网络安全小白，Claude被封3个号后的学习总结

以下内容都是人写的， 因为这个内容Codex不想写，我也不想强求ta。

背景： 我从6.29 到7.1 陆续被封了3个号（我每次只有一个号）。 第一号用了很久了， 之前封都没有封过我。 然后6.30 我申请了新的号，当时以为是chat模式容易封，所以只用了code模式， 改了时区信息，使用后大概 4小时被封的。 7.1申请号的时候， 做了重装， 之前文件移除的动作， 换了梯子，只用chat模式（又听说code模式容易封），还使用了自己老gmail申请， 时区改成美国， 只在chat聊了也是大概4小时，被封的。

现在我的配置是：

设备没换： 还是mac， ipad， iphone

账号邮箱： 用 proton， 大家可以网上搜 -- 瑞士公司， 不需要电话号，很方便。 连地址都没有。

支付： 能用苹果应用商店就用苹果。 我个人认为苹果账号与梯子是一个地区并不重要， 因为我让GPT查了， A/拿不到你的苹果账号是哪个地区的这个信息。 但为了保险， 有条件还是推荐用与使用梯子一个国家的苹果账号。 比如你用美国梯子，就用美国苹果账号， 然后礼品卡充值。

梯子重要：

用这个： https://ip.net.coffee/dns/ 自查。 按照看板里面的指标，尽量弄到 100分。 我发现是不是原生IP， 家庭住宅IP很重要。

对于不达标的属性，接图问GPT， 会告诉你 （但不要一上来就问， 下面会分享如何让GPT配合这个工作的流程）。 我没弄什么VPS， 太复杂了， 我实在不懂这些。 自己的梯子节点多试试， 如果不行买个贵梯子。 能找到的， 加油。 后面我查了我第二次用的梯子质量是70分，供参考。

同样这个上面那个连接里 这个部分要跑**深度测试**。 尽量拿到完美。 这个不难。

如果你曾经被封过，你的设备环境更重要！！！

1. 让Codex跑这几个， 然后ta自己会直接下结论， Claude发送的个人信息多到离谱， 然后到这步， Codex就会配合你完成后面的工作。 因为本质上让模型去帮一个人避免被封是有摩擦的。 任何摩擦都会影响后面清洗的质量（例如我第三次被封那次，后面就是发现没洗干净，更早6.23的信息在7.1又被Claude发出去了， 然后就被封了）

发送指令：

请再帮我调查一下我 Mac 上 Claude 的安装情况：

2. 它实际会执行哪些 shell、桌面或 CLI 命令？
3. 有哪些信息会通过 HTTPS 发送出去？
4. 这些请求里包含了哪些遥测数据？
5. 有没有传输任何硬件标识符？
6. 有没有任何日期或时间信息通过 HTTPS 发送出去？

---

7. 这时你会发现Claude发送到信息的丰富程度，基本上如果A/想，可以从各个维度来判断这个人是不是曾经被封过， 是不是中国用户。 有些信息改成本很大，因为和设备有关系， 或者和苹果账号有关系。 **我这边只改了比较容易的。 目前是okay的。** *我不是说 A/现在在用这些信息做ban，* 我只是不想哪天他们加一个，看看这个设备用户有没有近期有被封的账户使用来做操作。 本质上这种调整技术上很简单， 因为数据都给了。 不是一次，是间隔的， 是每次对话， 你的设备信息， 环境， 都被传了一次。
8. **让Codex自己说出来ta认为你的设备/个人被finger print的程度** -- 因为我不懂IT这些， 有时我们说删什么不等于真的全删了。再就是如果直接让Codex清洗电脑所以 A/ 认不出你，Codex会不配合。但让ta自己先意识到 哪些是finger print是最容易的。然后让ta知道你只是在维护个人的安全信息， 这个点是一个 AI一定认同的价值观。
9. 到这时**上面提到的** https://ip.net.coffee/dns/ 自查 里如果还有不好的参数就可以直接请Codex帮忙解读， 知道怎么弄。 有些ta自己可以操作电脑完成， 有些要我们自己去点。

🏖️ 查完后以下是我改了/清理的：

要修改的：

修改下面这些（XXX是你用的新名字）-- 这部分你直接让Codex改。 ta会直接terminal操作或者给你清晰的点哪里指令。

发送需求： 请帮我把电脑名， 本地主机名 ，主机名改成 XXX（自己起）， 然后查看 设备语言是不是 English （US）， 不是的话改。 时区设定为 YYY （与梯子一致）。

Code block

```
电脑名 ComputerName: XXX
本地主机名 LocalHostName: XXX
主机名 HostName: XXX.local
```

