Atitit 手机个人信息保护法 隐私保护法 总结

目录

[1. 敏感信息定义 2](#_Toc28328)

[2. 信息安全大原则 2](#_Toc6869)

[3. 重要的设置 2](#_Toc22900)

[3.1. 锁屏密码 2](#_Toc276)

[3.2. Sim卡绑定手机密码 2](#_Toc6381)

[3.3. 开启查找我的手机功能， 2](#_Toc14754)

[4. 敏感信息泄露 以即防止盗刷等 2](#_Toc8561)

[4.1. 防范手机丢失 2](#_Toc17453)

[4.2. 防止别人利用丢失手机卡用你身份注册贷款 3](#_Toc26033)

[4.3. 保护好身份证号码等敏感信息 3](#_Toc23406)

[4.4. 手机sim卡号挂失与服务密码 3](#_Toc17673)

[4.5. 设置 SIM 卡密码 sim lock 绑定sim卡和手机 3](#_Toc23222)

[5. 硬件设备与app安全 3](#_Toc18783)

[5.1. 使用非国产手机+rom+ 3](#_Toc14533)

[5.2. 海外app尽可能使用 4](#_Toc6433)

[5.3. 多机app隔离 私密手机另外一个 4](#_Toc2643)

[5.4. Rom加密 4](#_Toc26145)

[5.5. 定期更换设备手机 笔记本 路由ip等 4](#_Toc20983)

[6. 必要的密码保护 4](#_Toc10335)

[6.1. 锁屏密码（不要设置指纹解锁 4](#_Toc20572)

[6.2. 输入密码和图画密码安全性高。。刷脸其次。。 4](#_Toc11256)

[6.3. 查找手机的功能开启 方便远程抹除数据 4](#_Toc24276)

[7. 数据安全法 设备数据加密 5](#_Toc29665)

[7.1. 文件加密efs等 5](#_Toc28620)

[7.2. Rar加密法 5](#_Toc16140)

[7.3. 通讯录人名加密 不要使用原名 可以用绰号代号代替 5](#_Toc27573)

[7.4. 文档敏感词使用代称 方言加密 黑话等 5](#_Toc11310)

[7.5. 证件和银行卡要安全note存储防止直接查看 5](#_Toc5722)

[8. 防止暴漏身份 6](#_Toc6209)

[8.1. 定期更换名字（包括网名） 6](#_Toc18364)

[8.2. 制作伪装用的id 6](#_Toc30316)

[8.3. 定期更换手机号 银行卡等其他敏感信息 6](#_Toc23781)

[8.4. 定期更换护照等身份证件与编码 6](#_Toc5130)

[8.5. 多带棒球帽和口罩掩护身份 6](#_Toc10332)

[8.6. 雨伞革命 尽可能多打伞防监控，可以利用女友打伞 6](#_Toc4564)

[9. 防止被定位 6](#_Toc10005)

[9.1. 居无定所 狡兔三窟 定期更换地址 6](#_Toc25474)

[9.2. 防止长期ip定位，每天强制重启路由器，让其更换ip 6](#_Toc9755)

[9.3. 每天强制飞行模式一次，让手机获取新的ip 6](#_Toc29028)

[9.4. 打车，故意打车到附近，然后步行500米，不要直接打车到公寓楼下 6](#_Toc9792)

[9.5. 不要直接回家，反复兜兜几圈，待无人跟踪再回去 7](#_Toc5049)

[10. 其他手机的安全设置看一看 7](#_Toc30358)

[10.1. Auto fac rest 7](#_Toc7635)

[11. Ref 7](#_Toc906)

