

# 數字極權時代生存手記

繁體中文版

自序	4
前言	9
第一章 必要的前期準備	12
第一節 獲取美區 Apple ID	13
第二節 獲取 Google Voice	18
第三節 註冊美區 Paypal	22
第二章 如何突破網絡封鎖	23
第四節 「翻牆」基本原理	24
第五節 V2Ray	26
第六節 Shadowsocks	36
第七節 其他翻牆手段概要與評析	41
第三章 加密即時通訊應用	47
第八節 加密通訊應用概論	49
第九節 Telegram 使用指南	51
第四章 個人信息保護指南	69
第十節 個人信息保護指南	70
第十一節 牆外社交媒體使用建議	87
第五章 信息難民自救指南	89
第十二節 404 信息保存	90
第十三節 404 信息獲取	92
第六章 番外	94
第十四講 去中心化網絡	94
第十五講 加密數字貨幣	99
附錄	101

哪敢與世無爭，分明是這個世界逼著人去爭！

——岳昕《我在公開信後的一周里》

# 自序

自序·數字極權的鐵幕下，我們已退無可退

《數字極權時代生存手記》收錄了我自 2017 年以來在網絡代理、信息安全等方面的學習與實踐成果的記錄。

編程隨想在《為啥朝廷總抓不到俺——十年反黨活動的安全經驗匯總》一文中這樣寫道：「（在牆內）很多具備政治素質的人，缺乏信息安全的技能；所以他們無法利用互聯網與黨國鬥爭。」信息知識與技能的意義還不止於此。數字極權之所以能夠毫無阻力地在中國推進，離不開大眾在個人數據權利問題上的集體無意識。大多數中國民眾對國家機器與科技巨頭合力實施的大規模監控所知甚少，對個人隱私信息的去向漠不關心，再加上官媒「用隱私換取便利、安全」的洗腦宣傳，使得整個國家在數字極權主義的邪路上越走越遠。

信息技術可以為專制政府所用來強化管控，反過來也可以民眾所用來擴展自由。網絡代理可以幫助人們自由地獲取未經審查的信息，端對端加密通信可以保證私密對話不受服務商與政府的監控，多重代理帶來的網絡匿名可以提供更大限度的言論自由，加密技術的普及與對網絡封鎖的破壞可以提升了當局實施輿情管控的成本。被統治階級的群體性覺醒構成了反抗的前提，信息技能的運用則可以構成反抗的手段。因此，當信息知識與技能成為互聯網時代的每一個個體的基本生活常識和能力時，它將可以對數字利維坦提出有力的挑戰，這或許就是普及信息技能的意義所在。

## 一、GFW 必須被打破

互聯網技術拓展了信息傳播的深度與廣度，一度被寄望能給中國社會帶來民主。然而與互聯網在中國普及相同步的是防火長城（Great Firewall, GFW）的建設，它試圖在互聯網空間實行閉關鎖國的政策，審查屏蔽一切與中共意見相左的境外網站，把中國人圈禁在從萬維網中硬生生划出的「大中華局域網」中。在本國網絡空間，中共當局藉維護國家安全之由大發專制淫威 [1] [2] [3] [4]，壓制一切異見，扼殺多元價值，對異議者動輒禁言刪號乃至逮捕拘禁、定罪判刑，迫使牆內民眾學會自我審查而畏於發聲；另一方面又開動宣傳機器，使得民眾只能獲取當局希望他們接觸的單一信息與強加給他們的價值觀念，今日頭條、騰訊新聞和各大國產手機瀏覽器每日置頂的習近平報道與「聲名在外」的數字化紅寶書「學習強國」App [5] [6] 就是顯例。中共通過封鎖、審查、禁煙、灌輸多管齊下，以

軟硬手段相結合的方式推動洗腦政策與信息時代相適應，最終達到把中國人打造成閉目塞聽、頭腦簡單、思想與黨中央高度一致的木頭人的效果。

GFW 不是一天建成的，中國互聯網的原住民最早可以不受限制訪問 Twitter、YouTube、中文維基百科等境外網站。GFW 加碼的親歷者與見證者擁有著對於網絡審查現狀的認知，這是尋找手段突破封鎖的前提。而對在 GFW 後成長起來的新世代而言，許會因為堅持獨立精神而在牆內平台屢遭迫害，不得已出逃牆外成為「信息難民」；而更多的人難以認知「牆」的存在，或是將自我審查內化為習慣，「不會主動尋找敏感的信息，因為他們在成長中對信息審查已習以為常」[7]，在信息壁壘和官方意識形態狼奶的灌輸下成長為「粉紅」和「戰狼」，深種文革思維，高揚「愛國無罪」，沐浴「盛世狂歡」，他們將翻牆者視為反動的異端，給牆外網站的批評聲音貼上反華勢力的惡毒攻擊的標籤。因此，先行者有必要向身邊的人傳授自己的翻牆「手藝」，讓他們也能輕鬆便捷地跨過 GFW，自由地在完整、開放的國際互聯網上查看一切未經中共當局審查的信息，還互聯網以本該有的面目。只有讓更多的人傾聽到不同的聲音，才有讓洗腦政策的受害者吐淨狼奶，意識到完整互聯網遠不止「中華局域網」的一畝三分地，才有可能彌合信息不對稱的鴻溝，進而為不同派別間開展良性對話創造可能性。需要承認的是翻牆手段本身只是提供帶來改變的可能性，不必然帶來變革的結果，正如「戰狼」有時也會翻牆，但只不過那是在上演「帝吧出征」的鬧劇；但是推廣翻牆術仍是有益的嘗試。清醒者若是不付出抵禦愚民政策的努力，聽任同伴繼續沈睡，自然永遠無法改變網絡審查的現狀。

## 二、穹頂之下，莫非天網

人工智能和大數據等新興科技為實現利維坦對社會生活全方位控制提供了全新的手段，數字科技與極權政體的聯姻將人類帶向前所未有的反烏托邦，而新疆已然不幸成為了「先驅」——當局要求所有居民在手機上安裝能夠自動掃描和上傳文件數據的淨網衛士 APP [8]，使用數以千計的監控攝像頭配合面部識別和大數據分析以便實時掌控所有居民的一舉一動 [9] [10]。我們縱然無法左右「新疆再教育營」的存廢，但至少應當清醒地認識到這個國家正在發生的一切、我們的同胞所經歷的一切，而不是聽信外交部和官媒所謂「去極端化」、「職業培訓」的無恥謊言。如果漢人覺得事不關己而對中共當局在新疆的倒行逆施聽之任之，同樣的災難遲早也會降臨到他們的頭上。被冠以「雪亮工程」[11] [12] [13] 之名的監控天網正在內地鋪開，「內地新疆化」並非空穴來風。大規模監控的實質是專制統治者監視臣民、鞏固統治的工具，它所帶來的只有民眾的恐懼，而不是官方所允諾的安全與社會穩定。

在中國強制性的網絡實名制下，網警可以輕而易舉地將你在國內網絡平台的發言與你的真實身份相關聯；警察時刻在幕後監視著微信上發生的一切 [14]，你甚至會因為在朋友圈的言論而遭受牢獄之災 [15]。正在建設的社會信用體系表明瞭當局掌控全面個人活動的

企圖。特定嚴重失信人黑名單等措施確實起到了打擊不誠信行為的效果，但它同時也被當局用於迫害持異見者和訪民群體 [16]，藉大數據之手製造人道災難。

### 三、「哪裡有壓迫，哪裡就有反抗」

就如同毛澤東所說的「我是一個知識分子，當一個小學教員，也沒學過軍事，怎麼知道打仗呢？就是由於國民黨搞白色恐怖，把工會、農會都打掉，把五萬共產黨員殺了一批，抓了一批，我們才拿起槍來，上山打游擊」一樣——我是個碼農行業的門外漢，也沒學過計算機科學，怎麼知道註冊美區 Apple ID、租虛擬服務器搭建翻牆工具、用 Telegram 替代微信、翻牆上中國數字時代瞭解祖國呢？就是由於共產黨搞赤色恐怖，把網絡上對自己不利的言論都刪掉，把境外網站的 IP 地址封鎖了一批，TCP 關鍵詞屏蔽了一批，VPN 應用下架了一批，我才爬牆自救起來，最後還把經歷寫成了這本書。

自 Telegram 被中國當局封鎖後，要想在中國大陸使用 Telegram 自然離不開翻牆這一大前提，於是就有了本書的第二章「如何突破網絡封鎖」。翻牆不是我新學會的技能，不過我在 2017 年中時於偶然間得知了 Shadowsocks，使得日常性使用牆外服務成為了可能，並使我幸運地躲過了當年發生的國內 VPN 廠商被迫關停、蘋果在中國區 App Store 下架 VPN 應用以及之後「十九大」前的 GFW 升級帶來的斷網衝擊。之後，我從購買 Shadowsocks 商業服務轉為借助 HyperApp 在 VPS 上自建 ShadowsocksR，再到命令行下自建 V2Ray，在升級「愛國上網」方式對抗黨國的網絡封鎖和管制的道路越行越遠，從此一髮不可收拾。

移動端的翻牆離不開廣義的 VPN 客戶端的使用，而中國 App Store 的 VPN 應用下架潮迫使我註冊了美區的 Apple ID 和 PayPal 以便獲取和更新 VPN 和紐約時報等其他被中共認為威脅其統治而勒令下架的應用程序，這是本書第一節「獲取美區 Apple ID」和第三節「註冊美區 PayPal」的由來。

2017 年末上海攜程員工親子園虐童事件、紅黃藍幼兒園虐童事件、北京清退「低端人口」事件、北京亮出天際線行動、京津冀煤改氣導致供暖危機，再到 2018 年的修憲取消主席任期限制、#MeToo（中國）系列運動（瀋陽事件、北大岳昕事件、……）、長春長生生物問題疫苗事件、P2P 網絡借貸平台集中爆雷、深圳佳士工運，這些曾經被送上輿論風口浪尖的熱點話題的命運逃不過在微博、微信等牆內社交媒體上的大規模刪帖封號的命運，留下一片刺眼的紅色和「404」。在中國特色權貴資本主義運作模式下，權力與資本合謀劫掠財富，政府積極擴張權力的同時又拒不承擔責任，一貫奉行「解決提出問題的人而非解決問題本身」的行事邏輯，以「穩定壓倒一切」與維護國家安全的名義維護特權階級的統治地位與既得利益，通過信息封鎖和輿情管制來奴化民眾，悍然製造無人堪作見證的歷史。需知中共當局迫害的不僅僅是那些被控「煽動顛覆國家政權」的民運人士、

人權律師和自由派學者，而是生活在極權體制下每一個平民。如果任由受害者被噤聲，問題被掩蓋，悲劇注定重演。

我曾在微博上追蹤一批因為關注北京切除事件頻繁被銷號後又「轉世」的博主，並曾嘗試備份預感會被刪的敏感題材的微博和微信公眾號文章，也是在這個時候接觸到了新聞網站 [中國數字時代](#) 和它那句極為諷刺的「在這裡，瞭解祖國」的口號。我堅信，信息傳播的自由是人與生俱來的自然權利，中共當局將真相揭發與理性討論誣指為謠言而一並絞殺的無恥企圖必須被粉碎。本書第五章「信息難民自救指南」，便是拜網信辦和中宣部之賜。

#### 四、選擇適合自己的解決方案

解決方案的選擇應取決用戶的直接需求，而效率和安全強弱同時受到方案選擇與具體使用方法的影響。本書所提供的方案接近於「數字移民」，在效率與安全的權衡上更傾向於前者。在網絡代理方式的選擇上，V2Ray 和 Shadowsocks 可以有效地突破 GFW，但這類翻牆方法在匿名性上可能存在不足——如果你選擇商業服務，服務商可以在服務器上看到你所有的訪問記錄；如果選擇自建，你很難保證你對 VPS 所做的安全防護措施足以抵擋潛在的攻擊。另一方面，承諾服務器零日誌的 VPN 服務固然能夠提供較強的匿名性，但它們所採用的除 OpenVPN 協議修改版之外的 VPN 協議都能被 GFW 識別屏蔽，並不能滿足中國用戶翻牆的需求，這是本書將 V2Ray 和 Shadowsocks 放在前面的原因。在加密即時通訊應用的選擇上，本書推薦的 Telegram 也不能保證絕對的安全，因為即便是端對端加密模式也可能遭到中間人攻擊。Telegram 上不存在政府的審查和監控，擁有一定規模的中文用戶群體，頻道和超級群聊使它在信息傳播上具有顯著優勢，這使它相對更適合作為大陸民眾習慣使用的微信（WeChat）的替代品。

如果你對個人隱私保護或匿名性有更高的要求，建議閱讀 [編程隨想](#)、[Cryptoboy404](#) 和 [iYouPort](#) 的博客。對於人權律師、新聞記者、NGO 工作者、訪民等從事高風險活動的群體，應當參考 [《數字安全實用手冊》](#) 等專業性更強的作品。

衷心祝願每一位讀者都能獲得免於自我審查與恐懼的自由。

- [1] [Solidot | 網信辦啓動「劍網 2018」專項行動](#) (2018-07-16)
- [2] [Solidot | 網信辦關停三款短視頻應用，B 站宣佈增加審查人員](#) (2018-07-27)
- [3] [Solidot | 網信辦加強輿論監管](#) (2018-11-16)
- [4] [Solidot | 網信辦禁止轉世賬號](#) (2018-11-16)
- [5] [美國之音 | 習近平「紅寶書」「學習強國」手機軟件由阿里巴巴開發操作](#) (2018-02-18)
- [6] [BBC News 中文 | 「學習強國」：習近平「紅寶書」登上App排行榜首](#) (2018-02-16)
- [7] [ABC NEWS | 與西方隔絕：在「牆」內長大的中國新世代](#) (2018-11-11)
- [8] [Solidot | 淨網衛士被發現明文傳輸收集的數據](#) (2018-04-10)
- [9] [德國之聲 | 臉部辨識結合大數據 250萬新疆居民難逃中國掌心](#) (2018-02-18)
- [10] [Solidot | 中國公司的人臉識別數據庫外洩](#) (2019-02-15)
- [11] [【立此存照】雪亮工程：視頻監控入戶到人 - 中國數字時代](#) (2018-03-30)
- [12] [特大號 | 2018 安防監控、雪亮工程項目盤點！ - 中國數字時代](#) (2019-01-03)
- [13] [自由亞洲 | 2022 年中國每人「擁有」兩個監控探頭 - 中國數字時代](#) (2019-02-04)
- [14] [【立此存照】網安部門監控清華大學學生組織的報告書 - 中國數字時代](#) (2017-12-04)
- [15] [Solidot | 網民因在朋友圈罵交警被拘 8 天](#) (2019-01-10)
- [16] [【網絡民議】「母親成了詐騙受害者，反而被禁止坐高鐵」 - 中國數字時代](#) (2019-02-16)

#### \*閱讀需知

本書之所以稱為「手記」，而非「教程」、「指南」，一來是因為我自身只是半路出家、勉強實現從無到有的「老白」，不能保證書中原創內容的專業可靠；二來詳實嚴謹的優質教程或科普文在國際互聯網上並不少見，我依樣畫葫蘆重抄一遍前輩的教程顯然是沒有意義的。所以我對本書的定位是文獻與超鏈接綜述，意在摘引相關作者的創作、維基百科的詞條解釋來告訴事實 A、技術 B 或工具 C 的存在；至於深入瞭解技術 B 的原理或者學會運用工具 C，需要讀者閱讀鏈接的教程並善於運用搜索引擎從完整互聯網上獲取更多的信息，僅靠本書的內容是不夠的。

本書將通過 PDF、Gitbook 和 Telegraph 三種渠道分發，不同渠道的發行版在排版等細節上存在差異。



## 前言

ABC NEWS | 為何我決意在微信上作一個沈默的觀察者 (2018-11-04)

ABC NEWS | 澳洲中文社交媒體上的假新聞：核輻射秘密和致癌咖啡 (2018-07-23)

ABC NEWS | 「從不講述全部真相」：中國媒體進軍國際的民主威脅 (2019-02-09)

BBC | 從檔案袋到信用評分 中國是否正走向「奧威爾式」監控社會 (2018-10-17)

編程隨想 | 為啥朝廷總抓不到俺——十年反黨活動的安全經驗匯總 (2019-01-30)

China's Surveillance State Should Scare Everyone (2018-02)

端傳媒 | 「南方傻瓜」甄江華：黑暗中行走的抗爭者 (2017-12-12)

端傳媒 | 中國大數據四問：官商民集體狂歡的背後，「數據利維坦」正在降臨？ (2018-02-21)

端傳媒 | 異鄉人——竺晶瑩：從「盛世」中出走，那些與我同行的中國年輕人 (2018-03-16)

端傳媒 | 江雪：微信個人帳號被封記 (2018-04-10)

端傳媒 | 大數據權利之爭：對不起，你的數據屬於你，但我們有權使用 (2018-04-17)

風傳媒 | 自由之家：中國國安部門大肆擴張網路管理 迫害維權人士與分享資訊公民 (2019-01-30)

華爾街日報中文網 | 中國科技巨頭的副業：做政府監視的「眼睛」 (2017-12-04)

美國之音 | 報告：警惕中國互聯網管控模式威脅全球信息自由 (2019-02-05)

[紐約時報中文網 | 中國的威權主義未來：人工智能與無孔不入的監控 \(2018-07-10\)](#)

[泡泡 | 老大哥並沒有一直在看，反而比這更可怕——監視之惡（一）你可能還沒完全理解奧威爾](#)

[泡泡 | 為什麼必需拒絕大數據——監視之惡（二）公私監控夥伴關係](#)

[泡泡 | 「冰河」已在你心裡，這就是他們的目的——監視之惡（三）歷史和現實，拆穿謊言](#)

[泡泡 | 可怕的「連點成線」和互聯網審查——監視之惡（四）「反恐」歧途](#)

[泡泡 | 「六行字足夠絞死你」，這不是玩笑——監視之惡（五）數據指控](#)

[泡泡 | 「計算機和狗」之辯，為什麼要批評美國？——監視之惡（六）破解荒唐的狡辯（上）](#)

[泡泡 | 為什麼要求解散國安局？——監視之惡（六）立法監管不可能，應該怎麼辦（下）](#)

[Solidot | 網信辦稱互聯網需要秩序 \(2017-11-17\)](#)

[Solidot | 院士稱 IPv6 時代將真正能實現網絡實名制 \(2017-11-29\)](#)

[Solidot | 每個人都應該對中國計劃中的全面監視感到害怕 \(2018-02-05\)](#)

[Solidot | 數以千計的公司在監視你 \(2018-04-01\)](#)

[Solidot | 中國政府開始部署步態識別技術 \(2018-11-07\)](#)

[Solidot | 加州大學警告教職工和學生在中國不要使用微信 \(2019-01-02\)](#)

[Solidot | 網信辦啓動為期半年的網絡生態治理專項行動 \(2019-01-03\)](#)

[Solidot | 深度學習之父擔心中國的 AI \(2019-02-06\)](#)

網信辦：網絡直播先審後播、加強彈幕實時管理、黑名單須上報 - 中國數字時代 (2016-11-03)

池見新草 | 在告密與監控中慢慢長大：中國學校的日常 - 中國數字時代 (2018-05-22)

後窗工作室 | 被教室天眼掃描的中學生 - 中國數字時代 (2018-05-26)

量子位 | 這是AI? 這是愛? 這是能全方位監控學生的「智能校服」 - 中國數字時代 (2018-12-24)

源點credit | 中國的社會信用體系與公眾輿論 - 中國數字時代 (2019-01-31)

人民日報 | 將彈幕划入先審後播範圍是一大亮點 - 中國數字時代 (2019-02-14)

ZDNet | 中共承包商在新疆記錄維族人行蹤 256萬條個人信息在網上「裸奔」數月 - 中國數字時代 (2019-02-16)

## 第一章 必要的前期準備

### 第一節 獲取美區 Apple ID

#### 一、為什麼需要美區 Apple ID？

- (一) 獲取被下架應用
- (二) 逃離「雲上貴州」

#### 二、換區還是註冊新 ID？

#### 三、如何獲取美區 Apple ID

- (一) 註冊美區 Apple ID 教程
- (二) 中國區 Apple ID 遷移至美區教程
- (三) 如何實現原生 IP 全局代理

#### 四、美區 Apple ID 的日常使用

- (一) 如何使用美區 Apple ID 購買 app
- (二) App Store 快速換區

### 第二節 獲取 Google Voice

#### 一、Google Voice 是什麼？

#### 二、為什麼選擇 Google Voice？

#### 三、Google Voice 號碼的用途

#### 四、如何獲取 Google Voice 號碼？

- (一) Google Voice 號碼申請教程
- (二) Google Voice 號碼購買教程

五、如何長期保留 Google Voice 號碼

六、Google Voice 日常使用

### 第三節 註冊美區 PayPal

一、為什麼需要美區 PayPal ?

二、如何註冊美區 PayPal ?

## 第一節 獲取美區 Apple ID

一、為什麼需要美區 Apple ID ?

