的下载Astrill的网站。在网上搜索也能出来很多可用的VPN对比。在中国使用Astrill时，记得总是添上组件StealthVPN，否则VPN可能无法使用。要找到最新的可用的VPN清单，只要在Google中一搜就能找到很多相关的信息和比较。

使用VPN能强有力的保障你的IP地址，但也不是100%安全，如果有人花费大量精力搜索你的上网痕迹，也是有可能的暴露的。对于真正的敏感上网活动，你需要用到TOR。

## TOR

TOR也被称作洋葱路由器。与VPN不一样，当使用TOR时，一个免费的服务会带你穿过多个来自全世界不同的服务器，最后才抵达你要访问的网站。TOR非常安全可靠，同时也非常慢。通过TOR看线上视频那就算了吧。如果你需要查一些较为敏感的资料，而这些信息有可能会对你不利，请使用TOR。在电脑和手机上的设置也都不难。

被叫做洋葱路由器是因为它不像VPN一样使用一个服务器，而是会在最终到达你要访问的网站前跳转到不同的服务器，最多能达到20个，就像剥洋葱的表层一样。也是因为使用到了多个服务，到最后就几乎不可能通过网络追踪到你的IP地址了。

你可以将TOR浏览器安装到你的电脑或USB（WIN10+OSX·34）。它的使用非常简便，只要你打开了TOR浏览器，功能就自动运行了。这样就可以仅在一些特定的搜索时用到TOR，电脑中不会有任何痕迹。如果要整个电脑都使用TOR的话，则需要安装这个程序，一旦安装，所有的连接都会通过TOR，比如其他的浏览器，后台连接数据，Skype等等。





## Tor Browser Downloads

*To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.*

<b>Stable Tor Browser</b>			
Language	Microsoft Windows (6.0.5)	Mac OS X (6.0.5)	Linux (6.0.5)
English (en-US)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
العربية (ar)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Deutsch (de)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Español (es-ES)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
فارسی (fa)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Français (fr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Italiano (it)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
日本語 (ja)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Korean (ko)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Nederlands (nl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Polish (pl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Português (pt-PT)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Русский (ru)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Türkçe (tr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Vietnamese (vi)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
简体字 (zh-CN)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)

TOR浏览器的下载，进入 <https://www.torproject.org/projects/torbrowser.html.en> 根据你的电脑系统和语言选择合适的浏览器，TOR也有手机的App。

将文件下载到你想要存储的位置，可以是USB也可以是隐匿的加密硬盘。如果你还没有隐匿的加密硬盘或存储，可以先根据第5章：存储信息的操作介绍做出相应的设置后再回到这个章节。

可以将Tor安装到USB（如下），或安装到你的加密硬盘，不是你的普通硬盘。安装后，如果你开了VPN，请先关闭掉，这样通过访问一个被封锁的网站以测试Tor是否可用。

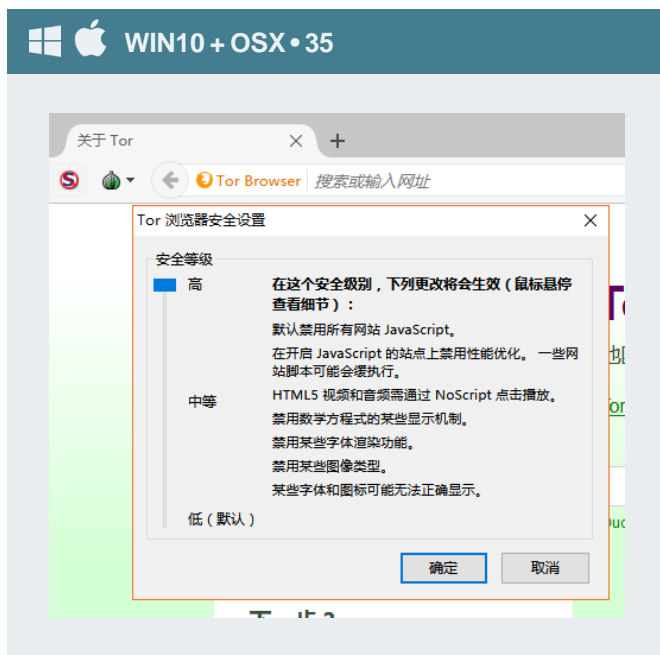
当启用这个程序时（WIN10+OSX·35），你有两种方式连接，首先可以用直接连接，因为是最简便的方式。这个选择只是在第一次使用时需要，后续都会记住你的选择和设置，会直接像一个正常的浏览器一样使用。

Tor浏览器的外观是参照Firefox的，在第一次打开TOR浏览器后，到选项区域，将所有的选项都设置成与这个章节前面教的Firefox设置一样，它们看起来都是一样，可以直接做同样的设置。

TOR还有另一个设置区域，在网页地址栏前面有一个绿色的洋葱图标，点击后选择安全设置，会跳出一个安全等级的滑动键，在这里你能设置安全等级，我们建议你从一开始先选高级别，如果后续在使用中有的网页无法完全的显示，则可以试试将级别调低应该就能使用了。

## TOR在USB 内

TOR也可以被安装在USB内，同样是内嵌的浏览器。你只需要将USB插入电脑，开启里面的浏览器，这样它的连接都是通过TOR，也是因为通过USB运行，相比电脑的运行要留下更少的痕迹。可以考虑买一个小小的USB或SD卡，将TOR安装到这个USB或SD卡，确保这个卡不会作为其他任何用途，比如存储文件等。安装的过程与上面的一样，只是将文件下载和安装到USB，安装在USB的浏览器也与在电脑内的一样，记得做与上面教过的步骤设置浏览器。同样地，在使用之前进入设置区域做出相关的安全设置。



## DUCKGOGO.COM 和 SAFE SURFING

DuckGoGo是一个搜索引擎，就像百度和Google一样。与一般的搜索引擎不一样的是，DuckGoGo不会基于你的地理位置和搜索历史记录来给予结果，不会保存使用者的任何数据。这是比较安全的上网方式，因为不会被收集到一些不利的信息。也意味着没有广告，没有根据搜索历史、地理位置等定制的广告。DuckGoGo仅有英文版本，不过界面非常的简单，语言应该不是问题。

如果结合TOR/TOR浏览器和DuckGoGo的使用就意味着不会留下任何访问痕迹，既没有ISP也没有你进入的最后一个网页痕迹。如果要搜索的是可能被人监视存储下来而用于对你不利的信息，可以用TOR浏览器，用DuckGoGo搜索信息。为了最大化的安全性，从USB中打开TOR浏览器，以此减少在电脑中的信息存储痕迹。

DuckGoGo + USB内TOR 浏览器应该是你真正的安全网页访问的选择。

网页访问的安全级别可以简单概括如下：

TOR提供最好的安全性，比使用VPN的安全性高，使用VPN又比正常连接更安全。在选择浏览器的方面，在USB中使用TOR浏览器是最安全的方式，而电脑中的TOR浏览器比设置完备的Firefox安全性高，设置完备的Firefox仍然比使用一个普通设置的浏览器要安全得多。

## 本章问题

- 哪些是你应该安装的最主要的安全插件？
- 为什么要将Firefox设置为下载时总是询问保存文件的位置？
- HTTP和HTTPS直接有什么不同？哪一个更安全？
- 你怎么知道你的网络路由器有没有被加密？
- 一个强大的密码有哪些特征？

## 本章要点

- 你是否已经设置了双重浏览器，在Firefox作了必要性的变更设置？（或其他指定的工作浏览器）
- 你是否理解了VPN和TOR的工作原理，它为何能帮到你，除了能越过审查制度外？
- 确保经常使用VPN，最好一直处于开启VPN状态，也学着在搜集敏感信息时使用TOR和TOR浏览器。

## 清空收件箱，自动删除带来安全的一天

一个常住上海的律师在2000年左右成为了一名维权律师，他不仅仅只是为政治敏感人士辩护，而且很多的工作因为他的努力都得到了不错的结果。随着他的知名度的增加，随之而来的骚扰和威胁也越来越多。他决定为了家人的安全，得改变策略，由于他本人对法制和正义的坚定追求，他开始接手越来越少的案件，取而代之的是创办了一个非正式的NGO，为各地的维权律师提供培训、支援和各种形式的帮助，特别是一些刚起步的律师。同时，他也渐渐开始学习更多的数字安全知识，确保他的信息维持在安全状态，不会落入到错误的人手上。

在一次对律师的大面积打击活动中，随着事件的火热升级，他自然而然的认为他自己也会成为打击目标，但是因为已经从很久前就不再接手个人案件，他估计一旦他被锁定，很可能被讯问的范围仅在强迫给出关于“中国人权律师团”的信息。这个团体实际上只是一个线上的群，一般用于律师们分享信息，但是在政府看来这是一个有组织的反对派，遂成为这次打击的关键目标。

他估计的没错，在2015年，他成为了打击目标。但是政府并不止是带走了他，同时还有他的助理和另外一些他合作过提供培训的律师。他误会了警方只会因为对这个线上群的兴趣而带走他，他们同时也在关注他创立的这个提供培训和法律援助的小NGO。

很快的他发现作为已经长时间没有接手敏感案件的律师，他不需要回答线上群有关的很多问题，这样也就避免了归罪他人的风险。不过，他担心（现在也是）他们找到可以用于对他不利的证明他为其他律师组织培训的证据材料，虽然培训的律师们都是完完全全的合法。最后，他被拘留了17天，但有被威胁要将他转移到“指定住所监视居住”（RSDL），不管是否有任何切实的嫌疑罪名，都可以被关押6个月的地方。甚至到他被释放后，他仍然是每天生活在担惊受怕中，于是他停止了这个小NGO的运作。

他说有两个主要的原因在他的拘留和审讯期间救了他。一个是他有确保所有的工作邮箱总是为空，另一个是他工作使用的聊天软件要么是通过安全聊天服务中自带的自动销毁功能，要么是定期会清除聊天记录。

警方之前声称有理由拘留他是一份从他的助理手机里找到的信息，他的助理在警方的威逼利诱下很快就交出了手机的密码。助理并没有及时删除手机内的聊天记录，他们从聊天记录中发现很明显他们确实有组织培训并支持维权人士，以致于警方声称这已经构成了犯罪。

这位律师也犯了一个错误，那就是在他的手机上使用Tutanota邮箱。虽然他拒绝了给警方交出邮箱的密码，但是他们因此得知了他所使用的加密邮件服务商，转而向他的助理胁迫交出他的密码，他们打算通过助理的邮件记录找到打击这位律师的证据材料，幸运的是助理虽然忘了删除手机的会话记录，但他有坚持采用零收件箱策略，这样一来当警方进入他的邮箱时也没有发现对他不利的信息。

另外他的两位临时同事似乎并没有严格的遵守将会话程序和邮件清空的行为，他也就无从得知到底有多少的资讯已经被警方从他的工作伙伴那儿掌握了，但是应该也足以让警方了解到他的工作范围，虽然他们从来没有得到过全部的细节。有了这些基本的信息，也足以让警方以更大的惩罚来威胁他，虽然甚至可能都没有确切的起诉理由，这也是他不敢继续继续运行这个NGO的原因。



## 第5章 存储信息



本章节中会介绍两种加密方式。第一种是基础化的加密，使用电脑内置的自动加密和USB等类似于现今智能手机加密的方式。第二种也是更重要的加密形式，在硬盘或USB内建立一个隐蔽的、高度加密的区域用于存储你的重要工作文件。

加密是现今提及率很高的一个词，它包括从邮件到聊天会话、浏览网页、到存储信息都与加密的概念密不可分。加密意味着数据是被保护的，这样外人无法读取到。只有拥有用于加密数据的代码的人才能读取（称作解密）。本章节专门介绍数据加密，针对你的存储使用，比如硬盘、USB等等，不包括邮件、网络连接等。

我们从使用习惯开始，确定什么样的信息是你应该保留的。

## 删除过量信息

你需要不断的分析如何减小那些可能会造成安全的威胁。也应该分析如果所做的某一步安全预防被攻破时会如何影响你。比如说，你的工作文件的加密存储被打开了，什么样的信息会被外人看到。

存入更少的信息表示要担心的信息就更少。这样你就只需要专注于保存那些你真正需要的文档。当写一个长篇报告时，会需要做大量的搜集工作。如果你写一个申请书，很可能到最后产出了很多的信息。通常当完成一个产物时，也许建立了很多文档，有制图、表格等等，每一个单独的word文档为不同的方面，当这些相关的信息合成一个最终的文档，到最终的文档生成后，你觉得建立的那些单个的文档还需要保存吗？应该是不用吧？如果是的话，将他们删除，仅仅存储这个最终的文档。

也不是所有存储的文档都要永远存着。很多建立的文档可能都在某一天可以被删除，一旦发现某个文档你已不再需要了，删掉它。

另外，试着保存和储存越少越好的必要文件，以防万一你的密码被攻破，能尽可能的保护你自己的安全。

## 基础化加密

如果你的iPhone或安卓手机是来自中国大陆以外，你会发现手机有已经自动开启的加密功能。就算没有自动开启，手机也允许你轻易的启用加密，你需要做的只是设置一个PIN或密码。（在这个过程中现有的数据不会被删除）

现在的Win10和OSX都有同样的功能，允许你轻易的加密电脑硬盘以及设置PIN和密码。和手机不一样，在买电脑时它的加密并不是自动开启的，你必须手动设置。启用加密并不会格式化或删除电脑硬盘，或删除任何电脑内存储的文件。在启用加密后，电脑内的所有内容都在原处，不会有任何改变。

要注意的是，只有最新版的OSX才包括最完整的加密功能 (FileVault2)，以及最专业版的Win10才有完整加密 (Bitlocker)，如果你没有这几个版本，也无法升级和更换的话，可以直接跳过这整个基础化加密的部分，移到隐藏加密的部分。

作为用户，加密所带来的使用差别对你来说并不大，如果启用了加密，你只需要在进入电脑或手机前输入密码，如果不输入密码则无法进入，因为这样就无法进入硬盘，也就无法开启操作系统了。你也可以为外部硬盘和USB等开启加密形式。（就是要输入密码才能进入这个驱动器的形式）

鉴于大多数的手机和电脑都要求输入密码才能打开，你会好奇它们的区别在哪里。区别就在于传统类型的密码输入只是用于打开电脑或手机的界面（从锁屏到操作系统的界面）。这些密码只是在操作系统已经启动和运行后才需要的，也只预防人们进入电脑和手机的界面而已。也就是说数据并没有被加密，如果有人想要你的数据，他们可以轻易的取下你的硬盘或其他存储空间，接入另一台电脑就能读取上面的每一个数据。但如果对硬盘有进行加密，这个设备和硬盘就能避免这个情况了。

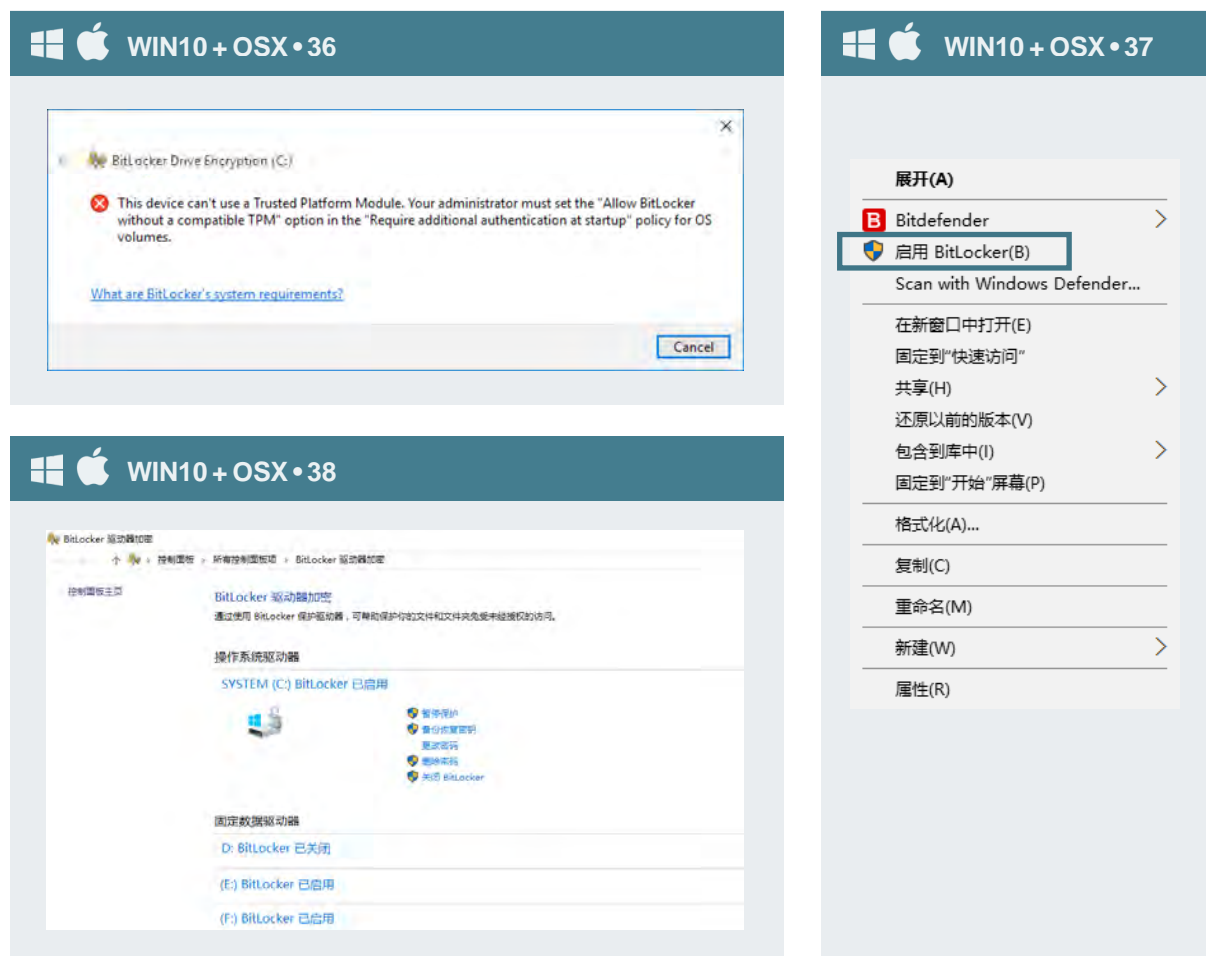
仅有锁屏的密码以及进入界面就好比家里的门，加密就好比给门上锁，一个没有锁的门对防范小偷并没有什么作用。

## 设置

Win10内处理正常加密的内置程序叫BitLocker，Mac内的叫作FileVault。要开启这两个程序都可以在电脑的搜索区域搜索它们。它们可以加密你的操作系统硬盘，其他硬盘以及USB等。

当打开BitLocker时，你可能看到的是如图 (WIN10·36)，意思是你需要开启TPM，你可以按照屏幕上显示的步骤操作，这个过程会要求你重启电脑，下一次再打开BitLocker你就会看见如图 (WIN10·37)的屏幕。

你可以从BitLocker的主菜单(WIN10·37)内选择要加密的硬盘或可移动媒体（USB，

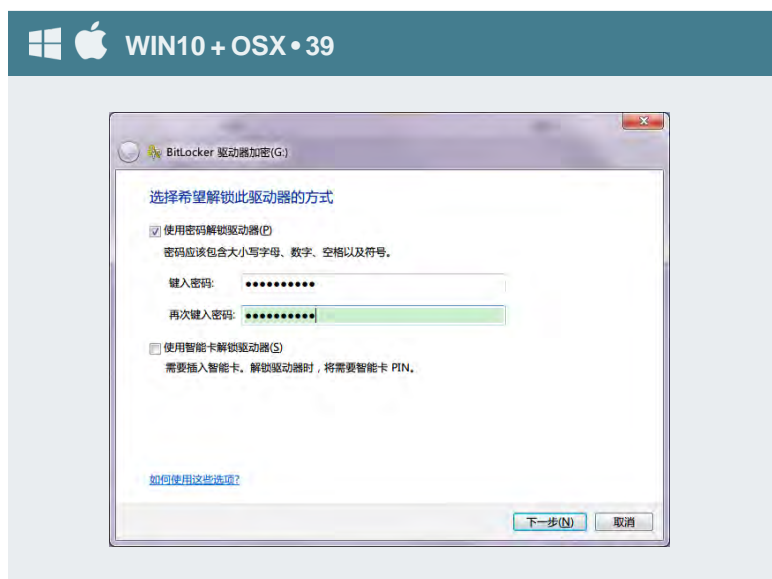


SD卡等)，或者右键点击硬盘后在跳出的窗口中点选开启BitLocker (WIN10·38)。在开启之前，确保你身旁有一个USB或SD卡用于临时存储即将生成的恢复密匙。

通过点击启用BitLocker开启任何硬盘或USB的加密过程，第一步会被问到如何解锁这个新的加密硬盘，选择使用密码 (WIN10·39)然后点击下一步。因为这只是一个基础化的加密，可以使用一个PIN码或简单的密码。

