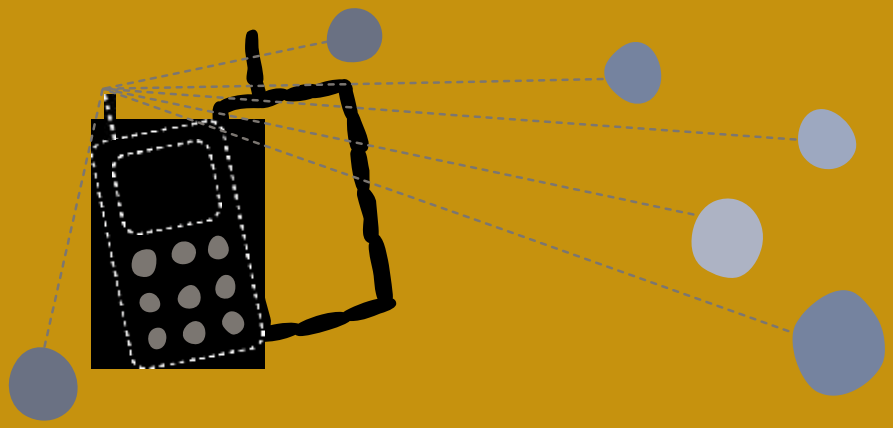
网络和手机之安全及隐私



诸如手机和网络这些新科技是非常强大的宣传工具，但是使用这些科技来传达敏感信息会为你、你的联系人、朋友和同事带来风险，此卡的目的为帮助你使用手机及网络时安全地获得以及保护资讯。

什么是数位安全和隐私？

资讯权利和数位安全遭到破坏的迹象可能包括：

- 密码在你不知情的情况下被更改了
- 私人信息似乎被收件人以外的人读过
- 网站在某些国家无法浏览
- 官员透露私人信件的资讯，包括数据、名字或者主题。
- 行动电话被监测。

我有必要关心吗？

如果上述情况会损害你的项目，或者暴露或迫害你或者你的联系人，那么你就应该留意。这些攻击隐私的知识和电脑软件在互联网上都能找到，如果攻击者有足够的权限侵入你国家的网络或者是手机基础设施，进行攻击所需的科技是十分简单的，除了政府机构，网络服务提供者（ISPs），和手机公司有权限进入这些基础设施，你的公司同事、邻居和网吧营运者也可能具有这些权限。

本卡包含哪些安全议题？

本张卡片主要针对网络工具和行动电话的安全，然而，还有许多其他的科技能使你受到审查、监视和迫害，尽管这些科技不在此卡讨论范围内，重要和基础的防护措施包括经常更新电脑操作系统、使用并更新可信赖的反病毒软件和经常性地备份文件。如果你有理由相信你的电脑或者数据储存装置，包括你的备份，有遗失、被盗或者被没收充公的风险时，又或者你的组织可能遭到网络监视的时候（或者此情形普遍存在於你所在的地区），那么你需要Tactical Tech（战略科技组织）的安全工具包。

網絡宣傳工具

当使用如博客，Facebook和Twitter这些网络工具来动员或者协调活动时，别忘了你储存在这些平台上的资讯在某种程度上已成为这些工具营运者的财产，许多平台工具会泄露超过你所预计的讯息量。

当你在线上平台储存敏感的资讯，请阅读它们的隐私政策或者用户协议，记住，即使在最开放的政策和条款里，你的讯息也是在平台工具管理者的直接控制下，你的资讯可能在未经你授权也未告知你的情况下，被泄露、销售、以及转移，即使你注销你的帐户，许多平台和工具并不会删除你发表过的内容或者你提供的私人讯息。最后，除非你有特别的理由必须使用大型商业平台服务，例如它易於浏览使用，或者因为这些大型平台吸引一些低调的用户，否则尽量使用一些支持人权及资讯权的平台工具：例如用Blip.tv代替YouTube; 和用riseup.net代替Gmail，如果你有技术等资源，你也可以营运自己的网络服务。

如果你用大型商业平台，小心保护你自己，避免怀有恶意的人士从这些服务平台上挖掘你的私隐资讯，尤其是诸如Facebook和Myspace的社交网站，对这些平台的隐私保护政策要有深入的理解，并仔细考虑哪些信息是你可能会在不经意的情况下泄露，例如你的真实姓名、住址、旅行目的地，和即将举办的活动或会议的相关细节。如被监测一段时间，这些讯息可以大致描绘出你的日常生活和工作模式的。

如果你用大型商业平台，小心保护你自己，避免怀有恶意的人士从这些服务平台上挖掘你的私人资讯，尤其是诸如Facebook和Myspace的社交网站，对这些平台的隐私保护政策要有深入的理解，并仔细考虑哪些资讯是你可能会在不经意的情况下泄露，例如你的真实姓名、住址、旅行目的地，和即将举办的活动或会议的相关细节。如被监测一段时间，这些讯息可以大致描绘出你的日常生活和工作模式的。