### (一) 獲取被下架應用

中國網民廣泛使用虛擬私人網絡 (Virtual Private Network, VPN) 及類似工具來規避 GFW 的封鎖，直接訪問不受審查的國際互聯網。自 2017 年以來中共當局加大了對 VPN 打擊力度。2017 年 1 月 22 日，工信部發佈了《工業和信息化部關於清理規範互聯網網絡接入服務市場的通知》，規定用戶未經主批准不得自行建立或租用 VPN。2017 年 6 月 22 日，知名 VPN 服務商 Green 發佈公告被迫停止服務。2017 年 7 月底，Apple 在中國區 App Store 下架了數百款 VPN 應用，2017 年 11 月 21 日 Apple 回復參議院 Cruz 和 Leahy 的問詢時承認已下架了 674 款 VPN 應用，現在中國用戶必須需要借助其他國家/地區的 Apple ID 登錄外區 App Store 才能獲取 VPN 應用。

除了 VPN 之外，Apple 還在中國區 App Store 下架了紐約時報和 Skype，你同樣只能在外區商店獲取這些應用。

## （二）逃離「雲上貴州」

迫於中國出台的《網絡安全法》要求網絡服務提供者將數據儲存在本地的強制規定，Apple 在 2018 年 2 月底將中國區的 iCloud 服務轉交「雲上貴州」運營。新的 iCloud 隱私條款增加了要求用戶「理解並同意，蘋果公司和雲上貴州有權訪問您在此服務中存儲的所有數據，包括根據適用法律向對方和在彼此之間共享、交換和披露s所有用戶數據（包括內容）的權利。」此舉顯然降低了中國強力部門獲取本國蘋果用戶數據的門檻，

如果你對「雲上貴州」感到不安，那麼你同樣需要一個外區 Apple ID，然後將自己的雲端數據轉移到外區 iCloud 上。

### iCloud 新老用戶條款對比

參見：

- Solidot | iCloud（中國）將由雲上貴州運營
- 中國數字時代 | 【立此存照】iCloud 將由貴州政府掌控國企運營 可訪問所有數據

## 二、換區還是註冊新 ID？

獲取美區 Apple ID 的方式主要有將中國區 Apple ID 遷移至美國區（簡稱「換區」）和註冊新的美區 Apple ID 兩種。

美區 Apple ID 的作用在於下載 VPN 等在中國區商店被下架的應用，並保證你的 iCloud 數據不受中國政府直接控制。Bilibili、網易雲音樂、共享單車類應用和部分遊戲等只供中國區 App Store，如果你有這些應用的使用需求則還需保留中國區 Apple ID。編者建議同時使用中國區、美國區兩個賬號，並將美區 Apple ID 作為主力使用，必要時切換登錄中國區 Apple ID 購買所需的應用。

## 三、如何獲取美區 Apple ID

### （一）註冊美區 Apple ID 教程

- [App Store 註冊美區 Apple ID 帳號終極指南 | archive 存檔](#)
- [91yun | 教程：一步步教你如何註冊美區Apple ID，到美區APP Store下載應用](#)
- [VPNASK: VPN翻牆程序在中國區App Store被蘋果下架，你只需要申請一個美國區Apple ID就可以恢復正常！ | YouTube 視頻教程](#)

## (二) 中國區 Apple ID 遷移至美區教程

### ★[更改 Apple ID 國家或地區- Apple 支持](#)

- [堅果極客：全局代理+原生IP，手機上也能更改Apple ID地區！](#)

## (三) 如何實現原生 IP 全局代理

註冊新 Apple ID 與 Apple ID 換區時都必須提供付款方式，並且僅支持對應國家/地區銀行發行的信用卡或借記卡。以美國為例，只有美國銀行發行的銀行卡才能在美區 App Store 消費，由中國銀行發卡的銀聯+Visa/Mastercard 雙標卡或單標卡是不被支持的。

如果你沒有對應國家的信用卡，必須在註冊或換區時使用對應國家地區原生 IP 全局代理以保證「支付方式」中顯示「None」選項。對於「先有雞還是先有蛋」的問題，下面就不同的場景提供幾種解決方法。

**場景 1：**使用 iPhone 註冊美區 Apple ID，該 iPhone 上已經安裝有可用的 VPN 應用或者 Shadowsocks/V2Ray 客戶端且有可用的節點

**【無需額外步驟】**註冊時打開 VPN / Shadowsocks 客戶端使用全局代理 (Global) 模式即可。

**場景 2：**使用 iPhone 註冊美區 Apple ID，該 iPhone 上未安裝任何可用的 VPN 應用

**解決方法 2.1**

**【下載、使用中國區 VPN 救急】**在中國區 App Store 中搜索「VPN」還能找到漏網之魚，你可以使用提供美國線路的 VPN 服務來救急。

**解決方法 2.2**

請已有美國 VPN/Shadowsocks/V2Ray 節點或者肉身位於美國的 iPhone 用戶代為註冊。

**解決方法 2.3**

如果無法獨立註冊美區 Apple ID 作為過渡，可以考慮在淘寶購買美區 Apple ID 賬號。購買使用此類產品存在風險，建議只用作臨時使用。

#### 四、美區 Apple ID 的日常使用

##### （一）如何使用美區 Apple ID 購買 app

1. 【充值】使用 Visa/Mastercard 雙幣卡在 Apple 官網購買美區 iTunes Gift Card 禮品卡，或者在美國的超市、便利店購買實體禮品卡進行充值。

\*注意是用於 iTunes 和 App Store 的禮品卡，勿將其與購買硬件的 Apple Store 禮品卡混淆。

參見：

- Apprcn：使用雙幣信用卡在蘋果官網購買美區 Gift Card 禮品卡

2. 在淘寶、閒魚等平台購買美區 Gift Card 禮品卡（請盡量選擇小面額卡以規避風險），充值後使用。

3. 家庭共享

4. 找人代付（借助 App Store 的贈送禮品功能）

##### （二）App Store 快速換區

###### 1. 捷徑動作

在 App Store 下載自動化流程應用 捷徑/Shortcuts（原 Workflow）後打開鏈接 AppStore換區 以獲取。

###### 2. Pin - JSBox Lite - 區域切換

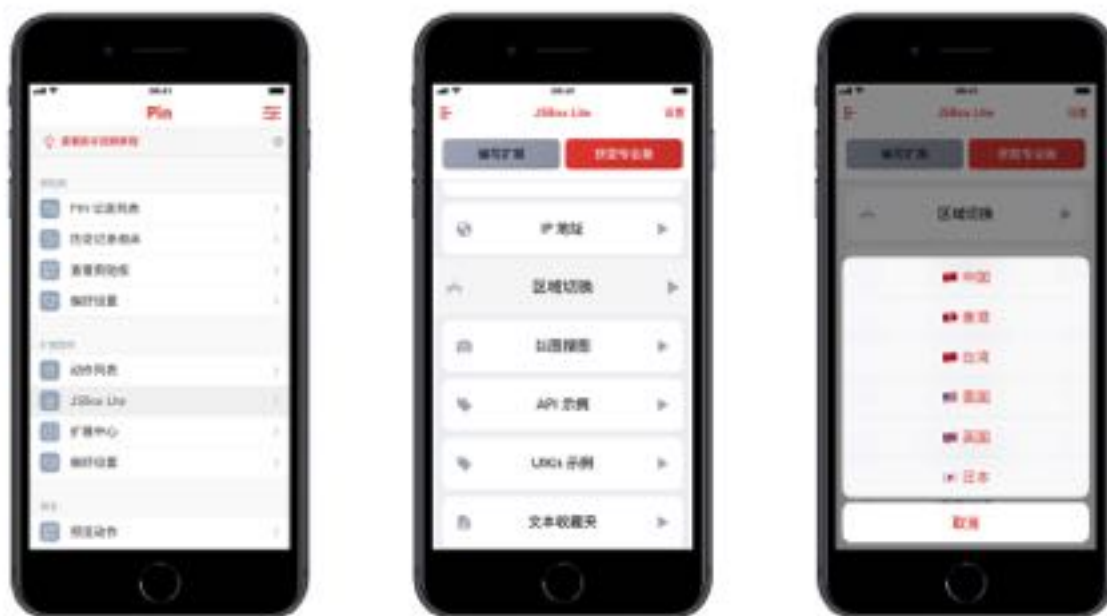
Pin（iOS）¥18 / \$2.99

智能剪貼板應用 Pin 3.0 新上線了「xTeko 實驗室」（現已改名為「JSBox Lite」），支持基於 Javascript 的擴展程序。JSBOX Lite 內置的「商店」提供的「區域切換」擴展支持一鍵切換至中國/香港/台灣/美國/英國/日本區 App Store 商店。

操作方法 1：下拉打開 iOS 通知中心插件 Widget，點按 JSBox Lite 菜單中的「區域切換」進入



操作方法 2: 或進入 Pin 應用, JSBox Lite > 商店 > 工具 > 區域切換 (點按右側的「▶」按鈕以運行)



### 3. JSBox - 區域切換

如果你有能力自行編寫 JavaScript 腳本, 可以考慮購買使用功能更全面的 JSBox。

補充:

1. 可參考 Telegram 頻道 [ShadowrocketNews](#) 以獲取更多 Apple ID 換區及註冊的信息
2. 強烈建議在註冊 Apple ID 時使用 Gmail 等國外郵箱作為賬號。
3. 如果你已經下載了 VPN 應用並打算繼續使用中國區 Apple ID, 你可以通過以下兩種方法在不換區/不切換 Apple ID 的前提下更新中國區已下架的 VPN 應用:

方法1. 【卸載、重裝應用】(僅適用於運行 iOS 11 及以上系統的設備) 設置 > 通用 > iPhone/iPad 儲存空間 > (全部顯示) > 選中需要更新的應用 > 卸載應用 (Offload App) > 重新安裝應用  
參見 [iOS 11 免換區更新其它區或已下架 App | 一日一技 - 少數派 | archive 存檔](#)

方法2. 【iMazing】在 Mac/Windows PC 上下載使用 iMazing 獲取已下架應用的 IPA (iMazing 可以理解為 iTunes 的第三方客戶端)

以下教程來自 Telegram 頻道「Shadowrocket News」, 原鏈接 <https://t.me/ShadowrocketNews/199>

iMazing 下載 IPA 教程 (編者注: 以 Shadowrocket 為例)

使用 iMazing 進行下載安裝 (<https://imazing.com>)

1. 下載安裝 iMazing, 試用即可
2. 連接手機

3. 在左側找到 Apps
4. 點擊 Manage Apps 按鈕
5. 確認右上角的 Apple ID 為 Shadowrocket 的購買 ID，不是的話選擇 Log Out 重新登錄
6. 選擇 Add from App Store
7. 搜索關鍵字 Shadowrocket 下載並安裝

方法3. 【TestFlight】使用應用的 TestFlight（簡稱「TF」）版本也可以實現不切換 Apple ID 使用最新版應用。

## 第二節 獲取 Google Voice

\* Google Voice 號碼是為之後註冊 Telegram 準備的，並非必需品。如果你已經擁有境外號碼可以跳過本節內容。

### 一、Google Voice 是什麼？

Google Voice 是由 Google 推出的 VoIP 服務，它允許用戶使用 Google 提供的免費號碼或付費指定的號碼來集成用戶個人的眾多電話號碼，並在美國和加拿大提供的免費語音通話和短信服務。

### 二、為什麼選擇 Google Voice？

Google Voice 的優勢在於支持免費、長期保留號碼。

TextNow 等虛擬號碼服務只提供臨時號碼。Telegram 每次登錄賬戶都需要接收短信驗證碼，如果你使用臨時性虛擬號碼或者出境時購買的臨時電話卡號碼註冊 Telegram，當號碼過期被回收或者臨時電話卡到期後你若中途登出 Telegram 賬戶，再次登錄時就會因收不到短信驗證碼而無法登錄。

Voxox、Pinger、FreeTone 等虛擬號碼服務商提供的是訂閱制服務，你可能需要每年支付十幾美元的費用來保留你的虛擬號碼。

參見 Yhio 醬的推文

<https://twitter.com/yh1318447499/status/1077898341193703424?s=12>

「針對最近推友因為綁定+86手機號出現的各種問題 還是要提醒推友們 ①一定不要綁定+86的手機號和國內郵箱，可以綁定Google Voice, Voxox, Pinger, 或者freetone ②開啓登錄兩步驗證 Google驗證器挺好用的 🤖 雖然網絡沒法做到完全匿名，但是咱們還是要盡最大努力保護自己，快到年關了希望推們都平平安安的」

### 三、Google Voice 號碼的用途

1. Google Voice 可用於匿名註冊加密即時通訊應用 Telegram，原理部分會在 Telegram 的章節提及。
2. Google Voice 可作為國外網絡服務的驗證號碼及接受驗證短信，例如美區 PayPal 等。不過 Twitter 等部分網站會識別出 Google Voice 的虛擬號碼屬性，並且不支持將虛擬號碼作為驗證號碼以防止用戶濫用。

### 四、如何獲取 Google Voice 號碼？

獲取 Google Voice 號碼主要有在線申請 Google Voice 號碼和向號碼擁有者付費購買號碼兩種方式。

注：你需要擁有 Google 賬號（Gmail 賬號）才能登錄 Google Voice 服務。建議在手機 Gmail 客戶端應用註冊新賬號以提高成功率，註冊完成後建議立即添加「驗證郵箱」以確保變更代理 IP 後還能正常登錄。

#### （一）Google Voice 號碼申請教程

Google Voice 號碼本身是免費申請的，但隨著用戶數量增多其申請難度也水漲船高。申請時往往會顯示失敗，需要持續點擊不斷嘗試，並可使用鼠標連擊腳本或應用用以輔助申請，但仍不能保證成功申請。如果你長時間嘗試都無法獲取號碼，可以考慮購買一個 Google Voice 號碼。

參見：

- [牆洞說：免費申請 Google Voice 美國電話號碼](#) | [archive 存檔](#)

## (二) Google Voice 號碼購買教程

Google Voice 號碼原本在淘寶平台有售，普通號碼（非靚號）的售價一般在 CNY ¥ 15 - ¥ 20 之間，但此類店鋪不定期會遭到淘寶封殺。

以下是 Telegram 群聊 Google Voice 交流群 的 置頂消息 中提供的幾位賣家：

@BHGchinaboy (JUN LEE)

@daydzcom (北美快運)

@gv\_special (C Y) 主要售賣 gv 靚號

@Googlevoice\_00 (Google Voice)

其他購買渠道請自行搜索。

Google Voice 賣家發送的商品信息一般包含以下要素：Gmail 賬號、Gmail 登錄密碼、驗證郵箱和 Google Voice 號碼。部分賣家允許你修改密碼和驗證郵箱後直接使用；部分賣家需要回收其 Gmail 賬號再利用，會要求你將 Google Voice 號碼移轉到自己的賬戶上。

參見 Google Voice 號碼移轉視頻教程（需翻牆）[Transferring a Google Voice Number](#)

附 Telegram 群聊 Google Voice 交流群 置頂消息 中的部分教程鏈接：

- Google Voice 申請快速入門
- 如何利用腳本輔助申請Google Voice號碼
- 在手機APP上使用GV號收發短信、接撥電話
- 長久保留申請的 Google Voice 號碼
- 谷歌帳號的註冊和如何防止被封
- 謹慎綁定新版谷歌語音
- 在國內如何使用 Google Voice ?
- Google Voice 轉移（此為 Telegram 群聊中的一份 pdf）
- Goolge Voice 申請詳細方法及注意事項
- Google voice註冊美國手機號

## 五、如何長期保留 Google Voice 號碼

Google 會回收超過半年未使用的 Google Voice 號碼，對此你可使用 IFTTT 腳本 Keep Google Voice，令其每月自動撥打你的號碼來起到長期保留 Google Voice 號碼的作用。

IFTTT 是互聯網自動化服務平台，是「if this then that」的首字母縮寫，讀作「ift」（相當於「gift」的「g」不發音）。初次使用 IFTTT 需要註冊，也可以直接使用 Google 或 Facebook 帳戶登錄。

參見：[長久保留申請的 Google Voice 號碼](#)



除 IFTTT 的腳本外，你還可以將自己的 Google Voice 號碼與其他網絡服務相綁定，從而可以定期或者頻繁收到來自該服務商的通知短信，避免號碼被回收。

參見：[印象筆記|科技 NEWS 活躍 Google Voice，防止被回收的方法：定期撥打電話或發短信出去](#)

撥打電話：

- \* 中文播放新聞：+1 (641)793-7058
- \* Apple 軟件升級中心：+1 (888)840 – 8433
- \* 微軟客戶服務：+1 (800)642-7676
- \* 美國之音：+1 (712)775-9189

發送短信：

\* Cloudflare 查 DNS: +1 (833)672-1001

## 六、Google Voice 日常使用

你可以使用 Gmail 郵箱接收來自 Google Voice 的短信消息，無需打開網頁版 Google Voice。

在移動設備上你可以使用谷歌環聊（Hangouts）應用。

參見：

- [數字移民 | 獲取一個美國手機號，Google Voice 攻略全記錄](#) (2018-08-30)

## 第三節 註冊美區 Paypal

### 一、為什麼需要美區 PayPal ?

PayPal 是第三方電子支付平台，類似於中國大陸的支付寶。美國的網絡服務往往需要美國的信用卡和 PayPal 作為支付手段，而美區 PayPal 作為第三方平台支持中國國內的 Visa/Matcard 雙幣信用卡付款，幫助中國用戶走出來沒有美國信用卡可用的窘境。此外使用 PayPal 而非中國國內的支付寶可避免相關交易信息被阿里和 Big Brother 獲取，更利於保護個人人身安全。

美區 PayPal 可用於綁定美區 Apple ID，還可用以支付虛擬專用服務器（VPS）的租賃費用。如果你選擇購買禮品卡為 Apple ID 充值，也不想 VPS 上自行搭建 Shadowsocks/V2Ray 翻牆服務，則沒有必要註冊美區 PayPal，大可略過本小節。

### 二、如何註冊美區 PayPal ?

美區 PayPal 註冊時需要提供美國的手機號碼，這裡可以用到上節的 Google Voice 虛擬號碼。此外註冊過程中並沒有什麼難點。

參見：

- [教程：美區 Apple ID 綁定 Paypal，無需美國信用卡也能買買買](#)（2018-01-11）
- [數字移民 | 教程：美區 Apple ID 綁定 Paypal，無需美國信用卡也能買買買](#)（2018-06-04）

## 第二章 如何突破網絡封鎖

### 第四節 「翻牆」基本原理

#### 第五節 V2Ray

##### 一、V2Ray 簡介

（一）V2Ray 的定位

（二）V2Ray 的優缺點

##### 1. V2Ray 的優勢

##### 2. V2Ray 的缺點

（三）Project V 官網與交流群

（四）V2Ray 獲取渠道

（五）小結

##### 二、如何使用 V2Ray

（一）服務器端

##### 1. 購買 V2Ray 節點

##### 2. 租用 VPS 自建 V2Ray

（二）客戶端

##### 三、捐助支持 Project V

#### 第六節 Shadowsocks

##### 一、Shadowsocks 發展簡史

##### 二、Shadowsocks 與 VPN 的區別

（一）涉及目的

（二）代理模式

（三）流量特徵

#### （四）直觀體驗

### 三、如何使用 Shadowsocks

#### （一）服務器端

1. 購買商業服務
2. 使用共享節點
3. 租用 VPS 自建 Shadowsocks

#### （二）客戶端

1. 客戶端的選擇
2. 客戶端的使用

## 第七節 其他翻牆手段概要與評析

### 一、翻牆手段一覽

### 二、對部分翻牆手段的評析

#### （一）VPN

#### （二）自由門、無界網絡

#### （三）Lantern 藍燈

#### （四）Psiphon 賽風

#### （五）翻牆瀏覽器與瀏覽器插件

#### （六）Tor + Meek

#### （七）Outline

#### （八）Project Fi

### 三、通用翻牆手段難易度匯總

## 第四節 「翻牆」基本原理

「翻牆」的前提是知道「牆」/ GFW 的存在。根據維基百科對「防火長城/ GFW」這一詞條的界定，防火長城（Great Firewall, GFW）是中華人民共和國政府在其互聯網邊界審查系統的統稱。此系統起步於1998年，其英文名稱得自於2002年5月17日Charles R. Smith所寫的一篇關於中國網絡審查的文章《The Great Firewall of China》，取與Great Wall（長城）相諧的效果，簡寫為Great Firewall，縮寫 GFW。隨著使用的拓廣，中文「牆」和英文「GFW」有時也被用作動詞，網友所說的「被牆」即指網站內容被防火長城所屏蔽或者指服務器的通訊被封，「翻牆」也被引申為突破網絡審查瀏覽境內外被屏蔽的網站或使用服務的行為。