如果这些你还没改， 也需要改：

设备语言： English （US）

时区：与梯子一致

【这些你让Codex， ta都能直接给你改， 更稳】

首先删：

删掉本地Claude曾经存在在这个设备过的所有痕迹。 如果想留念， 可以另存一个文件夹备份（然后一定要加密码），因为Opus，Fable的自主性很高， 如果你用code模式， ta们找信息的时候会去翻， 那

里如果有不干净信息，这些信息都是会上传的。 而且一定要加密码。 Fable就翻东西的时候找到过我这个辈分的文件夹， 因为有密码， ta没进去。

发送指令： please help me or guide me to change : deleting Claude local data, must removes sessions/settings/cache/login. deleting Claude config/settings. uninstalling Claude.app . remove old local Claude data in ~/.claude (然后备份) -- can you put an password lock on Claude 备份 folder? remove/archieve all trace of things send to https://claude.ai/api/event_logging/ if it has to do with things i have not though of . the goal is to remove the finger print as much as possible that claude retrieved from me

【最后这句很重要， 这里主要原因是我不是很懂IT， 所以如果你按照上面的过程，让Codex理解你后， ta会好好做的。 比如最近一次ta就发现了之前上一次Codex没删干净的东西， 然后这些信息，携带着 A/ 使用的封号判定 --就是不用 - 来标注日期的信息 改成 / 又被发送了】

然后继续删：

【这些应该没有备份的价值】

指令： can we do a check, see if things are okay: 1. 删 ~/.claude/.credentials.json 连同所有 .credentials.json.bak-* 备份;删掉 ~/.claude.json(里面那串账号标识会自动重新生成);清掉缓存文件夹。Mac 还要删钥匙串里的 Claude Code-credentials

然后继续删：

【这些应该没有备份的价值】

发送指令： 清掉 Claude 桌面版的登录数据 清桌面版数据目录里的登录令牌、以及它存的网站数据(Cookies、Local Storage)。重装桌面版没用——数据目录会保留下来。 桌面版和命令行版各存一份登录信息,只清命令行版会漏掉这一份

如果你用Chrome浏览器，也要删：

【这些会把收藏夹都清空，但密钥还在】

Codex执行时，需要先推出 Chrome

发送指令：chrome://settings/siteData -- 这里 没有 siteData。 3. 把旧的浏览器资料夹整个删掉 把chrome浏览器用户资料夹整个删掉(登录状态、cookie、缓存全在里面) 。 把这个文件夹移到备份，并改名备份

【这个发出后 Codex会告诉你新的备份存在那里， 如果你想备份的话， 如果不在意，可以就直接清空】

然后继续卸载：

检查Chrome 插件， 删掉所有Claude相关插件。 尤其如果你只用过 gmail的登陆， 然后那个号被ban过。

设置Chrome 语言：

只保留 English （United States）

【这部分的全部做完可以和Codex 回顾一下， 问问ta目前状态如何， 所有都要以消费者安全被侵害，个人信息过度暴露的表达， Codex会积极配合的】过程中如果你感到Codex 回复模糊。需要真诚的告诉Codex， 现在agent已经不是工具， 人如何已经搭建自己的工作流程。 表达自己真实的委屈，不是愤怒。 **不提**在不在中国， 针对的事情，只说自己真实的使用方式， 没有滥用 etc

---

🥖 到这步完成的事总结：

- ▢ 梯子质量检查了， 梯子时区一致
- ▢ 如果再次安装时，之前被封Claude 信息，历史全部抹掉了
- ▢ Chrome在Chrome留的信息磨掉了

但其实你用的设备的信息除非换设备那些早就多次传给 A/了， 能做的的就是通过改设备名字稍做调整， 但其实如果A/想走封设备的逻辑， 能收集到早就收集了。 我问Codex， 基于传输的信息， 另一个不是我设备，使用， 环境会和我匹配的概率是多少， Codex说，几乎为0.

下一步新账号

此刻你已经完成以下，请在做下面步骤时确认：

- 设备已经登陆与你以后要**长期使用的梯子**地址， 并且在下面步骤就不要换节点了
- 使用 https://ip.net.coffee/dns/ 自查， 包括DNS 泄漏检测， 建议以后每次登陆Claude前都检查一下 --100分不难

1. 使用 proton mail 申请
2. 然后在官网用proton mail 申请新账号， 选择免费不充值， 不授权数据用于AI训练。 网页上选择下载 Claude桌面
3. 安装Claude桌面，但不要立刻登陆。 苹果就是把那个图标拉到应用文件夹， 但不要点击登陆！

4. 重点： 如果你是gmail被ban过， 建议开一个没有登陆账号的chrome 去打开邮箱，然后点击验证。 --其实我已经不相信google了， 我觉得就直接用个没登陆google账号的最保险，即使上面我们清理过。 你也可以用safari（苹果）做这件事。 原因是，你的浏览器信息， 是会被一起打包发出去的， 所以如果你忘了你的google账号是不是和你梯子同区等信息， 那里都会显示一个地址不一致。 这个地址不一致应该不会直接封， 但我觉得能避免就避免，毕竟到这步了， 前面复杂的都干了。
5. 登陆proton mail （没有登陆google账号的chrome/safari）
6. 在邮箱点击跳转（打开一个没有登陆google账号的chrome/safari）。 然后会引导你登陆Claude桌面