下一步会问你在哪儿保存你的恢复密匙，这个码是一串字符，如果你丢失或忘记了密码，可以用这一串字符来解锁你的加密硬盘，这也是一个很大的安全威胁。

对于这个威胁的解决办法，如果你有打印机的话则点选打印恢复密匙，如果没有，可以选将恢复密匙保存到文件 (WIN10·40)。保存





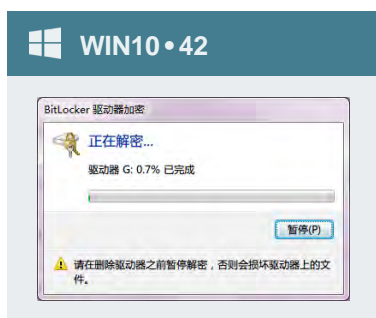
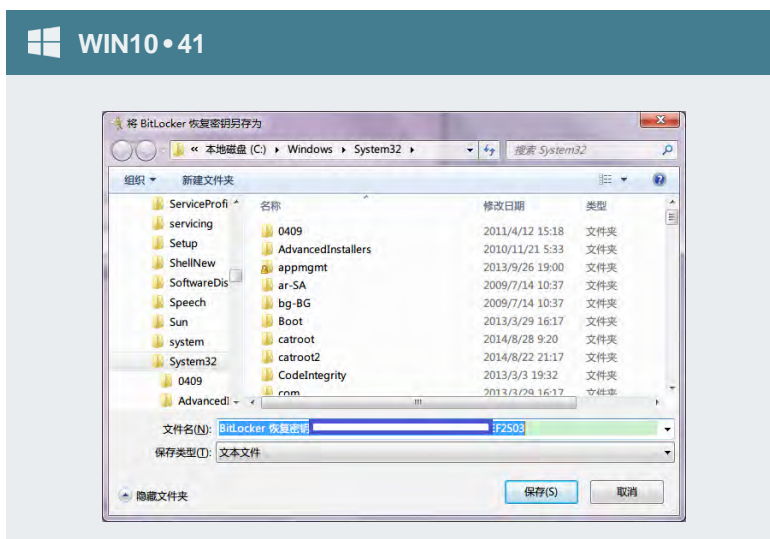
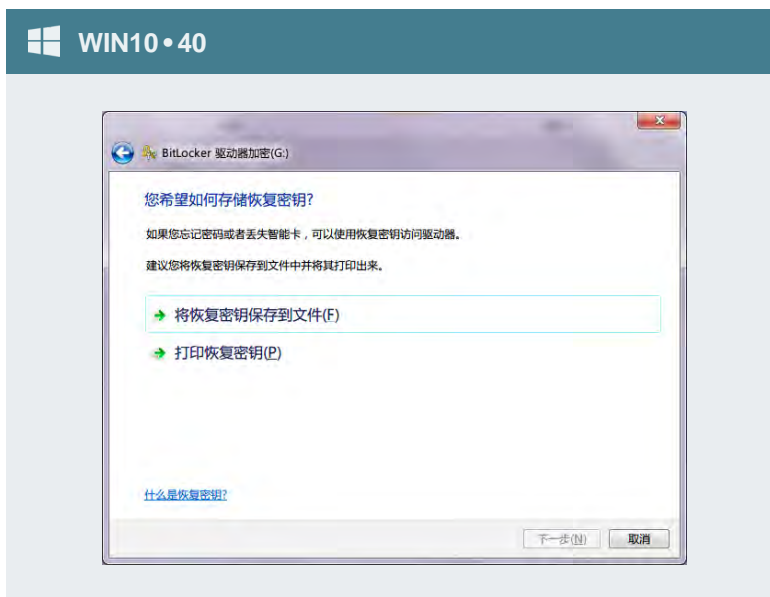
后, 更改文件名, 可以是一串随机的字符或其他, 如图(WIN10·41)。

在保存恢复密匙后, 点击下一步会被问到加密多少硬盘和USB, 在这里你记得点选加密所有硬盘。在下一个页面依照最适合自己情况点选加密模式, 通常新加密模式是最好的, 但是第二个兼容模式选项, 是在你有需要将USB或外部硬盘在没有最新版本的Windows系统电脑上使用时才用得到。

现在你已经准备好加密硬盘了, 点击开始加密然后让它在后台运行(WIN10·42)。越大的硬盘会需要越久的时间。这是一个后台操作过程, 就放在那儿让它运行。

最后, 加密完成后我们可以删除恢复密匙了, 如果你是用的打印, 则可以直接将它用碎纸机销毁掉, 如果是存储到USB或SD卡, 则进去将这个存入的恢复密匙删掉。

在删除了恢复密匙后, 右键点击USB或SD卡, 在跳出的菜单中选择格式化, 它会移除这个USB或SD卡内的所有数据, 所以如果里面有其他重要的文件, 请另外保存起来, 这个步骤就会移除恢复密匙的所有痕迹了。请不要点选快速格式化, 因为快速格式化无法确保能移除数据。(WIN10·43)。

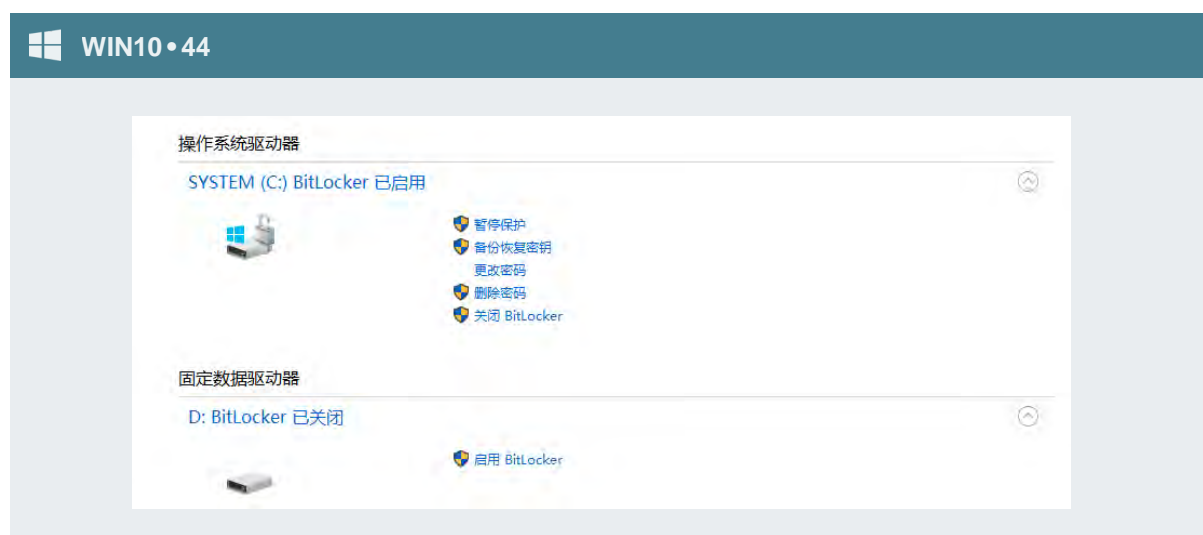


## 调整和使用基本加密

从BitLocker的菜单你能看到在开启加密后有好几个选项，你可以关闭某个硬盘的BitLocker，也可以设置哪个设备启用或禁用自动解锁。自动解锁是指你会被要求输入密码来解锁任何非操作系统硬盘和USB等。一旦电脑找到它们，如果没有启用自动解锁，则需要通过点击硬盘，从跳出的任务栏中会要求你输入密码的选项。

这个自动解锁的启用或禁用不适用于操作系统的硬盘，这个硬盘总是需要在开启电脑时输入密码，否则电脑就无法开启运行系统。(WIN10·44)图中显示了一些不同的选项。

一旦解锁了一个硬盘，它会直到关机前都处于解锁状态。现在你已经完成了启用电脑的基础化加密了。



## OSX

在OSX系统中负责基础加密的程序叫FileVault (10.7以上版本都有)。早期的OSX系统仅有限制版FileVault OSX 10.3–10.6，不是完整的FileVault，只是加密了硬盘中的一小部分。如果你的Mac没有完整版的FileVault，也无法升级的话，可以跳过此基础加密的部分。

从电脑的搜索栏键入FileVault就能找到这个程序，或是在系统偏好设置的安全下。前面有说过，这只是基础加密，你可以用一个PIN码或简单的密码。关键是，BitLocker的密码是不能忘记的，一旦忘记，数据和硬盘就永远丢了。

如果你用的是旧版本的FileVault (也就是没有加密整个硬盘)，文字显示是FileVault保护你的个人文件夹。参见下图的(OSX·45)和(OSX·46)。如果用的是完整版，则显示的是保护磁盘上的数据，如下图。如果你用的是旧版本，可以直接完全跳过这个部分。

先点击开启FileVault。(OSX·46)



下一个窗口就会显示修复码，接着会被问是否需要Apple存储你的修复码，接着关于你个人的问答方式以获取修复码副本。但我们不建议你使用此功能。如前面所说，只需要用简单的密码，应该都能轻易的记住，如果让Apple存储你的修复码反而会增加安全威胁。

点击继续后，电脑就会重启，在重启后程序就会加密你的电脑硬盘了，加密的过程需要一段时间，在结束之前电脑的速度会稍慢。

加密完成后，下一步就只需要在启动电脑时输入你设置的简易密码即可，这就是所有你要做的了，不需要再做其他任何步骤。

## 隐藏加密空间与储存工作文档的位置

以上的部分能给电脑带来基础安全。从今往后，你都需要输入密码才能开启电脑。接下来我们讨论稍微复杂一点的步骤，也就是讨论你的工作文档应该存入的位置。就算你没有使用基础化加密，这个隐藏加密也能保证你的文件安全，对外保持隐匿。

我们来建立一个更安全、隐蔽的存储工作文件的加密空间。正如我们在之前的章节中提到的零收件箱策略，关键的威胁不是有人使用高级的黑客技术破解你的加密空间，而是当你被警方带走时他们强迫你交出密码。如果你交出了（通常也很有可能），所有的保障都没有了。比如浏览器和邮箱的信息，最有效的保障措施是让他们不知道你有这个硬盘，因为他们不知道某个东西的存在，也就无从问起了。

有一个非常简单又聪明的办法，叫做隐藏加密空间。这个办法的作用是没人会知道它的存在，当然也就没人能强迫你交出任何密码。这个部分和零收件箱策略以及关于删除的部分是整份手册最重要的内容，有了这几个部分的结合才能保障你的安全。而且我们一再强调这些操作并不困难，只是需要花一些时间设置，一旦设置完成，只需要点击确认键就可以了。

创建这个隐藏加密空间，你需要下载安装以下叫Veracrypt的程序。



**Veracrypt:** <https://veracrypt.codeplex.com/wikipage?title=Downloads> 

下载到电脑或USB都可。USB会更加安全，不过需要先将USB插入电脑才能操作。同样地，总是记得将文件直接下载到你将要安装的位置，不要下载到桌面或默认的下  
载位置。

当下载VeraCrypt到Mac时，也需要下载OSXFUSE，将这个程序安装到Mac是用于支持VeraCrypt。可以在下载VeraCrypt的同一个网站上下载。将OSXFUSE像普通程序一样安装到电脑，一旦安装成功，你可以去到下一步设置VeraCrypt和隐藏加密空间了。

与基础加密不同，当要使用隐藏加密空间时，就好比下载一个新的文件一样，需要打开Veracrypt并加载隐藏加密硬盘，就会跳出一个看起来和普通的硬盘或USB一样的窗口，一旦使用结束后点击退出即可。载入在Veracrypt的术语叫加载（mount），退出叫卸载。新建的加密空间叫加密卷。在接下来的章节我们都会使用这些术语以让你更熟悉。一旦载入了加密空间，就会出现一个新的硬盘，比如E: 名称，一旦卸载后，这个硬盘就会消失。

是什么建立了这份安全？

当一个硬盘、部分硬盘或USB等被加密了，电脑就不能读取这部分的数据。通过使用技术分析，警方也许能猜到你有在使用加密空间（或是硬盘被损坏了）。接下来他们就会试着强迫你交出被加密部分的密码，这是肯定的。最好的应对方式则是选择USB来加密而不是电脑硬盘，但是这样就要保证USB的安全，也不能弄丢。一旦这个USB被发现，上面提到的同样的分析也能显示是加密过的，如果被弄丢，就意味着所有的数据都永远消失了。

解决这个问题的办法是不要只创建一层加密，而是在同一个空间内创建双层加密。这个双层空间的叫法是外部加密卷和内部（隐藏）加密卷。一个密码用来打开外部加密卷，另一个更安全的密码用来打开内部加密卷。像Veracrypt这样的程序提供多种类型的普通加密，但也提供隐藏加密。这样就算是用Veracrypt或其他类似软件，一旦被警方找到，他们并无法确定你在使用这个双层加密的功能。

因为内部加密卷是在外部加密卷里面，没有任何技术分析能找出你的内部加密卷的存在。

也就是说，当选择载入加密区域，输入一个密码它打开的是外部加密卷。外部加密卷存在的意义就好比一个诱饵，意味当你的对手强迫你交出密码后，而出现的内容不会过于敏感不利，但又能令他们满意，实际上你并没有交出加密空间的所有信息。这个功能可以用在整个硬盘、部分硬盘或USB。

Veracrypt的隐藏加密功能大大提升了你的安全系数，如果能将它安装到USB甚至会更安全，这样警方或对手就无法从电脑中找到这个软件。总之，你自己决定要如何安

装这个软件，取决于你自己的需要和实用性，无论如何，它们的安全逻辑都一样，换句话说：

防止他人进入到真正的隐藏加密空间（内部加密卷）的能力在英文里叫做“Plausible deniability”，字面上的意思用中文来说差不多是“合理的推诿”，意思是通过交出外部加密卷密码让事情合理化，而实际上你并没有交出内部加密卷内真正敏感的材料，这是保障自身安全的关键。

不过，要真正起到作用，它得是可信的。在这里可信的意思是在外部加密卷（诱饵）内的信息必须是很明显你不会愿意分享出去的。一旦你被强迫交出加密空间密码（外部加密卷），当警方读取里面的资料时，要令他们相信那是你在保护的东西。如果里面的内容为空，或只是电影音乐文件等，他们则会轻易知道那不是他们在找的东西，会继续向你施压。

所以，确保在外部加密卷内存入的是敏感但又不是太敏感的文件。比如你可以存一些银行账户相关文件，一个黑名单书名的PDF文档，同时也应该放一些工作文件，比如你写的报告、文件之类的，但是不需要用到的。每过一段时间添加一些新的文件到外部加密卷，这样表示你有一直在使用。如果有更高的安全系数要求，可以多复制几个文件到外部加密卷。

总之，不要将真正的敏感文档存在那儿，这里只是作为诱饵。设立诱饵的原因是让警方远离你真正的敏感资料，一旦他们以为已经找到了所有的信息，并满意了，那他们很可能就不会再施压了。

需要不断更新外部加密卷的原因是每个文件和文件夹都有显示这些文件最后被转移或修改的时间的数据，如果他们进入你的外部加密卷发现在过去两年内这些文档都没有被动过，那他们会意识到你并没有在使用这个硬盘，要么是一个老硬盘或圈套，这样也会再次向你施压以获取更多的信息。

要建立这一套系统最简便的方式就是先将所有的工作文件移到你的内部加密卷，在这之后，浏览一遍所有文件的内容后，将一些工作相关但又不是特别敏感的、不包括人名、细节、或可能牵连他人的信息文件存到外部加密卷。

鉴于外部加密卷应该是可信的，我们也建议你存入那些一般来说被认为敏感的文件，以及个人隐私方面的文件，比如以下这些：

- 建立密码清单，比如网上购物网站登录密码、私人的社交媒体等与工作无关的隐私，存进来。
- 也许在过去你有写过一些肉麻的情书或个人笔记，如果有，存进来。
- 也许你有与恋人发过一些私密的短信、照片或短信，如果有，存进来。

总的来说就是外部加密卷以普通角度来说会非常安全，只有在被警方强迫打开的情况

下才有威胁。如果事态很严峻，到了他们要强迫你交出了密码的时候，那就要保证你在里面存入了这些个人的信息以供他们读取，要知道因为你交出了这个外部加密卷，也许能帮你一个大忙，这样就能让他们相信你在外部加密卷的信息确实是不愿意被他们发现的。

要让事情看起来可信的话，不要一开始就轻易的交出外部加密卷的密码。如果被问起你还是要先拒绝，作出一副无奈的样子，推脱几次后，再很不情愿的将密码(外部加密卷)交出去，否则对手可能会起疑。如果他们相信了，真正敏感的信息就会处于安全。当然，没有人愿意让警方看到你发给恋人的裸露照片之类的，但是与坐牢比较，就很容易做抉择了。如果你没有上面提到的这些个人隐私类型的信息，建议现在建立一个存进去，如果有必要的话也可以PS一个。这一系列操作意味着自由与坐牢的区别。

## 设置

设置时要先决定隐藏加密空间的位置。你是用USB？还是整个硬盘，还是硬盘中的一部分？我们会教你如何在USB和整个硬盘中建立加密系统，一部分的硬盘加密在某些版本中也可以操作，但是我们并不建议，所以在此会跳过这个选项。

操作步骤如下，在程序安装完毕到电脑或USB后，打开程序。

跳出的第一个窗口（WIN10·47），也就是通常使用（加载或卸载）的主窗口，点击创建加密卷。

点击创建加密卷之后，你会看到两个选项（在Win10内也会显示加密系统分区的第三选项，不过与我们没关系）。最容易使用的选项是加密一个非系统分区/设备，这个选项可以加密一整个系统分区或硬盘（但不包括操作系统盘），也适用于外部硬盘和USB。另一个选项是创建文件型加密卷，（WIN10·48）可以由你自己决定硬盘或USB内的多少空间需要被加密。

点选上面任何一个选项后点击下一步，你会被问到是否创建标准Veracrypt加密卷或隐藏的Veracrypt加密卷。点选隐藏，再点下一步。接下来的选项是常规模式和直接模式，点选常规模式（直接模式是





在你已经有一个加密空间的情况下)。  
(WIN10·49)

在这之后，取决于你当时选的是创建文件型加密卷还是加密非系统分区/设备。  
(WIN10·50)

如果你选的是创建文件，则需要去到查找栏，找到你打算创建加密空间的硬盘或USB，然后创建一个文件，文件可以是任何形式，只是作为去到加密空间的通道。创建的文件可以是一个PPT文件，Microsoft Access文件等，命名为一个很正常的名字，记住这个文件的一处位置。

回到Veracrypt界面，点击选择文件并找到你刚刚所创建的文件位置并选择，它会提醒你这个文件内的所有数据都会被删除。

如果你选的是加密非系统分区/设备，也需要点击界面的选择文件按钮，从跳出的窗口中选择你要加密的硬盘、外部硬盘或USB。(WIN10·51) 在加密的阶段会删除里面的所有数据，所以在操作之前务必将里面要保留的数据转移。

在操作完这个步骤后，下面的步骤针对两种选项都是一样的。

系统会先创建一个外部加密卷，你不需要在加密选项内作出任何改变。(WIN10·52)

点击下一步会出现大小的选项，如果你选的是加密非系统分区的话则无法选择，整个空间(某个硬盘或USB)都会被加密。如果选的是创建文件型加密卷，则会被问到要建立的空间大小，如果不是有很多的视频文件，通常10GB就够了，填写一个合适的空间大小，(WIN10·53) 点击下一步。

下一个窗口是为外部加密卷创建密码。(WIN10·54) 这是诱饵加密卷，所以密码不需要太高阶。可以选一个好记的密码。

点击下一步后，加密的过程就启动了，在加密过程中，将鼠标尽可能的在屏幕上移动，这个干扰能加强加密的作用。一旦加密完成，点击格式化按钮。(WIN10·55)

完成后，会显示如下的窗口，点击下一步。(WIN10·56)

在上面的过程完成了，创建内部(隐藏)加密卷的步骤开始了。点击下一步，又会重





新开始所有的操作过程，不过是为内部加密卷。唯一要更改的是空间大小，必须要小于外部加密卷（我们建议是一半大小），另外也需要设置一个更复杂的密码，一个你不会忘记、永远不会进不来的密码。其他的步骤都是一样，一旦完成后，下面的窗口就会跳出来，点击退出。

## 使用VERACRYPT

现在所有的设置都已经完成，后续就不用再操心设置的问题了。要使用Veracrypt时打开这个程序就可以了。

要进入加密空间，有两个方法。先点击任何界面上显示的硬盘字母，一旦载入，你的加密卷就会在电脑中以一个硬盘的形式显示，如果你选了硬盘E或F，那么它就会按照这样显示在电脑中。

如果你之前创建的是整个硬盘或USB空间，则点击选择设备，根据跳出的窗口选出你设置的硬盘或USB，在密码栏中输入你设置的密码。简单的那个密码自动打开外部加密卷，复杂的密码自动打开内部加密卷。如果你被强迫交出你的加密空间密码，你要在几番交涉后交出的应该是外部加密卷的密码，而不是内部加密卷。

如果选的是创建文件型加密卷，则点击选择文件，然后找到你当时创建的那个文件位置，再次强调，输入简单密码会自动加载外部加密卷，更高阶的那个密码自动加载内部加密卷。

也有一个自动加载设备键 (Auto-mount Devices button)，点击这个键能自动识别任何可被载入的设备，并询问你的密码。其他的与前面的工作原理是一样。不过自动加载功能并不是总能顺利的操作，但是如果可以的话，这是载入你的加密卷的最简便的方式。

一旦加载了加密卷后，可以将窗口关闭，专心工作。工作完成后，如果不再需要使用工作文件，或是你得离开电脑，则再次点开Veracrypt界面，选择全部卸载 (Dismount all)。这样所有载入的加密设备都会关闭 (这个硬盘的显示也会从电脑中消失)。

以后的每次使用你都只需要在界面操作这个加载 (Mount) 和全部卸载 (Dismount)的步骤了。(WIN10·57)



## 文件位置的选择

关于这点我们在使用浏览器的章节有简短的提到，在接下来关于删除的章节中也会提到，不管怎样，因为太重要，我们在这里还要再次提到。

任何通过邮箱或浏览器下载的文件，以及新创建的文档 (比如新的word文档)，都总是直接将他们下载到最终要存储的地方。不要下载到操作硬盘或桌面后再转移到加密空间 — 这样会留下痕迹，并轻易的被他人找到。记得总是将文件直接下载或保存到安全的存储位置。