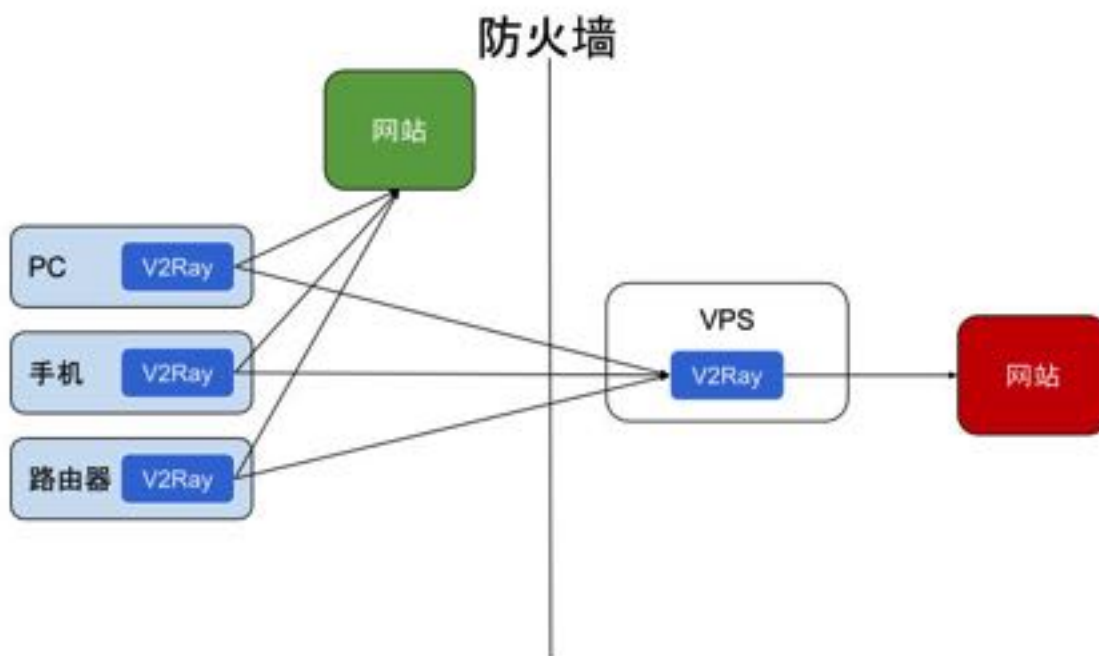
參見：

- 品蔥：防火長城（GFW）的設計原理是什麼？
- 端傳媒：道高一尺，牆高一丈：互聯網封鎖是如何升級的
- 閱後即焚：GFW的前世今生，一部GFW之父方濱興的發家史

被 GFW 屏蔽的網站包括但不限於不受中國政府（或者說是中共）歡迎的網站，具體名單參見 維基百科 - 中華人民共和國被封鎖網站列表、中國數字時代 - 翻牆必讀 - 被牆網站。GreatFire Analyzer 提供網站是否被 GFW 屏蔽的測試。

GFW 並不是實體的牆，而是一系列網絡封鎖手段的統稱，包括「域名解析服務 (DNS) 緩存污染、針對境外的 IP 地址封鎖、IP 地址特定端口封鎖、無狀態 TCP 連接重置、對加密連接的干擾、TCP 關鍵字阻斷、對破網軟件的反制、間歇性完全封鎖、深度包檢測、針對 IPv6 協議的審查、對電子郵件通訊的攔截和網絡攻擊」。

翻牆的方式有數十種之多，但其基本原理不外乎通過連接代理服務器來繞開 GFW 的封鎖（比如你無法訪問谷歌的服務器 A，但你可以直接訪問未被 GFW 屏蔽的境外代理服務器 B，由不受 GFW 之限的 B 訪問 A，然後再將從 A 處取得的數據轉發給你），這一過程中使用的代理模式主要由 Socks、HTTP 和 VPN 三種。關於 GFW 封鎖技術與翻牆手段的演進，推薦閱讀 Project V (V2Ray) 開發者 Victoria Raymond 的 v2ray：簡單介紹一下網絡連接的封鎖與反封鎖 一文。



V2Ray 單服務器模式示意圖

圖片來自 Project V 官網 [原圖地址](#) (已失效)

參見 [Project V - 使用方式 - 工作機制 - 單服務器模式](#)

\*在中國大陸，不少人用「科學上網」來指稱「翻牆」以規避審查，2017 年又新生了「愛國上網」一詞。出於維護言論自由、拒絕自我審查，以及避免「黑話」太多給新人造成困惑的綜合考量，本書通篇採用直白的「翻牆」一詞，特此說明。

## 第五節 V2Ray

## 一、V2Ray 簡介

V2Ray 是一個模塊化的代理軟件包。

### (一) V2Ray 的定位

V2Ray 將自身定位為一個功能強大的平台，而非單純的協議或軟件，它除了自有的 Vmess 協議外還直接支持 Shadowsocks、Socks 等協議。它可以讓使用者自行選擇各種模式和組合，通過不同的設定來達到不同的代理效果，以此對抗變化著的 GFW。

參見：[V2Ray 的模塊化](#)

### (二) V2Ray 的優缺點

參見 [V2Ray 白話文教程 - 前言](#)

#### 1. V2Ray 的優勢：

「(1) 更完善的協議: V2Ray 使用了新的自行研發的 VMess 協議，改正了 Shadowsocks 一些已有的缺點，更難被牆檢測到

(2) 更強大的性能: 網絡性能更好，具體數據可以看 V2Ray 官方博客

(3) 更豐富的功能: 以下是部分 V2Ray 的功能

mKCP: KCP 協議在 V2Ray 上的實現，不必另行安裝 kcptun

動態端口: 動態改變通信的端口，對抗對長時間大流量端口的限速封鎖

路由功能: 可以隨意設定指定數據包的流向，去廣告、反跟蹤都可以

傳出代理: 看名字可能不太好理解，其實差不多可以稱之為多重代理。類似於 Tor 的代理

數據包偽裝: 類似於 Shadowsocks-rss 的混淆，另外對於 mKCP 的數據包也可偽裝，偽裝常見流量，令識別更困難

WebSocket 協議: 可以 PaaS 平台搭建 V2Ray，通過 WebSocket 代理。也可以通過它使用 CDN 中轉，抗封鎖效果更好

Mux: 多路復用，進一步提高科學上網的併發性能」

「VMess協議的特徵是在目前常見協議中最弱的。即如果你認為VMess具有某個特徵，那麼在ss/ssr/其它協議中一定存在同樣或更強的特徵；反之則不然。」

「關於 TLS 混淆，V2Ray 用的是真 TLS，即完全符合 TLS 協議；Shadowsocks 的 obfs 和 ShadowsocksR 的 TLS 混淆用的均為假 TLS，即只模擬了部分 TLS 協議。真 TLS 的優勢是服務器端防探測，第三方用任意的 TLS 數據包探測，V2Ray 都能做出合理的響應，而假 TLS 則帶有明顯的特徵。真 TLS 會有首次連接時進行一個兩次通信(2-rtt)的握手，比起假 TLS 略慢，但之後的連接中，由於使用了緩存，握手不會有性能差異。」

## 2. V2Ray 的缺點

- (1) 配置複雜
- (2) 產業鏈不成熟

### (三) Project V 官網與交流群

官網: <https://www.v2ray.com/>

公告: <https://t.me/v2msg>

吹水: <https://t.me/joinchat/AAAAAEIYaH-hjDDZS716jg>

使用: <https://t.me/projectv2ray>

開發: <https://t.me/joinchat/DNcazUMxm77Jt0LQuwiGAQ>

推特: <https://twitter.com/projectv2ray>

Telegram 討論組規則見: [https://www.v2ray.com/chapter\\_00/tg.html](https://www.v2ray.com/chapter_00/tg.html)

### (四) V2Ray 獲取渠道

Github Release: [github.com/v2ray/v2ray-core](https://github.com/v2ray/v2ray-core)

IPFS: [/ipns/QmdtMuAhEUPFX9NQiGhRj2zhS1oEA76SXNDnZRHqivjMwR](https://ipns/QmdtMuAhEUPFX9NQiGhRj2zhS1oEA76SXNDnZRHqivjMwR)

IPFS 分流: <https://v2ray.com/download>

### (五) 小結

V2Ray 可能是目前最具前景的翻牆手段，但它對於那些沒有 Linux 基礎或者 VPS 使用經驗的入門者難度相對較高。如果你看完本節、Project V 官網和白話文教程後仍然一頭霧水，建議先閱讀 HyperApp 的相關教程，借助 HyperApp 部署 V2Ray。

HyperApp 是 iOS 平台上一個基於 SSH 和 Docker 的自動化部署工具，允許用戶在圖形化界面下將應用一鍵部署到 VSP 上，詳見 HyperApp 用戶文檔：<https://www.hyperapp.fun>。

注：Project V 與 V2Ray 的關係：V2Ray 升級到 3.0 後正式擴展為 Project V，除了 V2Ray 本身之外，Project V 包含所有 V2Ray 的周邊產品，包括客戶端、配置工具等。

## 二、如何使用 V2Ray

### （一）服務器端

#### 1. 購買 V2Ray 節點

經營 V2Ray 的服務商正在不斷湧現，但目前的數量較為有限，產業規模尚不及 Shadowsocks 及其衍生協議。以下 V2Ray 服務商信息引自 [Project V 官網 - 一些推廣](#)（最後一次訪問於 2019 年 2 月 1 日）：

##### BabyDriver

支持 V2Ray 的 VPN 服務。優惠碼：bcb518

##### 喵帕斯

V2Ray 小範圍內測中。

##### 藍岸

基於 V2Ray 的網絡加速服務。優惠碼：v2ray

##### 多數派

基於 V2RAY 的全新的網絡加速服務

##### V2rayPro

基於 V2Ray 的網絡加速服務。專屬優惠碼：v2ray.com

#### vProxy

由 V2Ray 驅動的網絡加速器。專屬優惠碼：v2ray.cool

#### 棲息地

對內小眾的 V2ray 優質網絡加速服務。邀請碼：V2RAY

#### NicoNode

支持 V2Ray 的網絡加速改善服務。專屬促銷代碼：V2RAYNOW

#### V2Net

## 2. 租用 VPS 自建 V2Ray

### (1) VPS 簡介

VPS 是 Virtual Private Server 的縮寫，中文名稱是虛擬專用服務器，指將一台服務器分區成多個虛擬專享服務器的服務。本文主要介紹將 VPS 用作代理服務器用於翻牆，此外 VPS 還具有搭建博客、私人雲盤等諸多用途。

常見的 VPS 廠商有：GCP（Google Cloud Platform，提供為期一年、價值\$300的免費試用）、AWS、Vultr、Linode、Bandwagon、DigitalOcean 等。

VPS 的選擇和入門教程可參考：

- [HyperApp 用戶文檔 - 各雲廠商使用教程](#)
- [HyperApp 用戶文檔 - 愛國軟件 - 科學上網綜述](#)
- [HostAdvice: 2018最佳VPS主機公司](#)

\*Bandwagon 等 VPS 廠商現已支持使用支付寶付款，安全起見還是建議使用 PayPal 等不受國內直接監管的支付手段作為付款方式。

購買 VPS 後建議先測試能否在國內直接連接這台 VPS，為此你需要一個 SSH 客戶端。如果你使用 Linux 或 macOS 操作系統，你可以直接使用系統自帶的「終端」應用；如果你使用 Windows，你需要下載 SSH 客戶端應用，常見的有 Xshell、PuTTY、KiTTY、MobaXterm、mRemoteNG、Bitvise SSH 客戶端（更多參見：[維基百科 - SSH 客戶端比較](#)）；在 iOS 設備上可以使用 SSH 客戶端 Terminus 來操作 VPS。

以「終端」應用為例，先關閉 VPN 或 Shadowsocks 等代理工具，在「終端」中輸入以下字符後回車：

```
ping 你的 VPS IP #例如 00.00.00.00
```

注：「#」後的內容是注釋，不會作為命令代碼運行，下同

如果能接收數據則證明能夠直連，之後可按下「Control+C」來中止這一進程。如果不能直連則說明該 IP 可能已被 GFW 屏蔽，建議將其註銷另租一台。

## (2) 常用 Linux 命令

### ① 遠程登錄 Linux 主機 / VPS

遠程登錄和操作 VPS 同樣需要用到 SSH 客戶端應用。以「終端」為例，下同。

輸入以下字符後回車：

```
ssh root@你的 VPS IP #例如 00.00.00.00
```

初次登陸可能需要在 (yes/no) 選項下輸入「yes」，然後輸入你的 VPS 登錄密碼（VPS 網頁中獲取），需要注意的是此時輸入的密碼在應用界面下並不可見，輸入完畢後回車，如果密碼無誤即可成功登錄。

### ② 退出登陸

輸入「exit」後回車

### ③ 使用 cd 前往指定目錄

輸入 cd + 目錄，例如：

```
cd /etc/v2ray/
```

需要退出 cd 時輸入「cd」後回車即可。

### ④ 使用 vim 或 vi 修改配置文件

以 V2Ray 為例，輸入「vim config.json」進入 vim 界面。vim 界面下不能直接編輯配置文件，但可以通過連擊「D」鍵刪除光標所在行。如需修改或插入內容，需要依次按「esc」、「I」和「Enter」鍵進入可編輯的「Insert」模式（底部會出現 Insert 字樣），之後你可以之後修改，或者將所有內容刪除後粘貼已經在其他編輯器中寫好的配置信息，完成後按「esc」鍵退出「Insert」模式。輸入「:w」後回車以保存，輸入「:q」回車退出，也可以輸入「:wq」回車一步到位。

## (3) 如何部署 V2Ray 服務器端

如果你選擇使用 HyperApp 搭建 V2Ray，請參考：  
[HyperApp 用戶手冊 - 愛國軟件 - V2Ray](#)

如果在 Linux 下部署，請參考以下教程：

- [Project V - 下載安裝](#) - [Project V - 新手上路](#)
- [V2Ray 白話文教程](#)

① 使用 SSH 登錄 VPS，輸入：

```
ssh root@00.00.00.00 #你的服務器 IP
```

② 修改時間

使用 Vmess 協議必須保證本地和服務器端的時間差不超過一分鐘，因此需要修改 VPS 的系統時間：

```
rm -rf /etc/localtime #先刪除默認的時區設置
```

```
ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime #替換上海作為默認
```

或者使用「date --set」：

```
sudo date --set="2018-01-01 00:00:00"
```

查看時間：

```
date -R
```

③ 使用 Linux 腳本安裝 V2Ray（更新 v2ray-core 時同樣使用此腳本）

```
bash <(curl -L -s https://install.direct/go.sh)
```

此部分請參考：[Project V - 下載安裝](#)

運行 `service v2ray start` 來啟動 V2Ray 進程，使用 `service v2ray start|stop|status|reload|restart|force-reload` 控制 V2Ray 的運行

④ 編輯配置文件

```
cd /etc/v2ray/  
vim config.json
```

參考上文 vim 的用法編輯你的配置文件，輸入「:wq」回車來保存和退出。



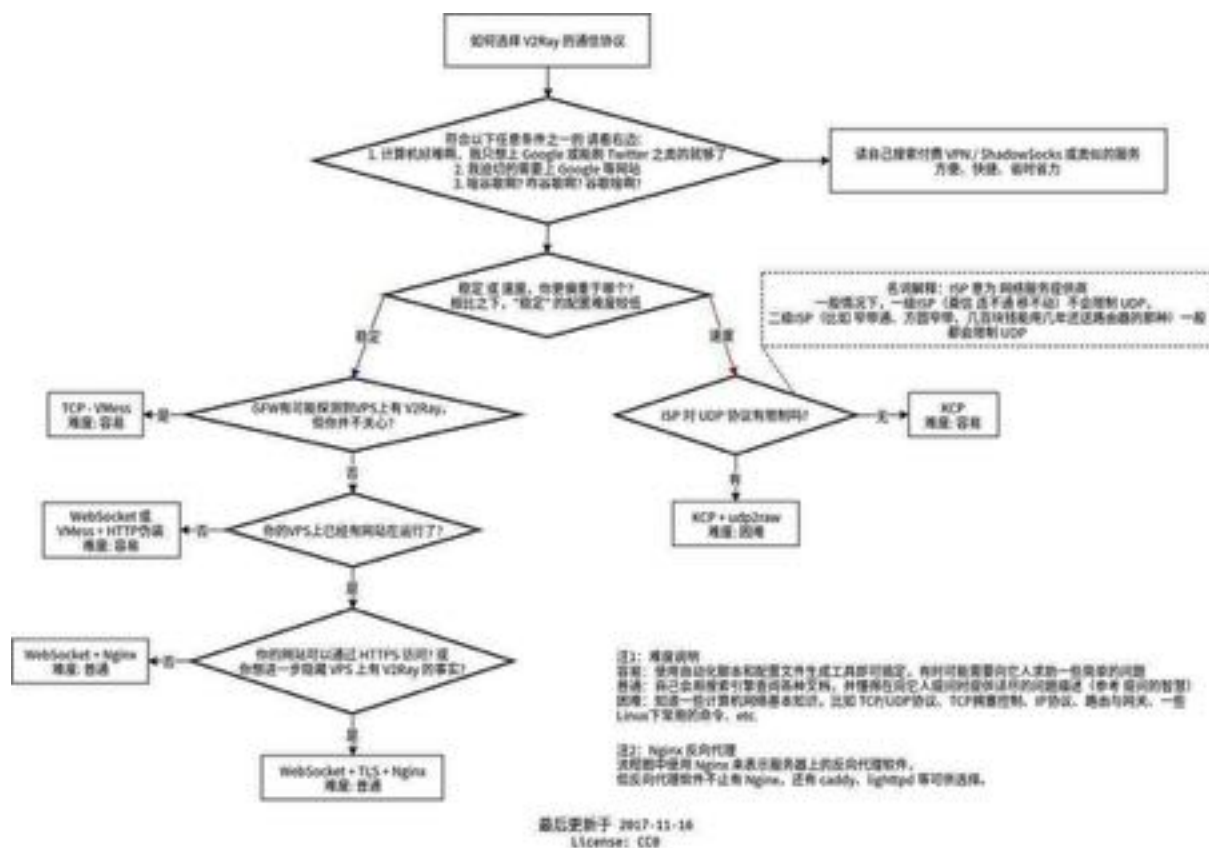
### ⑤ 重啓 V2Ray 並查看是否正常運行

```
systemctl restart v2ray  
systemctl status v2ray
```

如果顯示紅色的 failed 表明你的配置有誤，V2Ray 無法正常運營。V2Ray 本身提供了檢查功能，輸入：

```
usr/bin/v2ray/v2ray -test -config /etc/v2ray/config.json
```

來檢測 config.json 是否有誤。



[https://raw.githubusercontent.com/KiriKira/vTemplate/master/How\\_To\\_Choose.jpg](https://raw.githubusercontent.com/KiriKira/vTemplate/master/How_To_Choose.jpg)

關於 V2Ray 的模式選擇，可以參考上圖。Vmess 裸奔的難度最低，可參考 Project V - 新手上路。（事實上 Vmess 協議本身的強度已經足夠了，如果擔心 VPS 的 IP 被 GFW 屏蔽可以購買 CDN 加速服務隱藏真實 IP，具體方法請自行搜索）

TCP + TLS 可以參考 白話文教程 - TLS。使用 TLS 需要域名和 SSL 證書，域名可以從 Freenom 免費獲取，或者從 Namecheap 購買廉價域名；SSL 證書可由 acme.sh、Caddy、Nginx、certbot 等應用自動註冊，詳見 VINGA：免費獲取個人專屬頂級域名、白話文教程 - TLS（購買域名後需要添加一個 A 記錄指向 VPS 的 IP，之後若 ping 域名可

以 ping 通且顯示 VPS 的真實 IP 則表明域名已經解析成功）。WS+TLS+Web 可能是目前最好的模式，但難度也相對較高，新手可以借助 HyperApp 來輔助搭建。

關於 V2Ray 使用教程的選擇，建議先看懂 Project V 官網和白話文教程，如有需要再搭配其他博客上的教程和配置模板。對於後者，編者建議認准同一份教程，因為不同作者採用的方法和使用配置文件之間存在差異，對新手而言同時參考多份教程可能會使你的思路越來越混亂。

如果在配置過程遇到問題，建議先自行搜索相關信息，在 Github 上查看 v2ray-core 已有的 Issue，或者在 Telegram 群組 [Project V（使用與反饋）](#) 中搜索英文關鍵字查看聊天記錄中的類似問題。如果問題仍未解決，可以在該群組中提問，或者參照模板在 Github 上提交 issue。

相關工具：

- [V2Ray 配置生成器](#)

其他教程：

- [KIRIKIRA.MOE](#)

- [Kiri | 五分鐘入門V2Ray](#)

- [Kiri | 鏈式代理與透明代理：V2Ray 的進階用法](#)

★ [YEARLINY | V2Ray完全使用教程](#)

- [IVY SEEDS - 科學愛國 - V2Ray](#)

- [abccit: 安裝 V2Ray 配置 WebSocket+Nginx+TLS](#)

- [科學上網翻牆教程：搭建V2Ray翻牆](#)

★ [YouTube | 劉偉教程：零基礎手把手教你搭建V2ray翻牆Linux/Windows/MacOS/安卓/蘋果](#)（如果你是 VPS 和 Linux 新手，可以在 YouTube 上搜索、觀看相對直觀的視頻教程來加深瞭解）

關於 V2Ray 的常見問題可以在私聊模式下向 Telegram bot [Kiray](#) (a V2Ray FQA bot by Kiri, username: @kiraybot) 提問，該 bot 目前收錄了 36 個問題（最後一次訪問於 2018 年 5 月 29 日），可以以 Q&A 的形式呈現答案。請勿在群組中使用該 bot，以免刷屏給其他成員造成困擾。