密码

绝大多数网络工具以及平台使用一个密码来保护你的帐户，如果一个恶意人士或组织知道了你的密码，那么无论你多么信任网络管理员，或是多么小心的保护你的隐私：你都将立刻失去你的隐密性和匿名性。

比较不为人知的盗取密码的方法包括：恶意人士在你用来登录安全网站的电脑上安装恶性软件，或者在你登录不安全的网站时监测你的网络连结。

为了防止受到第一类密码盗取攻击，建议使用你自己的电脑，或使用你信任的人维护的电脑，确保电脑的操作系统和反恶性软件是最新的。为了防止第二类密码盗取攻击，使用安全连结上网，绝大多数的网络邮件服务，社交网络平台，博客，地图和视频平台都提供安全连接，叫HTTPS，你可以在浏览器的地址栏里检查地址是否以”https://”开始(而不仅仅是”http://”)，然而除了当你输入你的的密码，许多网络工具并不使用HTTPS去保护任何资讯，这样的结果是如果有人长时间监控你的网络连结，他们即得知你在那个网站上储存的资讯，所以最好的防卫就是找在所有网页里都使用https的网络工具。

规避审查

你可以使用安全网络代理主机，审查规避工具或者匿名软件诸如Tor，在你浏览的网站中隐藏你的身份，或绕过互联网过滤器，这些工具在你需要进入被审查的网站时很有效，例如为了搜集资料浏览网站，或者为了上网络平台如Facebook。

在网上匿名

当你不想泄露你浏览过什么网页的时候，像Tor这样的匿名软件很有用。 Tor让你的网络连结在几台随机的自愿电脑之间跳跃，以防止你的ISP或者政府级的观察员知道你在网络上做什么，然而除非你透过HTTPS网页连结，不要用Tor在不安全的网站上发送或者接收敏感信息，否则那些你连结的自愿电脑有机会监控你所传输的内容，Tor基本上是安全的，但是它的缺点是会让你上网的速度变慢。

行动电话

行动电话在世界各地被普及地使用，但他们往往储存大量需要保密的资讯，除了通信录，手机还记录了通话记录、日历、短讯和电子邮件。

想想储存在你手机里包含哪些资讯，尤其因为手机极易被没收，如果你正从事敏感的争权工作，如争取人权，你可能不需要在手机的通信录里储存你所有的联系人，你也应该随时删除手机和SIM卡上的资讯因为短讯是容易被搜索和过滤的，所以在发短讯时避免写入敏感关键词。只要手机是开机状态，就可以被用来追踪你所在的方位，参加敏感聚会的人在出发前应该关掉手机并拿出电池，直到他们返回时再安装电池，将手机开机。行动电话的通信业者保有所有通话呼叫的细节：在何时何地与谁通话等资讯，这些资讯记录可能被保存几年，如果政府官员要求这些业者提供相关电信资讯，电信业者可能负有法律责任必须提供这些资讯。

行动：辨识安全风险

使用以下问题进行你的安全风险评估，帮助你决定使用何种方法来降低风险。

1. **我经手敏感资讯**。知道你所处理的资讯是否可能导致他人对你的监控是非常重要的，你是否在从事一些可能被政府、警察、军队或是私人企业视为敏感或干扰性的活动？如果是，除非你执行一些安全的措施，你可能置自己和他人于危险。
2. **我和需要保护身份的人共事**。也许你正在收集一些私人隐私的资讯，例如有关家庭暴力的资料，或是强迫劳动又或者有关强奸的资讯。如果他人向你提供的资讯会置他们于险地，则你必须采取防护措施以确保资讯的保密性。
3. **我在网上和处理敏感信息的人交流**。即使你觉得你没有安全顾虑，如果你在网上和有这些安全顾虑和风险的人进行交流，那么你就可能成为他们对手的目标对象，这是因为他们可以利用你而得到他人的私人资讯。
4. **我在敏感网站上浏览或发布讯息**。也许你向人权组织网站提供讯息，或者发表文章公开反对那些你认为不尊重人权的团体，其实仅仅是浏览敏感网站都有可能使你成为目标。

互联网安全和隐私资源

更多资讯和下载安全工具

1. **Security in-a-box**是由Tactical Tech和Front Line所共同制作，满足人权运动和捍卫者的电子安全和隐私需要。 http://security.ngoinabox.org/
2. **电子安全和人权捍卫者的隐私是由**Front Line所提供的可用于评估和处理电子安全的威胁。 http://bit.ly/1aCkSs (frontlinedefenders.org)
3. **Mobiles in-a- box**有整个部分是针对手机安全和隐私保护。 http://mobiles.tacticaltech.org/security
4. **使用Wordpress和Tor的匿名博客。** Global Voices编制了这个指引来支持人权拥护者，帮助他们揭示真相和在线上表达他们的看法，最重要的是避免随发声而来的风险。 http://advocacy.globalvoicesonline.org/projects/guide /
5. **匿名在线和规避审查。** Tor的设计为增强在线活动的隐秘性，它也可以用来避开网络过滤搜寻，你可以电脑上下载后使用它，或者把电脑连结USB来运行。 http:/ /www.torproiect.org/