## 关于SSD

现在最新的硬盘通常被称作SSD (固态硬盘)，而在一些新的电脑上也仍在流行使用

旧式硬盘HDD（硬盘驱动器）。SSD比HDD的速度更快，体积也更小，通常是比较贵的电脑才会配备。因为它们的构造，让SSD能更勤奋的彻底改写和删除之前的文件和数据。不管怎样，CCleaner的程序倒是能带来一些帮助，但是早期的HDD硬盘，你无法确定删除的数据是否有被彻底覆写，也就是说要多加小心。也意味着使用完备的加密功能的重要性，留意下载的每一个文件的存储位置。如果要了解你的电脑用的是SSD还是HDD盘，用Google或DuckGoGo搜一下就知道。

## 本章问题

- 是否已经开启了电脑的基础加密功能？
- 是否已经完成设置隐藏加密空间，并测试过了？
- 是否已经理解了为何要使用隐藏加密空间（内部 VS 外部加密卷）？除了避免数据被黑客攻击外，是否了解合理推诿的概念是如何帮到你？
- 记住，要保护的信息越少越容易，删掉那些不必要保留的工作文件。



## 隐藏加密和文件修复

一个经验丰富的维权律师收到她信任的同事通过Telegram发来的消息，提到警方盘问了很多与她有关的问题，同时提醒她可能会被拘留或讯问。

她接触过许多维权案件，也和很多其他类似的律师合作过多年。她对于数字安全非常在行，总是在担心警方可能将她拘留，或是带走她的电脑，试图找到一些对她不利的信息。她几乎不用微信，至少是从不会在工作中用到。她也从很久前就停止了使用QQ，她还知道如何使用隐藏加密，已经用了至少一年了，不仅仅用来保护数据，更是隐藏这个加密盘本身的存在。

这个人并不像记者那样需要保护很多秘密的信息来源，但是她有很多客户的信息以及与他人相关的敏感信息。如果这些信息落入错误的人手里，她十分担心自己可能就此入狱，而且也可能给予警方机会打击他人。确保这些文档不会落入警方的手中是关键，对她自己、她的同事和她的客户的安全来说都是。

她一直都知道普通的加密并没有多大用处，如果警方有目的性的询问密码，她并没有把握能反抗很长的时间，她自己就是一名律师，太清楚在中国对禁止酷刑和虐待的法律保护没有丝毫的价值。因为对现状的了解，所以让她认识到开始使用隐藏加密的重要性，虽然一开始需要花点时间去理解。

当这一天终于来了，警察来带走了她，把她一个人关押在某个地方，经历长达一个多月的审讯，他们同时也没收了她的电脑、手机和USB。

在几天的关押后，她非常讶异警察开始每天向她出示一点从她的电脑里面找到的文件，她记得这些文件都被存在硬盘的加密空间内，而且警方也完全没有进入硬盘的密码，警方甚至没有找她要加密空间的密码，她更加确信他们并没有发现这个加密空间的存在。

每一次当警察拿出一份新的文件时她都感到心悸，这些文件危及到她做过的一些敏感案件的曝光，也提供证据以让警方更便利的打击她的客户们。

在被带走之前，她已经和其他可能会被带走的同事协商了一个掩饰说辞，其中一些被警方找到的文件和她的说辞背道而驰，大大的增大了他们的风险。这让她的忧虑感越来越强，很多晚上她都无法入睡，胆怯的想象怎样面对警方下一次出示的文件或指控。不停的想知道他们到底是怎样获取到这些文件的，很多只有她自己才有的文件，其他的任何同事都没有。

警方找到的文件都很随机，幸运的是只有少数几个是较为敏感的文件，多数

的文件都只有一部分，要么是来自大word文档中的几页，或大excel文件中的一到两个excel表。她还是想不通，他们到底是怎么得到这些文件的。

后来，因为警方并没有找到他们想要找到的“确凿证据”，尽管这样，她也没有获得真正的自由，她被取保候审，也就是警方可以在任何他们想要的时候再次带走她。不过总的来说还是因为大部分被保护的文件没被找到的情况救了她。

在她被放了的日子，通过在网上搜索信息，最后才终于弄清到底是哪出了问题。是文件修复程序让警方能够时不时的找到一些零碎的文件。因为自己的亲身经历，使得她又如狼似虎的去学习这个连很多在数字安全方面很厉害的人都不明白的东西，或者说就算他们明白，但也忽略了这能带来多大的威胁。

她后来发现数据就如记忆。它们停留的时间很长，甚至在它们开始消失时，也消失的很慢，只有其中的一部分消失掉。她发现，数据一旦被“删除”，并不意味着被真正的删除了，它会继续躺在硬盘里，只是不会出现在一般的用户眼前。但它一直都在那儿，直到这个数据所在的位置被新的东西填满。事实是大部分的数据都在加密空间内其实并不够，因为过去的多年里她的很多文件都是先创建在了桌面，后续才将它们转移到加密空间的。这是一个典型的偷懒行为，从同事处收到的很多文件和在网上下载的研究材料都会经常保存到桌面，仅仅为了再转移到加密空间。

那会发生什么呢？所有那些在普通硬盘内存在过的文档，一旦被转移到加密空间，就意味着准备好被警方用文件修复一网上一个使用方便的免费程序。他们只需要用程序仔细扫描硬盘，一步步的找出删除的旧数据，然后将他们拼凑起来。

## 暗网

网络就像一座冰山，只有10%是你能看得见的。谷歌和百度这些搜索引擎将这些网站用网页的方式呈现出来，而能被搜索引擎索引的这一部分网络，是非常小的一部分。

余下的通常被叫作深网。其中大部分并没有任何害处，很多的信息数据都直接由大学、研究所、公司或政府掌控，这些信息通常都在内部网，除非你进入到内部网，否则是无法获得这些信息的。同样的，如果是使用隐私设置，大部分在社交媒体上的信息（比如Facebook账户）也属于深网的范畴，因为这些信息无法直接用搜索引擎搜到和浏览。

在深网的内部是一个叫作暗网的区域。就算是获得了一个暗网的网站地址也无法用浏览器打开。所有的暗网网站使用的域名是.onion，在暗网中是没有.com, .org, 等域名的。所有的网址都是随机化的，它们看起来是这样的：“572abeh6g9gfd8gfd438gfd975.onion”。暗网是完全匿名的，这也意味着有些人会用来做一些非法活动，比如武器拍卖网站、网上毒品交易、拐卖儿童活动的聊天室等等。也有一些合法的原因，比如网上用比特币购物或其他的交易币，还有在有匿名需求的情况下网上聊天等等。

接入暗网的唯一方法是连接TOR或打开TOR浏览器。这也是唯一能读取和连接.onion网址的办法。如果要了解更多，开启TOR和它的浏览器，然后进入这个地址：

<http://zqktlwi4fecvo6ri.onion/> 

这是类似于维基百科的网页，提供了暗网的基本说明和其他链接，也包含了一些资料，这样你可以从中了解到暗网是什么，它是如何运行的，是否对你来说有用。使用暗网完全是合法的，我们推荐你试一试，学学看。不管怎样，关于会话的解决办法我们在手册提到的已经足够保护你了，所以在此就不再赘述暗网的细节。关于如何使用TOR和TOR浏览器，请见前面已经介绍过的章节。



## 第6章 分享信息





通过邮件安全的通信对很多人来说都是个关键的问题。本章节会介绍如何简单的发送安全邮件，当形式严峻时，如何用得以保护自己的方式操作。

本章主要讨论发送邮件，因为邮件很可能是你工作中的主要通讯工具。聊天工具、短信和手机通讯会在第11章：可用的安全APP中讨论到。除了一些针对电脑中使用的聊天软件的内容外，本章主要内容包括邮件加密，介绍一些简单易用的自动加密网络邮件选项以及云存储。

加密的功能非常有用，不过大部分时候都非常复杂。基于这个原因在此章节我们不会专注于PGP加密。一旦你被拘留或交出了电脑密码，单单是加密也并不能救你。要安全，最重要的是一定要使用工作浏览器（Firefox），这样他们才无从得知你所使用的邮箱服务，要记得使用零收件箱策略，这样就算他们知道了你的密码也找不出任何东西。这样你的工作也更有效率，因为一旦收到邮件，相当于要赶在清空邮件之前先做出回复，或甚至有必要的话将特别重要的邮件复制存储到隐藏加密空间。

## 普通加密 VS “端到端加密”

要为任何数据加密，就应该生成一把密匙。这个密匙是独一无二的，有了它就能为你的数据进行加密了。大部分的服务都能够自动生成，密匙用来加密或解密信息，只有那些有密匙的人才能读取或解密信息。

“普通”加密，密匙是由服务供应商生成的，比如说发送Gmail邮件，Gmail的服务器会加密后再发送到收件人再解密，很明显的缺点就是只有服务商才有密匙，也就有潜在的可能被服务商利用这个密匙以读取信息，一旦服务商的系统被黑，或将信息交给政府，里面的信息就会被泄露。优点就是服务商能够自动生成和管理密匙，用起来很

方便。以内部安全性以及拒绝向政府交出用户信息的方面来说，Gmail应该是最最好的邮箱，Yahoo则是最糟的。千万不要使用中国的邮箱服务，比如Baidu, QQ等。

如果某个服务提供端到端加密，意味着密匙是由你的电脑或手机生成的，然后再自动与收件人交换。也就是指服务供应商并不能读取你的邮件或信息，因为他们没有密匙。在现实中就意味着第三方无法阅读和插入你们的会话，就更无法在警方要求的情况下交出你们的会话信息，因为他们根本看不见，不过他们还是能提供元数据（可参考后续元数据的介绍）。

在任何时候，都应该尽可能的使用端到端加密。

## 安全邮件比较

安全收发邮件最好的方式就是使用专门提供高级安全性能的网络电邮。现阶段，这三个安全的邮箱服务都没有被中国封锁。这里说的电邮服务，比如Gmail, yahoo等都是指通过连接浏览器登录邮箱，而不是将邮箱的客户端安装到电脑（比如Thunderbird, Outlook和Mail之类的）。

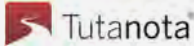
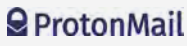

**“不要在安全邮箱的设置上填入你的真实名字或昵称，这样会让外人轻易分辨哪一个邮箱是你的账户”**

除了使用下面我们推荐的几个安全邮箱外，我们也建议你设置一个Gmail邮箱，它提供比较强大的安全性能，特别是如果你设置两步验证，也保持零收件箱策略的习惯，对于那些不是特别敏感的工作来说，使用起来会更简便有效率。不要因为国内封锁Gmail就却步，用VPN登录Gmail虽然比较麻烦，不过能保证你的安全性高出一个级别。

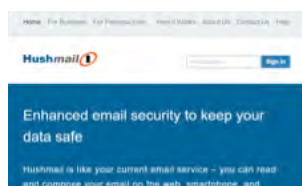
不过，在某些时候你还是会需要彻底安全的邮件，从下面的清单中选一个，设置一个账户。

**“大部分的邮件服务商和加密系统并不会加密主题栏，记住，由于大部分的加密邮件还是会直接显示邮件的标题，最好是写一个意思不明确的标题，以免引起注意。”**

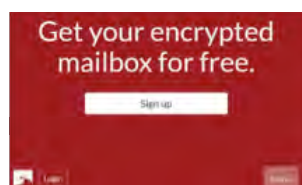
这些安全电邮有一个缺点，就是它们发挥最大安全性能是在内部账户之间的通讯上。意思是指如果你使用的是Tutanota邮箱，最好另一个人也应该使用Tutanota。也有方法能够让你从Tutanota邮箱（或其他安全邮箱）发送到别的普通邮箱，通过输入密码的方式才能读取邮件，不过安全性还是不够高，也不太有效率。但因为你的收件人还是需要向你要密码才能打开，在下面我们还是教你如何使用这个功能。

			
<b>End-to-End Encryption</b>	YES	YES	OPTIONAL
<b>Chinese Language</b>	YES	NO	NO
<b>Phone App</b>	Android + iOS	Android + iOS	Payable Service (iOS Only)
<b>App Lock</b>	NO	YES	NO
<b>IMAP</b>	NO	NO	Payable Service
<b>Export Key</b>	NO	YES (only public)	YES
<b>Encrypt Subject Line</b>	YES	YES	NO
<b>Autodestruct Old Messages</b>	NO	YES	NO

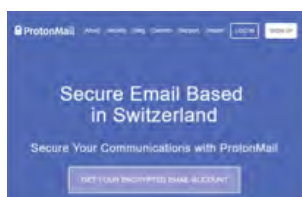
为了使用起来更有效率，你应该与你常联系的同事确保都选择同样的服务商，这样你们可以一起使用。也就是说，如果你的大部分同事和朋友使用的都是ProtonMail，你一个人使用Hushmail就不是很聪明了。



**Hushmail** 在过去很长一段时间都是唯一的安全电邮供应商。来自加拿大，少有功能的提升，现在似乎没有选择用Hushmail的必要因素，除非你的大部分同事已经在使用，否则，我们建议还是使用别的安全电邮。



**Tutanota** 快速的成为在中国工作或做与中国相关工作人们的热门电邮，也包括国外。它来自德国，并且有中文版，也有用来收发邮件的安卓版和iOS版App。缺点是它没有一个专门的打开App的密码保护功能，意味着任何拿到你的手机的人都能进入你的Tutanota邮箱。当然你还是得要保持零收件箱策略的习惯，但是也还是会有一定的安全风险。Tutanota也能加密主题栏，这是通常其他的加密电邮没有的功能，这样又能多一层的安全性。



**ProtonMail** 是一个来自瑞士的新电邮服务商，是那些非常重视信息安全的人们的新欢。与Tutanota一样，也有安卓和iOS的App，不过有内置的密码保护功能。并且还有一个可设置发送给其他ProtonMail限时自动删除的功能（从你和收件人双方的邮箱中删除），这样能帮你保持邮箱为空。目前还没有中文版本。ProtonMail也有加密主题栏以及一些其他的元数据的功能，这样其他人就无法读取。

Tutanota和ProtonMail都不能使用邮件客户端，因为密匙是无法导出的。而且，安全电邮本来也不应该使用客户端，所以这样也正是好事。

就是这三个主要的服务商，与你常邮件往来的朋友讨论，从中选一个使用。

我们首要推荐ProtonMail，如果有中文服务对你来说很重要，则可用Tutanota。

建议你不要安装这些邮箱的手机App，特别是没有自带密码保护的App。在手机内装上App意味着任何拿到你的手机的人都能发现你在使用的是哪个邮箱，要是那个APP还没有密码保护功能，那他们更是可以直接进入你的收件箱。这部分我们会在第三部分做更多的讨论。

在完成了邮箱的注册后，进入设置区域熟悉各个选项，不过通常并不需要做任何更改，因为邮箱本身就有很高级别的安全性能了。

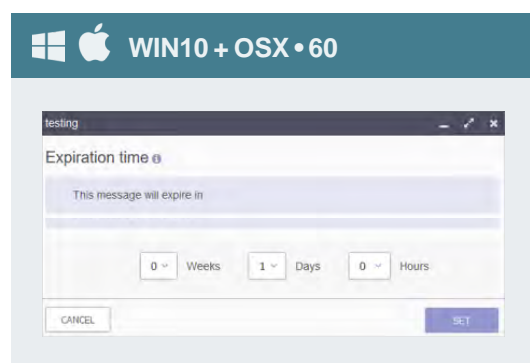
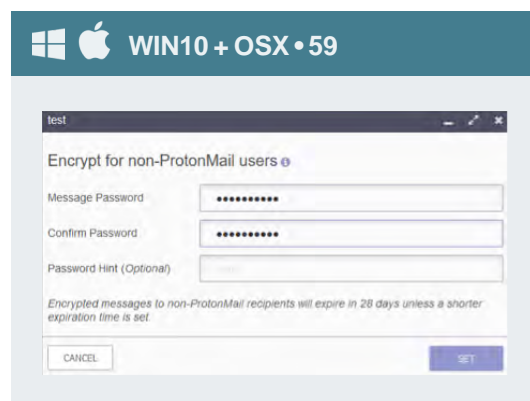
## 用安全电邮发送邮件到普通邮箱

这几个安全电邮的使用方法都很简单直接，并不需要特别介绍使用方法。不过，如果你要用它们发送邮件到普通邮箱，比如Gmail，就需要设置一个密码。当发出邮件后，收件人就会收到一个链接，他需要点击这个链接跳出一个新的浏览器窗口来读取这封邮件。要能读取邮件的内容，收件人需要知道你在发送邮件时所设置的密码，否则就不能读取（解密）。也就是说你要将这个密码用一个很安全的方式发给收件人，我们推荐用Signal或Telegram（电报）发送密码，开启自动销毁（删除）功能，关于Signal和Telegram的更多介绍在第11章：可用的安全APP。下面我们会用ProtonMail示范如何操作，以及如何设置自动销毁邮件。

打开新建邮件(WIN10+OSX·58)，在窗口的左下角有三个图标，分别是附件、加密/创建密码和限时自动销毁。点击中间那个图标创建邮件密码。

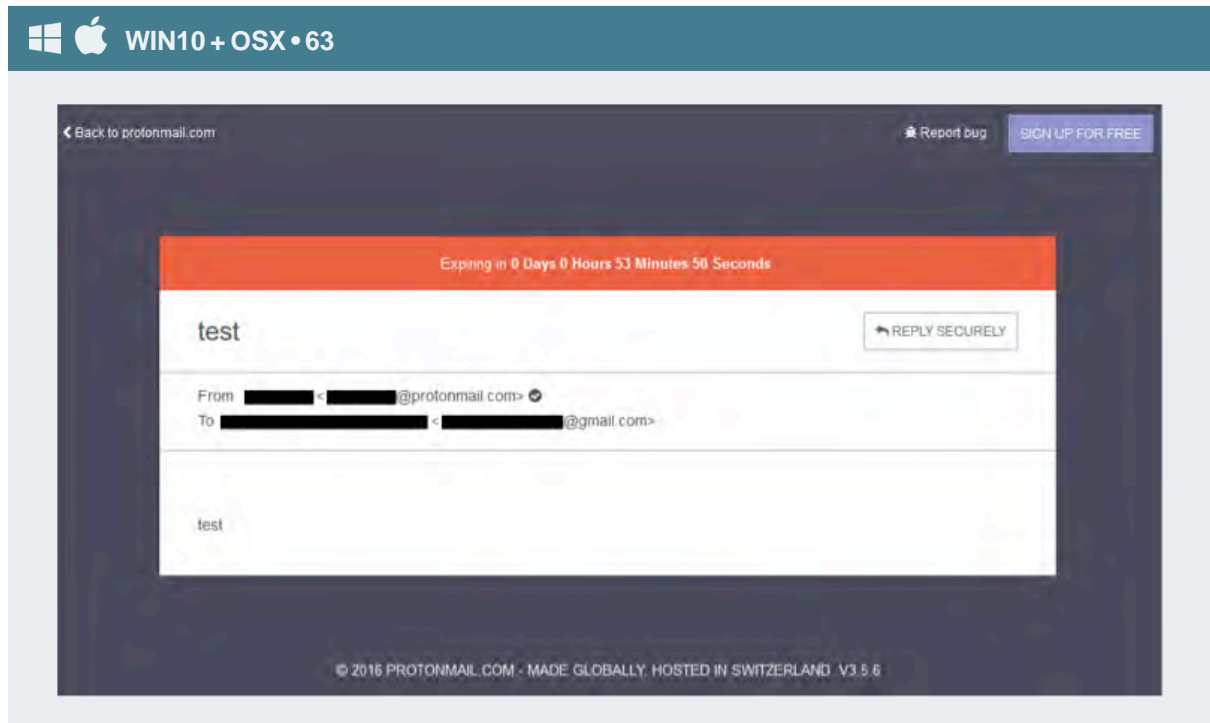
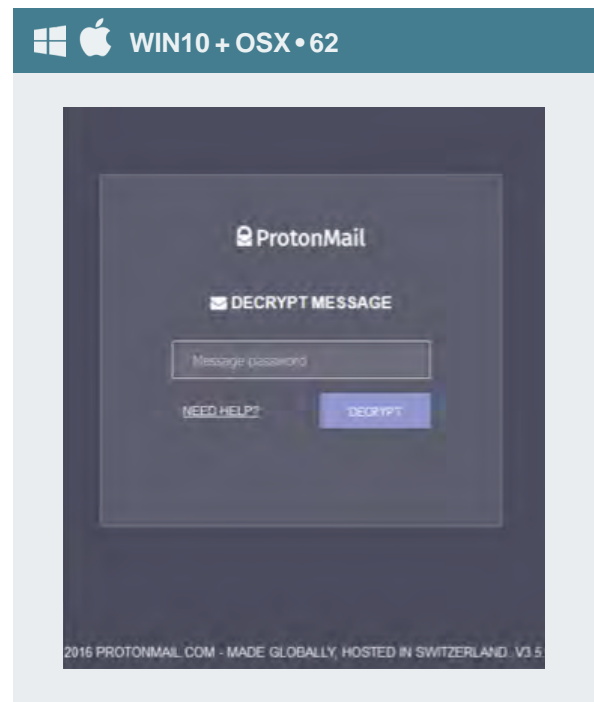
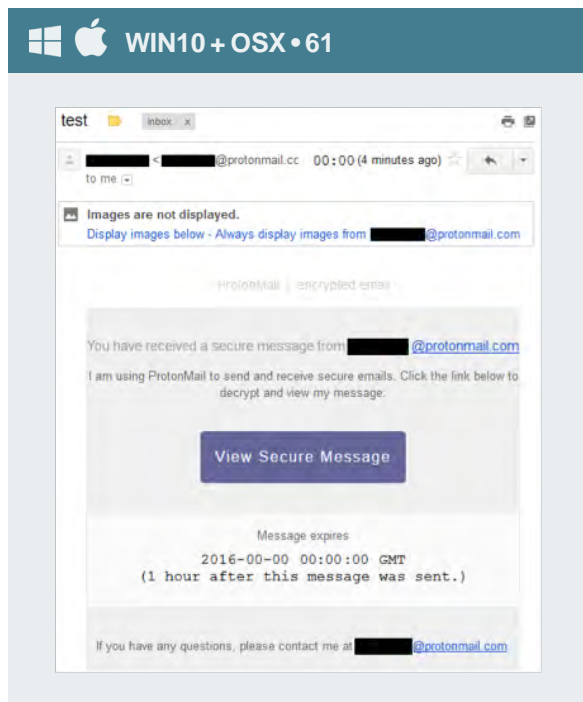
创建完密码点击Set（设置）(WIN10+OSX·59)后，你会回到刚刚第一个窗口，再点击第三个图标设置限时自动销毁。