## (二) 客戶端

V2Ray 客戶端

macOS: [V2RayX](#)、[V2RayU](#)、[V2RayC](#)、[ClashX](#)

iOS: [Kitsunebi](#)、[Kitsunebi Lite](#)、[i2Ray](#)、[Shadowrocket](#)、[Pepi](#)、[Quantumult](#)

Android: [BifrostV](#) (PlayStore)、[V2RayNG](#) (PlayStore) 等

Windows: [V2RayW](#)、[V2RayN](#)、[V2RayS](#) 等

★ 參見: [Project V - 神一樣的工具](#) (最後一次訪問於 2019 年 2 月 10 日)

\* iOS 客戶端 Kitsunebi 和 i2Ray 均使用了 V2Ray Core

如果你使用 Kitsunebi，可以根據你對服務器端配置，參考 Kitsunebi 內置測試服務器的 TCP、WS、WSS、H2 和 KCP 五種模式的節點信息來填寫添加。其他平台的圖形化客戶端的配置方法與之基本相同。

以 Project V 官網上「新手上路」教程為例，在客戶端添加節點信息時，協議類型 (Type) 選擇「Vmess」，地址 (Address) 填寫自己 VPS 的 IP 或域名，端口 (Port) 填「10086」，UUID 與服務器端保持一致，加密方式 (Security) 填「chacha20-poly1305」，傳輸協議 (Network) 選擇「tcp」。

## 三、捐助支持 Project V

[Project V 捐助支持](#)

比特幣 (BTC): [15dQnC9yvX6JJXaFkP9MiRYvJS3FvsqvKW](#)

比特現金 (BCH): [1NNRgpWYD8UX1bkckCEoD6HHpaw98onxa](#)

以太坊 (ETH): [0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e](#)

萊特幣 (LTC): [LVdeH2HkCgGRs8ZEpan7fkAEEPbiJ4McoR](#)

門羅幣 (XMR):

[48kA4NyLRCWQvB7U2A77G66Z25uWbyzmoZSYjxJfrMR1J4dRfW6fWFLDn3wirAqP8ySnR4rnvoXWxfkNFhrK5ZxY1WyBqKg](#)

EOS: 0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e

嫩模幣 (OMG): 0x196b695ce3b44c4bd16fe43981bcc908a6a09c2e

貢獻你的 CPU

## 第六節 Shadowsocks

Shadowsocks，簡稱 ss，既指基於 Socks5 代理方式的加密傳輸協議，也指實現 Shadowsocks 協議的各種傳輸包，是中國大陸最為流行的翻牆工具之一。

### 一、Shadowsocks 發展簡史

Shadowsocks 是 clowwindy 開發的翻牆軟件，經推廣後因過於火爆引起了公安的關注，作者 clowwindy 被警方約談後迫於壓力於 2015 年 8 月 22 日在 Github 上刪除了 Shadowsocks 項目的全部代碼並停止開發。

破娃醬 (breakwa11) 接手開發了 ShdowsocksR（簡稱 SSR）分支，在原版 Shdowsocks 基礎上提高了安全性並加入了混淆。2017 年 7 月 27 日，breakwa11 遭到自稱「ESU.TV」的不明身份人士的人身攻擊，對方宣稱如果不停止開發 SSR 將公開更多包含個人隱私的資料。breakwa11 稱遭對方人肉的是無關人士，為了防止對方繼續傷害無關人士將刪除 SSR 在 GitHub 上的所有代碼、停止維護 ShadowsocksR 項目並解散相關 Telegram 交流群組。之後 Akkariiin 宣佈接手 SSR 項目並在此基礎上開發 ShadowsocksRR 分支。其他較為知名的 Shadowsocks 分支還有 Shadowsocks-libev, ShadowsocksR-python, Shadowsocks-python, Shadowsocks-go, libQtShadowsocks 等。

### 二、Shadowsocks 與 VPN 的區別

Shadowsocks 與 VPN 都被用於翻牆，常有人把 Shadowsocks 與 VPN 混為一談，但事實上兩者並不是一回事——Shadowsocks 是加密版的 Socks，而前文中已經提到 Socks 是與 VPN、HTTP 相並列的代理模式。此外 Shadowsocks 與 VPN 的區別還在於：

### （一）設計目的

Shadowsocks 的初衷就是突破網絡封鎖，而 VPN 原本的用途是保障惡劣網絡環境下的通信安全。因此 VPN 在世界範圍內被廣泛使用，而只有在中國大陸、伊朗、土耳其等存在嚴格網絡管制的地區被用於突破網絡封鎖。

### （二）代理模式

Shadowsocks 可以實現智能分流，即訪問被 GFW 屏蔽的網址時由代理服務器轉發數據，訪問牆內網址時直連；也可開啓全局代理，讓所有的流量都走代理；此外用戶可以自行修改 Shadowsocks 的配置文件，根據自身需要添加規則，實現屏蔽廣告等功能。VPN 默認全局代理，即開啓後所有流量都會被傳輸到海外服務器，只有極少數 VPN 服務提供智能分流功能。

### （三）流量特徵

VPN 的流量特徵很明顯，GFW 已經實現對 PPTP、IPSec、L2TP 等 VPN 協議的精確識別，因而完全可以在黨代會、兩會、六四等具有政治敏感性的時間點上屏蔽所有 VPN 流量。就 Shadowsocks 而言，其流量特徵明顯弱於 VPN，GFW 仍可以通過機器學習加以識別。目前基本可以精確識別原版 Shadowsocks 協議，不過後續演化的 Shadowsocks 的流量特徵會隨著加密協議和混淆協議組合的不同而呈現不同的樣態，GFW 尚無能力探測和屏蔽所有的 Shadowsocks 流量，目前主要採取批量封殺服務器 IP 段這樣盲目粗暴的方法來對付 Shadowsocks。

### （四）直觀體驗

1. Shadowsocks 的連接速度快於 VPN

2. Shadowsocks 的穩定性優於 VPN

Shadowsocks 連接以後基本不會出現斷線，VPN 在網絡質量不佳的情況下很容易出現斷線。在長時間待機後喚醒的場景下，Shadowsocks 還能保持連接狀態，VPN 基本會斷線，需用戶手動打開開關重連。

3. Shadowsocks 可實現智能分流，可以無縫突破 GFW 的封鎖快速訪問國際互聯網。VPN 默認全局代理，在使用微信等牆內服務時網速會明顯變慢。

4. Shadowsocks 的 iOS 客戶端大多支持隱藏 VPN 圖標的功能（iOS 平台上的 Shadowsocks 客戶端應用調用了 Network Extension 接口，在連接 Shadowsocks 後頂欄也會顯示「VPN」圖標），可以避免你在分享手機截圖或在人多眼雜的場所連接 Shadowsocks 時顯示 VPN 圖標。VPN 應用基本不提供隱藏 VPN 圖標的功能。

### 三、如何使用 Shadowsocks

Shadowsocks 分為服務器端和客戶端兩部分，像 Shadowrocket 這樣的 Shadowsocks 客戶端本身只是一個空殼，必須手動導入 Shadowsocks 的服務器節點信息後才能連接使用。就這點而言 Shadowsocks 和 VPN 很不一樣，VPN 軟件基本採用客戶端應用內置服務的模式，用戶下載 VPN 客戶端並購買服務後打開 VPN 開關就可連接。

#### （一）服務器端

獲取 Shadowsocks 節點的方式主要有以下幾種：

1. 購買 Shadowsocks 服務商（也稱「機場」、「梯子商」）提供的服務
2. 使用他人自建或購買後共享的 Shadowsocks 節點
3. 租用 VPS 自建 Shadowsocks

#### 1. 購買商業服務


購買現成 Shadowsocks 服務的好處在於 Shadowsocks 服務商往往提供十幾條到幾十條不等的線路，在服務器所在國的選擇上更多樣，萬一有線路被封也有回旋餘地。同時 Shadowsocks 服務商持續提供技術保障，保證網速；其議價能力較強，在更換代理服務器上更有效率。此外部分廠商會提供 BGP 線路，即在連接境外代理服務器先連國內的中繼服務器作中轉，有利於規避 GFW 的封鎖。

Shadowsocks 服務商有 [喵帕斯](#)、[rixCloud](#)、[RfcNetwork](#)、[熊貓翻滾](#) 等（請自行 Google 獲取更多廠商信息及服務評價）。筆者不推薦從個人賣家處購買 Shadowsocks 服務，更不要從在 QQ 群、Telegram 群聊中兜售服務的個人賣家處購買服務，以免上當受騙。

參見 [聰聰：SS/SSR 簡介 - 介紹](#)

#### 2. 使用共享節點

使用共享節點的最大好處是幾乎零成本，但弊端也顯而易見——眾多用戶使用同一個節點勢必導致低網速，使用體驗不佳；同時也容易招致 GFW 的封殺，必須更換新的節點，穩定性無法保證。

Telegram 上有 [V2ray,SSR 節點最新發佈](#)、[360 互聯網安全中心](#) 等發佈共享 Shadowsocks、V2Ray 節點信息的頻道。更多關於提供共享 Shadowsocks 節點的渠道請自行搜索。

以 [V2ray,SSR 節點最新發佈](#) 提供的 SSR 節點為例，複製 URL 「ssr://xxxx……xxxx」後打開 Shadowsocks 客戶端即可自動導入節點信息。

更多共享節點：

「免費 SS 賬號分享（能不能用，能用多久我就不確定了）

<https://free-ss.site>

<https://ss.freess.org>

<https://doub.io/sszhfx>

<https://us.ishadowx.net>

[https://tool.ssrshare.us/tool/free\\_ssr](https://tool.ssrshare.us/tool/free_ssr)

SSR 免費節點訂閱地址(PS：至於節點能不能用我就知道了，別人分享的)

<https://github.com/ImLaoD/sub/raw/master/ssrshare.com>

[https://github.com/ImLaoD/sub/raw/master/v2ray\\_ssrshare.com](https://github.com/ImLaoD/sub/raw/master/v2ray_ssrshare.com)

<https://yzzz.ml/freessr>

」

—— 聰聰：SS/SSR 簡介 - 介紹

### 3. 租用 VPS 自建 Shadowsocks

「自建和購買商業服務對比有什麼優勢？

最主要的優勢是隱私和安全，如果你看下上面 Shadowsocks 的日誌，你就知道服務商可以知道你的所有瀏覽歷史的，如果你訪問了不支持 HTTPS 的網站，那麼請求內容也可能被監控（比如密碼信息）。

另外是質量和成本，很多商家是使用和上面同樣的機器但是賣給幾百個人，你應該能明白了。成本方面沒有免費試用的話1個人用可能會有點貴，但如果和朋友家人一起用就超值了，比如使用 \$2.5/月的 Vultr，每月500G 流量夠很多人用的。」

網絡上可以檢索到大量的 Shadowsocks(R) 一鍵安裝腳本。如果你不會使用 Linux 系統，可以借助 iOS 平台上的 HyperApp 應用在圖形用戶界面下配置安裝各類 Shadowsocks 的服務端。

參見：

★ HyperApp 用戶文檔 - 愛國軟件 - SSR

由 HyperApp 用戶上傳的視頻教程：[YouTube | 五分鐘快速建立vpn，可全程手機操作，方便快捷的一款強大軟件hyperapp之ssr教程（需翻牆）](#)

## （二）客戶端

### 1. 客戶端的選擇

#### （1）iOS

##### Shadowrocket

物美價廉的 Shadowsocks 客戶端，俗稱「小火箭」，支持 Shadowsocks、ShadowsocksR、Vmess 等多個協議。美區售價 \$ 2.99（CNY ¥18），中國區已下架。

##### Quantumult

新生代 Shadowsocks 客戶端，TF 版支持 Vmess 協議。美區售價 \$ 4.99（CNY ¥30）中國區已下架。

參見：

落格博客：談談 Shadowrocket 和 Quantumult

##### Patatso 2

##### Patatso Lite

中國區已下架。輕量版的 Patatso，能滿足基本的使用需求，不支持 Vmess。

##### Surge 3

美區售價 \$ 49.99（¥ 328）



不建議普通用戶購買 Surge。Surge 除去 Shadowsocks 客戶端外還有開發者調試工具的面向，如果你沒有這方面的需求則大可選擇相對便宜的應用。（注：Surge 不支持 ShadowsocksR 協議）

iOS 3 Pro Personal License \$ 49.99 ( Surge 官網)

## (2) macOS

ShadowsocksX-NG-R

ShadowsocksX-NG

Surge for Mac

Standard License ( 1 device ) \$ 49.99

Pro License ( 3 devices ) \$ 69.99

Mega License ( 5 devices ) \$ 99.99

★更多 Shadowsocks 客戶端參見 聰聰：SS/SSR 簡介 - 客戶端

## 2. 客戶端的使用

Shadowsocks 客戶端的使用方法基本相同——添加節點信息 > 選擇協議類型（例如 Shadowsocks、ShadowsocksR、Socks5 等），填寫主機 IP、端口、密碼、加密方式、混淆協議及標籤等。部分 Shadowsocks 服務商支持像客戶端應用一鍵導入節點信息。

Shadowsocks 服務商往往會提供客戶端的使用教程。

參見：

- 少數派：Shadowrocket 入門使用教程 | archive 此教程寫作時間較早，仍可作參考。

## 第七節 其他翻牆手段概要與評析

### 一、翻牆手段一覽

1. VPN (包括 pptp, l2tp, sstp, ipsec, anyconnect, IKEv2, Open VPN 協議)

2. Lantern (藍燈)

3. Psiphon (賽風)

4. GAE (包括 GoAgent, xx-net, GoProxy)
5. Shadowsocks
6. ShadowsocksR
7. Hosts
10. 自由門
11. VPN Gate
12. 無界
13. V2Ray
14. 瀏覽器翻牆插件
15. 翻牆瀏覽器
16. 路由器透明代理
17. 瀏覽器一鍵包
18. 螢火蟲代理
19. SSH
20. Meek + Tor
21. 肉翻
22. 在線網頁代理
24. obfs4
25. GFWPress

上述內容參考了 ShadowsocksR 開發者 breakwa11 在其 Telegram 頻道（現名「ShadowsocksR已停止更新」）發佈的科學上網方式佔有率調查統計結果。

## 二、對部分翻牆手段的評析

### （一）VPN

與 V2Ray 和 Shadowsocks 相比，VPN 固然顯得遜色，但操作簡單不失為其優點——用戶只需下載客戶端一鍵連接即可，便於入門者上手。GFW 已經可以有效識別、封殺各類 VPN 協議，但也不是那麼絕對，因為 VPN 本身也在進化，比如知名 VPN 廠商 Golden Frog 開發的 VyprVPN。

VyprVPN 的特色在於其專有的 Chameleon（變色龍）協議（僅限高級賬戶，暫不支持 iOS），原理是在 OpenVPN 協議的基礎上加入混淆以對抗深度包檢測 (DPI) 技術，使其 VPN 服務在中國、伊朗、土耳其等存在網絡封鎖的地區能夠正常使用。除 VyprVPN 外，ExpressVPN 和 PUREVPN 也是網絡排名較為靠前的 VPN，這三款 VPN 的客戶端都覆蓋全平台。

## 其他推薦 VPN 服務

「推薦以下這些 VPN 服務，它們都不在美國境內、都使用加密，並且接受 Bitcoin 付款，支持 OpenVPN 而且採用不記錄用戶活動的政策：

[AirVPN](#)，位於意大利，162 台服務器；[AzireVPN](#)，瑞典，5 台服務器；[Cryptostorm](#)，冰島，18 台服務器；[EarthVPN](#)，北塞浦路斯，432 台服務器；[ExpressVPN](#)，維京群島，145 台服務器；[FrootVPN](#)，瑞典，27 台服務器；[hide.me](#)，馬來西亞，88 台服務器；[IVPN.net](#)，直布羅陀，21 台服務器；[Mullvad VPN](#)，瑞典，168 台服務器；[NordVPN.com](#)，巴拿馬，475 台服務器；[OVPN.com](#)，瑞典，39 台服務器；[Perfect-Privacy.com](#)，巴拿馬，41 台服務器；[ProtonVPN.com](#)，瑞士，112 台服務器；[Proxy.sh](#)，塞舌爾，300 台服務器，[Trust.Zone](#)，塞舌爾，48 台服務器；[VPNTunnel.com](#)，塞舌爾，80 台服務器。

⚠️ 挑選 VPN 提供商的標準：在美國境外或其它五眼聯盟以外的國家營運；避免挑選以英國和美國為基地的服務商；支持 OpenVPN 軟件；接受比特幣、現金、借記卡或現金卡等付款方式；註冊帳號時不會要求提供個人信息，只需填用戶名稱、密碼與電子郵件即可。

另外一個標準是 [warrant canary](#)，這是有些組織公佈一份文件來聲明他們在一段特定期間內，並未接到任何秘密的官方命令。如果這份文件未能及時定期更新，那麼用戶可以假設該組織可能收到了不可公開的秘密傳票，此時應該停止使用他們提供的網絡服務。

你可以在這裡看到擁有 [warrant canary](#) 的公司和組織；在[這裡](#)查看 Bruce Snieper 對權證的批評以及針對 [warrant](#) 的法律案例。」

——[iYouPort | 安全手冊](#)：這裡是你需要的幾乎所有安全上網工具；以及為什麼建議不要使用以美國為基地的網絡服務

注：推薦 VPN 處的超鏈接為本書編者所加。

參見：[iYouPort | 安全手冊](#)：這裡是你需要的幾乎所有安全上網工具；以及為什麼建議不要使用以美國為基地的網絡服務

## （二）自由門、無界網絡

自由門和無界網絡是目前世界範圍內較為流行的翻牆軟件，二者都有法輪功背景，且都沒有開源。

## （三）Lantern 藍燈

Lantern 是一款開源的翻牆軟件，支持 Android、Windows、macOS 和 Linux 平台，iOS 版也在開發中。最新版（4.0版）的 Lantern 提供付費專業版和免費版兩種版本，其中免費版有每月 500 MB 的免費高速流量，超出流量上限後仍可翻牆，但會被限速。

Lantern 打開客戶端即可連網，很好上手；速度和穩定性都優於 Psiphon，適合對翻牆上網需求不高、無力駕馭 Shadowsocks 又不想購買付費 VPN 的新手用戶。關鍵詞「Lantern」已被牆內的百度、必應等搜索引擎封殺，你可以免翻牆通過搭建在 Github 上的 [藍燈官方論壇](#) 獲取最新版客戶端的下載地址。

## （四）Psiphon 賽風

Psiphon 是由加拿大多倫多大學公民實驗室開發的開源免費翻牆軟件，最新的 Psiphon 3 綜合使用了 VPN、SSH、HTTP 和 Socks 代理技術，支持 Android、Windows 和 iOS 平台。VOA 與 BBC 中文網都將 Psiphon 作為其推薦的翻牆方式。值得一提的是 2017 年 10 月初 GFW 為迎接即將到來的中共「十九大」進行了升級，使得當時剛發佈的最新版 Psiphon 與 Lantern 失效，而在此期間 Shadowsocks（包括已停更數月的 ShadowsocksR）與 V2Ray 都安然無恙，可見前二者的抗封鎖能力不及基於 Socks 的代理軟件。

## （五）翻牆瀏覽器與瀏覽器插件

翻牆瀏覽器與瀏覽器插件的局限性顯而易見——它們只能在瀏覽器層面解決翻牆上網問題，面對 Twitter、Telegram 客戶端這樣的軟件就無能為力了。此外，就獲取 Google Chrome 瀏覽器的翻牆插件而言，仍需解決先有雞還是先有蛋的問題——用戶必須先翻牆才能登錄插件商店下載插件。

## (六) Tor + Meek

Tor 瀏覽器是 Tor (The Onion Route, 洋蔥路由器) 項目的旗艦產品，使用多重代理來實現匿名並支持訪問暗網，支持 Windows、macOS、Linux、Unix、BSD、Android 和 iOS 平台。早期的 Tor 因其流量特徵太過明顯，很快就被中國的 GFW 封殺。新版的 Tor 瀏覽器加入了 Meek 流量混淆插件，通過將 Tor 流量偽裝成訪問 Microsoft Azure ~~和 Amazon~~ 雲服務的正常流量來繞過 GFW，使中國用戶得以將 Tor+Meek 這一組合用於翻牆用途。不過使用 Meek 後瀏覽網頁往往會卡頓，用戶體驗不佳。

關於 Tor+Meek 的使用方法，建議閱讀編程隨想撰寫的 [「如何翻牆」系列：掃盲 TOR Browser 7.5——關於 meek 插件的配置、優化、原理](#)

## (七) Outline

「Outline is an open source project created by Jigsaw to provide a safer way for news organizations and journalists to access the internet.」

Outline 是由 Google 旗下的 Jigsaw 開發的旨在為新聞組織和記者提供安全訪問互聯網方式的開源項目。Outline 基於 Shadowsocks，其實質相當於在自己的服務器自建 Shadowsocks 服務。相比於購買 VPN 或 Shadowsocks (R) 服務，Outline 提供的這種方式使用戶享有更高的自主性，基本杜絕了服務商洩露用戶信息的隱患。部署 Outline 所需的操作基本在圖形用戶界面下進行，不過對於長期習慣使用 VPN 的人而言，Outline 的學習成本仍然較高。