# 敏感信息定义

照片 ，名字（包括网名，也需要定期更换）， 手机 住址 ，身份证号码 ，银行卡号码

，im聊天记录，定位信息等.。公司 行业资料

# 信息安全大原则

时刻记着信息安全。。

伪装，加密，定期更换 ，物理隔离 是安全三大原则

# 重要的设置

## 锁屏密码

## Sim卡绑定手机密码

## 开启查找我的手机功能，

远程定位、锁定设备，帮你尝试找回，还能及时抹除数据

# 敏感信息泄露 以即防止盗刷等

## 防范手机丢失

今以技术为中心的时代，任何企业或个人拥有的最有价值实体就是他们拥有的数据，但数据丢失可以以任何形式发生，其中设备丢失就是其中一种。

据《福布斯》报道，每年有7000多万部手机丢失，而这个数字预计将呈指数增长。此外，从2005年到2015年，近41%的数据泄露事件是由丢失的设备引发的。

## 防止别人利用丢失手机卡用你身份注册贷款

## 保护好身份证号码等敏感信息

## 手机sim卡号挂失与服务密码

## 设置 SIM 卡密码 sim lock 绑定sim卡和手机

设置 SIM 卡密码。在手机设置中的安全选项中，有一项 SIM 卡锁定的功能，设置密码之后，当 SIM 卡被犯罪分子安装到另外一个手机中时，就需要输入密码才能使用。如果密码输入错误多次，则需要 PUK 码才能解锁，PUK 码可以在 SIM 购买时的卡片上找到，或者联系运营商获取。

# 硬件设备与app安全

## 使用非国产手机+rom+

目前貌似只能选择三星和苹果了。。不要选择国行版本，间谍软件众多。。选择海外版。。

如果囊中羞涩，可以选择海外版国产手机rom组合，组成廉价整列，及时替换。。

## 海外app尽可能使用

## 多机app隔离 私密手机另外一个

国内软件app只用wechat和alipay。。装在安全的手机里，和海外app做隔离。。

私密手机随时可以设置静音。。如果遇到检查，只掏出安全手机来。。

## Rom加密

## 定期更换设备手机 笔记本 路由ip等

# 必要的密码保护

## 锁屏密码（不要设置指纹解锁

设置好手机的锁屏密码，这是防止手机中联系人、相册等个人信息被盗取的第一道屏障。

## 输入密码和图画密码安全性高。。刷脸其次。。

密码和图画密码安全性高。。刷脸其次。。指纹密码安全性较低，不能防止睡梦中或醉酒，等失去意识的情况下，以即 轻微强迫的情况， 被别人解锁。。

## 查找手机的功能开启 方便远程抹除数据

如果锁屏密码被破解，查找手机的功能就可以派上用场

# 数据安全法 设备数据加密

## 文件加密efs等

## Rar加密法

## 通讯录人名加密 不要使用原名 可以用绰号代号代替

## 文档敏感词使用代称 方言加密 黑话等

## 证件和银行卡要安全note存储防止直接查看

这样他会注册新号，然后绑定银行卡消费。。

使用evernote二次加密。。或者secury note等安全记录。。

或者相册提供 安全保险箱。。。

Google photo即提供安全保险箱。

# 防止暴漏身份

## 定期更换名字（包括网名）

## 制作伪装用的id

## 定期更换手机号 银行卡等其他敏感信息

## 定期更换护照等身份证件与编码

## 多带棒球帽和口罩掩护身份

## 雨伞革命 尽可能多打伞防监控，可以利用女友打伞

# 防止被定位

## 居无定所 狡兔三窟 定期更换地址

## 防止长期ip定位，每天强制重启路由器，让其更换ip

## 每天强制飞行模式一次，让手机获取新的ip

## 打车，故意打车到附近，然后步行500米，不要直接打车到公寓楼下

或者其他tower

## 不要直接回家，反复兜兜几圈，待无人跟踪再回去

# 其他手机的安全设置看一看

Lock secury关键词搜索下，堪忧哪些安全新特性。

## Auto fac rest

三星手机的，如果15次尝试解锁失败，则自动reset。。到工厂模式。。

不要开启，防止意外屏幕开启，在包里。。

# 设备丢失或转让预案

## Reset 清除手机数据

## 注销各种app的设备ms 和google等重要

## 手机卡丢失或注销预案 解绑手机号

## 解绑特定的设备和手机

重要的信息类app ms google，。以即重要的支付类app支付宝 微信等

## 定时启动设备管理 注销丢失设备和手机号

# Ref

Atitit 信息设备加密机制 手机 电脑 tpm bitlock EFS加密

Atitit sim lock pwd