设置完自动销毁的时间后，在点击Set回到原来的窗口。（WIN10+OSX·60）





发送邮件后，收件人会收到一个包含链接的邮件，他可以点击链接进入到一个新的网页，键入密码即可。只有键入密码才能读取邮件(WIN10+OSX·61-63)。最后，如果点击reply (回复)，通过ProtonMail来回复，使用同样的密码即可。(WIN10·61)。



## IMAP 和 邮件客户端

我们建议将安全电邮设置到邮件客户端，比如Outlook, Mail或Thunderbird。这些客户端并没有可靠的进入程序所需的密码功能，那些有此功能的程序被各种Bug充斥，都很不安全。上面提到的几个安全电邮刚好也并不支持设置客户端的功能。客户端只会带来没有必要的威胁，如果坚持零收件箱策略的话，客户端也并不实用。一旦将邮箱的程序安装到手机或电脑里就意味着只要你被带走，别人就能发现你在用的邮箱，接着就会强迫你交出密码。在手机或电脑里面装上了邮件客户端就意味着我们前面讨论的那些重点都付诸东流，所以重点是在于隐藏使用痕迹，确保他人无从得知你在使用的邮箱。

### 4个关键行为

#### 零收件箱策略

在之前的多次强调中我们已经了解到邮箱的最大威胁并不是被高阶黑客入侵，而是一旦被拘留，警方强迫你交出邮箱密码。如果被拘留，警方就有机会得到进入你邮箱的密码，要么你交出你的密码，就算你不交出，你的同事或朋友也有可能交出他们的密码给警方，这样你和他们之间的所有邮件来往记录都会被警方看到，这就是为何零收件箱策略如此重要的原因了，它是为你带来安全的重要工具之一。

#### “零收件箱策略是保障安全的重要工具之一”

设想在你被带走后，警方进入了你的邮箱，零收件箱策略则能保证进入你的邮箱的人发现不了任何的内容。简单来说就是保持你的收件箱（和其他的文件夹）为空。在99%的情况下，这不会带来任何问题，因为大部分的邮件都不需要长时间的保留。它的重要性我们在此已经说的够多的了，同样的，让你的同事和朋友也如此操作。

#### 无回复约定

无回复约定是零收件箱策略的延伸版。如果你的邮箱已经被他们掌控了，他们只需要稍微等一等就能了解到你的大量信息，这是因为我们通常发送邮件的方式。当发邮件时，我们通常都是在当前的邮件下点击“回复”，而不是重新写一封。鉴于此，早前的通信内容会包含在同一封邮件内，通常这样来来回回的通讯可以持续一段时间，也因为这样，一封不长的新邮件会包含一段长长的早期邮件内容。也就是说，如果你的邮箱被控制了，那个人只要等人用回复功能回复你的邮件，就能读到你们先前的通信内容。

所以，当你回复同事或朋友的邮件时，避免使用邮箱的回复功能，或说如果

要用的话，确保删除原先的邮件文字。这能确保在被带走的情况下，如果警方在查看你的邮件，一封新的邮件到来时，也只会包含尽可能少的资讯。请告知你经常通信的朋友或同事避免使用回复功能。

### 自动登录与交叉服务登录的危险

自动登录有很大的安全隐患，特别是当进入了一个账户就能进入同一个服务商的其他账户。比如在浏览器登录了Gmail后，不用重新登录就能进入到google drive（云存储服务）和Youtube等。同样的情况也适用于其他家族式服务商，比如苹果、微软等等。

最好的方式来避免这类情况就是尽量一家公司只使用一个服务。比如你在用Gmail，那云存储的服务就不要用Google Drive，这样能避免自动登录和账户同步的威胁。

## “绝不要启用任何邮箱或云服务的自动登录和同步服务”

现在的很多服务都擅于用同步服务（Auto-sync），比如你在手机中有了Chrome，再在电脑的Chrome浏览器中登录，如果没有禁用同步功能，Google会将这两个不同设备中的浏览器信息同步合并。在电脑中保存的书签都会出现在手机中，浏览器历史记录、保存的密码等等都会被同步。这是一个很大的问题，不要用账号登录你的工作浏览器。

### APP ACCESS

虽然现在Windows10也有了在电脑中安装App的服务，就好像手机一样，不过我们强烈建议不要使用此类App。首先，大部分App都没有原始（内置）密码保护，也就是说任何能进入你的电脑的人都能进入这个App的界面并读取里面的信息、聊天记录或邮件等等，甚至是装作成你发送信息。在电脑中安装了App也让他人一目了然地了解你在使用服务，这样一旦你被拘留也就失去了你本应有的保护自己的能力和能力。

## 云存储

云存储通常是指信息的线上存储。有些云服务只用于工作文档的备份，有些用于更新和存储电脑内的设置和程序，还有些如协作平台在运行，可以用来与他人分享文档以及同时编辑等。一般来说，线上存储都不算安全。鉴于这个原因，敏感工作文件绝不要使用OneDrive (Windows), iCloud (Mac)和Google Drive服务。虽然不是所有的

云服务都很糟糕，不过只有在你懂得如何使用的情况下才能安全使用。

你也许已经有云存储服务了，虽然你可能都没有留意。如果你有Gmail那就肯定有Google Drive，如果在用Mac电脑，一定有了iCloud，如果有Windows系统或是用Hotmail，那你一定有了OneDrive，很多的这些云服务都是随着手机和电脑进行预先安装的。

如果一定要用云服务的话，应该用一个有选择备份功能服务的程序。这样的程序会在电脑和手机后台运行，任何时候作了任何文档的更改，这个云存储都会自动更新。这样相当于就算手机和电脑弄丢或被没收，你也有备份，另一方面也说明云存储是一个可能被他人利用获取你的信息的途径，所以要谨慎使用。

首先，全面检查你的手机和电脑，看有哪些服务和App被安装和启用了，没有使用的都应该设置禁用。特别是现在的手机都是自带保存照片、视频和文档等个人信息的配置，这些都可能成为威胁，特别是在手机里的这些程序几乎都是不需要输入用户名和密码就能进入的。移除和卸载那些你不会使用到的云服务。

其次，如我们在隐藏信息的部分中提到过的，不要依赖于用手机里的App进入云存储。App确实很方便，但很容易带来风险。任何拿到你的手机或电脑的人都能轻易发现你在使用的服务，然后强迫你交出用户名和密码。如果不按照步骤来保障在网上备份的同隐藏加密空间一样的数据，使用隐藏加密空间的意义就不大了。

记得要用工作浏览器通过VPN登录到云服务。

有些云服务会在后台运行程序中自动将新的文档和工作中做的改动上传，这样并不好。还有一些是需要手动进入云服务，上传那些你希望存在线上的文档，我们建议你用这个，因为它的安全性更高，而且得以隐藏你使用的服务，有人一旦进入你的手机或电脑也无从得知。还是那句话，绝不要使用中国公司提供的云存储服务。

下面是一些云存储提供商的概况，你能发现其中大部分都有安全风险，这个清单内只有两个是被推荐使用的，因为这两个都提供强大的加密功能，而且App也有密码保护，仅存储那些你手动筛选上传的文件和档案，不会上传电脑内其他的东西，比如设置等。

可见，实在要用云存储的话，仅有SpideroakOne和Tresorit相对比较安全。

	Free Space	End-to-End Encryption	Encrypted Storage	App PIN	2-Step Verification
Google Drive	15GB	No	Yes, but weak	No	Yes
iCloud	5GB	No	Yes, but weak	No	Yes
OneDrive	5GB	No	No	Yes	Yes
Dropbox	2GB	No	Yes	Yes	Yes
SpideroakONE	2GB	Yes	Yes	Yes	No
Tresorit	5GB	Yes	Yes	Yes	Yes



## 本章要点

- 只有在真正需要的时候才使用云服务；
- 使用安全的云服务，而不是设备内预装的；
- 卸载或禁用任何没有在使用的云服务；
- 通过VPN的网络连接用工作浏览器登录云服务；
- 云服务只用来备份工作文档，不要用于同步或其他会存储你的设置、个性化和程序的配置等功能；
- 如果你需要使用App，确保它有密码保护功能（输入密码才能进入App）；
- 如果要一个用于分享文件和协作的线上云服务，选一个与用于备份的云服务不一样的服务商。

## 本章问题

- 普通加密和端到端加密之间有什么不同？
- 你会选择哪一个邮件供应商 (Protonmail, Tutanota, Hushmail)用于联系你的工作伙伴？
- 从这个章节中你学到了哪四个关键的安全发送邮件的行为？
- 云存储的优势和劣势分别是什么？你是否已经了解如何安全的使用云存储？

## 向正处于安全威胁的人发送信息

如果你需要向某个可能正处于安全威胁的人发送信息，不管是问问题、聊天或给予指示，都应该用尽量减小潜在风险的方式。这个人可能正面临被拘留或绑架的风险，也可能被视为网络攻击的目标，或者仅仅在于你并不完全信赖此人能安全的保障你所发送的信息。毕竟不是所有的人都会遵循安全的存储信息的步骤，这样一来你自己能够用减小潜在风险的方式发送信息就显得尤其重要。

对于一个普通的电脑用户来说没有任何办法可以在已经将信息发送到别人的电脑时不失去控制的，因为一旦任何程序或脚本有类似的功能比如阅读后删除数据等，都会被对方的电脑认为是病毒而拦截掉。

首先，你应该尽可能发送内嵌的消息：就是内容在邮件的正文内而不是用一个附件形式。如果不是特别的有必要都不要使用附件。如果非得用附件的形式不可，则尽量减少附件里的内容，在添加附件前将文档内的元数据清除掉，请看如下的操作方法。

### 发送可以自动销毁的邮件

ProtonMail因为它的自动销毁功能从众多的邮件服务中脱颖而出。类似的服务在两个聊天软件上也有，Telegram和Signal，我们在手册内的手机安全部分有提到。你可以在给某人写一封邮件时设置一个时间，这个时间从你发出这封邮件时就开始计时，这一点很重要，时间是由你发出邮件时开始计时，而不是从读取时开始计时。你可以设置一个合适的时间，比如1小时或一天等，这个时间点一到，邮件就会被自动销毁，而且是在你与收件人双边同时销毁。确保当你发送了这样一个安全邮件时，收件人能及时的读取邮件。

另外一个ProtonMail的优点在于就算你的收件人不是ProtonMail的账户，也仍能发送高度安全的自动销毁功能邮件。收件人会收到一封邮件告知如何取得这个ProtonMail的邮件内容，在第5章：分享信息的部分有详细介绍。一旦这个预设的自动销毁时间已过，这个读取ProtonMail的链接即失效，也就是这些信息已经被自动销毁了。在邮件中的附件也会被销毁，不过，如果之前已经从链接中下载了的文件就不会被自动删除，所以，尽可能的不要添加附件发送。

如果要想此类安全通讯更有效率，与他人的联系必然要用到Signal或Telegram这一类软件。因为你要告知收件人你发出了邮件，他需要尽快读取，如果没有及时读取，邮件会被自动删除。所以ProtonMail应该与此类安全聊天软件合并使用以达到更高的效率。如果你用ProtonMail发送邮件到非ProtonMail邮箱，则需要设定一个密码，而收件人需要知道这个密码才能打开，参见第5章：分享信息了解如何操作。一旦你设置好了邮件密码，接着就



要通过安全聊天软件将这个密码发给收件人，Telegram和Signal这样的软件都提供自动销毁功能。

使用自动销毁的功能意味着你不需要担心收件人是否有严格遵循安全使用电脑的步骤，比如删除邮件的习惯，或是坚持零收件箱策略等，因为你知道在这个设置的时效一过，不管收件人的行为如何，这个邮件就会被自动删除。如果你刚发出邮件，这个收件人就被带走了，你发送的信息也仍然会在时效内被自动删除，当然还是希望在被邪恶的第三方看到之前，这样就不会因为某人忘了删除敏感的信息而给他人带来威胁了。

## 在有必要的时候才添加附件

正如我们在后续的元数据部分有提到的，任何的文档中都包含了比你想象的要多的信息。不止是文档中的内容，还有元数据。元数据所包含的信息是一旦你建立了一个文档，建立文档的这部手机或电脑的型号、用户名、地理位置，甚至是包含有的照片因为手机自动脸部识别功能所标注的名字等。要了解元数据的更多信息以及如何移除，请参见手册第二部分的元数据章节。

如果你确实要建立一个文件作为附件发送，要考虑到下面几个点：

- 不要包含照片、Excel、图表等绘图信息；
- 在保存文档前使用Office软件内置的功能检查和删除所有的元数据（“检查文档”功能）；
- 不要发送Word, excel等形式的附件，将文档转换成PDF再发送；
- 为PDF文件设置密码保护。

当你将word或excel文件转换成PDF格式时，会有为文件设置密码的选项，我们建议你将这个选项作为必要的操作，然后使用安全的聊天软件，如Telegram或Signal，告知你的收件人打开文件的密码。有密码保护的文件就像被清空的收件箱，能保障收件人避免受到具有伤害性的攻击，毕竟他人所能获取的结果有一定的限制性。大部分你收到的附件一般也不需要一直保留，一旦用完附件中的信息，比如更新一个案件档案，添加到一篇文章，完成一份上诉状等等，就应该可以安全的将这个附件档案删掉了，删除步骤可参见第7章：安全删除。

最后一个重要的提醒，记得总是遵循“零收件箱策略”，也将这个习惯普及给其他与你频繁联系并可能面临风险的朋友。“零收件箱策略”是保障你的人身安全的最大武器。

## 第7章 删除信息





这部分内容会教你如何真正的删除文件和信息，你会发现以前所理解的删除很可能是错误的。彻底的删除、为工作文档建立隐藏加密空间、以及用安全的方式收发邮件，这几个方面的结合才能最大化的保障你的安全。

在阅读这部分内容之前，你需要先了解一个重要的信息 — 你的硬盘是HDD（硬盘驱动器）还是SSD（固态硬盘）。如果你用的是Win10系统，只需要打开搜索功能键入搜索词 Disk Defragmenter（中文：碎片整理和优化驱动器），进入程序就能看到窗口中所显示的连接电脑的硬盘类型、分区、USB等等。OSX的系统中则需要找到并点击 概览> 系统报告 > 硬件> SATA（查看“介质类型”）。

本章大部分的内容都是基于传统的HDD硬盘，因为HDD硬盘目前仍然是普遍被使用的硬盘。如果你最近购买了更新、更高端的外部硬盘，则很有可能就是SSD硬盘，如果你用的是SSD硬盘电脑，这章的大部分内容都不适用。关于SSD我们在下方有专门的一段介绍，但是你最好还是不要跳过本章的其他内容，特别是内容中也有包括其他的硬盘和USB的介绍等。

你认为什么算是严重的威胁呢？当你点击删除文件、或清空回收站时，实际上信息都没有彻底地被删除，你以为昨天或是两年以前已经被删掉的文件，也仍然躺在那儿随时等着被任何心怀不轨的人翻出来。对那些有必要保护信息和资料的人，必须说如何彻底删除是一个最大的问题。被删除的文件也许无法在搜索栏中被找到，但其实它们仍然躺在那儿，很轻易就能被警察或安全局找到，操作的方法也并不难。

删除的概念对于很多人来说还是一个知识盲点。就算很多对于信息安全有一定认识的人，也常常忽视了安全删除的问题。

要理解不安全的删除所带来的风险，就需要了解硬盘的工作原理。包括所有形式的数字存储，比如USB、SD卡、电脑硬盘等。

## 数据存储

不同类型的存储格式运行的方式有所不同。这也让安全删除更困难。鉴于这个原因，加上已经提及的其他原因，你需要尽可能减少电脑、手机、硬盘和USB等工作相关的设备，要留意的设备越多，实际的操作就越难。

所有的数字存储空间（硬盘、USB、SD卡等）以最基本的级别来说包括两种类型，空闲空间（或可用空间）和已使用空间，已使用空间当然是指已经被你的文档、视频等占据掉的空间，空闲空间则指那些剩余的空间。不过，空闲空间并不等于清空的空间，它是指电脑中当前没有被已用数据占用且可以被存入新的数据的空间。

当删除某个文件或清空回收站或垃圾桶时，那些数据实际上没有真正的被删除，它们仍然在那儿，还在之前所在的硬盘中的同一个位置。只是当你点击删除时它会告诉电脑不再需要这个数据，一旦数据被标注不再需要，那个部分就会变成空闲空间，用于以后存入新的文件数据。对于用户来说，虽然看不见已经被删除的数据，但是它们并没有消失。

这些“被删除的”数据还能被读取，更糟糕的是要读取它们并不需要多复杂的技术。你只需要下载一个免费的程序，点击几个按钮就能找到这些数据，这种程序叫做文件恢复程序，在法律实施和刑事案件中是比较普遍被用到的工具。

更重要的一点是要清楚“被删除的”数据并不是按时间顺序排列的。当存储一个新的数据并不表示会覆盖较早的空闲空间或最新的空闲空间，它是随机的。也就是说不要期待某个特定的数据会被覆盖或留下。这也是为何要确保真正和彻底地删除所有数据的重要性。

要让数据能被彻底的删除，就需要被新的数据覆写。只有在被旧数据占据的那个空间被新的数据覆盖（覆写）掉，旧的数据才算是真正的被删除了。

进一步说，比如一个word文档，你可以“撤销”一个动作，也许你不小心删除了一句话，可以点击撤销就能恢复了。类似word撤销功能的方式也能用在恢复你所删除掉的数据上，外人至少可以恢复一些被你删除的文件，甚至有的已经被覆写过的文件。所以，旧的被删除的数据必须要被覆写多次，这样才能确保没有人能够将其恢复。

幸运的是，有程序能为你解决这个问题。这个程序叫做CCleaner。操作方法非常简单，在下面的技术解决方案：CCleaner中有介绍操作步骤。

## INFO-BOX. SSD 固态硬盘

大部分的电脑硬盘都是HDD类别，直到今天最普遍的电脑中都还是在使用HDD硬盘。长久以来，为了安全的从此类设备中删除数据而开发了很多的技术和程序，比如CCleaner的使用。不过，现在一种新型的硬盘渐渐变得普遍，叫做SSD(固态硬盘)。它比传统的HDD硬盘尺寸更小、速度更快、而且性能更高。所以，它通常都被用于高端的电脑中，尽管你买一台新的普通电脑，也很有可能是自带HDD硬盘，而不是SSD。

它的优点：电脑中的SSD硬盘自带一个新的特殊性能，叫做TRIM。它的功能是比较传统的HDD硬盘更能安全的清除那些你删除掉的数据，大大增加了警方利用“文件恢复软件”恢复数据的难度。

它的缺点：本质上的问题是CCleaner的（或其他类似的软件）覆写和擦除“已删除”的数据功能在SSD硬盘无法运行，或者说，无法取得效果。实际上，在固态硬盘的OSX系统中CCleaner的这个擦除空闲空间功能已经被彻底的移除了，就算你能看到有这个功能，但也没有什么用，它的使用反而会对SSD固态硬盘带来伤害。因为CCleaner的这个功能无法在固态硬盘电脑中使用，也就无法确定电脑中被删除的数据信息是否彻底地被清除，因为你不知道TRIM具体是什么时候运行和进行删除动作的。

TRIM在OSX电脑中都是有自动启用的，在Win10的电脑中也通常是被启用的。要确保是否有启用的话，在搜索区域键入“命令提示符”后点击右键，选择“以管理员身份运行”。在跳出的窗口中复制粘贴字符“fsutil behavior query DisableDeleteNotify”回车（请不要将引号包括进去）。回复的指令应该是“NTFS disabledeletenotify = 0”，这个0表示启用了，如果显示1则表示没有启用。如果回复的指令中显示为1，则复制粘贴这个指令“fsutil behavior set disabledeletenotify NTFS 0”回车，电脑就会设置为启用TRIM了。

## 转移文件

了解转移文件的确切意义很重要。当转移一个文件时，很简单，通常就是新的位置创建一个拷贝文件，而在原来位置的文件则“被删除”，就像我们上面讨论过的。也就是说如果你在桌面上（也就是存储在系统盘）创建一个新的word文档，然后转移到你的加密空间，那之前的位置就会被标注为可用空间，其他人则可以轻易的用文件恢复程序就能找到原来的文件。同样地也适用于你将任何文件通过浏览器先下载到电脑默认的文件夹（几乎都是存到系统盘内的），再将她们转移到加密空间的情况。

将文件从一而终的存储在安全的空间内如此重要的原因是它能保证不会被他人追踪到痕迹。任何在普通硬盘中存在过的文件，不管有多短暂，比如说C盘，都能被文件恢复程序在相应的硬盘中找到。另外如果你将文件直接保存在一个USB上，一旦删除后，它的痕迹就会留在这个USB上。你可以用CCleaner轻易的彻底删除这个USB内的文件痕迹。

这也是另一个不管在任何情况下都不要用手机存储工作文件的原因，就算是短时间的。绝对不要通过邮箱下载文件到手机，就算是阅后即删，也绝对不要。

## 虚拟内存

最后，在这里插一段，在第2章：电脑设置中你有做过一个本地安全策略（Win10）的设置，用于在关机时自动清除“页面文件”。在OSX中这个设置是在使用安全虚拟内存标签下。建议你做出这个设置的原因是电脑会用记忆来保持你工作的最新信息，当你关机的时候，这些随机存储信息（被称作RAM）就会被清除。通常电脑也会利用一部分的硬盘来协助这个动作，所以当你在使用电脑时它也会收集一些你的操作信息，这