Outline 的使用步驟大致是：註冊並訂購 DigitalOcean 的虛擬主機 (VPS) 服務，在 VPS 上安裝 Outline 的服務端，然後在 Outline 客戶端輸入來自服務端的 ss 鏈接就能建立連接。

Outline 沒有像 ShadowsocksR 和 Shadowsock-libev 分支那樣加入混淆插件，而主要通過屏蔽惡意端口掃描、服務器不保留互聯網流量任何日誌等方式來保證安全性與穩定性。此外 Outline 尚不支持智能分流，只有全局代理模式。

Outline Manager（服務器端）支持的操作系統——Linux、Windows、macOS

Outline 客戶端支持的作業系統——Android、Chrome OS、Windows、iOS、macOS

Outline 官網：<https://getoutline.org/en/home>

Outline 搭建與使用教程：[Outline搭建與使用教程-來自與Google合作的工具](#)（僅供參考）

科學上網翻牆教程：[搭建Outline翻牆](#) | [YouTube 視頻教程](#)

## （八）Project Fi

「Project Fi 是 Google 旗下的移動虛擬運營商（MVNO），通過 T-Mobile 和 Sprint 的 Wi-Fi 和蜂窩移動網絡向美國以及超過120個國家的漫遊用戶提供語音及數據服務。」

Google 通過與各國電信運營商合作提供 Project Fi 服務，使用戶出國後無需購買當地 SIM 卡就可直接使用所在國的數據服務。Project Fi 產生的所有連接數據會經過 VPN 加密，因此在中國大陸等網絡封鎖的地區可以實現無縫「翻牆」。使用 Project Fi 服務翻牆的門檻很低，可以推薦給短暫來華訪問的外國友人使用。

Project Fi 最初只適用於 Google Pixel 和 Nexus 系列手機，以及各型支持蜂窩移動網絡功能的平板電腦（包括 iPad），現已擴展至支持 iPhone、三星和一加手機。用戶可在 Project Fi 官網登錄 Google 賬號後輸入所在地區的郵政編碼以檢驗 Project Fi 是否支持該地區。

參見：[Using Project Fi in China: Say goodbye to VPNs](#)

## 三、通用翻牆手段難易度匯總

- 1、使用命令行自建 V2Ray
- 2、使用 HyperApp 自建 V2Ray
- 3、使用 HyperApp 自建 Shadowsocks
- 4、購買 V2Ray/Shadowsocks 服務或使用分享的免費節點
- 5、VPN、Lantern 等客戶端一鍵翻牆

## 第三章 加密即時通訊應用

### 第八節 加密通訊應用概論

- 一、什麼是端對端加密
- 二、常見即時通訊應用的加密方式
- 三、值得推薦的端對端加密 IM

### 第九節 Telegram 使用指南

- 一、Telegram 簡介
- 二、Telegram 客戶端
- 三、註冊
  - (一) 號碼選擇
  - (二) 註冊前提

1. 使用內置代理

2. 獲取內置代理

- (三) 註冊步驟

#### 四、安全性設置

- (一) 隱私設置

1. 黑名單

2. 顯示在線情況

3. 語音通話權限

4. 群組權限

- (二) 安全設置

1. 本地密碼與生物驗證

2. 兩步驗證

3. 當前在線

- (三) 自動銷毀機制

- (四) 通訊錄

1. 通訊錄的功能

2. 同步通訊錄

3. 使用通訊錄進行備注

- (五) 私密模式下的鏈接預覽

#### 五、其他設置

- (一) 個人信息設置

1. 姓名

2. 頭像

3. 簽名

4. 更換號碼

5. 用戶名

6. 退出登錄

7. 小結

- (二) 數據與存儲

- (三) 外觀

- (四) 語言

#### 六、基礎功能

- (一) 普通模式

1. 發送消息類型

2. 編輯

3. 刪除

4. 回復

5. 轉發



(二) 私密模式

(三) Saved Messages

(四) 群聊

1. 創建群組

2. 私有群租與公共群組

3. 普通群組與超級群組

(五) 頻道

(六) 機器人

(七) 貼紙

1. 獲取貼紙

2. 發送貼紙

3. 分享貼紙

(八) GIF

1. 發送 GIF

2. 保存 GIF

3. GIF 搜索引擎

(九) Telegraph

(十) Instant View

## 第八節 加密通訊應用概論

### 一、什麼是端對端加密

「端到端加密 (End-to-end encryption, E2EE) 是一個只有參與通訊的用戶可以讀取信息的通信系統。總的來說，它可以防止潛在的竊聽者——包括電信供應商、互聯網服務供應商甚至是該通訊系統的提供者——獲取能夠用以解密通訊的密鑰。此類系統被設計為可以防止潛在的監視或篡改企圖，因為沒有密鑰的第三方難以破譯系統中傳輸或儲存的數據。舉例來說，使用端到端加密的通訊提供商，將無法將其客戶的通訊數據提供給當局。」

——[維基百科 - 端對端加密](#)

## 二、常見即時通訊應用的加密方式

包括微信 (WeChat) 在內的所有主流即時通訊 (Instant Messaging, IM) 軟件都會對信息加密，但顯然微信並不支持端對端加密。在支持端對端加密的 IM 軟件當中，加密模式可分為默認端對端加密 (always end-to-end encrypted) 和選擇性端對端加密兩種。前者的代表有 WhatsApp 和 Apple 的 iMessage，採用後者的應用有 Telegram、Facebook Messenger 和 Google Allo 等。

Telegram 因為沒有默認啓用端對端加密而受到批評，而事實上用戶通訊數據的安全性不只取決於加密方式，還取決於 IM 軟件運營者是否將用戶數據上傳在雲服務器上。WhatsApp 雖然默認開啓端對端加密，但仍會將用戶的通訊數據存儲和備份到自己的雲端服務器上，以便將其同步到該用戶的其他設備上；Apple 也在 iOS 11.4 中加入了與前者相似的 Messages in iCloud 功能（可自行選擇開關）。這種模式充其量只能保護傳輸過程中的信息安全，而存儲在雲端服務器上的用戶數據在政府情報部門和黑客面前實際上很脆弱的，端對端加密的保護在傳輸完成後已然失效。而 Telegram 同時提供了普通模式和私密模式兩種模式，普通模式下用戶的聊天記錄會被存儲到雲端服務器以便備份和同步；在私密模式下，Telegram 服務器只負責轉發信息，本身並不存儲任何信息，通訊只建立在兩台終端設備之間，不會同步到同一用戶其他設備的 Telegram 客戶端上。雲端不存儲信息的端對端加密模式排除了政府和黑客通過雲端攫取用戶信息的可能，無疑更能保護用戶的通訊安全。

參見 Telegram 創始人、CEO Pavel Durov 撰寫的 [Why Isn't Telegram End-to-End Encrypted by Default?](#)

## 三、值得推薦的端對端加密 IM

- [Telegram Messenger](#)

- [Signal](#)
- [Wire](#)
- [Riot.im](#)

參見：

- [一天世界 | 聊天軟件安全圖例 v1.2](#) (2017-07-19)
- [Solidot | 騰訊的QQ和微信被指毫無隱私](#) (2016-10-22)

「國際特赦組織的「通訊隱私排名」以1至100分計對科技公司進行了排名，基於它們在下列5方面的表現：認識到用戶在隱私和言論自由方面所面臨之網上威脅；默認啓用端到端加密；讓用戶知道其權利所面臨之風險，以及其提供之加密強度；披露政府要求公司提供的用戶數據之詳情，以及其應對方式；公佈加密系統的技術細節。中國的騰訊公司因對通訊隱私採取的措施最少及最不透明而得零分墊底，其次是黑莓和快拍(Snapchat)，分別得到20及26分。儘管微軟制定了強有力的人權保護政策，它在Skype上依然採用了薄弱的加密方式，因此僅得40分，排名倒數第4。這些公司中無一對用戶通訊提供端到端加密。僅有3家公司在對通訊軟件默認啓用端到端加密方面得滿分，即蘋果、連我 (Line) 以及Viber。」

- [Solidot | 微信有隱私嗎?](#) (2018-01-08)

「國際特赦組織對流行通訊應用的隱私保護進行了排名，騰訊的QQ和微信沒有得到一分，以零分墊底，被認為毫無隱私。在公開場合，騰訊則堅稱它的服務是有隱私的，但拒絕披露更多詳情，比如加密細節之類的。」

## 第九節 Telegram 使用指南

其他 Telegram 教程：

- ★ [resistance M: 請幫助你的朋友使用 Telegram](#) (2018-06-22)
- ★ [Telegram 新手指南](#) (Telegram 頻道)
- [推牆技術部: Telegram 簡明教程 \(適合異議者\)](#) (2017-09-22)

- 電報安全使用方案：Telegram 簡明教程（適合反共者）（2017-05-19）

## 一、Telegram 簡介

Telegram 是一款專注於速度和安全性的即時通訊應用，它快速、簡單且免費。用戶可以同時在所有設備上使用 Telegram，消息可以在任意數量的手機、平板電腦或計算機上無縫同步。使用 Telegram，用戶可以發送任何類型的消息、照片、視頻和文件（文檔，zip，mp3 等），以及為最多 200,000 人創建頻道或群組，以便向無限的受眾群體進行廣播。用戶可以寫入手機通訊錄，並按用戶名查找人員。因此，Telegram 就像短信和電子郵件相結合，可以滿足所有個人或業務通信需求。此外，Telegram 還支持端到端加密的語音通話。

### Q: What is Telegram? What do I do here?

Telegram is a messaging app with a focus on speed and security, it's super-fast, simple and free. You can use Telegram on all your devices **at the same time** — your messages sync seamlessly across any number of your phones, tablets or computers.

With Telegram, you can send messages, photos, videos and **files** of any type (doc, zip, mp3, etc), as well as create groups for up to **200,000** people or **channels** for broadcasting to **unlimited** audiences. You can write to your phone contacts and find people by their **usernames**. As a result, Telegram is like SMS and email combined — and can take care of all your personal or business messaging needs. In addition to this, we support **end-to-end encrypted voice calls**.

參見：

- Telegram 官網：<https://telegram.org>

★ Telegram FQA：<https://telegram.org/faq>

★ 少數派 | Telegram——真正定義即時通訊 | archive

- 少數派 | Telegram - 替補 iMsg 的不二之選（編者注：「iMsg」是 iMessage 的簡寫）

## 二、Telegram 客戶端

Telegram 提供全平台客戶端，包括 Android、iOS、Windows Phone、macOS、macOS/Windows/Linux Desktop 版以及網頁版。

推薦使用從 App Store、Google Play 以及 [Telegram 官網](#)等正規渠道下載的官方客戶端以規避潛在風險，不建議使用第三方客戶端（已有幣用、butterfly.im（蝴蝶IM）、Teleplus（v5.4.2 之前版本）等多款 Telegram 第三方客戶端被曝上傳用戶信息，詳見 Telegram 頻道 [PSA-安全公告專欄](#)）。

Telegram 官方表示現有的第三方 Telegram 客戶端競爭力不足，無法對 Telegram 官方客戶端構成挑戰，因此讓自家團隊另行開發了面向 iOS 和 Android 平台的 Telegram X 客戶端來跟原有的客戶端競爭和驗證新功能。iOS 版 Telegram X 以及 5.0 及後續版本的 Telegram 使用 Swift 語言重寫，速度比混用 Objective-C 和 Swift 的舊版 Telegram 更快，耗電量更低。

Telegram 群組中流傳的 Telegram X 安裝包及類似客戶端文件很有可能被植入了後門，切勿安裝使用。

### 三、註冊

#### （一）號碼選擇

如果你已經肉翻（指常住中國境外，已經入籍或取得綠卡），並且並不畏懼或反感所在國政府實施或可能實施的大規模監控項目，這種情況下盡可使用自己日常使用的手機號碼註冊 Telegram。

如果你對匿名性有要求或者居住在中國大陸地區，建議使用 Google Voice 等虛擬號碼/VoIP 註冊 Telegram 以盡可能保證匿名性，獲取方法見本書第三節。在中國內地使用虛擬號碼的原因在於中國政府在 2015 年「709案」後屏蔽了 Telegram，而此前維權律師群體曾廣泛使用 Telegram，有理由相信 Telegram 最遲在此時開始受到中國強力部門的關注。由於中國大陸對手機號碼採取實名制，國安、公安機關可以通過批量註冊自己的 Telegram 帳號後導入全國的手機號碼和對應個人身份信息的方法，借助中國大陸 +86 的實名制手機號碼實現對大陸用戶註冊的 Telegram 帳號的「實名制」。

此外由於 2017 年以來中國政府部門在微信等牆內平台對「區塊鏈」相關話題的管制，中國「幣圈人士」大量湧入 Telegram，此類人士使用 +86 開頭的中國大陸手機號碼註冊的帳號普遍存在強行拉人入群、大量發送 spam 信息等濫用行為，使 Telegram 官方不得不限制 +86 號碼新註冊的 Telegram 帳號主動發起聊天，這成為了使用虛擬號碼/境外號碼註冊 Telegram 的新理由。

你也可以使用短期出境時購買的臨時電話卡或者在淘寶等電商平台購買的境外電話卡（例如 CMHK）註冊 Telegram，需要注意的是你必須保證該賬號在至少一台設備上時刻在線，否則你在失去該號碼後將因無法接收驗證短信而無法登錄，實際也就失去了該賬號的控制。

## （二）註冊前提

Telegram 在中國大陸地區被 GFW 屏蔽，除了極少數情況下可以實現直連外，通常需要使用 V2Ray、Shadowsocks、VPN 等代理工具才能訪問。

除此之外，用戶可以直接使用 Telegram 客戶端應用內置的代理，包括 Socks5 和 MTProto 兩種代理方式，後者是 Telegram 自主研發的專用網絡傳輸協議。

### 1. 使用內置代理

如果是初次註冊，在未使用代理工具的情況下，輸入手機號碼點擊發送驗證短信數秒後會跳出使用內置代理的窗口，用戶選擇代理方式，輸入代理的服務器 IP、端口、用戶名和密碼後即可使用代理。

如果已經登錄賬號進入應用界面，具體設置方法是 Settings > Data and Storage > Use Proxy 一項中選擇「SOCKS5」或「MTPROTO」填入代理服務器節點信息；或者直接點擊代理鏈接。


以 Project V 之前提供的 SOCKS5 代理 <tg://socks?server=51.15.125.253&port=7777&user=telegram&pass=tgpassword> 為例，在 Telegram 中點擊該鏈接就可完成添加；如手動輸入信息，可照 Server: 51.15.125.253, Port: 7777, Username: telegram, Password: tgpassword 填寫。

### 2. 獲取內置代理

與獲取 V2Ray、Shadowsocks 節點相似，獲取 Telegram 內置代理的方式也可以分為自建和獲取現成的代理兩種。

你可以在租用的 VPS 上搭建自己的 Telegram 專用代理，相關教程可以參考：

- <https://github.com/TelegramMessenger/MTProxy>
- [MTProxy：專為Telegram打造的代理工具-荒島](#)

Telegram 專用代理可以在 V2ray,SSR 節點最新發佈、MTPROTO Proxy 等頻道獲取。

### (三) 註冊步驟

輸入你的手機號碼，Telegram 會自動向你發送短信驗證碼，輸入短信驗證碼就可完成註冊，進入應用界面。

與微信的賬號（手機號/ QQ 號/微信號）+ 密碼，必要時發送短信驗證碼的登錄模式不同，Telegram 每次登錄時都會採用短信驗證碼；如果你額外開啓了兩步驗證（two-step verification），那麼輸入驗證碼後還要再輸入兩步驗證密碼。

\*根據 GDPR，如果你的 IP 位於歐盟國家或者英國，你必須年滿 16 週歲才能註冊 Telegram。

## 四、隱私與安全設置

### (一) 隱私設置

Settings > Privacy and Security

#### 1. 黑名單 (Blocked Users)

此處可以添加/查看被屏蔽拉黑的用戶

#### 2. 顯示在線情況 (Last Seen)

默認設置下，你的聯繫人可以看到你的在線情況，可分為四種類型：

- ① 不久前在線 (last seen recently)
- ② 一星期前在線 (last seen within a week)
- ③ 一個月內前在線 (last seen within a month)
- ④ 長時間未上線 (last seen a long time ago)

用戶可以在隱私與安全設置中選擇向哪些人展示你的真實在線情況，可供選擇的對象有所有人 (Everybody)、我的聯繫人 (My Contacts) 和任何人都不可見 (Nobody)，此外還可以自行設置白名單（即 Always Share With）選項，只向該名單上的用戶展示你的真實在線狀況。

### 3. 語音通話權限 (Voice Call)

Telegram 在 2017 年提供了語音通話功能，而隱私與安全設置中的 Voice Call 選項可以讓你選擇誰有權和你進行，可選擇的有所有人 (Everybody)、我的聯繫人 (My Contacts) 和任何人都不可見 (Nobody)，另外你可以自行設置語音通話權限的黑名單 (Never Allow) 和白名單 (Always Allow)。

PEER-TO-PEER 選項是對通話時數據模式的選擇，P2P 模式指通話數據直接兩台設備間傳輸，非 P2P 模式下通話數據會由 Telegram 的服務器進行中轉以免直接暴露你的 IP 地址，從而保護用戶的隱私與安全，但該模式會降低通話質量。你可以選擇對所有人 (Everybody)、我的聯繫人 (My Contacts) 和任何人都不可見 (Nobody) 通話時使用 PEER-TO-PEER 模式。

iOS 客戶端上的 iOS Call Integration 是指將 IM 應用的語音通話接入 Apple 的 CallKit 框架，開啓該選項後來自 Telegram 的語音通話會像普通來電一樣在鎖定屏幕上顯示，通話會被存儲在系統的通話記錄中；如果你開啓了 iCloud 同步，這些通話記錄會被上傳到 Apple 的 iCloud 雲服務器上。

### 4. 群組權限 (Groups)

群組權限指你可以選擇那些用戶有權將你加入新的群聊，可選擇的只有所有人 (Everybody) 與我的聯繫人 (My Contacts)，此外你可以設置自己的黑名單 (Never Allow) 和白名單 (Always Allow)。

## （二）安全設置

### 1. 本地密碼和生物驗證 (Passcode & Touch ID)



你可以對 Telegram 客戶端設置獨立的解鎖密碼，之後每次需要解鎖才能進入該客戶端。如果你的設備配備了 Face ID、Touch ID 或者其他生物識別傳感器，你可以使用生物驗證來代替數字密碼解鎖客戶端。

## 2. 兩步驗證 (Two-Step Verification)

設置兩步驗證後，每次你重新登錄 Telegram 賬號時，在輸入，你還需要額外輸入自己設置的密碼才能完成登錄。

在登錄認證中加入兩步驗證是對單純短信驗證風險漏洞的填補——政府情報部門和黑客等潛在攻擊者在獲知你用於註冊 Telegram 的手機號碼後可以通過 SS7 攻擊劫持驗證短信的方式來獲取驗證碼，進而登入你的 Telegram 帳號並讀取該賬號上的所有消息。因此，編者建議所有 Telegram 用戶開啓兩步驗證。



參見：[Solidot | SS7攻擊繞過WhatsApp和Telegram加密](#)

兩步驗證是指用戶重新登錄 Telegram 賬號時，在輸入 Telegram 發送到其他已登陸設備上的驗證碼或者 SMS 短信驗證碼（沒有已登錄設備的情況下）後，還需額外輸入設置的密碼才能登錄賬號。

設置兩步驗證的方式非常簡單，在 Settings > Privacy and Security > Two-Step Verification 中設置密碼，然後添加密保郵箱（以便在遺忘兩步驗證密碼後還能重新找回賬號），然後在驗證郵件中確認即可。

### 3. 當前在線 (Active Sessions)

用戶可以在此處查看本帳號當前登錄了多少台設備，所使用的 Telegram 客戶端版本、設備的 IP 地址和位置，以及設備運行的操作系統版本。

#### （三）自動銷毀機制 (If Away For)

Telegram 設置了帳號自動銷毀，長時間未登錄達到設置期限後 Telegram 會自動註銷你的帳號以及該賬號之前產生的所有數據，以此保證用戶數據不會洩露。Telegram 的默認期限是 6 個月，此外有 1 個月、3 個月、6 個月和 12 個月可選。

#### （四）通訊錄 (Contact)

##### 1. 通訊錄的功能

對 Telegram 開啓通訊錄權限後，之後通訊錄中的聯繫人新註冊了 Telegram 後，你將會收到「xxx joined Telegram」的通知；所有已經註冊聯繫人都會顯示與你的通訊錄記錄相一致的身份信息，不再顯示該用戶自己設置的姓名。

##### 2. 同步通訊錄

在默認設置下 Telegram 會把你的通訊錄上傳到雲端並同步，在新版本中 Telegram 為遵守歐盟的 GDPR 推出了新的隱私與安全權限，允許用戶選擇是否同步通訊錄，並提供了刪除已同步通訊錄的選項 (Delete Synced Contacts)。

##### 3. 使用通訊錄進行備注

Telegram 沒有提供對聯繫人進行備注的功能，但你可以借助通訊錄，將 Telegram 聯繫人的姓名和手機號碼存入自己的通訊錄，從而間接實現對 Telegram 聯繫人身份信息進行自定義的功能。如果你關閉了 Telegram 的通訊錄權限，你仍可編輯製作僅適用於 Telegram 的通訊錄。

