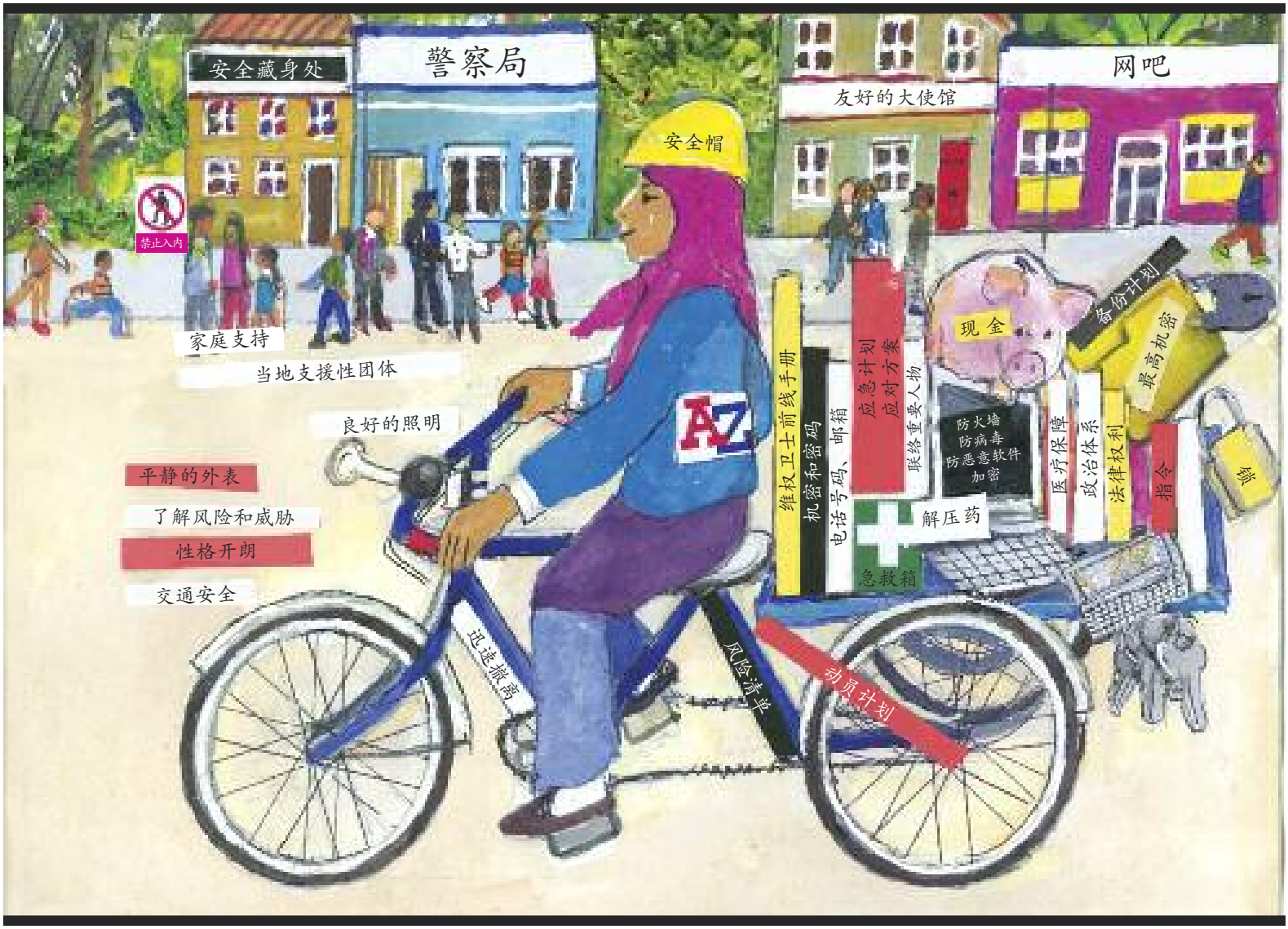
安全手册：
维权卫士身处险境时的实用指导手册



FRONT LINE DEFENDERS

附录14

电脑和电话安全

该检查列表并不是一个安全计划，关键因素还要取决于你自身的实际情况。综合考虑自身面对的风险、威胁以及自身弱势，对该检查列表进行补充，使其更加个性化。同时这里也仅仅列出几个关键点。

更多详细信息请查看“安全工具箱”HTTPS://SECURITY.NGOINABOX.ORG/

下列信息包含在“安全工具箱”项目中的“意识卡片”所提供的一系列建议当中——参见上述网站链接。

1. 确保你的电脑不会受到恶意软件和黑客的攻击

- 安装反病毒软件，反间谍软件以及防火墙
- 不要使用盗版软件——由于疏于更新，可能会使你的电脑易受攻击，也可能会被指控为使用非法软件
- 可以使用自由及开放源代码软件，例如AVAST反病毒软件、SPYBOT反间谍软件以及COMODOR防火墙
- 可以使用火狐等自带安全防护、更加安全的浏览器