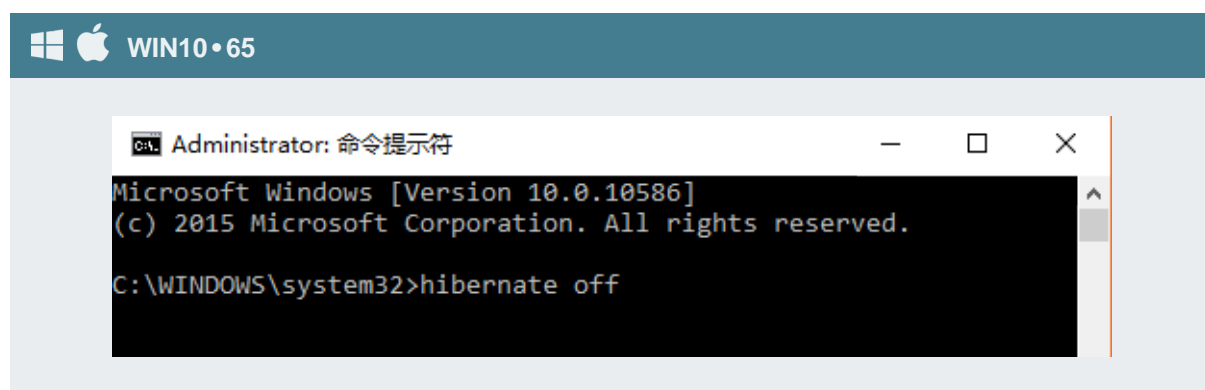
个“虚假”的记忆有很多称呼，比如虚拟内存、交换文件、页面文件等。也许你已经在电脑中做了设置，每当关机的时候电脑会彻底的删掉这些信息。但是如果你没有设置的话，硬盘中就会包括你早前工作过的一些数据痕迹，一旦有人没收你的电脑，稍微有点技术的人都能读取到这些信息。所以这个问题在此就算是被解决了。

## 设置睡眠和休眠时间

休眠是Win10中能让电脑在关机后迅速回到你当时离开时的界面的功能，这个功能的方便之处是能快速的回到电脑的使用中。它工作的原理是操作系统会将离开时的电脑信息全部都存储在硬盘，这样当你再回到电脑时，它就会重载所有的信息。也就是说如果你开启了休眠状态，一旦电脑在这时候被带走，开机就能看见你上一次使用时的所有信息，比如浏览器的日志以及其他更多的信息。这个被存下来的信息是没有被加密的存储，非常危险。

要在Win10中禁用休眠功能，按住Win键+X，在出现的菜单中选择命令提示符（管理员）（WIN10·64），跳出的窗口中在光标后输入powercfg.exe /hibernate off，回车即可。（WIN10·65）

关于睡眠和电源的设置可以到电脑设置内搜索电源和睡眠就可以根据情况设置了。



- 总是将工作文档存储在隐藏加密空间
- 建立一个新的文档或文件，直接在隐藏加密空间操作或是任何你打算存储的位置操作
- 要当心转移文件，它们会留下痕迹
- 不要在手机和Pad上下载和读取工作文件
- 不要使用休眠功能，当要离开电脑很长一段时间或电脑进入了睡眠，请直接关机。

## 技术解决方案：CCLEANER

CCleaner 是一个能帮助我们解决很多问题的程序。这个程序不仅能确保删除电脑所收集的的各种信息，比如你工作的痕迹、cookies、临时文件、在编辑的word文档数据等等，而且还能确保擦除电脑的空闲空间和“已删除”的文件。

注意：如果你用的是SSD固态硬盘的电脑，“擦除空闲空间”的功能是没有作用的。不过，除此之外其他的功能如擦除痕迹和日志等还是可以正常使用，不管怎样你还是应该安装并使用这个程序。

Win10和OSX都可以在 [download.com](http://download.com) 中下载这个程序，下载后进行安装。

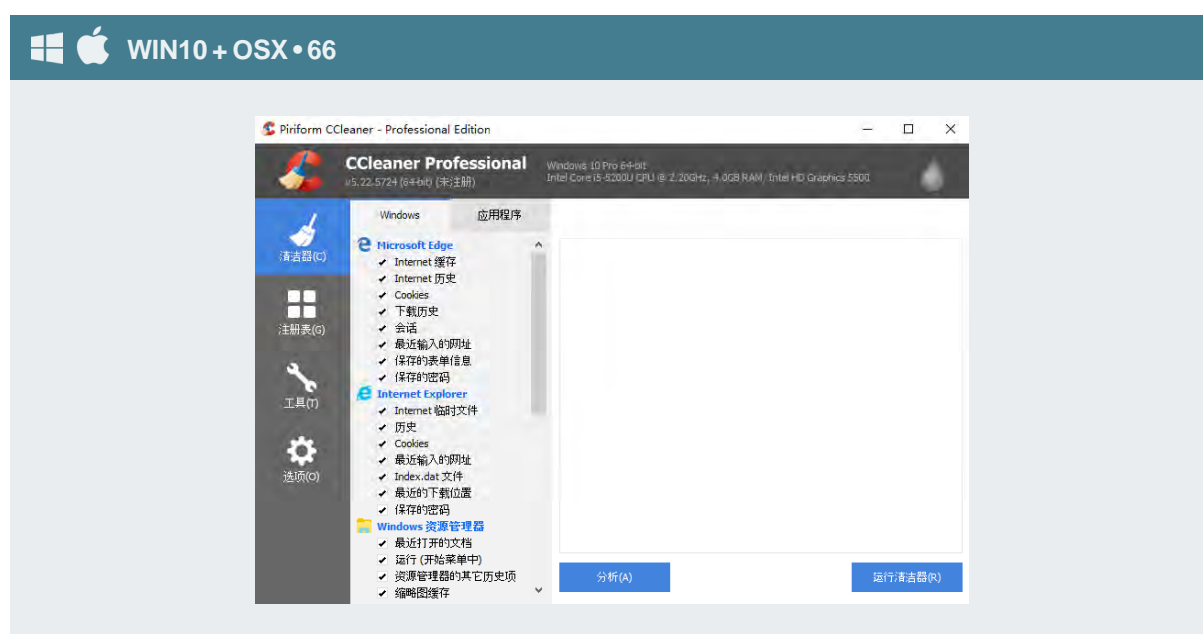
安装完成在桌面或程序文件夹内找到图标，在Win10系统中还能在回收站点击右键选中打开CCleaner。

打开程序后在左边能看到有多个标签，Win10版本的标签比较多，OSX的版本只有三个，不过它们包含的设置和选项都大致差不多。

打开程序第一眼就能看见清洁器的图标，在清洁器图标的右边也能看到两个标签，一个是运行系统 (Windows或Mac OSX)，另一个是应用程序。在Windows (或Mac OSX) 的下方点选所有的框，这些是在你运行这个程序时会被安全删除的所有不同类型的信息。在Win10版本的中这个清单的最下方是擦除空闲空间的选项（先不要点选此项，特别是如果你用的是SSD固态硬盘）。

在应用程序标签下能发现更多的安全删除选项。具体的选项取决于电脑中所安装的程序。在这里你可以勾选所有的框，不过如果不打算删除个人使用的浏览器痕迹，则可以不要点选那个浏览器的框。或是依照对这个浏览器的具体需求点选。（比如可以删除浏览器历史纪录，但是不删除已保存的登录信息）。如图(WIN10+OSX·66)。

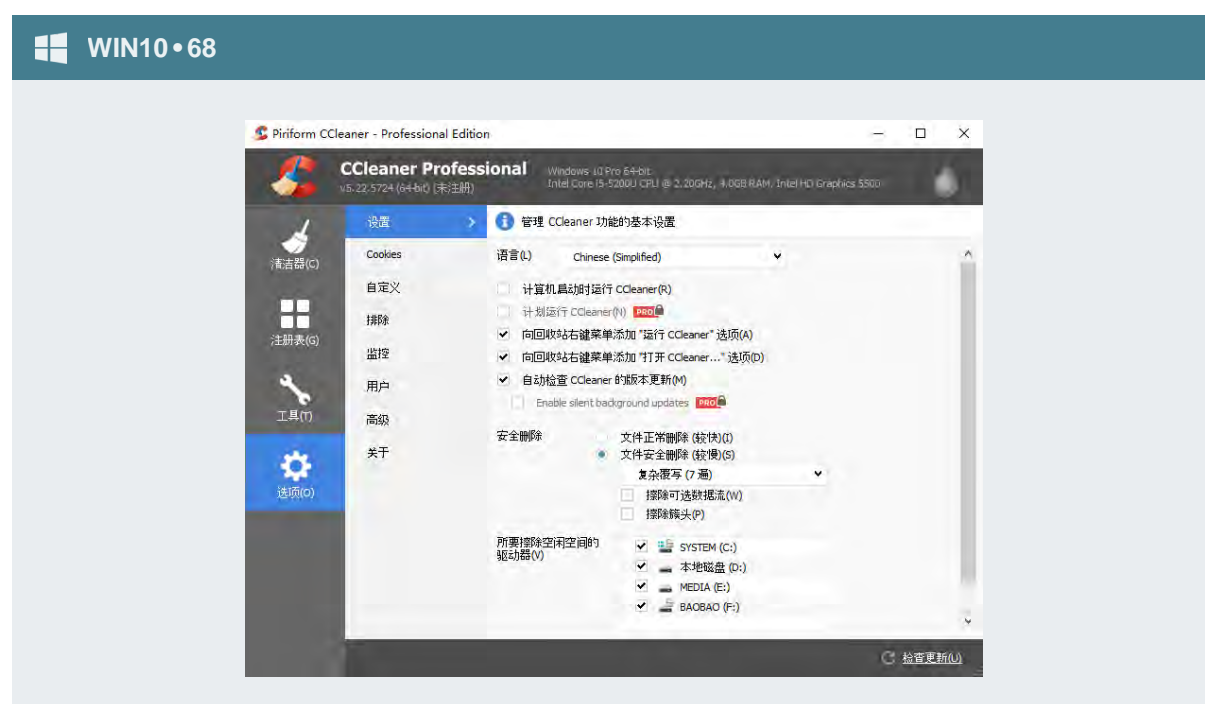
在这之后，点击主菜单左下方的选项，右边显示的第一个是如下图所示设置的按钮。



在OSX系统中你需要选择彻底删除资料，在下方的下拉菜单中选择复杂覆写7遍（OSX·67）。选择的数字越高就表示安全删除的比例越高，当然所花费的时间也会越长。



在Win10系统中，你也可以做同样的选项（WIN10·68），或者也可以有其他的选择，在自动检查CCleaner的版本更新选项前打勾，然后到最下方的所要擦除空闲空间的驱动器选择哪个硬盘需要被擦除空闲空间。如果电脑有插入USB，也会显示在这个清单内，这样你也可以勾选这个USB的擦除空闲空间。

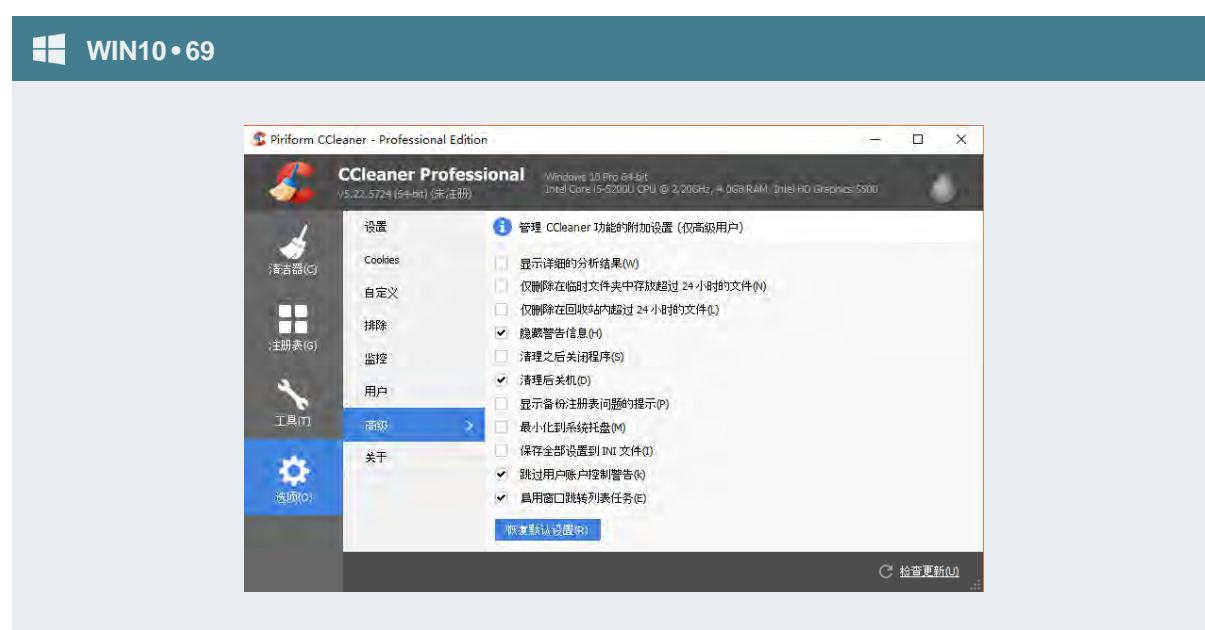


注意：如果你的加密空间（硬盘）在启动CCleaner时是开启/加载的，那这个驱动器清单

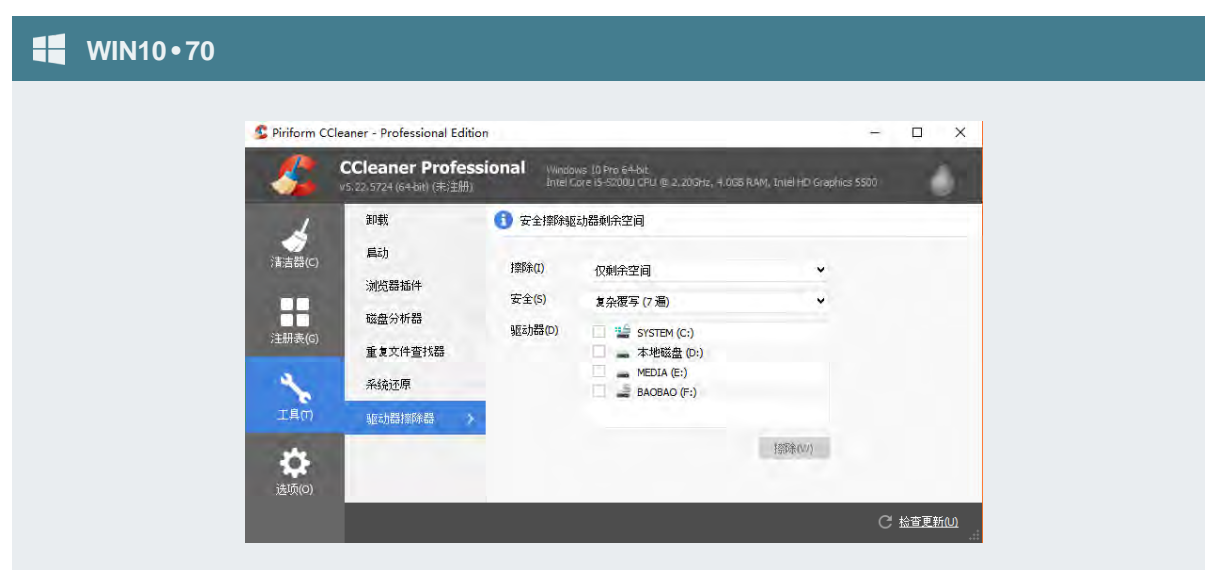


中也会显示，没有必要选中加密空间，一般情况就只需要选通常的C盘（系统盘）即可。

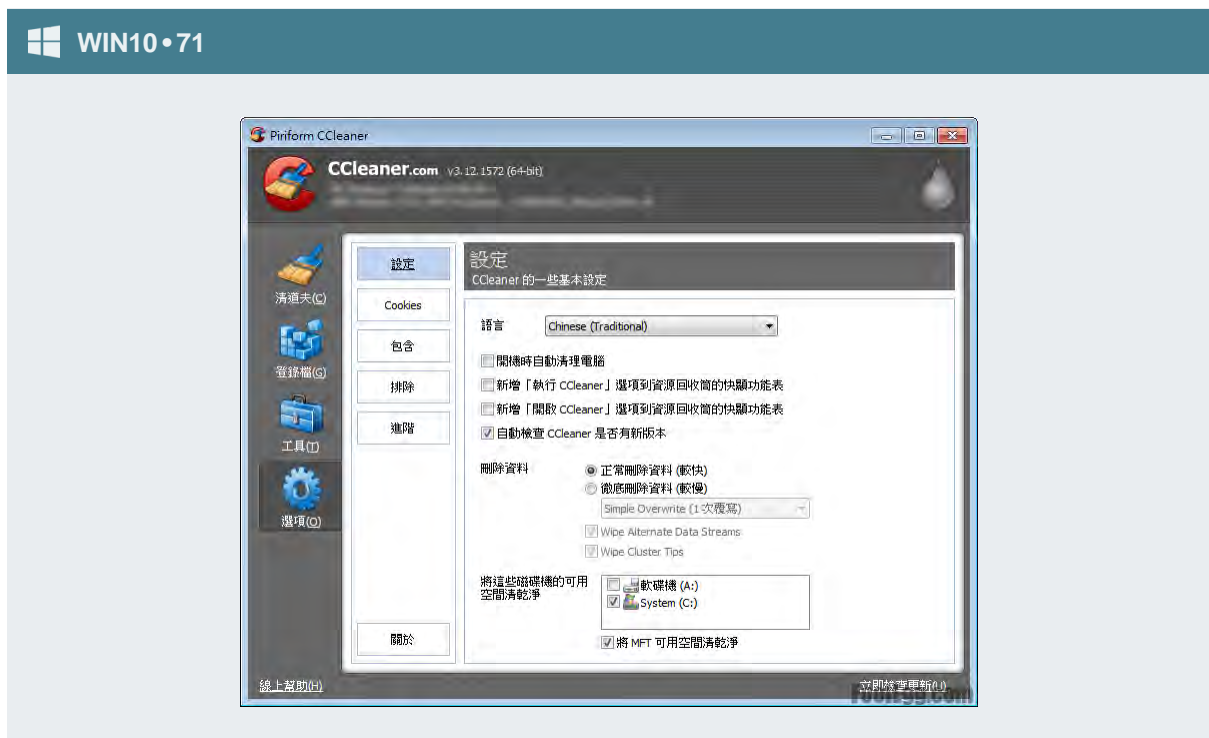
在Win10的版本中在选项内还有一个高级的标签，点击它，再选中隐藏警告信息，或者也可以点选清理后关机，这样一旦CCleaner结束了清理工作后电脑就会自动关机。（WIN10·69）



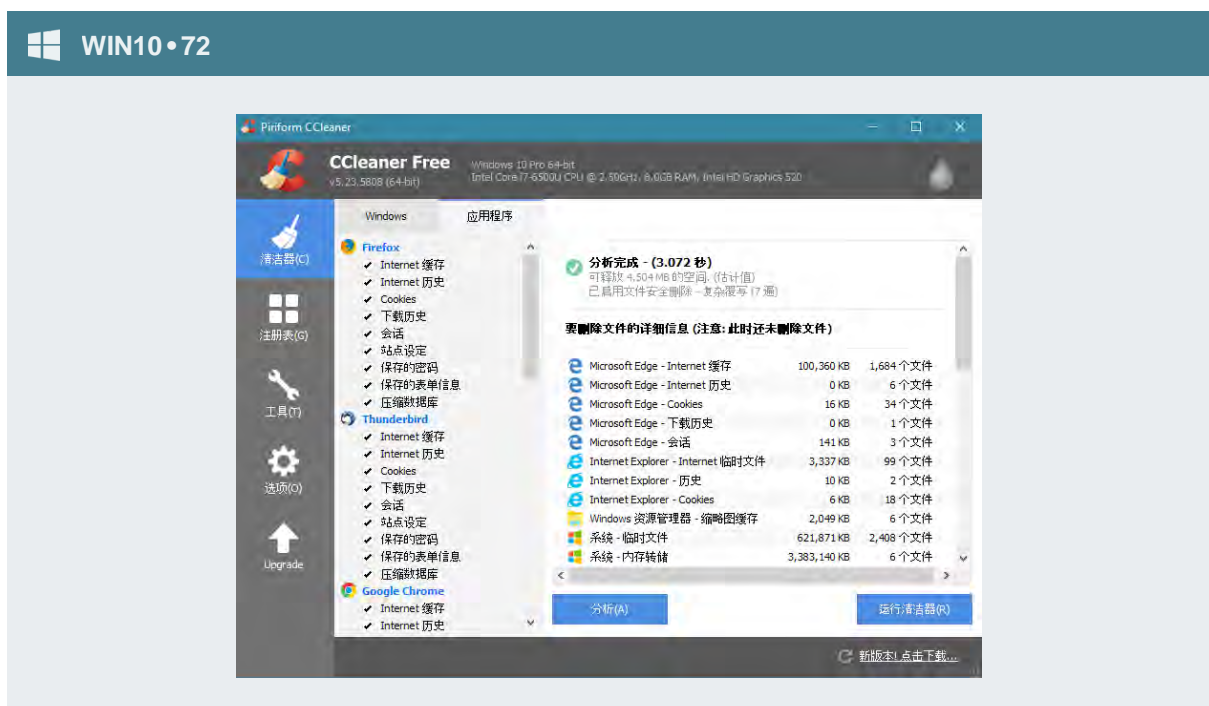
最后，Win10版本的工具下还有一个驱动器擦除器的标签，这个功能是在不用运行整个清洁器的情况下，仅擦除空闲空间——还记得早前我们讨论过的空闲空间就是残留的那些本来应该被你删掉了的旧文件吗？请记得点选如图所示的仅剩余空间（WIN10·70），否则电脑里面所有现存的数据也会被删掉。