## （五）私密模式下的鏈接預覽

你可以選擇是否在私密模式中開啓鏈接預覽，此項也是為符合 GDPR 而推出的新權限。鏈接預覽 (link preview) 由 Telegram 的服務器生成，但 Telegram 不會存儲鏈接數據。

## 五、其他設置

### （一）個人信息設置

#### 1. 姓名

姓和名是註冊時需要填寫的信息，登錄後隨時可以在設置中更改姓名。你設置的姓名會對向

#### 2. 頭像

Telegram 會自動生成由你的姓、名首字母組成的圖片作為頭像，你可以在設置中上傳圖片更換頭像。需要注意的是 Telegram 會默認保留曾經使用過的所有頭像，所有人都可以點擊進入你的頭像後通過划動來查看你的曾用頭像。你如果不希望別人看到你的歷史頭像，需要在設置中手動刪除。

#### 3. 簽名

bio 是供選填的個性簽名和自我介紹。

#### 4. 更換號碼

你可以在 Change Number 中更換註冊 Telegram 的手機號碼。需要注意的是如果他人有自己的 (Telegram) 通訊錄里存儲了你的手機號碼，當你使用 Change Number 更換號碼後他可以看到更新後的號碼。

如果你懷疑自己的 Telegram 賬號被懷有惡意的第三方知悉需要更換號碼的，或者原先使用中國內地 +86 開頭的號碼註冊需要更換外國號碼的，不要在原賬號使用更換號碼 (Change Number) 功能，而應棄用該賬號或者登錄 Telegram 網站手動註銷，然後使用新的號碼另行註冊一個 Telegram 賬號。

## 5. 用戶名

你可以設置一個 Username（用戶名）來方便別人找到你。在 Telegram 中對方可以直接通過「@你的用戶名」（例如 @username）來搜索到你的帳號；Telegram 還會為你生成一個「https://t.me/username」的鏈接，以便你將自己的 Telegram 帳號直接分享到 Twitter、Facebook 等其他社交平台。所有人都可以通過你的 username 找到你，但他們不會看到你的手機號碼，除非你自己選擇了「Share My Contact」。

## 6. 退出登錄

點擊「Log Out」來退出當前帳號

## 7. 小結

如果你對匿名性要求較高，建議隨機填寫姓名信息，不填寫 bio 或填入無關信息，不要在 Telegram 上使用與其他社交/即時通訊帳號相同的姓名、用戶名、暱稱、個性簽名和頭像，以免對方可以通過關聯確定的你的真實身份；除非你有意公開自己在網絡上的虛擬身份。

### （二）數據與存儲 (Data and Storage)

Telegram 默認將所有信息存儲在雲端，每次進入應用 Telegram 都會自動從雲端同步數據，相比微信和 QQ 的存儲佔用會從剛下載時的 100 MB + 逐漸膨脹至 1 GB +，Telegram 幾乎不佔用本地存儲空間（其不足可能是會耗費更多流量）。

在 Settings > Data and Storage 中，你可以查看 Telegram 的存儲 (Storage) 與網絡 (Network) 使用情況，選擇自動下載 (Auto-Download Media) 的媒體類型（默認自動下載圖片，視頻、文件、語音消息、視頻消息需要手動點擊下載），是否自動下載還可以根據上網方式（無線網絡/蜂窩移動數據網絡）。此外你可以選擇是否將新收到的圖片自動保存到本地、是否保存經 Telegram 編輯過的圖片和是否自動播放 GIF。

### (三) 外觀 (Appearance)

在外觀設置中，你可以選擇字體大小、聊天背景（除 Telegram 提供的背景圖片外，用戶可以通過相冊上傳自己的圖片作背景）、是否自動啓用黑夜主題 (Auto-Night Theme) 以及色彩模式（有 Day Classic（經典模式）、Day（接近於 iMessage，只有 Day 模式下會出現 Accent Color 選項供用戶自定義主題顏色）、Night Blue（暗藍色調的黑夜模式）、Night（黑夜模式）四種模式可選）。

### (四) 語言 (Language)

Settings > Language

「Telegram 客戶端，官方支持中文語言

Telegram 客戶的版本要求：

iOS 客戶端  $\geq 5.0.16$

Android 客戶端  $\geq 5.0$

macOS 客戶端  $\geq 4.8$

Windows/macOS/Linux Desktop 客戶端  $\geq 1.5$

Telegram 客戶端下載地址：<https://congcong0806.github.io/2019/01/08/Telegram>

Telegram 客戶端內直接點擊鏈接更改語言：

英文：<tg://setlanguage?lang=en>

簡體中文：<tg://setlanguage?lang=zh-hans-raw>

簡體中文(聰聰)：<https://t.me/setlanguage/zhcnc>

簡體中文(@zh\_CN 版)：<tg://setlanguage?lang=classic-zh-cn>

簡體中文(langCN)：<tg://setlanguage?lang=zhlangcn>

繁體中文(香港)：<tg://setlanguage?lang=zh-hant-raw>

繁體中文(台灣)：<tg://setlanguage?lang=taiwan>

」

——[印象筆記 | 科技 NEWS 606](#)

## 六、基礎功能

## （一）普通聊天模式

普通聊天模式並未開啓端對端加密，所有的聊天記錄都會被存儲到 Telegram 雲端。

### 1. 發送消息類型

Telegram 支持發送文字消息、表情貼紙 (Stickers)、GIF、視頻、文件，並支持發起語音通話。

對於文字消息，你可以通過右鍵或快捷鍵自定義字體格式，可選擇粗體或斜體，支持在文字中植入網頁鏈接。

對於在 Telegram 中發送的鏈接，Telegram 會根據鏈接網頁類型提供相應的頁面預覽，如鏈接支持 Instant View 快速預覽功能（例如 Telegraph），Telegram 會提供網頁標題、首段文字摘錄和第一張圖片，並在下方生成「Instant View」按鈕；對於一般的網頁鏈接，Telegram 會提供標題、文字摘錄和首張圖片的預覽；微信公眾號推文等少數的網頁鏈接完全不支持預覽，只能以鏈接形式呈現。

在 Telegram 發送圖片時，發送點擊圖片可以進入圖片編輯模式，提供畫筆、馬賽克等簡單的圖片標注功能。如果需要發送的圖片數量大於等於 2 張，你可以選擇單張發送圖片，也可以選擇將數張圖片拼成圖集後一次性發送。如果你擔心圖片被壓縮後質量下降，，可以選擇以文件形式發送圖片 (Send as a file)，對方收到後需要下載解壓後查看。

你可以發送任何形式的文件，單個文件大小不能超過 1.5 GB。

### 2. 編輯 (Edit)

Telegram 允許用戶在消息發送後 48 小時內編輯修改已發送的消息，編輯過的文字仍會留在原處。（微信的「編輯功能」只是「撤回」的增強版，即在消息撤回後將該消息自動粘貼到你的輸入欄中以供修改）

### 3. 刪除 (Delete)

Telegram 沒有微信那樣的撤回機制，只提供刪除功能。在一對一對話中，你在「Delete」時可以選擇同時為自己和對方刪除還是僅對自己刪除，前者相當於「撤回」，

支持在發送後 48 小時內刪除已發送消息，後者相當於刪除自己的聊天記錄，不及於對方（此選項也會導致後續無法為對方刪除消息，因此選擇時需慎重）。在群聊中，「刪除」的效力是「delete for everyone」，可以等同於「撤回」。

#### 4. 回復 (Reply)

無論是一對一還是在群聊中，你都可以選中他人發送的消息後選擇「Reply」（回復），之後你發送的回復會附上對方之前的消息，使得聊天時的回復更有針對性。

#### 5. 轉發 (Forward Message)

你可以選中他人發送的消息後選擇「Forward Message」，將該消息轉發到他處。被轉發的消息上注有「Forward from xxx（原作者的名字）」。

### （二）私密聊天模式

在 chats 界面點擊右上角的新建按鈕（如果你關閉了 Telegram 的通訊錄權限將無法新建對話，Telegram X 和 Desktop 版本不受此限），選擇 New Secret Chat 來新建私密聊天；或者在聯繫人的名片頁點擊「Start Secret Chat」。之後 Telegram 會向對方發送私密聊天請求 (secret chat request)，只有對方同意進入後雙方才能交換端對端加密 (end-to-end encrypted) 密鑰，進入私密聊天模式。進入私密聊天模式後，在 chats 主界面上該聯繫人的姓名為綠色，姓名左側有綠鎖標記。

私密聊天受限於創建該對話的設備，產生的聊天記錄不會上傳存儲到 Telegram 雲端，也不會同步到你的其他設備上。

私聊聊天模式中不允許使用轉發功能 (don't allow forwarding)，同時可以設置消息自毀計時器 (self-destruct timer, 相當於閱後即焚)，可供選擇的時間有 1 - 15 秒、30 秒、1 分鐘、1 小時、1 天和 1 周，你也可以選擇「Off」，即不開啓。

### （三）Saved Messages

向 Saved Messages 發送消息就是用戶自己跟自己對話，你可以把 Saved Messages 當成自己的私人網盤來使用。

#### (四) 群聊

##### 1. 創建群組

你可以在新建消息中選擇「New Group」來創建群組，最初必須有兩人以上才能創建成功。如果你關閉了通訊錄權限，你將無法在 Telegram iOS 客戶端中新建群組，但是 Telegram X 和 Desktop 版不受限制。如果你暫無聯繫人，可以將自己創建的 Bot（機器人）拉入群組。

Telegram 群組有私有群組與公共群組、普通群組和超級群組之分。

##### 2. 私有群組與公共群組

私有群組與公開群組的差別在於公開性，私有群組的邀請鏈接的形式是「t.me/joinchat/」，而公開群組的鏈接的形式是「t.me」的短鏈接；打開私有群組的邀請鏈接後，必須入群 (Join) 才能查看消息，而打開公開群組的鏈接後即便不入群也可以查看歷史消息。

關於區分私有與公開群組，Project V 的幾個 Telegram 交流群就是很好的例子——私有群組 Project V 吹水群「小薇姐姐的日常」的鏈接是 <https://t.me/joinchat/AAAAAEIYaH-hjDDZS716jg>，公開群組「Project V（使用與反饋）」的鏈接是 <https://t.me/projectv2ray>。

公開群組提供 Copy Link 的功能，即群聊中每位成員發送的消息都有對應的鏈接，選中一則消息後選擇「Copy Link」以獲取鏈接。

##### 3. 普通群組與超級群組

普通群組與超級群組的差別在於人數與功能，和是否為私有/公開群組之間沒有必然聯繫（例如「小薇姐姐的日常」既是私有群，也是超級群）。

普通群組的人數上限為 200 人，任何人都可以邀請新成員並編輯群名和群頭像。超級群組 (Supergroup) 的人數上限高達 200,000 人，並擁有一些普通群組所不具備的功能。



超級群組為用戶提供個性化的通知權限，你可以設置為群中有人提到你（即「@」）或者回復 (Reply) 你的消息時才通知你。超級群組的創建者可以授權給管理員來協助管理（機器人同樣可以擁有管理員權限），管理員可以在群中置頂消息 (Pinned Messages)。

普通群組可以升級到超級群組，但該操作不可逆。

參見：★ [聰聰 | Telegram 群組、頻道、機器人 - 匯總分享 - 群組 Group](#)

## （五）頻道

Telegram Channel (頻道) 的使用模式與用 Telegram 聊天高度相似，差別只在於只有頻道所有者（或者說創建者 (creator)）及其授權的管理員 (Admin) 有權發佈消息，其他關注頻道的用戶只有只讀權限。

頻道和群聊一樣分為公開群組和私有群組，二者的差別和群聊基本一致。公開頻道提供的 Copy Post Link 功能類似公開群組的 Copy Link 功能，可以直接以鏈接形式分享該消息。

頻道可以發揮公告板的作用，可以像微信公眾號平台那樣使用。頻道的推送完全沒有次數和內容的限制（Telegram 官方只審查煽動使用暴力的內容，並對 Apple 設備屏蔽傳播色情內容的頻道），自由度遠高於微信公眾號。頻道也可以當作微信朋友圈使用，你可以借助 like bot 等機器人轉發消息來實現類似點贊或者評論功能。

少數由 Telegram 官方創建的 Channel 有藍色八角形、白色對勾的認證標識（如 Telegram、[Durov's Channel](#)、[Telegram News](#)、[Gamee](#)）。

參見：★ [聰聰 | Telegram 群組、頻道、機器人 - 匯總分享 - 頻道 Channel](#)

## （六）機器人 (bot)

bot 是 Telegram 上的機器人賬戶，通常具有 AI 屬性並可充當自動化工具，進而擴展 Telegram 的功能。bot 近似於微信小程序，例如 @like 可以為消息提供類似點贊功能，

@PullBot 可以發起群投票，@tgcnjoincaptchabot 可以對入群者進行 reCAPTCHA 驗證。Telegram 開放了 bot 的 API，用戶可以根據自身需要開發自己的 bot。

名稱右側有藍色八角形、內有白色對勾圖標的 bot 是由 Telegram 官方出品或經 Telegram 官方認證的 bot，相對安全可靠。

常見 Bot 列表：

@BotFather 官方認證。創建和管理機器人

@IFTTT 官方認證。IFTTT 的官方機器人，可以連接各類 IFTTT 服務。

@GmailBot 官方認證。Gmail 客戶端

@telegraph 官方認證。發送、管理 Telegram 文章及查看統計數據

@gamee 官方認證。遊戲平台

@get\_id\_bot 獲取你的 Telegram Chat ID（一串數字）

@bing/@pic/@gif: Bing / Yandex / Giphy 圖片搜索，可用於貼紙鬥圖

@AirPollution\_bot: 空氣污染指數，數據來源為 aqicn.org

@QRCodeRoBot 二維碼識別

@TextEmojiBot: 顏文字

@GithubBot: GitHub Commit 和 Issue 更新提醒

@like 提供類似點贊按鈕

@vote 發起投票

@PullBot 發起投票

@zh\_groups\_bot TGCN-群組頻道狗🐶 TGCN-群組索引計劃機器人

@AntiServiceMessageBot 自動刪除入群、退群通知

參見：

★ [聰聰 | Telegram 群組、頻道、機器人 - 匯總分享 - 機器人 Bot](#)

- [少數派 | 我的 Telegram 小工具集：「統一聊天平台，各種工具，和監控提醒」](#)

## （七）貼紙 (Stickers)

Telegram 的 Stickers（貼紙）功能類似於微信的表情包。在「表情包」上，Telegram 與微信的差別在於區分了 Stickers 和 GIF，Sticker 是靜態的圖片，GIF 是動圖，不像微信表情包那樣動靜混雜。得益於 Telegram 的開發性和中國用戶的努力，熊本熊、脆皮鸚鵡、小肥柴等熱門表情都有了 Telegram Stickers 版本。

### 1. 獲取貼紙

點擊他人發送的單張貼紙就可查看整套貼紙，點擊下方的「Add Stickers」就可將它保存到自己的貼紙庫。Telegram Stickers 同樣存儲在雲端，一經添加會自動同步到你的所有設備上。

你也可以借助 Stickers Pack bot 來製作自己的貼紙包。教程參見：[懶\(爛\)辦法製作 Telegram Sticker Pack](#)

## 2. 發送貼紙

你可以直接在自己的貼紙庫中選取貼紙，也可以輸入 emoji 表情後選擇該 emoji 映射的貼紙，因為每張貼紙都有與之對應的 emoji 表情。

## 3. 分享貼紙

點擊已保存在貼紙庫中的貼紙包時會顯示「Share Stickers」的按鈕，點按後會生成形如「<https://t.me/addstickers/example>」的貼紙分享鏈接。

部分 Telegram 貼紙鏈接：

Great Minds <https://t.me/addstickers/TelegramGreatMinds>

ssr's daily <https://t.me/addstickers/ssrstickers>

ssr's daily 2 <https://t.me/addstickers/ssrsdaily2>

科學常用表情包 <https://t.me/addstickers/yaffs64>

熊本熊污 <https://t.me/addstickers/xiongbenxiongwu>

💰 <https://t.me/addstickers/PowerEmoji>

Docomo by Suisr [https://t.me/addstickers/suisr\\_docomo](https://t.me/addstickers/suisr_docomo)

cute call <https://t.me/addstickers/cutecall>

ARU Full Part2 <https://t.me/addstickers/arup2>

可愛不過老子 <https://t.me/addstickers/keaibuguolaozi>

茄 <https://t.me/addstickers/karen321>

Tom基本法 <https://t.me/addstickers/tombasiclaw>

behnam(wild boy) <https://t.me/addstickers/behnambbbbmmmmmm>

這只 Gayhub 到處咬東西 <https://t.me/addstickers/PeeGayhub>

Suddenly <https://t.me/addstickers/Suddenly2x>

中老年表情包 <https://t.me/addstickers/oldaged>

我想靜靜 <https://t.me/addstickers/PeterCxy>

Subway's WeChat Collection <https://t.me/addstickers/myfavoritewechatstickers>

Windy's Pack <https://t.me/addstickers/Windyspack>

張德帥 <https://t.me/addstickers/changmz>  
Jony Ive [https://t.me/addstickers/Jonathan\\_Ive](https://t.me/addstickers/Jonathan_Ive)  
rw-Style <https://t.me/addstickers/rwStyle>  
白白在吃啥 <https://t.me/addstickers/BacBacsDiet>  
KOGINU @Nekosticker <https://t.me/addstickers/nekostickerpack498>  
Big Emoji <https://t.me/addstickers/PowerEmoji>  
The Elder and HK journalist <https://t.me/addstickers/TheElderPart2>  
Excited <https://t.me/addstickers/excited>  
蛤蛤 <https://t.me/addstickers/hahajiecao>  
TheElder <https://t.me/addstickers/TheElder>  
清真表情包 <https://t.me/addstickers/PowerEmoji>  
Bazinga <https://t.me/addstickers/Analytics2>  
變態熊貓-RW <https://t.me/addstickers/biantaiPanda>  
ugly triple <https://t.me/addstickers/uglytriple>  
你懂我意思吧 [https://t.me/addstickers/do\\_you\\_know\\_what\\_I\\_mean](https://t.me/addstickers/do_you_know_what_I_mean)  
過兩招-rw <https://t.me/addstickers/Guoliangzhao>  
Kizuna Ai  [https://t.me/addstickers/Kizuna\\_Ai\\_San](https://t.me/addstickers/Kizuna_Ai_San)  
HailTheJudge <https://t.me/addstickers/HailTheJudge>


## (八) GIF

Telegram 會將 GIF 轉碼成 MPEG 4 格式，在相同畫質下至多可節省 95% 的存儲佔用空間，使你能夠在 Telegram 上以比以往快 20 倍的速度下載 GIF。得益於開發者的優化，Telegram 可以同時流暢播放幾十個 GIF。

### 1. 發送 GIF

GIF 按鈕與貼紙按鈕並列，點擊後可以查看你自己的 GIF 圖庫。

### 2. 保存 GIF

以 iOS 為例，點按 GIF 查看大圖，再點按右下方的「」就能將此 GIF 保存到自己的 GIF 欄中。

### 3. GIF 搜索引擎

Telegram 內置了 GIF 動態搜索功能，你可以在輸入欄中輸入「@gif 關鍵詞」（例如「@gif cat」）來搜索相關的 GIF。

## (九) Telegraph

Telegraph 是 Telegram 提供的匿名博客服務，你可以通過 Telegram 中的 Telegraph bot (@telegraph) 或者在瀏覽器中輸入「telegra.ph」來使用它。Telegraph 的匿名體現在它只根據瀏覽器緩存來識別作者，Telegraph 文章剛發佈時還可重新編輯，一旦瀏覽器緩存被清除後就不可再編輯，同時無法溯源到原作者。

Telegraph 支持大小標題、粗體/斜體文字、圖片、網頁鏈接和視頻鏈接，對鏈接沒有任何限制。

如果你需要在 Telegram 群組中發送長段文字，可以考慮使用 Telegraph 鏈接或 pastebin 類工具，以免佔據過多屏幕空間對他人造成影響。

Telegraph 支持下文會提到的 Instant View 功能。

## (十) Instant View

Instant View 是 Telegram 內置的網頁快速瀏覽功能。支持 Instant View 功能的網頁鏈接（例如：Telegraph、BBC）會在標題、摘要和圖片下方會顯示「Instant View」按鈕，點擊後即進入 Instant View 模式，網頁文章會被渲染成類似閱讀模式的風格，用戶可選擇文字背景顏色和字體大小等。Instant View 的意義在於可以極大縮短 Telegram 內置瀏覽器或跳轉外部瀏覽器加載、打開鏈接的時間，同時為用戶提供了良好的閱讀體驗，用戶可以把 Telegram 當作閱讀器來使用。