（关于如何保护你的电脑，更多信息请见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-1）

2. 设置并保持安全的密码

- 密码越长越好。你的密码应该要多于12个字符，包含大写字母、小写字母、数字、特殊符号，如果可以的话还应该有空格
- 你的密码里最好不要包含完整的单词以及/或者关于你的公开信息，比如生日或者朋友的名字——将单词字母顺序打乱或者用特殊字符、数字代替字母，或者使用不同的语言
- 可以用一个词组来作为你的密码——可以是一本书的名字或者一首歌中的歌词（用符号或者数字代替字母）
- 经常更换密码
- 不同的服务要使用不同的高强度的密码，定期更新密码，同时不要重复使用密码（可以使用KEEPASS密码管理工具来储存你所有的密码——关于KEEPASS密码管理工具的信息参见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-3 ）
- 绝对不能公开你的密码
- 绝对不能允许网站及项目存储你的密码（关于安全密码的更多信息，参见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-3）

3. 如何保护你电脑上的敏感文件

- 定期对你的文件进行备份，并将备份文件存放在安全的地方
- 为敏感文件起普通无害的文件名，以掩盖其敏感性
- 可以对你的文件进行加密处理（不过在某些国家，加密设置是非法的，可能会引起别人对你的主意）
- 一个名为TRUECRYPT的自由及开放源代码软件既能对你的文件进行加密处理又能隐藏你的文件
- 你电脑上被删除的文件仍然可以被技术人员复原——可以使用安全的删除工具，例如CCLEANER软件（清除临时文件）以及ERASER软件
- 如果可以的话，对你的互联网提供商的背景以及你打算接入因特网的地方（例如网吧）进行核查
- 确保与你进行通信联系的人同样有保密和安全意识。通信联系是双方的事情。如果只有一方重视安全和保密性，那也是没有意义的。（更多信息参见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-4 和 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-6）

4. 确保你网络交流的保密性

- 很多网络邮箱账户都是不安全的（包括雅虎和HOTMAIL），会将你的IP地址通过你发出去的信件而发送出去。GMAIL和RISEUP邮箱更安全一些（尽管谷歌之前曾对政府提出的限制数据自由的要求做出了让步）
- 使用网吧服务可能会使你受到监视——要意识到这些风险，清楚自己正在与何人进行哪些方面的信息交流。使用之后删除你的密码和浏览记录
- 任何时候，只要条件允许，接入因特网时使用HTTPS代替HTTP，这样你的用户名、密码以及其他信息就会被安全地传输
- 不要打开陌生者来信或者可疑来信中的附件
- 在网络上发送、接收或者浏览敏感信息时都特别警惕

• 上网的时候可以使用代理服务或者申请匿名服务。
这就可以使你利用其他电脑的IP地址来接入网络，进行网上交流
• 及时消息（在线聊天）一般来讲也是不安全的，不过SKYPE可能比其他方式更安全一些
（更多信息参见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-7和
HTTP://SECURITY.NGOINABOX.ORG/EN/CHAPTER-8 ）

5. 社交网络

• 对你分享的关于自己、自己的行踪以及自己朋友的信息要小心谨慎
• 公开他人的信息、资料、图片以及方位之前要征得对方的同意
• 你的密码一定要安全，而且要定期更换
• 在公共网络环境下登陆自己的社交网站账户要小心谨慎——
只有在确保该处网络安全的情况下才可以使用。在使用了公用浏览器和公用电脑之后要删除你的密码和浏览记录
• 阅读并清楚了解终端用户协议（EULA），使用条款以及/或者保密建议文件。
这些文件以后有可能会变更，所以一定要定期重读这些文件
• 一定要了解你社交网站账户的保密设置。不要依赖默认设置——
自己重新进行设置并定期更新设置，因为网站服务也许会发生变化
• 谨慎安装社交网络服务所建议使用的程序。 只有你信任这些程序的来源、
了解这些程序会公开哪些信息，以及能够控制自己信息传播的时候才可以使用这些程序。
（更多信息参见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-10）

6. 移动电话安全

• 目前移动电话的设置及技术（包括短信服务与语音服务）都是不安全的——
你的方位会被暴露，通话信息也会被拦截，所以在传递重要信息的时候要选择最安全的方式
• 最安全的移动电话是便宜的、未登记的、充值电话，使用之后就可以扔掉
• 激活移动电话的密码功能或锁机功能
• 不要在移动电话中存储敏感信息，如果必须要存的话，设置加密功能
• 使用移动电话时要时刻警惕周围的环境，在高风险的地方及情况下不要使用移动电话
• 在出售或者修理你的移动电话之前，确保你所有的信息都已经被删除了
• 扔掉不再使用的手机和旧的SIM卡之前要进行销毁处理
• 在与个人或组织进行敏感信息交流的时候，应该考虑工作和个人使用要有不同的手机和SIM卡
（更多信息参见 HTTPS://SECURITY.NGOINABOX.ORG/EN/CHAPTER-9）