如果要在OSX中操作同样的功能，找到工具标签，然后点击磁碟抹除器进行抹除即可。（仅限HHD硬盘）（WIN10·71）

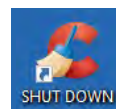


好了，现在已经完成了设置，可以先试着运行一次。回到清洁剂标签下，点击分析。在快速的分析后，会显示哪些数据会被删除，点击运行清洁剂删除这些文件。按照目前我们在上面的步骤设置，清洁剂内勾选了擦除空闲空间选项，这会花费很长时间。如果你只打算清理操作系统的痕迹或浏览器的上网活动痕迹等，可以再回到清洁器的选项内取消勾选擦除空闲空间选项，重新分析 (WIN10·72)。如果开启分析时没有关闭已打开的word文档、相关的程序或浏览器，会被要求先关闭它们，否则CCleaner无法清理。



## 运行CCLEANER

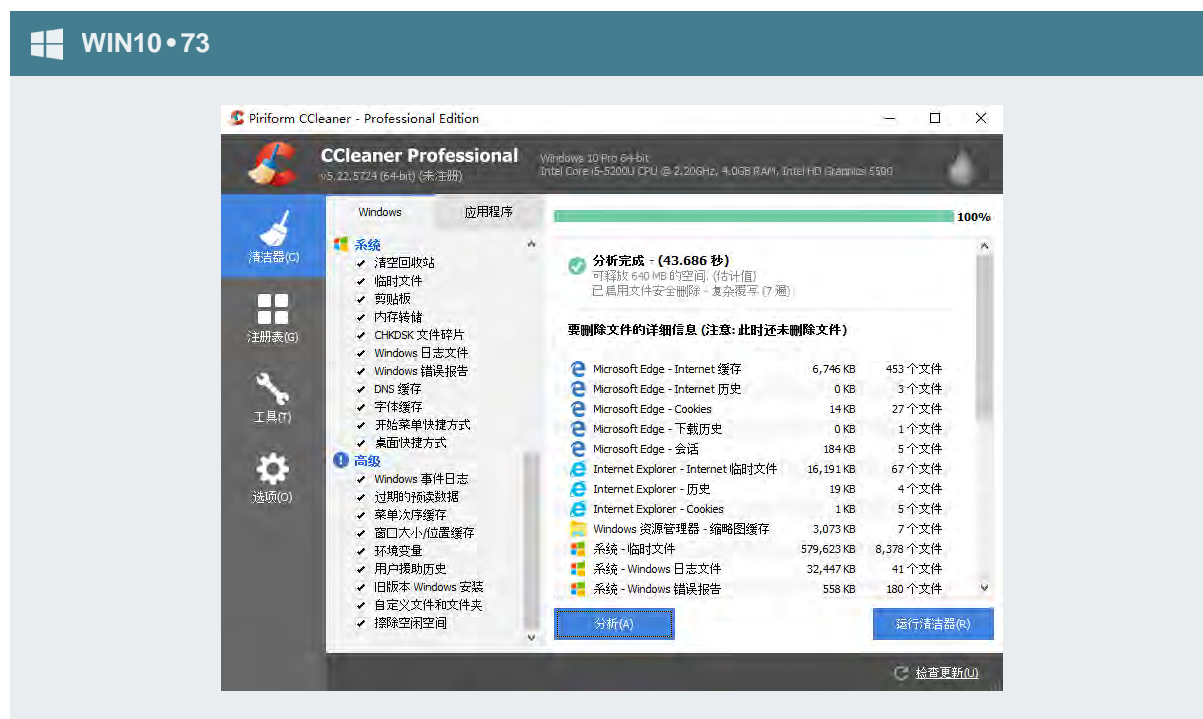
CCleaner的运行一般分为包括或不包括擦除空闲空间。包括擦除空闲空间通常会花费较长的时间(除非你的硬盘空间很小)。如果你只是要清理数据痕迹的话,可以不要勾选擦除空闲空间运行程序。要常清理,实际上每天当你结束电脑的使用后,在关机前都应该进行例行的CCleaner清理工作。



当你的安全现状处于比较严峻的时期，你应该花些时间在硬盘中运行擦除空闲空间，可以在运行清洁器时就将此擦除的选项包括进去，也可以用我们介绍过的专门擦除硬盘空闲空间的工具。如图S-WXX 和 S-OXX。

## 用CCLEANER关闭WIN10

很遗憾在OSX系统没有这个功能。在Win10系统的CCleaner进入左边菜单选项内的高级标签下（WIN10·73），就能看见有一个清理后关机的选项，在框里打勾，一旦勾选了这一项，电脑就会在完成了CCleaner的清理后自动关机。



如果你在用Win10系统，我们强烈建议你点选这一项，这样一来你不用再像平常一样点击关机键，而是用CCleaner。反正你已经结束了电脑的使用，也就不在乎电脑要花多久时间才能关机，因为反正你都是要离开电脑了。



## 元数据，分享发布，MICROSOFT OFFICE

元数据就是内容之外的数据信息。比如邮件，元数据包括这封邮件发出的时间、大小、使用的IP地址、标题栏信息以及谁收发的。如果是word或PDF文档，元数据就表示何时建立或编辑的、是谁操作的（指电脑的用户名）、更改的时间点等等。同样的也适用于那些出版和设计工具，比如MS publisher，InDesign等。

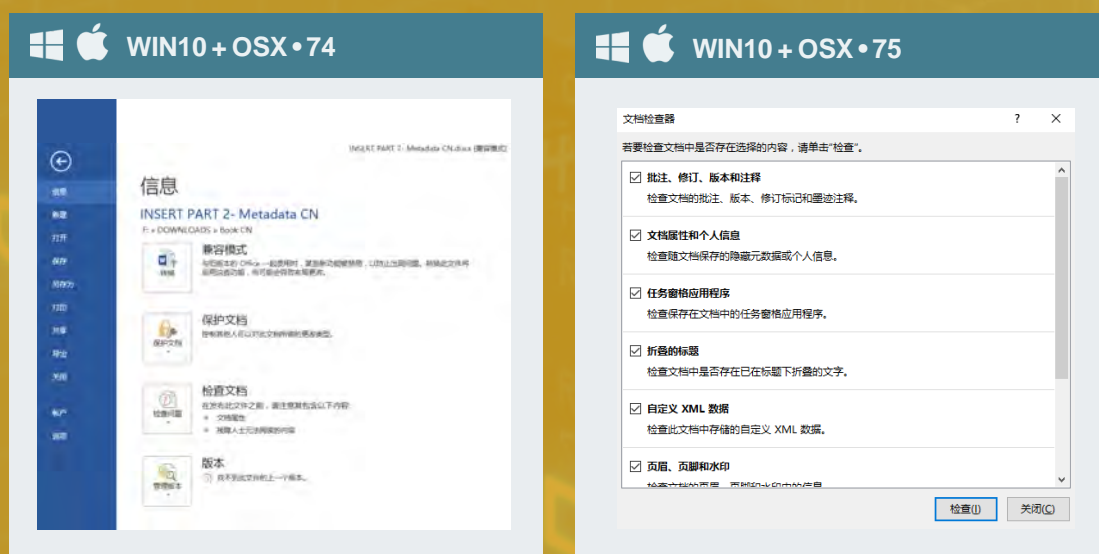
当今，用手机拍的照片或视频，通常都可能包含了这些元数据。如果允许了地理位置的接入，那就会包含拍照时的地理位置信息，更神奇的是，现在的照片软件甚至会基于你的电话簿以及早期拍过的照片，辨认出你所拍照片中的人并自动嵌入他们的名字。想到这个，应该就能想象你发布的一个PDF文件或是传送给某人的照片中所包含的有多少数据了。

在这里讨论元数据的原因是确保你不至于分享或发布比你所认为的更多的数据信息，因为元数据能留下大量的证据。

### OFFICE和PDF文档

微软Office办公套件包括Word，Publisher，Excel等，都有自带的从文档中移除元数据的功能。也就是在转存为PDF前是可以先移除掉元数据的，操作的方式在Win10和OSX是一样的，位置也很容易找到，只需要点击文件，就会出现如下面图示中的信息窗口。

点击检查文档前的检查问题，如图（WIN10+OSX·74）会出现一个下拉菜单，点选检查文档（WIN10+OSX·75）会跳出一个窗口显示所有会被检查到的问题，点击检查按钮。





在点击了检查后，窗口会显示在每一个问题下所找到的信息（WIN10+OSX·75+76），只要有找到信息的问题，就会在右边出现一个全部删除的按钮，点击全部删除的按钮，然后点击关闭。这样所有的元数据就已经被移除了，你可以按照你想要的方式再存储这个文档，转换成PDF格式等。

在旧版本的OSX系统中的Word操作有些许的不同，打开文档后，点击word > 首选项 > 安全性，在保存时从文件中删除个人信息框前打勾。（OSX·77）

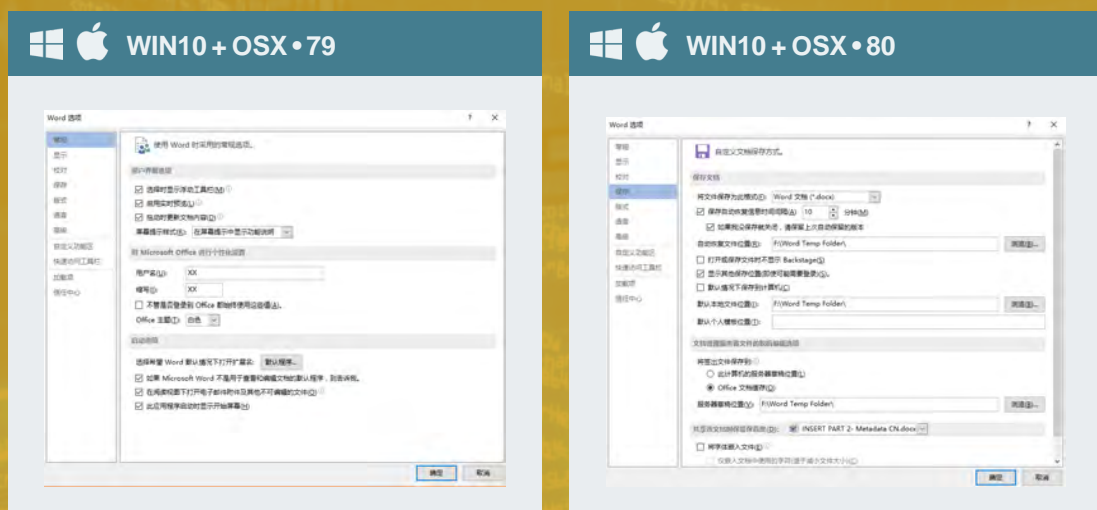
## 微软OFFICE 设置

到了这一步是时候查看一下你的Office套件的设置情况了。打开一个Word或Excel文档，点击文件后，左下角有账户和选项的标签，如果你点击账户（WIN10+OSX·78），你看见有显示如现今的大部分浏览器一样的登录按钮，一旦登录后就会同步你所有的Word或其他Office套件的设置，如果你要确保工作文件都不要有元数据的话，就不要登录。

另外如果你点击进入左下角的选项标签，它会跳出一个窗口，左边的标签中有两个是你要注意的，一个是常规。在窗口的中间部分（WIN10+OSX·79）是你的用户名和缩写，用于显示在你的文档中，要确保你的真名不会出现在这，你可以修改后再点击Ok。







另一个相关的标签，也很重要，就是保存。有两个地方需要注意（WIN10+OSX·80）。就是自动恢复文件位置和默认本地文件位置这两栏。

在Word或其他Office软件的使用中，文件会不时地自动将文件保存一次，这是以防万一电脑当机的情况下不至于丢失掉所做的工作。总之，如果你没有手动改过这些自动保存的数据的话，应该在电脑操作系统盘的Office文件夹内，在你保存了这个文档并关闭后这些数据才会被删掉。正如我们在删除章节内所学习到的，这种形式数据其实并没有被完全的删除，也非常的不安全。所以，要躲开这个小却很危险的威胁，要确保点击浏览后选择你的隐藏加密硬盘（或USB）内建立的文件夹作为自动保存数据的地方。

照片

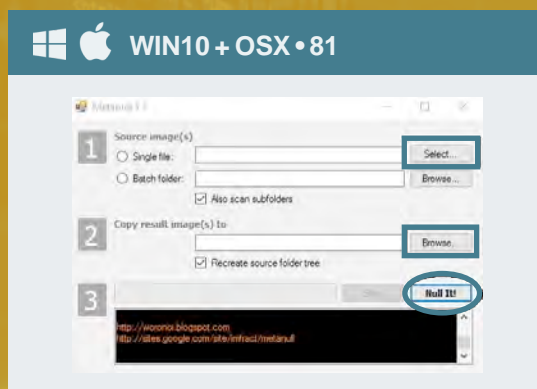
针对电脑内保存或使用的任何照片，有简单高效一键清除元数据的软件可用，也可以手动的在Win10或OSX中删除。如果你有意要从电脑中将照片上传到网上，或是在一份报告、Word、Pdf中使用，我们强烈建议你先将照片中的元数据删除掉。

“WIN10和OSX中的任何文件，都可以用操作系统内自带的删除元数据功能或专门的元数据清除程序”

Win10系统的电脑，我们推荐MetaNull, 可以在这个网站下载 [http://download.cnet.com/Metanull/3000-20432\\_4-75732772.html](http://download.cnet.com/Metanull/3000-20432_4-75732772.html) 。

很简单，开启程序后，点击Select选择你要清除元数据的文件或照片，点击Browse选择无元数据的版本应该存储的位置（WIN10+OSX·81），点击Null It。完成后你可以试着右键点击新版本文件（或照片），查看属性里面的详细信息，再对比之前版本的属性，就能发现元数据已经被删除了。





如果你不想要下载程序，也可以用WIN10自带的功能直接删除元数据。右键点击文件，再点击属性--详细信息，在窗口的最下方能看见删除属性和个人信息，如果你点进去，选择全选，再点击确定就会删除数据了(WIN10·82)。



OSX的电脑，从<https://imageoptim.com/mac> 下载并安装ImageOptim，将图标放在桌面比较明显的位置，(OSX·83) 在需要使用或发布一张图片时，开启ImageOptim，将图片拖到窗口中，再选择删除元数据。

另外也可以去到 ImageOptim Preferences 点选所要删除的数据。在General标签下，在Enable下面的所有选项前面打勾 (WIN+OSX·84)。一旦做过这些设置后，意味着以后每次你拖进一张图片到ImageOptim 窗口，这些勾选的数据都会被移除。

要手动删除OSX系统内的图片文件元数据，先打开相关的图像与预览拉下“工具”菜单，然后选择“显示检查器”点击 (i) 图标，再选择GPS (OSX·85)，接着点击移除地理信息。这样还是会有留下一些其他的元数据，不过移除任何潜在的地理位置信息。





## 元数据和JOHN MCAFFEE

这个故事是关于2012年发生在国际上有名的电脑专家的事件，它让人们意识到元数据的危险性。大部分的人还是不清楚元数据是什么，以及它是如何带来危险的。美国人John McAfee（约翰迈克菲）是迈克菲杀毒软件的开发者之一，世上开发的最成功的杀毒软件之一。当他2012年还在伯利兹居住时，因为被谋杀的邻居而被通缉，后来最终被引渡回美国而得以免罪。虽然他是无辜的，但是因为他自己对警方的疑心，所以他躲了起来，他的秘密地点最后因为接受了一位VICE的记者采访而暴露。这位记者在采访过程中拍了一些照片，然后与VICE的文章一起发布到网络，这位记者并没有意识到发出一张照片意味着多少的数据会暴露。

当这篇文章发出时，就很容易让人们下载这张照片并扫描到它的元数据。任何就算只有基本电脑技能的人也能轻易的找出这张照片是在哪里拍的，用的什么手机型号拍的，拍照当时的GPS地理位置。在这篇文章发出不久，McAfee就被伯利兹的政府逮捕，在后来被引渡回国前，他在破败的看守所中度过了极度痛苦的一段时间。

这个故事的寓意很明显，特别是对在强权下的人权捍卫者们尤其重要，比那些单单只是不希望被找到的人重要多了，比如McAfee。

# 第三部分 手机安全

本手册的第三部分包括多个章节，都是关于手机安全的内容。

## 第8章

了解手机安全，介绍包括手机的运行以及面临的主要问题是哪些。

## 第9

手机的使用，介绍了关于如何安全的使用手机以及手机使用习惯相关问题的指引。

## 第10章

手机设置，同电脑部分的第2章一样，是关于手机基本设置的枯燥章节，教你如何通过改变这些设置提高安全性。

## 第11章

可用的安全APP，会介绍一些相应的既便于使用又有更高级别安全性的APP。



## 第8章

# 了解手机安全





在这个章节我们会包括智能手机是如何被监视的，面临的主要威胁有哪些，各种App的安装是如何增加安全风险的。

尽管在今天手机就像一个小型电脑一样，但它们的性能还是有限的，因此在解决安全威胁上能做的就更加有局限性。总的来说，手机从来都不安全，记住这点很重要。如果有疑心或在需要提高安全性的情况下，都不要信赖手机。关机，如果可以的话将电池取下，将它放到安全的地点，只要你的电池还在手机内你就仍然可以被追踪到。如果你不得不带着手机，可以参考第9章手机的使用中让手机“中断通讯”部分。

## “总的来说，手机从来都不安全”

你可以测试看看手机是如何的给你添麻烦的。取下手机的SIM卡，去散个步，然后再查看你的地理位置功能就能发现它在没有SIM卡的情形下也仍在运行，如果可以在Google地图或其他的程序上追踪你的动态，那意味着警方或任何在有需要的情况下也是可以追踪到你的活动的。这是因为只要你的手机不在飞行模式，手机都会持续使用无线电波的原因，是手机能连接到网络、信息、电话和追踪的通道。也是在手机没有SIM卡的情形下还能使用紧急电话服务的原因。这意味着警方在任何需要的时候都能追踪到你。

这带给了我们第一个问题，地理位置追踪。地理位置追踪功能大部分情形是这样工作的：你的手机每隔一小段时间就会向外发送无线电波（就算你没有打电话或发短信），离你最近的手机信号塔（基站）会接收到电波，手机会持续性的如此与信息塔保持

通讯，以便于有人给你打电话或发短信时你的手机能随时接收。在大城市有许多的手机信号塔，只需要分析你的手机是如何与它们通讯的，就能非常准确的找到你手机的地理位置，有时候能够精确到在你房子的哪个房间（用各个不同的信号塔进行三角测量）。现今手机也有GPS功能，也能利用你的Wi-Fi连接找到。也就是说你的手机唯一安全的时候是在飞行模式或是连接到这些信号的通道被拦截时。现在很多的App都要求连接地理位置，比如微信，这相当于是给警方更多的途径获取你的位置，而地理位置追踪的问题还不是唯一要担心的问题。

如果担心与同事、客户之间的会话被监听，这时你的手机又带来了另一个问题。以技术的层面来说，用你的智能手机窃听你的通话叫做“roving bug,”但是通常情况我们就称它为窃听。

警方要窃听你的手机通话首先会辨认你的手机，这很容易，因为在中国的SIM卡注册都是实名制，非实名制的黑卡或许能减缓这个过程，但也不能保证，因为警方仍能通过你的手机发出的电波找到你的地理位置，比如你的家里或办公室。当你的手机被确认后，就很有可能连接你的手机后打开麦克风，记录下从你的麦克风范围内传输的一切。这是一个后台操作服务，在你没有收到任何通知的情况下就能执行。同样的，在你不知情的情况下手机的摄像头也可能被打开用来记录你或周边的环境。记住，远程接入你的手机麦克风和摄像头的威胁也同样适用于电脑。

## “手机的摄像头和麦克风可以在你不知情的情况下被打开”

现今的智能手机给我们带来了更多的问题。早期的手机只需要取掉电池就能避免这些威胁，现在的手机通常可以关机，但电池是不能被移除的，或是就算电池可以被移除，但大部分手机内部还有一个内置的备用小电池，这个功能的作用是比方说你在晚上将手机关机，第二天早上闹钟仍然会响，还有短时间的关机后，在开机时日历和时间区域的设置还是正确的。就算你的手机已经关机，也已经取下了电池，在一些国家的警方仍然能够进行窃听，就因为这个麻烦的内置小电池。所以，单单是关机并不能带来足够的安全，移除电池也变得越来越不能像曾经那样能保障安全了。

## “单单是关机并不能带来足够的安全”

如果你是警方的眼中钉，当然就有更多的方式令他们设法连接你的手机，浏览你的文件、截屏等等。现在不需要成为一个黑客就能做到这些事。

由于这些威胁，你的手机在通常情况下应该仅仅作为一个通讯设备，而不是一个小型的工作电脑。千万不要用手机下载或存储敏感的文件、文档和照片。彻底的从手机中删除文件是非常困难的，如果你还记得，在关于删除的章节里我们有提到过，仅仅是

删除文件并不意味着真正的移除了，因此，不要用手机存储（甚至只是暂时）任何工作文件。

IMSI捕捉器 是近来最受多国警方青睐的一个监视工具，是小型、容易使用且成本低的手机监视工具。通常用于有大量人群聚集的游行和活动中。IMSI捕捉器会装成一个手机信号塔，所有附近的手机都会以为它是信号塔而连接到这个IMSI捕捉器。现在的IMSI捕捉器设备小到随时都能带在身上。手机的加密标准通常都是由信号塔设置的，而不是手机本身，所以IMSI捕捉器会引导你的手机仅使用（或不使用）最基本的加密功能。警方可以在任何区域都能识别出所有的手机，记录下所有的信号数据，然后直接读取。IMSI捕捉器的位置居于你的手机和信号塔之间，所以通常情况下被叫做“中间人”攻击，这个词也用于电脑和网络流量，不过它们的原理并不相同。