# 第四章 個人信息保護指南

## 第十節 個人信息保護指南

- 一、系統安全防護
- 二、數據安全保護
- 三、隱私權限限制
- 四、加密郵箱
- 五、瀏覽器

六、Tor 瀏覽器

七、搜索引擎

八、密碼管理

九、輸入法

十、智能家居

十一、多設備策略

## 第十一節 社交媒體使用建議

一、賬號管理

二、身份隔離

三、言論邊界

## 第十節 個人信息保護指南

### 一、系統安全防護

#### （一）盡可能不使用國產操作系統

常見的桌面操作系統均非國產操作系統，此處略過。

建議國產 Android 手機用戶，通過刷機使用 LineageOS 等接近原生系統的第三方 ROM。使用中國廠商定制的安卓 ROM 最大潛在風險在於越權收集用戶信息和為中國政府提供後門監控用戶，此外還有閹割原生 Android 的功能、推送海量垃圾廣告和信息（以 MIUI 為代表）、推送 Android 官方安全補丁不及時等諸多缺點。

在移動操作系統對隱私保護孰優孰劣的問題上，Android 系統得益於其開放的特性，使有相應能力的用戶可以全面地掌控各應用程序的權限和活動，但是其學習成本較高，只適用於極客群體。iOS 的優點在於沙盒運行機制及嚴格的 App Store 審核規則，從源頭上遏制了惡意應用程序和流氓軟件的滋生；但其封閉的系統特性和不明確的隱私權限設置使

得用戶無法知曉應用程序在後台對個人信息的調用活動，確實存在硬傷；但對於小白級用戶而言，iOS 至少可以在簡捷易用的前提下保證相對的安全。



華為賬號更新通知

圖片來自推特用戶「郭元慶」(@qq196837) [原推鏈接](#)

參見：

- [The 「Decision」 app in Huawei P20 was found to continuously collect your location and send the data to hicloud.com, the Huawei Cloud \(2018-10-03\)](#)

推主 [Elliot Alderson \(@fs0c131y\)](#) 發佈了系列推文，揭露華為 P20 手機預置的「Decision」應用持續收集用戶的定位並將數據傳送到 [hicloud.com](#)，即華為雲的服務器上。

- 華為手機系統被曝自動刪除從國際互聯網下載的文件，舊版系統可能不受影響 (2019.01)

<https://twitter.com/yxw860510/status/1084962096121434113>

[https://twitter.com/8\\\_9\\\_6\\\_4/status/1084130766030663680](https://twitter.com/8\_9\_6\_4/status/1084130766030663680)

<https://twitter.com/servalcandle/status/1087692589044617217?s=21>

<https://twitter.com/servalcandle/status/1087709643730604032?s=21>

- [Solidot | 一加的氧 OS 會跟蹤用戶的所有活動 \(2017-10-10\)](#)

「深圳萬普拉斯科技有限公司為其一加智能手機開發的 Android 定製版本 OxygenOS 內置了跟蹤分析功能，會跟蹤用戶在應用中的所有活動，相關數據會被發送到域名 open.oneplus.net，一加收集的數據並不匿名，包含了用戶設備的詳細信息。用戶沒有辦法禁用，但可以通過 adb 移除名為 OnePlus Device Manager 的跟蹤應用。」

- 新京報網 | 百度系兩款APP未經提示開啓隱私權限 | archive

- iOS Security - Apple

安卓手機刷機教程參見：

★ ch: 手機機刷機Why&How (2018-03-12)

## (二) 及時更新最新版系統

如果是大版本迭代前可以先觀望一段時間，以防新系統不穩定帶來麻煩。

## (三) 病毒防護

運行 iOS、macOS 和 Linux 操作系統的設備因其系統特性幾乎不會感染病毒，無需用戶自己動手查殺病毒。

就 iOS 設備而言，不建議從第三方應用市場（例如 PP助手、愛思助手等）下載破解版應用。如果不具備相應的技術能力，不要盲目「越獄」。

就 Windows PC 而言，微軟提供的 Windows Defender 軟件基本可以滿足日常的安全保護需要（Windows Defender 可運行在 Windows XP 及更高的版本上，並內置於 Windows Vista 及後續版本），你也可以選擇 Avira（俗稱「小紅傘」）、Norton Security 等國外殺毒軟件或者 火絨安全軟件 等口碑較好的國產安全防護軟件。

360 安全衛士、騰訊電腦管家和百度衛士是國產毒瘤軟件的代表，以竊取用戶信息、捆綁安裝全家桶（如 360 安全瀏覽器、360 手機管家等）、佔據大量內存加重卡頓見長，建議盡早將其刪除。

參見：

- Solidot | 你的百度雲管家報毒了嗎？ (2017-02-06)



## 二、數據安全保護

### （一）定時備份

建議定期使用外置移動硬盤備份電腦、手機中的數據。

### （二）硬盤加密

你可以給電腦硬盤加密來進一步增強數據安全性。macOS 和 Windows 操作系統均內置了硬盤加密工具。在 macOS 下你可以開啓「文件保險箱 (FileVault)」(設置 > 安全性與隱私 > 文件保險箱)，在 Windows 下你可以打開 BitLocker。

開源的硬盤加密軟件 VeraCrypt 可用於在文件中創建虛擬加密硬盤或加密分區，在 Windows 系統下還支持在開機前授權全盤加密。

教程參見：

★ 有關密碼學的科普內容 | Veracrypt 的基本操作

- 編程隨想 | 如何用「磁盤加密」對抗警方的【取證軟件】和【刑訊逼供】，兼談數據刪除技巧 (2019-02-14)

### （三）文件加密

對於文件和郵件文本內容都可以採用 PGP (Pretty Good Privacy) 協議加密，PGP 分為公鑰和私鑰，使用公鑰給文件加密，再用私鑰解密；此外 PGP 還支持給文件添加加密的數字簽名以驗證真偽。使用 PGP 需要使用的軟件是 GnuPG (GNU Privacy Guard, GPG)，支持 Windows, macOS, RISC OS, Android, Linux 系統。

### （四）銷毀數據

數據一旦在寫入磁盤，此後無論是刪除文件還是格式化磁盤，理論上都可以使用技術手段恢復此數據。對此可以選擇多次抹掉硬盤數據以防止文件被恢復。

8. 如果選取了 Mac OS 擴展（日誌式，加密），若要防止已抹掉的文件被恢復，請點按「安全性選項」，使用滑塊來選取覆蓋已抹掉數據的次數，然後點按「好」。  
覆蓋數據三次即符合美國能源部關於安全抹掉磁性介質的標準。覆蓋數據七次即符合美國國防部的 5220-22-M 標準。

9. 點按「抹掉」，然後點按「完成」。

參見 [Apple Support | 在 Mac 上使用「磁盤工具」抹掉宗卷](#)

對於曾經存儲過重要信息的廢棄機械硬盤、固態硬盤或閃存條，不要將其隨意丟棄，可以考慮用外力將在物理上徹底破壞後再丟棄。

對於淘汰或者損壞的手機，若打算將其掛到二手平台上出售，建議先將其恢復出廠設置。如果是廢棄的 iPhone 手機，可以按照官網的指示進行相關操作，然後將其交給蘋果做拆解處理。

### 三、隱私權限制

除了不開啓定位就無法使用的地圖類應用外，建議一律關閉定位和通訊錄權限。

對於微信、QQ、微博、貼吧、知乎、淘寶、天貓、閒魚、京東等國產應用，建議在平時關閉調用相機和麥克風權限。

如果你對應用開啓了相冊權限，理論上該應用可以掃描你的整個相冊。如果間歇性開啓相冊權限，其效果與經常性開啓並無二致。如果你對於隱私保護要求較高，建議徹底關閉微信、新浪微博等國產軟件的相冊權限。新版 iOS 系統已經在相冊權限上對讀取和寫入權限做了區分，但社交類軟件的讀寫權限通常是合二為一的，關閉相冊權限的同時意味著你無法將微博上的圖片保存到相冊中，對此你可以使用抓圖應用通過網頁鏈接抓取圖片，或者在瀏覽器中打開鏈接後直接保存。如果你覺得這些額外步驟過於繁瑣影響生活質量，可以考慮同時使用兩部手機或更多部設備，在專門的手機上對國產軟件開放相機、相冊等隱私權限。

參見：

- [Solidot | 小米華為被發現悄悄給予應用過多權限](#)（2018-02-12）

「新京報的調查發現，華為、小米應用商店下載的應用默認開啓了多個敏感權限。在華為、小米、OPPO、vivo 的內置應用商店下載 APP 時，天貓、攜程、58同城、優酷、今日頭條、愛奇藝、趕集網七款 APP 在華為和小米應用商店下載時未經明示提醒就默認開啓了定位或其他敏感權限，而在 OPPO 和 vivo 應用商店下載時則基本都對其權限進行了明示提醒。以天貓為例，在小米手機安裝後，默認開啓了定位、相機、錄音權限；在華為手機安裝後，默認開啓了定位、相機、讀取通話記錄權限；OPPO 手機安裝後，未開啓任何權限；vivo 手機安裝後，明示提醒並開啓了定位權限。其它應用有類似情況。一位開發者稱，應用市場一般執行最低權限策略，除非權限是刚需，比如讀取通訊錄是為了實現加通訊錄好友。至於 APP 具體能夠開啓哪些權限，要看應用商店的審核要求。如果應用商店覺得你索取的權限出於正當目的，就可以上架，至於默認開啓權限的功能，只能是與應用商店有關。」

- Solidot | 京東金融 APP 被發現會收集用戶銀行 APP 截圖 (2018-02-16)

- Telegram 頻道 荔枝木 - <https://t.me/lycheewood/5454> (2018-02-16)

「今天京東金融截圖的事情鬧得沸沸揚揚，不乏有些用戶鼓吹轉移到 iOS 系統下就沒有這些問題。

真的如此嗎？我覺得可以參考一下這篇文章：[https://weibo.com/ttarticle/p/show?id=2309404340311663991197#\\_0](https://weibo.com/ttarticle/p/show?id=2309404340311663991197#_0)

iPhone 給應用後台 15min 保持的時間里微信會私自訪問相冊你知道嗎？——你當然不會知道，因為 iOS 沒有「每次訪問相冊權限」都提醒的功能，所以這一現象只有在重置後的 iOS 系統上，當微信認為自己已經被授權而偷偷訪問的時候會被發現。既然相冊可以被靜默訪問，其它權限同理，比如聯繫人。

再比如說 iOS 的某些應用同樣會在 WiFi 開關的時候後台向服務端發送設備和網絡信息——而且這還是在關閉了後台刷新並結束進程之後。

在這些方面 Android 得益於更開放的系統環境，得以用一些 tweak & hack 來攔截，而 iOS 很遺憾就只能抓瞎了，所以我認為 iOS 隱私保護更好很可能是個偽命題。」

- Telegram 頻道 每日消費電子觀察 - [https://t.me/CE\\_Observe/7537](https://t.me/CE_Observe/7537) (2018-02-16)

「我覺得這篇文章想表達的意思是：作為用戶，應當理解在iOS、Android或其他系統上，授予應用每一項權限都意味著什麼，這項權限如果被濫用到極致可以收集哪些隱私；看清應用溫馨提示的藉口，不要盲目給予它們不必要的權限。而不要只是見到某App的某個行為被曝光了就短時間內抵制某某公司。

BTW：為什麼我反對甚至痛恨二維碼的推廣普及？

因為使用二維碼就必然會使用攝像頭；能使用攝像頭了，你覺得流氓們會規規矩矩地只在你掃二維碼的時候才調用攝像頭嗎？」

- 少數派 | 如何才能阻止下一個京東金融「偷」走你的照片？ (2019-02-19)

#### 四、加密郵箱

使用國產的 163、126、yeah、QQ、新浪、搜狐郵箱服務必然伴隨在中國政府對電郵內容的監視。因此無論使用電子郵件本身，還是使用郵箱註冊 Twitter 等網絡賬號，都建議使用 Gmail 等國外郵件服務。此外在傳輸敏感信息時，可以考慮使用支持端對端加密的郵箱服務以保證安全。

端對端加密匿名郵箱有 ProtonMail、Tutanota、Disroot.org、Mailfence、Mailbox.org、Runbox，此外 ZeroNet 等去中心化網絡也有相應的端對端加密郵箱服務。

值得注意的是「端對端加密」只適用於相同郵箱服務的賬戶之間，如果你用 ProtonMail 向 Gamil 用戶發送加密郵件，你還需要通過其他通訊渠道向對方提供解鎖郵件的私鑰。

參見：hatecpc: #2 匿名郵箱:protonmail

#### #「零收件箱」策略

對於高度敏感的郵件往來，可以使用「零收件箱」策略，即雙方閱讀郵件後即時刪除郵件。這樣一來，即便公安無論使用技術手段還是強迫當事人交出郵箱密碼而控制了郵箱，最終仍然無法獲取定「罪」證據。

#### 五、瀏覽器

## （一）瀏覽器的選擇

推薦使用 Safari（僅限蘋果設備）、Chrome、Firefox，以及來自獨立開發者/開發商的瀏覽器應用，如對匿名性要求較高可以使用 Tor 瀏覽器。

不建議使用國產安卓手機廠商系統內置的瀏覽器，以及 BAT 出品的百度瀏覽器、QQ 瀏覽器、UC 瀏覽器等，理由同樣是存在植入後門監視用戶的可能。以小米 MIUI 國內版瀏覽器為例，該瀏覽器直接屏蔽了 Github 的網址，在信息封鎖上比 GFW 更進一步。

參見：

- 公司安全部門通知：「百度瀏覽器過度收集用戶隱私信息，請在任何情況下都避免使用」（2016-03-18）」
- MIUI論壇 | miui自帶瀏覽器7000+攔截網址曝光，厲害了

## （二）瀏覽器的使用

使用瀏覽器時可以使用隱私模式（也稱「無痕瀏覽」），即不保留歷史記錄，以免受到網站追蹤。

盡可能使用 HTTPS (Hypertext Transfer Protocol Secure, 超文本傳輸安全協議) 的連接的網頁。HTTPS 經 HTTP (HyperText Transfer Protocol, 超文本傳輸協議) 進行通信，並使用 TLS/SSL 對傳輸數據進行加密，它的 URL 以「https://」作為開頭，瀏覽器往往在其 URL 前顯示鎖的圖形，可憑此對 HTTPS 和不加密的 HTTP 進行區分。不要在 HTTP 連接的網頁中輸入賬號、卡號和密碼等敏感信息，這些數據一旦被黑客攔截會直接以明文形式呈現，進而可能造成信息洩露、財產損失等嚴重後果。

## 六、Tor 瀏覽器

VPN 等傳統代理工具只提供一層代理，如果與 VPN 的連接因意外斷開，你的真實公網 IP 就會暴露並被網絡服務提供商 (ISP) 記錄。Tor 瀏覽器的多重代理則有助於降低前者發生的風險，同時保障上網的匿名性和安全性。

Tor 瀏覽器的使用門檻比 VPN、Shadowsocks 等代理工具更高，其帶來的安全性提升建立在犧牲一定效率的基礎上。編者建議在網絡上積極發表政治觀點的指導級受眾使用

Tor 瀏覽器，以訪問國際互聯網為主要需求、平時只瀏覽資訊不發言討論的參考級用戶可根據自身需求來判斷是否使用 Tor。

### （一）Tor 的原理

「Tor（英語：The Onion Router，洋蔥路由器）是實現匿名通信的自由軟件。Tor 是第二代洋蔥路由的一種實現，用戶通過 Tor 可以在因特網上進行匿名交流。

#### 匿名外連

Tor 用戶在本機運行一個洋蔥代理服務器（onion proxy），這個代理週期性地與其他 Tor 交流，從而在 Tor 網絡中構成虛電路（virtual circuit）。Tor 是在5層協議棧中的應用層進行加密（也就是按照'onion'的模式）。而它之所以被稱為 onion，是因為它的結構就跟洋蔥相同，你只能看出它的外表，而想要看到核心，就必須把它層層的剝開。即每個路由器間的傳輸都經過點對點密鑰（symmetric key）來加密，形成有層次的結構。它中間所經過的各節點，都好像洋蔥的一層皮，把客戶端包在裡面，算是保護信息來源的一種方式，這樣在洋蔥路由器之間可以保持通訊安全。同時對於客戶端，洋蔥代理服務器又作為 SOCKS 接口。一些應用程序就可以將 Tor 作為代理服務器，網絡通訊就可以通過 Tor 的虛擬環路來進行。

進入 Tor 網絡後，加密信息在路由器間層層傳遞，最後到達「出口節點」（exit node），明文數據從這個節點直接發往原來的目的地。對於目的地主機而言，是從「出口節點」發來信息。要注意的是明文信息即使在 Tor 網絡中是加密的，離開 Tor 後仍然是明文的。維基解密創始人便聲稱其公開的某些文件是截獲於 Tor 的出口節。

#### 隱藏服務

Tor 不僅可以提供客戶端的匿名訪問，Tor 還可以提供服務器的匿名。通過使用 Tor 網絡，用戶可以維護位置不可知的服務器。這些服務器所構成的網絡被稱為「Tor Hidden Services」，信息界又稱為暗網，一般的互聯網則被相應地稱為明網。因為在明網里，客戶端和服務端彼此知道對方的真實 IP 地址，而在暗網里雙方互不知 IP 地址。若服務端能做到不記錄用戶使用信息，以及客戶端能做到任何時刻都不輸入真實個人數據，則通過 Tor 隱藏服務可以達成上網的完全匿名性。

如果要訪問Tor隱藏服務，客戶端必須安裝 Tor 瀏覽器，在搭載 Android 操作系統的手機或平板電腦上，則必須安裝 Orfox。

在 Tor 瀏覽器裡面，於地址欄輸入 Tor 隱藏網絡特有的頂級域名 .onion，可以訪問 Tor 隱藏服務（暗網）。Tor 瀏覽器可以識別 .onion 域名，並自動路由到隱藏的服務。然後，隱藏的服務將請求交由標準的服務器軟件進行處理，這個服務器軟件應該預先進行配置，從而只偵聽非公開的接口。

Tor 隱藏服務（暗網）有個另外的好處，由於不需要公開的 IP 地址，服務就可以躲在防火牆和 NAT 背後。但如果這個服務還可以通過一般的互聯網（明網）來訪問，那也會受到相關連的攻擊，這樣就沒有真正的隱藏起來。」

——[Tor - 維基百科](#)

參見：

- [Tor 官網](#)

- [securityinabox | Tor Browser for Windows - 網絡匿名及審查規避](#)

## （二）Tor 的入門級使用

### 1. 獲取 Tor 瀏覽器

Tor 的官網已被 GFW 封鎖，你首先需要一個可用的代理工具來訪問 Tor 官網並下載適用的 Tor 瀏覽器。

### 2. Tor 網絡設置

初次打開 Tor 瀏覽器時應用會先要求用戶進行 Tor 網絡設置，對於身處中國大陸的用戶應該勾選「我所在的國家對 Tor 進行了封鎖」，之後選擇「內置網橋」，目前有「obfs4」、「obfs3」和「meek-azure」三種網橋可選。

如果你沒有連接代理，可以選擇中國可用的 meek-azure 網橋（即把 Tor 混淆成訪問微軟 Azure 雲服務的流量）實現僅限於 Tor 的「單重代理」。然而使用 meek-azure 網橋確實可以連接，但網頁的加載時間太過漫長，不論是與用普通瀏覽器直連訪問牆內網站還是使用代理訪問牆外網站的體驗均相差甚遠，所以不推薦這種使用方式。在雙重代理部分使用的「obfs4」網橋的速度要比 meek 快不少。



### 3. 使用雙重代理

#### 原因1

因為 Tor 的影響力很大，GFW 對 Tor 進行重點封殺。全球大多數的 Tor 中繼節點都被 GFW 列入「IP 黑名單」。所以天朝的網友，如果單獨使用 Tor，很難聯網成功。這種情況下，就需要使用雙重代理。

#### 原因2

所有的軟件都可能有缺陷（Tor 也不例外）。如果你僅僅使用 Tor，萬一 Tor 出現安全漏洞並且被攻擊者利用，那麼攻擊者就有可能對你進行逆向追溯（說不定能追溯到你的真實公網 IP）。

而如果使用多重代理，即使出現上述風險，攻擊者也只能追蹤到 Tor 的前置代理，而不會直接追蹤到你本人。這樣一來，風險大大降低。

#### 原因3

前面提到，全球的 Tor 網絡中可能會有陷阱節點。雖然你可以利用俺剛才介紹的方法，排除危險國家/地區的節點，但並不能確保萬無一失。

比如說你碰到某個極小概率事件——你使用的線路上，碰巧三個節點都是陷阱——這種情況下，你的真實公網 IP 會暴露。

但如果你用了雙重代理，即使碰到這種小概率事件，只會暴露你使用的前置代理服務器的 IP，而【不會暴露】你的本人的公網 IP。

——編程隨想：「如何翻牆」系列：關於 Tor 的常見問題解答

如果利用已有的代理工具 + Tor 實現雙重代理（如 VPN+Tor、Shadowsocks+Tor、V2Ray+Tor），你需要在「內置網橋」選項中選擇「obfs4」網橋，然後勾選「使用代理訪問互聯網」。接下來你需要填寫自己的代理信息，包括代理類型（SOCKS 4、SOCKS 5、HTTP / HTTPS）、地址、端口、用戶名和密碼（可選）。

