数字安全实用手册

防御大于技术

引言：

基于行为的数字安全

practicaldigitalprotection.com

引言
基于行为的数字安全

简化版入门手册整理自完整版的

数字安全实用手册

practicaldigitalprotection.com

a project by

safeguard
DEFENDERS

contact@practicaldigitalprotection.com

目录

- 序言 4
- 了解你的威胁 5
- 预估你的风险和需求 8
- 基本保护行为 10
- 主要规则 15
- 手机存在的问题 19

序言

欢迎来到简化版的数字安全实用手册 — 为处于敌对环境的工作者设计的自学式数字安全实用手册。我们建议你按顺序阅读本手册中的章节，因为每一个新的章节会基于前面已经介绍过的知识。

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。

这份数字安全实用手册的简化版概括了在敌对环境中使用电脑和手机所需的基础安全意识和预防措施。

编写这份手册的目的之一是为在如中国、越南、缅甸等国家的记者、律师、NGO工作者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。

简化版手册会介绍基本的安全概念和行为。如果对任何特定的问题有兴趣，请移步到完整版的手册中阅读问题的技术解决方案以及其他的详细介绍。

“要提升个人的安全性通常不在于高阶的技术化解决方案，而在于相关的操作行为的细微改变”

了解你的威胁

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。

预估你的风险和需

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。试着从现在就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。他们需要有大概的方向，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。

网络电邮通常不仅免费，而且有高级别的加密性能，也有自动销毁邮件的功能，可参见ProtonMail.com，如果要中文版，可参见Tutanota.com。

可以自动删除对话的聊天软件，可参见Signal和Telegram。

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。

用于敏感工作的浏览器，可参见Firefox (火狐)，设置区域有很多插件可以提高安全，可在设置区域进行安装，比如KeyScrambler, TrackMeNot, RefControl, Better Privacy (或 Privacy+), 以及 NoScript。

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，你需要安装CCleaner，在各个选项下作出适当的设置，这个软件也能帮你清理浏览器的痕迹。

“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，但你“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。

幸运的是，在上面提到过的用于清理电脑使用痕迹的软件CCleaner，也可以彻底的删除(覆写)已经被你点击删除的文件。这个步骤是个关键，如果不使用软件彻底删除的话，你绝不可能真正维持安全。再说CCleaner中删除痕迹的操作的步骤也非常简单，当然所花费的时间也取决于硬盘的大小。

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。

想了解更多?

数字安全实用手册中包括了一些真实的事例，比如警方和国安如何利用一些工具获取信息，他们的成功与失败都取决于被打击目标是否有做好预防工作。

主要规则

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。

避免本国公司和程序

不像外国或至少西方国家的公司、服务和程序，本国程序通常没有强大的加密功能。本国程序收集到的用户信息不受法庭保护，比如像越南或中国，用户信息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大概是所有公司里面最糟糕的）。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人看到，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。

手机存在的问题

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。

“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、泰国等国家的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。

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。

不要让他们利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，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，并且不会太引人注意。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。

“用两层铝锡箔纸将手机的每个部位包住，就能将传输切断”