最后，再一次提醒你，除了这些因为手机本身的功能带来的威胁之外，那些通过手机下载的App也能允许同样类型的连接，App甚至更容易带来威胁。要当心你安装的程序，要清楚意识到任何中国的公司都是危险的，因为警方能直接连接到这些公司和他们的服务，这些公司也不会在警方需要的情况下为了给你法律保护和警方作对。

## 你的电话被窃听了吗？

在以前要找出电话有没有被窃听是件挺容易的事，如果你的电话线被窃听，通常很容易听见重复的喀喇声，或是手机里能听见不规则的干扰噪音。但现在，更多的窃听都是通过隐藏的App进行的，更像是电脑黑客而不是传统的电话窃听。不管怎样，正常的电话窃听也在继续的被广泛使用，鉴于此，有一些事项是我们需要注意的。

通常来说，如果你的电话线被监听了，它会发出一些噪音，因为这条线被别的窃听者分接了。如果你小时候的家里是那种一条电话线被分接了好几个电话的情况，你会知道如果你在通话时，如果家里其他的人拿起另一个电话，你会很明显听到电话里噪音背景的改变。

所以，要了解自己的电话是否有被窃听，应该要注意在你打电话给固定的某个人时里面的正常噪音是怎样的。如果你发现噪音的类型有变，这样就需要引起注意了。不管怎样，打电话给不同的人 and 地点都会有些许不同的噪音，所以你得用一个特定的人和电话来试，看看是否发现什么变化，典型的声响有：

- 重复地喀喇声
- 稳定的噪音干扰
- 尖锐的嗡嗡声



测试的时候确保不要靠近其他电子设备（比如电视、路由器、电脑等），否则可能会有干扰。

如果你的电话是通过手机App或后台进程被窃听，而不是通过电话线的分接，你可以通过以下的这些特点来分辨：

- 随机的短消息，包括随机的字符和数字等（监听软件内不小心流出消息的bug，本来这些消息是用于控制你的手机）
- 大量的电池消耗
- 突然跳出广告
- 手机用起来慢、卡和不稳定
- 流量使用增多
- 手机过热

## 本章要点

- 留意手机中存在的各种威胁类型
- 限制安装App的数量
- 浏览手机的设置区域，查看预安装的程序，移除所有你不需要的程序
- 如果你感到身处危险，不要使用手机，不要带手机，不要开机
- 不要将手机当成一个工作电脑，它只是一个通讯设备
- 避免中国公司的应用程序和服务
- 将Google (或DuckGoGo)当作朋友 — 任何在手机设置区域或预安装的应用程序中，有不明白的都可以问Google

## 第9章

# 手机的使用



这个章节会介绍手机使用习惯的重要性。你会发现使用手机的方式比提供技术化解决方案对你的安全来说更重要。

## 手机不是什么

跟电脑不一样，手机无法有效的保障里面的东西。尽管你已经加密过（现在大部分的手机都是自动加密的），但也没有比这更高端的方法了。手机中很少有几层的安全密码进入到手机的各个部分。要保障手机安全，问题不在于丢失手机，而在于你被警方带走后强迫你交出手机的界面密码，接下来，你的手机就失去了保障。

由于手机缺乏多层保护，加上经常性的使用App连接服务，而不是使用浏览器（也无法彻底清除手机上网痕迹），如果你被迫交出手机密码，他们就不仅仅是能进入你的手机，而是手机内所安装的所有App服务(比如邮箱)，以及那些近期使用浏览器上网遗留的内容。他们可以用你的手机作为后门。不要让他们用手机威胁你的安全，也就是不要将手机当成你的工作电脑。

## “与电脑不一样，没有任何有效的方式可以保障手机内的信息安全”

总的来说就是不要将手机当作后备工作电脑，绝不存储任何工作文件，或当作文件转移的工具，也绝不要用手机进入任何你已经在电脑中使用的工作服务。



## 手机可以是什么

尽管上面说了这么多，加上在前一章有提到的，你的手机可以是非常高效安全的通讯工具。关键是手机只需要用于这个目的，而不是任何其他的功能。另外以促进达成这个目的的步骤是为通讯安装安全的App，这类App能自动销毁会话，能防止外人进入你的手机后从早期会话获得不利资讯。端到端的加密聊天程序结合自动销毁聊天记录是一个强大而又效率的通讯工具。

## 中断通讯 GOING DARK

中断通讯，英文的IT术语叫Going dark，意思是将手机任何类型的数据传输都切掉，这是唯一能确保手机不会对你造成不利的方式。如果你正在进行一个会议，要确保没有被监听，这也是唯一的解决办法。同样的如果你不希望被摄像头偷偷记录，或是被人知道你的地理位置，都应该让手机“中断通讯”。中断的方法有几种，最简单的方式就是开启飞行模式。一旦开启，手机就会停止发送网络传输（手机向信号塔发送电波的过程），Wi-Fi传输，还有蓝牙。不管是否将手机接收GPS信号的功能关闭，只要其他形式的传输被关闭，你就是安全的。因为智能手机只接收GPS数据，并不会发送。

上面提到的方法有一个弱点，那就是在你不知道的情况下手机内某个App的数据传输被启用（只要你的手机被列为目标就能被暗中启用）。另一个是只要GPS为启用状态，所有的地理位置都会被记录下来，一旦关闭飞行模式，地理位置数据就能通过这个App发送出去。

另一个中断通讯的方式是一个非常简单的习惯，就是用铝锡箔纸。很多在敏感领域工作的人在有风险时都会带上几包铝锡箔纸。用两层纸将手机的每个部位包住，就能将传输切断。这是中断通讯的最好办法。现在网上也有卖特殊的小型手机袋，内部就是由铝锡箔纸制成的，也能起到同样的作用，并且不会太引人注目。我们希望你能试试，将手机用两层铝锡箔包起来，再试着打电话、发信息或邮件，看看是否能收到。如果能，再试着加一层，不过通常都不太可能。总之，如果你打算采用这个方式，就算只是备不时之需，也记得在使用之前先测试一下。

## 自动同步和云存储

另一个严重的手机安全威胁是很多的服务都会自动登录。这些App通常和在浏览器上的服务相比来说都只有比较简单的界面。但是，进入服务通常都是不需要输入密码的。只要进入到你的手机就表示进入了里面安装的所有服务，千万别低估它的威胁。所以，绝不要安装一般通过电脑中的工作浏览器进入服务的App程序，尽管它确实很方便。

也不要在工作电脑和手机上同时使用云存储服务或其他线上服务，使用分开的账户和服务。比方说你坚持要用云存储，那就在工作的电脑用Google drive，在手机里使用另外的如Dropbox或OneDrive存储。保持你的工作电脑和手机使用的服务分开。

因此安全的关键是限制手机的使用方式，将手机看作是一个单纯的通讯设备，除了通讯外不用于任何其他目的。不要用手机搜集资料、不要用手机下载文件、或存储工作文件。

## “将工作电脑和手机上使用的服务分开”

飞行模式也会开启NFC，在安卓上有时候叫Beam，这是一个短距离传输系统，也就是如果你将两个手机放在一起，它们之间就能互相传输数据。

### 预先三步设置保障手机安全

在我们继续下面两个章节，手机设置和安装使用安全的App，你需要先进行三个步骤的操作。

#### 第一步：出厂设置

除非你完全了解手机里的东西，也对目前手机的安全性非常的有信心，否则你需要进行出厂设置 (ANDROID·86+iOS·87)。这个步骤会让你丢掉手机内的所有资料，所以在操作之前进行要保留的文档和图片备份。

#### 第二步：加密

有可能在你购买手机的时候就已经是加密的了，但如果你使用的是安卓手机，那就很有可能并没有。手机和里面的SD卡都很容易被加密。在出厂设置后，第

#### ANDROID · 86



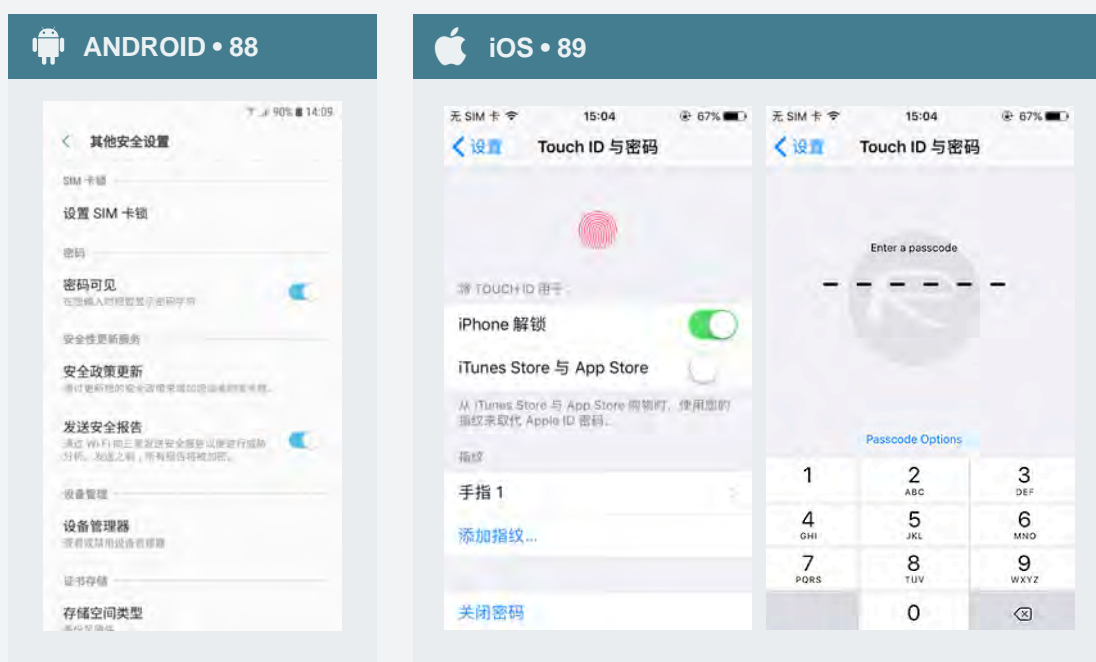
#### iOS · 87



一件事情就是开启加密功能，设置一个合适的密码，如果有SD卡在内的话也需要同样的操作。(ANDROID·88)

iOS的加密是自动的，一旦你在设置区域的Touch ID和密码的部分设置了密码后 (iOS·89)，整个设备的加密功能就已经自动启动了。

对安卓手机来说，你只需要到设置区域的安全下，点击加密设备，它就会需要输入一个密码然后开启程序。没有任何数据会被删除。如果你的手机使用外部的SD卡，也可以选择加密，但应该在加密了手机设备后再加密SD卡。



### 第三步：移除/卸载

在出厂设置和加密都完成后，浏览一遍手机内安装的所有App和服务，卸载和禁用那些不会使用的App和服务。有些手机甚至在出厂设置后都还是会有自带的App，移除它们，这会提升你的安全性，手机的反应会相应的更快速，也能让电池续航力更强。



## 一部手机是如何几乎毁掉一切的

这个故事背后的人既不是律师也不是记者，也没有长居北京、上海这一类的维权中心。相反，他居住在中国东部一个比较贫穷省份省会下的二级城镇，他也没有上过大学，连高中都没有毕业。不过，他虽缺少文凭，但却有十足的实践经验。十多年间在他自己的社区马不停蹄的帮助被当地政府违法行为所侵害的受害人，渐渐的他的声誉不仅在当地甚至在别处也越来越高。

虽然来自一个小地方，但在现代中国，他也要使用邮箱、电脑等方式去学习中国的法律，学习帮助那些他正在帮助的客户的方法，他的手机就是他主要的神经中枢，最有效率的组织援助的方式。通常，一旦有某个农民因为自己的土地被低的荒谬的赔偿金征走时，他会组织其他的农民和受害者一起支援。无数次他联系的很多人没有出现，有的在即将离家的时候被警方拦下，有的在来的路上消失了，过了几天才出现，在经历了“行政拘留”几天之后。他很快就明白一定是他发给他人的消息被第三方读取了，然后采取了拦截的行动。

他一步步的自学法律，也开始学习如何安全的通讯，尽可能的与他人分享他的建议、知识和意见。尽管有时候他被警察堵在家里被“喝茶”，有两次他被短暂的关进了“行政拘留”，作为一个小地方的活跃人士，似乎并没有什么更大的打击足以让他害怕的。

直到2015年下半年，他在家被两位当地与他有过多次接触的警察带走。抵达当地派出所时，见到一群从省里来的警察，接着他被带去了省会，他才意识到这次遇到了大麻烦。他意识到他已经踩到红线了，他的手机很快被没收，没多久他知道了自己的电脑、相机和其他的设备也被他们从家里搜走了。

他的手机落在了警方的手上并没有让他特别担心。大部分的聊天记录都设置了自动销毁，有几个聊天窗口也许能看到他有介绍过几个人参加几个活动，但是大部分也只是地址和短暂的聊天记录。仅仅是那几个聊天，很难说他是在鼓动他人，想到这里，他也就松了口气。

他和很多其他的活跃人士一样，心里暗自发誓过绝不归罪于他人，也就是说他绝不会将他所用邮箱的密码交出去。他用的是被国内封锁的Gmail邮箱服务，被公认的有很强大的安全保障系数，每次他都需要用VPN才能从手机或电脑中登录。这样一来他人能进入邮箱的机会就小了很多。

但最后，所有的功夫都是白费。警方并没有将他列为最主要的打击对象，只觉得他是个麻烦，所以他们也不会投入大量的资源攻破他的Gmail邮箱。不过，到最后他们根本不需要这样做，因为他在手机里装了Gmail的App，当警方拿到他的手机时，他们就已经直接看到了他的Gmail，虽然在App上并不能查看密码

和更改设置，但是所有之前已读的邮件都在那儿，他们只需要浏览那些之前的信息，然后就能呈现一个令人信服的专业煽动者的画面。另外他也有允许手机内的地理位置分享，日常微信通讯互动中很重要的功能，也意味着他拍的所有照片，通常是来自会议或公共纠纷中，这样相当于是给警方提供了这些会议的地址信息，因为照片都包含了元数据。

还好他有遵照一个邮箱策略，定期删除早期邮件，因为他总将这些邮件可能伤害到自己或他人这件事放在心上。如此一来，只有非常有限的“证据”，警方在给了他15天的行政拘留后放了他。虽然他逃过了正式的逮捕，但是警方很清楚的警告他已经越界了，下一次再次踩线就不会这么幸运了。

最后，也就是说，要输入长长的密码和用VPN连接才能进入的邮箱，如果是在手机内提供了一个直接进入的后门，那前者的一切都没有了价值。

这个错误他以后应该是不会再患了。

# 第10章 手机设置





本章节与第2章的电脑设置一样，介绍如何设置以便于更好的掌控手机安全。与电脑一样，了解这些设置，作出相应的更改是非常重要的步骤，也是保障手机安全的第一步。只有在最基础的第一步设置完成后，后面介绍的程序和软件才有可能保障你的手机安全。

现在我们已经准备好进行手机设置这一步了，为手机做一些必要的更改能带来基本的安全保障。因为各个品牌的安卓手机在设置区域的菜单显示方式都不尽相同，不过都几乎是用差不多的文字表述，所以我们会提供文字表述方便你在手机的设置区域找到并设置，而不是提供每一步的手机截屏，因为不一定与你们每个人的手机步骤一模一样。这样刚好也能让你熟悉一下手机设置区域的目录。

鉴于手机内的系统版本也不尽相同，如果以下的步骤介绍与你的手机操作不符，可使用DuckGoGo或Google搜索与你的手机版本相符的设置步骤。

## 设置与APP许可

我们会一步步教你设置iOS和安卓手机，如果在安卓手机有一个Google设置区域，我们也会教你如何设置。

设置手机和App的功能权限最容易的方式是进入设置下的应用程序，点击每一个App，查看那个App有哪些权限，比方说允许连接你的日历，地理位置等等（ANDROID·90+iOS·91）。很多手机还有另一个查看服务的设置区域，比方说地理位置、麦克风等等，看看有哪些App是允许使用这项服务的。（ANDROID·92+iOS·93）



三星：设置 > 应用程序 > 选择App > 点击权限

安卓：设置 > 应用程序 > 权限 > 选择权限类别



现在的App通常都是最大化的访问你的手机，尽管很多都没有必要，有时候一个App甚至根本用不到这个被允许的访问。因此很有必要花一点时间设置手机里的这两个区域，查看所允许访问的都是哪些功能，这是最好的方式彻底掌控App在手机中的所做作为。

这意味着你有两个选择，可以完全将一个服务关闭，比如地理位置，或是可以允许这个服务，但是设置尽量少的App能用到这个功能。将一个服务彻底的关闭总是最好的办法，但是可能有时候也会带来一些不便利。如果你的某一个服务是开启状态，确保查看（如上）哪些App是被允许访问的，每安装一个新的App都惯例性的查看权限。

地理位置，摄像头和麦克风 这三个是需要多加注意的关键服务。其他需要控制访问权限的服务类型包括读取/发送短信，进入存储，日历，联系人名单，读取/发送邮件等等。

在不需要使用连接服务时都应该将它们关闭。除了Wi-Fi，手机也提供蓝牙，NFC，Android Beam。只要在不需要使用的时候都保持关闭。这些都是短时间的网络连接选项，没有必要长期开启。

**三星：** 设置 > 连接 > 蓝牙 + NFC和支付 + 手机可见性都设为关闭

**安卓：** 设置 > 蓝牙 > 无线网络 > 更多...

**iOS：** 设置 > 蓝牙

什么可以安装？在锁定屏幕与安全选项下就能找到是否允许未知来源的设置，应该设置为不允许。这样就能拒绝任何无法被官方手机商店识别的安装，如果你需要安装某个特殊程序，可以短暂的允许后下载你的程序，然后再次设置为不允许。iOS手机则不需要担心这个问题，因为只有苹果商店的程序才被允许安装。

**三星：** 设置 > 锁定屏幕与安全 > 位置来源（选择关闭）

**安卓：** 设置 > 安全

## 通知，锁屏，自动锁定和自动销毁

如果要防止外人读取你手机内的信息和会话，设置手机屏幕密码是关键。大部分的手机自动设置为在锁屏状态下显示全部的通知消息，也就是在锁屏状态下不需要进入手机就能读取刚收到的信息和邮件等。这一点需要做出改变。和上面一样，你可以设置为隐藏所有的通知，或是设置允许，但是在设置下允许或禁止每个单独的App，当然，不要将你的工作相关服务设置为允许在锁屏上显示通知。



**三星：**设置 > 锁定屏幕与安全 > 通知 > 锁定屏幕上的内容（选择隐藏内容或不显示通知）

**安卓：**设置 > 提示音和通知 > 设备锁定时（选择隐藏敏感通知内容）

**iOS：**设置 > 通知 或 设置 > 控制中心

你也可以在手机内设置什么App被允许发送通知（收到提示，不是指显示在锁定屏幕上）。可能有的App你完全不希望收到通知，而只希望手动查看。

**三星：**设置 > 通知

**安卓：**设置 > 提示音和通知 > 应用通知 > 点击不同的App选择屏蔽或优先

**iOS：**设置 > 通知

解决锁定屏幕的部分时，确保有开启自动锁定屏幕的功能，将时间设置为类似5秒、10秒或15秒之类的短时间内上锁。如果可能也请开启开关机键的快速锁屏，一旦你按住开关机键，屏幕就会马上被锁住。最后，开启自动出厂设置，这最后一步意味着如果有人用一个错误的密码尝试进入你的手机，密码连续输错10–15次，手机就会自动重置。

**三星：**设置 > 锁定屏幕与安全 > 安全锁定设置 > 自动锁定

**安卓：**设置 > 安全

**iOS：**Touch ID 与密码

在启用加密功能的时候你已经设置了一个密码，但是如果因为不明原因没有在锁屏时启用密码，确保将它开启。另外，如果你的手机或平板允许指纹、声音、脸部或眼睛识别功能用于解锁，请关闭这些功能。

## 自动更新

和电脑一样，手机只有在最后更新状态下才最安全，确保有开启手机的自动更新功能。

**三星：**设置 > 系统更新 > 开启自动下载更新

**安卓：**设置 > 关于手机

**iOS：**设置 > iTunes Store与App Store > 更新（开启）

## 同步和云存储

找出手机内已安装的云服务，应该会显示在设置区域下，做一些必要的设置。确保任何云服务都已经设置为关闭，也不包括任何工作相关的内容。如果你要用云服务用作基础的存储或备份，请参考第6章：分享信息，然后选用最好的使用方式和最适合的服务。

## 最后几项手机设置

避免安卓和苹果手机基于你个人兴趣的广告追踪，需要设置为关闭。

**三星：** 设置 > Google > 广告 > 选择停用广告个性化功能

**安卓：** Google设置 > 广告 > 选择停用广告个性化功能

**iOS：** 设置 > 隐私 > 广告 > 限制广告跟踪

为了安全起见，也应该将声控指令关闭（如OK Google, Cortana, Siri等），或者至少确保在锁屏时不能使用。

最后，如果你用的是带Google设置的安卓手机，浏览手机设置区域，查看每一项设置是否正确，有哪些App和设备是连接到你的账户的，关闭密码的智能锁屏，其他的功能也视情况相应作一些改变。

iOS系统中，为避免你的隐私数据、密码和信用卡信息等被同步或存储在iCloud上，应该做出此设置：设置 > iCloud > 钥匙串（设置为关闭）。

## 本章要点

- 确保新的消息、邮件等不能在锁屏时直接读取
- 确保你完全掌握并了解了App和其他功能在何时何地可以接入你的地理位置
- 确保照相机从不连接你的地理位置
- 再次查看手机内不同的程序允许了哪些服务，根据情况作出改变