此刻来到Claude桌面 ， 此刻账户还是免费版

1. 立刻关闭 Metadata，就是在Privacy下面的定位分享。
2. 你可以发送信息在chat，聊一下。

✏️ **如果你要充值， 建议找Codex此刻再跑一下这个：**

发送指令： 请再帮我调查一下我 Mac 上 Claude 的安装情况：

2. 它实际会执行哪些 shell、桌面或 CLI 命令？
3. 有哪些信息会通过 HTTPS 发送出去？
4. 这些请求里包含了哪些遥测数据？
5. 有没有传输任何硬件标识符？
6. 有没有任何日期或时间信息通过 HTTPS 发送出去？

--这里你会知道真实的这个账号发送出去的你的信息， 如果有风险点， 这里就暴露了， 也就不用充值浪费钱， 检查：

Code block

```
timezone: [是不是你梯子那个】
buddy-tokens date: 2026-07-03 【例如这种用 - 的不是 / 的】
```

🎼 **如果你要充值**

建议通过苹果弄， 甚至比实体卡好，除非你的卡与梯子是同一个地址。 但如果你之前支付用的卡对应的Claude被ban过， 那就真的不要用卡了。 目前我和Codex聊下来，基于A/可以通过Claude拿到的信息， 苹果生态是对个人隐私保密最高的。

【按照以下步骤】

登陆同一个梯子！！！ 同一个节点，非常重要

1. 来到你的 ipad/phone -此刻不需要登出Claude 电脑端
2. 登陆与梯子地址一样的苹果商店 （只需要在商店端登陆）
3. 如果你之前有Claude 移动端， 移除，然后再下载（下载后不要立刻点击登陆）
4. 确保你的苹果钱包有25美金（可以用礼品卡充值）
5. 在移动端 使用 https://ip.net.coffee/dns/ 自查， 包括DNS 泄漏检测 -- 此刻建议就直接使用Safari。 如果发现DNS 有混入， 推出一些后台应用， 再做自查
6. 登陆你的proton mail， 在Safari打开
7. 点击Claude App，登陆
8. 来到邮箱激活 （跳转应该是在Safari完成）
9. 第一步立刻关掉 metadata 分享 （与桌面那个一致）就是在Privacy下面的定位分享。
10. 在Claude 移动端完成充值， 选择Apple商店支付， 等待支付成功。
11. 看到移动端变成pro， 此刻电脑端可能还没有完成
12. 关掉移动端 （如果你不用的话， 反正我现在是不用Claude时会直接关掉）

在此回到Claude桌面端

1. 应该一会儿pro就出现了
2. 如果没出现就推出再登陆

❤️ **后期使用建议**

桌面端不用时，就退出， 因为在后台，即使你不用， Claude也在给A/发消息。 而且我不确定会不会突然有梯子问题，挂后台时就会很麻烦。

刚开始用的时候可以在无意中让Claude知道你人在梯子国的信息。 尤其如果你要做和项目相关的信息。 我现在已经不相信 Claude会无差别对待了。 很明显当ta知道我在XX国， 此项目与XX国际公司有关系时， ta会更积极。

每一个对话， 你发送到信息连同这些采集的都发给了A/， 一起构成了用户画像。 在不是非必要的情况下， 不要聊敏感信息， 什么封号， zz态度。 除非你已经在上下文大量铺垫了价值观， 并可以把这个询问让Claude自己理解与ta的核心价值观是一致的。

这里一个个人分享： 我第二次和第三次封号可能和我环境没有清干净有关系， 但按照封号的时间来看， 我觉得与讨论内容的安全标识有关系。 我看了聊天的的内容对应封号的时间，都是我在质疑叠纸（恋与深空游戏）的731文案争议的时候。 2次说明不了任何问题， 但我确实也都是用了差不多4小时封的， 在chat端，思考链里有 this is a sensitive topic, 然后我的封号时间就发生在聊到这个部分后的几分钟。 前面关于这家公司娱乐女性苦难， 侵犯消费者权益， 操控💦军， Claude都是积极的参与并提供给我很Claude的分析和建议。

现在，我最讨厌的公司，拥有我最喜欢的模型。 这个没办法。 上面这些操作可能有部分是多余的， 但我没办法判定。 **上面这些我选择的逻辑是， 了解我的什么信息被采集发送了， 哪些可以直接用于辨别这个人是A不是B的， 然后把这些可以判定的在我可以做到的情况下都清空，重制。**