## 关于地理位置追踪的提醒

要知道如果你非常迫切的希望躲避追踪，要是已经被警察、安全局的人跟在后面，单单让手机“切断通讯”是解决不了问题的。你的车会自动被一路上的安全摄像头记录下每一个动向，另外你使用的银行储蓄卡或信用卡，任何用你的名字注册的卡，都能被当作地理位置追踪的入口。朋友发布的你的照片也能给出拍照的时间和地理位置，这些都很容易被自动分析识别出，所以只要是有人想要追踪你的位置，这些资讯就够了。

长时间的“切断通讯”几乎是不太可能的，甚至是短期的也非常困难，除非你准备好了大量的现金和交通工具等等。现在大型商场的普通安全摄像头都能快速的识别出脸部的轮廓，所以千万别小看这些科技能做到的事情。

手机是通过独有的识别码来辨认的，一个来自手机硬盘本身的，另一个来自SIM卡。这个码叫做IMEI (手机) 和IMSI (SIM卡)。这些号码是由手机塔和手机服务商注册的，比如中国电信。你无法隐藏或改变这些独有的识别码，如果你的手机号码已经被人掌握，那他们就很有可能至少知道了你的IMSI码，如果你的手机被没收，他们就能知道你的IMEI码并找到你存储的数据。这样，你在过去很长的一段时期拨过的号码、去过的地方、数据的使用等等都能被找出来。再次强调，手机是一个很大的威胁，不应该用于工作目的。

也就是说，如果已经成为了被跟踪的目标，上面提到的多种方法都能被采用为进行追踪的方法，所以绝不要让自己陷入被追踪的情形，工作很重要，但是你的安全必须放在首位。



# 第11章

## 可用的安全APP



本章节会介绍一些能够满足日常需求又更加安全便捷的应用程序。教你用提供端对端加密功能的短信管理程序取代一般的短信收发。我们也会介绍如何轻易地用Tor 畅通的浏览网页，还有不仅发起秘密聊天并且还能自动销毁会话记录的聊天软件。

当下载一个App时，先到它的设置区域，熟悉这个App允许更改的设置。一些安全性能高的App，比如Signal和Telegram，自带的有密码保护功能。也就是说这些App允许你单独为进入这个App设置一个密码，对Telegram和Signal来说，这是必须的。很多其他的App并没有这个功能。这个功能的益处是就算你的手机被人掌控了，但他们并不能进入这些自带密码保护的App，因此有更多一层的安全保障。

## 短信和通话



下载Signal Private Messenger，这是一个可以同时取代短信和手机通话的软件。当用Signal发送短信或拨打电话时，就会自动开启端对端加密功能，以保障手机的短信和通话不被监听。

它有一个内置的密码保护，开启后就能用一个特定的密码连接Signal（设置 > 隐私）。在Wi-Fi环境下能像普通短信一样运行（但不是发送SMS短信，而是经由Wi-Fi，这样也可以节省话费）。（设置 > 短信和彩信 > 启用Wifi呼叫）。最后，进入设置内的聊天与媒体，开启删除旧信息并设置限制量（比如设置对话数量限制为10条时自动删除旧的信息等）

当打开一个聊天窗口，点击右上角就能看见一个销毁信息的选项，点击并选择一个时间。这样所有发出和收到的短信都能在所设置的时间内自动删除（在已经被读过后）。

要使用聊天、短信和通话的“端到端”加密，你和聊天对象都必须安装Signal。确保你安装了，也让你的朋友、同事和伙伴都这样做。就算ISMI捕捉器将你手机正常的信号加密移除了，你也会保持安全，因为这个程序是使用它自己的“端到端”加密的。

## 聊天



除了**Signal**应用程序之外，我们还推荐安装Telegram（电报）。电报可以像一个正常的聊天程序运行（但有加密功能），并且有附加的加密聊天功能。如果使用加密聊天，消息就会进行端到端加密，也可以设置一个将所有收发的消息自动销毁的时间限制。

就像前面有提到过的，聊天记录的自动销毁是保障安全的关键，甚至比一些更高阶的加密都要重要，因为这样就不会遗留下任何痕迹和信息便于他人发现后用于对你不利，和Signal一样，电报也有内置的密码保护，可以自己设置一个特别的密码用于打开电报。

## 上网, TOR 和VPN

在安卓系统上浏览网页最安全的方式是使用Orbot或OrFox的应用程序。



**Orbot**是安卓系统的Tor，相当于为手机装上Tor的一个App。这样你可以在设置区域选择哪一个App要通过Tor打开（意思是哪一个App需要通过Tor连接来打开），可以选择所有你需要的App，设置后使用任何浏览器和上网都会通过Tor连接。



**OrFox**是另一个App，一个专门为了使用Orbot和Tor而创建的程序，如果开启了OrFox，浏览器就能自动通过Tor连接，不需要再做任何其他的设置。在这个情况下，只有OrFox浏览器是设置使用Tor的，其他的连接仍然是正常的。如果使用OrFox，在开始进入任何网页之前，先到设置区域选择隐私，然后点击退出时清除隐私数据，勾选所有的数据形式，这样在关闭App时就能清除所有的浏览痕迹了。

如果你要用其他的浏览器上网，请千万不要使用手机内置浏览器。记得卸载掉，要是不能卸载的话就禁用，下载那些比较靠谱的浏览器，比如Opera, Chrome或Firefox（火狐）。跟电脑的操作一样，确保有进入浏览器的设置区域禁用自动填充表单等，是否禁用保存密码则取决于你是否有严格遵守不用手机登录工作相关的账户的忠告，如果仅用于私人，比如淘宝等用于私人的账户，可以不禁用保存密码。另外也记得启用禁止跟踪，在结束浏览器的使用后记得要去清除数据。

再次强调，不要使用手机或手机浏览器连接工作相关服务，比如邮件，云存储等等。千万不要，只要通过手机连接过，数据就无法从手机内完全的清除掉。



截止到这本手册面世，在中国大陆还没有用于iOS系统的Tor浏览器或App。打开App store查找Tor App，通常都有特别强调目前是如何的无法在中国大陆使用。

手机和平板上的VPN与在电脑上的运行一样，如果你有一个付费的账号，通常VPN还会有一个手机客户端让你能更方便的连接使用VPN。

## 元数据

如在前面元数据章节里提到的，此类问题通常在手机上更糟糕，因为拍下的照片会包括地理位置，自动从联系人内获取名字标记在照片上等。所以不管你使用安卓还是iOS，在用手机拍照后上传到网上（社交媒体等），转移到电脑存档等等，都需要考虑到这一点。在手机内的元数据程序中通常会使用术语Exif或Exif 数据（可交换图像文件格式）。

如果将照片转移到电脑，可以用电脑和我们有教过的方法清除元数据。如果是要直接从手机直接发布的话，那你需要安装一个元数据清除程序。

安卓系统我们推荐Exif Eraser 或Metadata remover。这两个都很容易使用，当然也有其他的很多可选的程序。iOS系统我们推荐Photo Investigator 或 Metapho，你可以安装一个试试，试着了解怎么使用，如果不确定则可以再换另一个程序，直到你感到完全熟练。几乎所有的程序都有介绍使用步骤。

## 其他APP

The Guardian Project公司不仅提供简易的供安卓使用的Tor浏览器（上面提到过的Orbot），也出品一些其他的安全App。



其中一个**ChatSecure**，一个安卓和iOS系统都适用的管理和使用聊天客户端程序。用Chatsecure意味着有了强大的加密功能，比如用GoogleTalk。可以设置为自动通过Tor连接。也就是在这个账户下的所有会话都是通过Tor连接。你可以为程序设置打开保护密码，也可以设置自动删除信息。



另一个来自Guardian Project的App是 **ObscuraCam**. 这是一个能够将照片里的脸部模糊化的照片App，里面的人是无法被系统识别的。他们也还有一些其他的App，可以去他们的网站上看看。



如果想要了解你的手机在使用哪一个信号塔（基站或BTS），在手机可能被转移到IMSI捕捉器信号时收到警告，安卓手机可以使用**AIMSICD**（iOS无法使用）。这个程序只有英文版本，目前还没有中文版，可以在以下网页下载程序：

<https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/releases> 

需要手动安装，先去设置区域改为允许未知来源，在下载完成后回到设置区域改回不允许未知来源。这个程序会提供你的手机所连接的基站信息，一旦手机被接入IMSI捕捉器就会发出警告。同时也有一个地图功能描出在你周围的基站图。



AppLock到目前为止也是一个仅提供英文版本的程序，但中文的同类型程序应该也是有的。如果语言没有问题，还是建议使用AppLock，因为它是被证实过的安全程序。这是个能让你为App建立密码的程序，选择任何你要设置密码的App，就算App没有自带的密码保护，你也可以为你要保护的App设置一个进入密码。这个程序本身是隐藏的，其他人并不会轻易知道你在使用它。它仅允许设置一个密码（或图形），所以你选择的所有App都会使用同一个密码进入。

在下载AppLock后 (ANDROID·94)，会被要求再安装一个比 AppLock提供更多选项的支援程序，叫做高级 系统保护 (Advanced System Protection)。安装后就能为AppLock建立一个密码，程序 仍然是隐藏的，这样没有密码的人是无法卸载 这个软件的。

安装后，浏览界面看这个App有些什么功能。这个App有两个标签，Privacy (隐私) 和 Protect (保护)。隐私标签是你可以选择要保护的App程序，保护标签相当于设置，比如设置密码的形式，要PIN还是图形，是否要隐藏AppLock（当然要隐藏）。如果你选择了隐藏AppLock，在以后开启这个App时就需要打开拨号盘（打电话时的那个拨号盘），键入#1234后拨号，这样App就能启动了。如果高级保护没有被自动安装，则需要在Protect标签下启用Advanced Protection。



针对苹果手机系统，在苹果商店有类似的App，如Locker Lite等，取决于你的语言要求。

## 结合电脑的使用

如我们一再提到的，将电脑和手机分开使用非常重要。建议不要在电脑上使用基于手机的应用。比如Telegram (电报)有一个专供Windows电脑使用的App，从这个电脑客户端也可以直接使用这个聊天软件。不过电脑版本并不支持加密聊天，也没有密码保护。同样的，其他的一些App程序可能也有支持电脑版本，但是建议你不要去使用它。也有一些专门的电脑程序可以读取、发送和管理短信，同样也建议你避免使用。

只有一个例外，那就是Signal，在Win10和OSX系统都能使用，保留了自动销毁聊天记录的功能，甚至在群聊中也有这个功能。不过需要在手机端先开启一个聊天或群聊，设置为自动销毁记录，这个步骤无法在电脑中开启，一旦用手机开启后，就能在电脑上聊天和控制了。

## 如果...怎么办？

尽管你已经很清楚保障手机安全的困难性，但难免可能需要用到手机浏览器搜索资料，用浏览器登录邮箱或账户，或是用手机储存文件和数据的时候，请作出以下的预防。只要使用浏览器都确保有先进入浏览器的设置区域，保证密码没有被保存，所有的表单自动填充功能都为不允许，在使用结束后，浏览器设置里选择“清除数据”。

如果不小心在手机里存储了任何文件或数据，安装一个空闲空间擦除程序，在移除或删除了文件和数据后运行这个程序。通常这个方法不像在电脑中那样有效，但至少是简易文件恢复无法轻易找到的。针对安卓手机我们推荐Secure Eraser，苹果推荐iShredder（仅限英文版）。也有其他的类似App可选。如果你的手机有SD卡，则需要确保在SD卡和手机的内部硬盘都运行了“擦除空闲空间”程序。

### 本章要点：

- 在通过手机发布照片或其他文件时，确保你了解了它包含的元数据都有哪些
- 确保你的安全聊天软件有设置为自动清除聊天记录，如果你没有使用自动销毁的功能，则确保在聊天结束后手动清除聊天记录
- 设置Signal为手机默认的短信程序，使用Signal发短信和打电话



## 工作日常流程

在平常的工作日，以安全的习惯保障你避免受到未来可能面临的打击，需要注意以下推荐的工作流程。

准备开始工作时，先打开昨天晚上被完全的关机了（而不是让电脑休眠）的电脑。连接上VPN了才算是开启一天的工作了。开始浏览一些工作相关资讯，查看和回复邮件等等。任何工作相关的搜索都要保证用的是你做过安全设置后的工作专用浏览器。

最好是用DuckDuckGo.com作为你的工作搜索引擎，或是用Google，但不要在浏览器中登录进你的Google账号或Gmail。

在开始做文档相关的工作时，或是从邮件或浏览器中下载文件时，需要载入你的加密硬盘（隐藏内部加密卷）。最好是将文档存入USB，但也可以存入硬盘的分区或文件夹。只有要载入了加密硬盘后才开始下载（或创建新的）任何文件。任何下载或新建的文件都应该直接的存入这个硬盘，而不是存入桌面或任何其他临时的下载文件夹。

如果你要短暂的离开电脑时，第一件事是卸载加密硬盘，然后将电脑锁屏。如果是长时间的离开电脑，则需要关机。

如果你正在进行一项尤其敏感的项目，比如你需要发送一次性邮件沟通或尽可能隐藏IP和地理位置的搜索，则开启TOR，而不是VPN。在进入TOR浏览器后，可以用它登录你的匿名邮箱或其他服务。一旦这些需要特别安全和隐匿的工作完成后，则可以关闭掉TOR，重新开启VPN。因为TOR的运行特别的缓慢，只在需要进入匿名邮箱、敏感信息浏览这种安全大于速度的情况下才使用。

一天下来，任何创建的PDF、PPT，要分享出去的Word文档，或是在文档中用到的或要传上网的照片，都要确保已经移除了元数据。或者至少要弄清楚这个文件包含什么样的元数据，确保清楚知道分享了哪些数据出去，大部分情况下，为简单起见，直接移除元数据。

在使用手机的时候，处理基本的聊天，消息和短信用Signal或Telegram，这两个软件都有加密聊天和自动销毁消息的功能，所以你会话的内容和记录都不会被保留。

如果在一天的工作中建立了很多的文档，特别是一些比较小的文档，你需要决定它们是否还有必要保留，还是可以将它们整理到一个大的文档。如果很重



要，依然需要保留，要么将它们整合成少数的文档，或是在你的加密硬盘内按照你愿意的方式去整理。绝不要在一天的工作结束时桌面上留下任何文档或是文件夹。

一天的工作结束时，进入你的工作邮箱，除非是有特别的某个重要的邮件信息需要保留，确保你的收件箱、发件箱和垃圾箱为零，这样如果有人擅自进入你的邮箱也并不能找到任何遗留的信息。同样地，也要确保当天的所有文档和文件都已经存储在正确的（隐藏加密空间）地方，确保手动清除手机内没有被设置为自动销毁的聊天记录。

最后，在关闭浏览器以及卸载加密硬盘空间后，运行CCleaner，这样当天的上网活动痕迹都会被清除了。

如果已经有一段时间没有擦除电脑空闲空间了，或是在这期间你有一些特别敏感的上网活动，或是你正处于高级别的安全威胁中，可以将电脑放着擦除空闲空间一整晚，离开电脑时要锁屏。重申，如果你要操作这一步，一定要确保有锁屏电脑、加密盘是处于未加载的状态、如果加密硬盘在USB则要确保USB有从电脑中移除了。

## 本章要点

- 不要在私人浏览器上做工作相关的事
- 不要在没有连接VPN或TOR的情形下处理工作
- 不要在手机内下载工作文件
- 不要在加密硬盘以外的空间内保存或建立文档
- 不要忘了在关闭电脑时运行CCleaner

# 第四部分 预防性安全





## 第12章

# 预防性保护



如果你正在读这篇内容，意味着你目前或未来可能会面临个人安全和自由的威胁，无论几率大小，最好都不要忽视潜在的危险。请阅读以下的要点，大概在15分钟阅读以内，请执行下列建议的操作，这些操作会对你未来的安全起到重要的作用。

你可以根据我们提供的清单，建立一个文档，将所有需要的内容都包括进去，以及任何你希望提供的信息。

在开始写下来之前，需要分析你的个人情况，什么样的协助是你需要的，你是否将面临麻烦，基于这些，请阅读以下三个重点问题。

## 第一步：你可能面临的威胁是什么？

描述出你可能会面临的潜在威胁，威胁你的人是基于何种目的？假设你是一个记者，是否有可能因为报道一个事件而导致短期的拘留？或将资料没收并追踪到你的消息来源？或更严重的逮捕或指控令你无法继续工作？

不同的威胁类型需要不同的准备工作。你所做的哪一类行为或和哪一位一起工作可能提高你的风险？你是否有报导过关于当地政府的腐败？

一旦你清楚自己的行为可能招致的报复，这样就便于识别可能性的报复来源了。

你是否清楚谁最有可能是加害者（当地政府？警察？国安？）。你是否知道如果被采取对你不利的行动，可能会用什么方式和何种指控？请列出这些问题的答案，越全面越好，这样才能便于在有需要的情况下提供迅速的援助。

## 第二步：你需要什么样的援助？

基于上面各种问题，你已经分析了自身的安全状况，你认为到时候什么样的援助是你会需要的？在达到某种事态下你是否认为受到国际媒体的关注是必要的？如果是，以什么方式？（比如一旦被拘留，你是否认为只有在超过一周之后再让国际社会发声为好，还是也许你只希望国内的社交媒体关注，或不需要媒体关注而是更愿意得到低调的外交或联合国的援助？明白这些不同的交涉在不同的情况下有不同的作用很重要，你应该与你信任的同事聊聊你的选择，因为他们可能会成为帮你说话的人）。除此之外，有其他形式的援助需求吗？

你是否有家人依赖于你的经济来源？当你被拘留或强迫失踪的情况下会需要到一些援助的？什么样的援助？经济、医药、学费或租房等？

另外，如果被拘留，甚至更糟的状况，你是否需要法律援助？是否有任何具体的法律需求？

在什么情况下你可能会放弃指派自己的律师的权利？你是否已经有了在你需要的时候可以帮你辩护的律师？如果有的话，他/她是谁？我们如何联系到他/她？他是否已经有了你的委托书？

如果这些考量你都已经有了答案，你应该写一个无论如何都要自己指派律师的说明（或视频），明确的列出在任何情况下，你都不会接受一个官派律师，并且将这份说明交给不止一个你信任的朋友或同事。

## 第三步：指派一个信任的、安全的（不那么有风险）联络人

你的安全（紧急）联络人会将你提供的这些信息保存，在有事发生的时候将它们分享相关的人。在此提到的所有这些材料都会交给这个安全联络人，这个人联络人应该要知道在出事时他应该怎么做。

指派一个在有需要的时候能够签署律师委托书的家庭成员。在选择之前先想一想，因为有很多的家人在事发后一开始都很迟疑，他们不知道在这种情形下该如何去应对，而且有时候警方也会骚扰或拘留当事人的家人以作报复和威胁，所以确保在选择家庭成员前先商量，让他明白可能面临的风险。最好选一个理解你的工作的家人，告诉他你已经选了他，一旦有事发生，让他不要迟疑的签署委托书。将你的安全联络人和这个可以签委托书的家人的联系方式互相交换，让他们彼此知道对方。

以下是一个清单和说明，可以作为准备所有资料的指南。



清单：

- 个人简介
- 详述你自己和你的工作，尽量包括可能招致打击报复的主要活动的具体日期，这点尤其能检定警方对你采取的措施是来自对你的人权工作的报复手段，这对于外界对你个人的协助作用很大，不应该被轻视。
- 已经承诺提供法律援助的指派律师联系信息（最好是写一个介绍）
- 安全（紧急）联络人的联系信息（最好是写一个介绍）
- 已指派的签署委托书的家庭成员联系信息（最好是写一个介绍）
- 任何相关朋友和家人的联系方式（最好是写一个介绍）
- 任何你认识的记者和外交官以及其他你觉得会参与援助的人的联系信息（最好是写一个介绍）
- 一篇有联系方式的相关同事或工作机构的概述（这一条可能会带来额外的预防保护以及威胁识别）
- 准备几张在公众或媒体声援需要时可以采用的照片，你将有在媒体上的形象主控权。

## 预备材料

预备材料是在万一你被拘留或逮捕的情况下会公布的东西，也要提前特别说明这些材料你希望以什么形式/什么时候/如何公开。请参考如下范例，录制几个短视频应该会很有帮助。

要准备哪些预备材料完全取决于你自己，要基于你的工作和你预想中可能面临的威胁而定，比如：

- 近日被强迫认罪现象变得越来越流行，桂民海，一个瑞典籍公民，在泰国被劫持到中国，在他的被迫认罪视频中被要求说他不希望得到瑞典政府的任何外交协助，以及他希望放弃自己的瑞典国籍。假如他预先录好一个视频，强调如果他出现在中国都是因为他被国际绑架（他并没有去中国的有效证件），如果他声称永远不会放弃他的瑞典国际或拒绝外交协助，这将是给当局打好的如意算盘一记强有力的反击，同时也会增加外界对此案的关注度，因而增加案子的援助度。
- 很多人权人士被带走后被不允许与家人和律师见面和通讯，警方声称是这些人权人士说他们不想用自己的律师，而要用政府指定的律师。想象如果这人有一个提前录好的视频，清晰的声明自己永远也不会放弃自己指派律师的权利，永远也不会请一个政府指定的律师。
- 如果你大概知道警方会从你工作的哪一方面着手对付你，想象预录一个视频说明这份工作是怎么样的，为什么是完完全全合法的？如果你之前因为工作有被威胁或警告过，将这些受迫害的信息也记录下来。

- 如果你认为警方可能指控你非法组织NGO工作，或指控你金钱上的疏忽或贪污？那你可将你的财务报告等复制下来发给你的安全联络人，这样也能应对此类指控。

**重要：**如果你提供的档案发生了任何改变，比如地址、安全联络人的联系方式、家庭状况和你的工作，特别是在你的安全威胁有了阶段性的改变，这个文档应该更新你的最新状态和变更记录，你也应该重新发送新的版本给安全联络人。