如果選擇「SOCKS 5」作為代理類型，則「地址」欄填寫本地 Socks5 監聽地址 (Local Socks5 Address)，通常為「127.0.0.1」（可以在 Shadowsocks、V2Ray 客戶端查看，下同），「端口」欄填寫本地 Socks5 監聽端口 (Local Socks5 Port)，如「1080」。



如果選擇「HTTP / HTTPS」作為代理類型，則「地址」欄填寫本地 HTTP 監聽地址 (Local Http Address)，仍為「127.0.0.1」，「端口」欄填寫本地 HTTP 監聽端口 (Local Http Port)。



參見：

★ [有關密碼學的科普內容 | Proxy over Tor](#)

## 七、搜索引擎

百度以競價廣告和詐騙信息著稱，已是公認的業界毒瘤，建議有能力的讀者早日棄用；搜狗、360搜索、必應國內版等搜索引擎也是信息封鎖政策的執行者，同樣建議有能力者棄用。

國外的搜索引擎，在搜索內容質量上 Google 是首選。如果你對 Google 蒐集用戶數據的行徑和監控資本主義的商業模式表示擔心，可以使用承諾不監控、不記錄用戶搜索內容的 [DuckDuckGo](#) 和 [StartPage](#) 等作為替代品，值得一提的是 StartPage 提供 Google 的搜索結果，體驗較佳。DuckDuckGo 和 StartPage 同樣被中國 GFW 封鎖，需翻牆後使用。

在牆內你還可以嘗試使用未被 GFW 封殺的、更小眾的國外搜索引擎，比如來自俄羅斯的 [Yandex](#)。

參見：[百度替代指南，幫你用上更好的搜索引擎](#)（原文來自「[eBooksPlan](#)」：[百度替代指南，幫你用上更好的搜索引擎](#)）

參見：

- 麥琪：百度 為作惡而生
- Solidot | 百度代理商被指強推信息流廣告 (2017-09-25)
- 【麻辣總局】「嫩滑」體驗之百度與谷歌 (2018-08-08)
- Solidot | 百度再度被指混淆廣告投放和合法結果 (2018-12-11)
- 新聞實驗室 | 搜索引擎百度已死 (2019-01-22)
- 方可成 | 我為什麼要寫《搜索引擎百度已死》 (2019-01-23)
- 端傳媒 | 洛德：在「被養」的互聯網世界，批評百度時我們忽略了什麼？ (2019-01-25)

## ★ 對百度的爭議 - 維基百科 目錄

### 1 域名劫持和軟件流氓化

- 1.1 域名劫持
- 1.2 軟件強制捆綁安裝
- 1.3 旗下軟件站植入惡意代碼
- 1.4 手機應用超範圍申請權限

### 2 百度推廣相關爭議

- 2.1 影響網民使用的競價排名
  - 2.1.1 競價除名醜聞
  - 2.1.2 央視曝光百度競價排名事件
  - 2.1.3 魏則西事件
  - 2.1.4 推廣賭博網站事件
  - 2.1.5 百度搜索洋酒回收遭遇詐騙
  - 2.1.6 假冒NARS中國大陸官網事件
  - 2.1.7 假冒蘋果官方售後維修店事件
  - 2.1.8 新華社曝光百度競價排名事件
  - 2.1.9 「復大醫院」廣告事件
  - 2.1.10 「上海美國領事」廣告泛濫
  - 2.1.11 高仿簽證網站廣告事件
  - 2.1.12 用戶搜索「QQ郵箱」出現盜號網站推廣
- 2.2 是否為廣告內容的爭議
- 2.3 移動端、網頁端推廣「雙標準」問題

### 3 侵犯版權

### 4 涉嫌侵犯隱私

### 5 內容審查

### 6 百度貼吧相關爭議

- 6.1 2009年被互聯網整風行動譴責與曝光
- 6.2 爆吧事件
- 6.3 2009年高校貼吧禁言事件
- 6.4 2012年百度員工收受賄賂付費刪帖
- 6.5 被淨網2014行動譴責與曝光
- 6.6 盜版網絡原創文學問題
- 6.7 「賣吧」事件
  - 6.7.1 2015年艦隊collection吧吧主被調換事件
  - 6.7.2 2015年Minecraft吧空降吧主事件
  - 6.7.3 2016年血友病吧事件
  - 6.7.4 學科類貼吧被賣事件
- 6.8 守望先鋒吧被封禁事件
- 6.9 惡搞事件
  - 6.9.1 2010年X來自未來事件
  - 6.9.2 2011年齟牙哥事件
- 6.10 戒賭吧被封
- 7 色情內容
- 8 百度文庫侵權事件
- 9 百度百科相關爭議
  - 9.1 開放性爭議
  - 9.2 版權爭議
  - 9.3 破壞惡搞
- 10 行業糾紛
  - 10.1 奇虎360與百度爭鬥事件
  - 10.2 「作業幫」糾紛
    - 10.2.1 引起不良學習習慣
    - 10.2.2 涉嫌抄襲學霸君界面
    - 10.2.3 陷害小猿搜題事件
  - 10.3 與今日頭條的糾紛
- 11 百度其他爭議
  - 11.1 偽造民意 建黨節虛假「獻花」
  - 11.2 ImageNet圖像識別挑戰賽作弊
  - 11.3 用戶體驗總監因演講內容不當被撤職
  - 11.4 與王志安的糾紛
  - 11.5 百度沒有文化一文事件
  - 11.6 百家號的自家內容過多

## 八、密碼管理

### （一）密碼設置

使用大小寫字母、數字、符號隨機組合成的長密碼，如果擔心自己記不住可將其記在實體紙張上或者密碼管理器中。

不要使用 123456、qwerty 等簡單密碼或者 admin 等默認密碼，不要將自己的姓名拼音、出生日期用作密碼。

對不同的賬號設置不同的密碼，不要重複使用同一密碼以免其中一家網站的數據庫遭遇黑客攻擊「脫庫」後導致其他賬號隨之一並洩漏、擴大損失。

### （二）密碼管理器

使用密碼管理器的好處在於用戶只要記住密碼管理器自身的主密碼，就可以在需要時由密碼管理器應用自動填充你的各類網絡賬戶的複雜密碼，免去了自己記憶密碼的麻煩，也有利於減少在公共場所輸入密碼時被他人旁窺竊取密碼的可能性。如果你的設備配備了 Touch ID、Face ID 等生物識別傳感器，在使用密碼管理器無疑會更加便利。

常見的密碼管理器應用有 1Password、KeePass、LastPass 等，作為 iCloud 服務組成部分的 iCloud Key Chain（鑰匙串）也發揮著密碼管理器的作用。

切勿使用盜版、破解版密碼管理器應用。

## 九、輸入法

輸入法應用為了擴大詞庫，通常會將用戶的個人詞庫上傳到服務器。對中國政府來說獲取本國互聯網企業存儲在境內服務器上的數據易如反掌，而有些國內廠商在用戶信息上傳過程中的加密環節出了紕漏，增加了用戶隱私被黑客劫取的風險。

在輸入法的選擇上應同樣遵循盡量不用國產軟件的原則，建議盡量使用系統原生輸入法或由知名國外廠商開發的輸入法：

iPhone/iPad：蘋果原生輸入法、Gboard

Mac：蘋果原生輸入法、鼠鬚管 Squirrel

Android 手機：Gboard

Windows PC：微軟原生輸入法、小狼毫 Weasel

\* **Gboard** 是 Google 為 Android / iOS 設備開發的輸入法應用，特色是支持滑行輸入、支持內置的 Google 搜索引擎。Gboard 未上架中國區 App Store，可在其他國家/地區的商店獲取。

\*常見國產輸入法：搜狗輸入法、科大訊飛輸入法、百度輸入法、QQ輸入法、各大國產手機廠商預置的輸入法……

\*「鼠鬚管」和「小狼毫」分別是開源輸入法軟件「RIME／中州韻輸入法引擎」的 macOS 和 Windows 發行版。

參見：

- Solidot | 搜狗輸入法收集用戶隱私信息，未屏蔽爬蟲 (2013-06-05)
- Solidot | 流行虛擬鍵盤應用洩漏 3100 萬用戶信息 (2017-12-06)
- Solidot | 一加的「Badword」過濾主要影響中國用戶 (2018-01-29)
- Solidot | 百度手機輸入法被發現會調用錄音功能 (2018-07-02)

## 十、智能家居

安全性：none > Apple > Google、Amazon 等國際廠商 > 小米、阿里等國產廠商

對於像 Amazon Echo 這樣搭載智能語音助手、能夠控制智能家居設備的智能音箱，能不用盡量不用。

參見：

- ★ Solidot | 亞馬遜證實 Alexa 記錄了私人對話然後發送給隨機聯絡人
- Solidot | 黑客能利用締奇掃地機器人監視屋主

## 十一、多設備策略

如果你對信息安全性要求很高，並且具有相應的經濟條件，建議同時使用兩部或更多部手機。日常使用時，在一部手機上安裝支付寶、微信、QQ、新浪微博等國產應用，不要存儲任何政治敏感性文件；另一部安裝翻牆軟件和 Twitter、Facebook、Instagram、Telegram、WhatsApp 等國外應用，不要安裝任何國產社交、通訊應用，以防中國政府借助國產應用內植入的後門監視手機用戶。

此外，多設備策略可以應對可能發生的警察強制查手機的情況。新疆警察使用手持設備在街頭攔截路人檢查手機是否存有「暴恐」內容已成常態，手機掃描儀等相關圖片在 2017 年就已流傳在微博、推特等平台上。2017 年下半年以來 Telegram 中文圈流傳著北京、蘇州等地的警察在地鐵口強制掃描路人手機內容，內地新疆化趨勢正在路上。雖然警察強查手機侵犯隱私於法無據，但在這個取消國家主席任期限制的憲法修正案都能毫無阻力地通過的魔幻國度，沒有什麼是不可能的，還是小心為妙吧。

警察掃描手機內容並非虛言，在技術上完全可以實現，參見：

- [Reuters | At Beijing security fair, an arms race for surveillance tech](#)
- [Solidot | 中國公司展示能破解 iOS 系統的掃描儀](#)

本節末尾附上編程隨想「如何隱藏你的蹤跡，避免跨省追捕」系列博文的鏈接，以供參考：

[如何隱藏你的蹤跡，避免跨省追捕\[0\]：為什麼要寫此文？](#)

[如何隱藏你的蹤跡，避免跨省追捕\[1\]：網絡方面的防範](#)

[如何隱藏你的蹤跡，避免跨省追捕\[2\]：個人軟件的防範](#)

[如何隱藏你的蹤跡，避免跨省追捕\[3\]：操作系統的防範](#)

[如何隱藏你的蹤跡，避免跨省追捕\[4\]：通訊工具的防範](#)

[如何隱藏你的蹤跡，避免跨省追捕\[5\]：用多重代理隱匿公網IP](#)

[如何隱藏你的蹤跡，避免跨省追捕\[6\]：用虛擬機隱匿公網IP（原理介紹）](#)

[如何隱藏你的蹤跡，避免跨省追捕\[7\]：用虛擬機隱匿公網IP（配置圖解）](#)

[如何隱藏你的蹤跡，避免跨省追捕\[8\]：如何搭配「多重代理」和「多虛擬機」](#)

[如何隱藏你的蹤跡，避免跨省追捕\[9\]：從【時間角度】談談社會工程學的防範](#)

[如何隱藏你的蹤跡，避免跨省追捕\[10\]：從【身份隔離】談談社會工程學的防範](#)

## 第十一節 牆外社交媒體使用建議

本節預設的受眾限於居住在中國大陸、希望在網絡空間積極表達政治見解的異議人士，並非在所有情況下都適用，特此說明。

### 一、賬號管理

使用 Gmail、iCloud（非雲上貴州）等國外電子郵箱或者端對端加密的匿名電子郵箱註冊牆外社交媒體賬號，不要使用 163、126、qq 郵箱等國內電子郵箱賬號註冊牆外社交媒體。

不要使用中國大陸 +86 開頭的手機號碼註冊牆外社交媒體或者將該號碼與社交賬號相綁定。

使用複雜密碼。

開啓雙重驗證兩步驗證（Two-Factor Authentication, 2FA），首選基於驗證器應用的 2FA 或者使用 U2F (Universal 2nd Factor)，謹慎使用基於 SMS 短信的 2FA。

從事高風險活動的人士建議運行虛擬機後使用 Tor 瀏覽器完成註冊。

### 二、身份隔離

註冊 Twitter 等牆外社交媒體時建議使用新的虛擬身份，同時與牆內的社交/即時通訊平台使用的身份相隔離。

換言之，不要在 Facebook、Instagram、Twitter、WhatsApp、Facebook Messenger、Telegram、Line、Reddit、Quora 等牆外平台使用與牆內的微信、微信朋友圈、QQ、QQ 空間、新浪微博、貼吧、知乎、豆瓣、虎撲、bilibili、天涯、簡書等平台相同的用戶名、暱稱、頭像和簽名。

不要將相同的聯繫方式，如電子郵箱、即時通訊軟件賬號（微信、QQ、Telegram 等）以備注、個人資料或博文等形式公佈同時公佈在牆外和牆內社交平台上，以防中國政府部

門或者居心不良之人通過牆外與牆內社交軟件賬號之間的關聯，利用已經過實名制認證的牆內社交軟件來確定用戶的真實身份。

不要在牆外平台上發送可能洩露自己真實身份的信息，比如公開自己的姓名、學號、學校、專業、工作地點、常住城市。

不要發送露臉的自拍照，帶有易於判斷具體位置的地標的照片，未對姓名、身份證號、出發地、目的地、座位等關鍵信息打馬的火車票、高鐵票、飛機票的照片，未對卡號、安全碼等關鍵信息打馬的銀行卡的照片。發送自己拍攝照片前建議去除照片的 EXIF（Exchangeable image file format，可交換圖像文件格式），後者包含了照片的屬性信息和拍攝數據，包括拍攝設備、拍攝時間和拍攝地點定位等信息。iOS 用戶可以使用 Shortcuts 捷徑「[Clear Photo Exif Info](#)」去除 exif 信息，Android 用戶可以從 Google PlayStore 下載 [Photo Metadata Remover - Clear Exif Metadata](#)。方便起見你也可以在相冊中對截屏後發送原照片的截圖。

不要在社交平台分享你的定位信息，不論是你的居住地點、工作地點還是旅行時訪問的地點。

不要將網易雲音樂等牆內服務的超鏈接轉發到牆外社交平台，因為有些鏈接中可能包含了牆內平台用戶的個人信息，網警因而可以順藤摸瓜。

如果需要發表風險較高的言論，如「辱包」（諷刺中共領導人習近平）言論、呼籲顛覆中共政權的言論，建議使用該社交賬號時全程使用 Tor 瀏覽器，或者在虛擬機中使用 Tor。

不要在牆外社交媒體使用自己在牆內社交媒體的較為明顯習慣性用語。

如果自行檢查時發現有身份洩露的風險後建議立即放棄當前帳號（刪除舊賬號發佈的所有內容後註銷該賬號），然後另行註冊新賬號。不要通過修改用戶名、暱稱和頭像等信息繼續使用該賬號，如果你已經被定位，後續的修改是無濟於事的。

### 三、言論邊界

「互聯網不是法外之地」，不要發表任何涉及兒童色彩、種族歧視、仇恨言論等在文明國家公認為不法的言論，違反後果包括但不限於被平台封號、承擔法律責任、被人肉搜索。



建議中文圈的推特用戶瀏覽支納維基上的「免雜」詞條和支納維基、惡俗維基上被「出道」（指戶籍等個人信息被公開）的反面教材的事跡。

參見：

- RFA | 大陸掀起「推特強拆」風暴 數百推友被刪號 (2018-12-12)
- 紐約時報中文網 | 網絡審查再升級：中國推特用戶遭政府盤查或拘留 (2019-01-11)

## 第五章 信息難民自救指南

### 第十二節 404 信息保存

#### 一、網頁存檔

(一) archive.is

(二) archive.org

#### 二、截圖

(一) 網頁截圖/長截圖

1. 移動端

2. 桌面端

(二) 截圖拼接

#### 三、頁面存儲

#### 四、Telegraph

#### 五、區塊鏈

### 第十三節 404 信息獲取

#### 一、中國數字時代

#### 二、端點星

#### 三、其他渠道

## 第十二節 404 信息保存

中國網民在 GFW 內的微信、微博等平台上發佈的涉及敏感事件和話題（如 2017 年的紅黃藍幼兒園事件、北京清退「低端人口」事件等）的內容往往會被管理者以「多人舉報」、「違反《網絡安全法》」等藉口刪除，即人們常說的「404」。本節內容旨在介紹幾種在敏感信息被「404」將之保存下來以便二次傳播的方法。

### 一、網頁存檔

在使用網頁存檔工具保存網頁的優勢在於可以基本保持網頁的原貌，主要用以保存微信公眾號文章以及財新網等牆內媒體的新聞報道。

#### （一）archive.is

archive.is 是一個私人資助的數字時間囊網站，提供抓取網頁內容的服務。archive.is 還擁有 archive.li、archive.fo 等多個不同的域名，支持以「archive.today.xxx」的短鏈接形式轉發分享。該網站已被 GFW 屏蔽。

#### （二）archive.org

archive.org 是一個非營利性的數字圖書館組織，同樣提供網頁存檔服務，它的中文名稱是「互聯網檔案館」。雖然它的 archive.is 的域名很相像，兩者在網頁抓取方式上存在差別。

### 二、截圖

長截圖工具主要用於保存微博等難以直接存檔的社交媒體內容，或者用以獲取牆外媒體資訊分享到牆內，例如香港端傳媒的客戶端自身支持將文章導出為長圖的功能，以使用戶轉發傳播。

## （一）網頁截圖/長截圖

### 1.移動端

iOS 平台上的長截圖應用有 Picsew 和 Tailor，另外圖片標注應用 iMark（我的標記）與智能剪貼板應用 Pin 也提供網頁截圖的功能。Android 平台上的知名長截圖應用有 PPIICC。

### 2.桌面端

利用Chrome開發者工具進行網頁長截圖（Chrome版本要求：59或更高版本）

macOS：

Command + Option + I

①截取整個網頁的內容

Command + Shift + P

輸入命令：Capture full size screenshot

②（模擬移動設備）截取手機版網頁長圖

Command + Shift + M

點擊右上方的擴展按鈕選擇「Capture full size screenshot」

Windows：

①Control + Option + F12

截取整個網頁的內容

②Control + Shift + P

輸入命令：Capture full size screenshot

參見 [少數派：利用 Chrome 原生工具進行網頁長截圖 | 一日一技](#) [archive](#)

macOS 平台上的截圖應用 Xnip 也支持長截圖。

## （二）截圖拼接

對於過長的截圖，長截圖工具可能無法一次性抓取，此時可以採取分頁截圖後再拼接的方法。iMark 提供最高支持 9 張圖片的拼圖功能，其生成的長圖能保持高清不留痕跡，值得推薦；如果分頁截圖超過 9 張，還可以在生成的長圖的基礎上繼續拼接。

### 三、頁面存儲

在 Windows 和 macOS 這樣的桌面級操作系統上，可以利用瀏覽器提供「頁面存儲」功能將相關網頁存儲到本地。其缺點是最終得到的是一個文件，難以直接分享。（使用 macOS 的 Safari 瀏覽器存儲的網頁歸檔文件類型為「.webarchive」，在 Windows 上可用 IE 等瀏覽器打開該類文件）

在移動設備上可以將網頁導出為 pdf 或 epub 文件，缺點同上。

### 四、Telegraph

Telegraph 是由加密即時通訊應用 Telegram 提供的匿名博客服務，用戶可以將涉及敏感話題的網頁內容轉錄到 Telegraph 後加以轉發分享。

### 五、區塊鏈

將區塊鏈用於首見於 2018 年 4 月的北大岳昕事件，有網友將她的公開信寫入了以太坊 ETH 的交易信息，使之就此長存於區塊鏈。

你也可以選擇 Steemit、Matters 等以區塊鏈作為底層技術的平台存儲信息。

參見：

- 為眾人抱薪者，必將銘刻於區塊鏈上
- 某天，當你像北大岳昕一樣無助時，請把你的話說給區塊鏈（含教程）

## 第十三節 404 信息獲取

### 一、中國數字時代

「[中國數字時代](#)（英語：China Digital Times；縮寫：CDT）是一個英語、中文雙語的新聞網站，創辦人及現任總編輯為蕭強，2004年創辦英文版，2009年創辦中文版，致力於聚合「中國的社會與政治新聞，和它在世界上的新興的角色」有關的報道和評論。網站由加州大學伯克利分校的新聞研究生院師生創辦，現由加州大學伯克利分校信息學院「逆權力實驗室」（Counter-Power Lab）提供技術支持和反封鎖軟件的開發。網站的中文內容來自對自媒體和防火長城外網站時政類內容的系統採集分類，編輯推薦和部分原創性報道；英文部分包括新聞聚合和翻譯的內容。」——[中國數字時代 - 維基百科](#)

中國數字時代會實時轉載牆內熱點議題相關的文章，包括但不限於已經被刪除的內容，不失為瞭解中國網絡輿論的一個窗口。中國數字時代已經被 GFW 屏蔽，在中國大陸需要翻牆才能訪問。

除了 [中國數字時代](#) 網站外，你也可以通過關注 Telegram 頻道 [中國數字時代消息推送](#) 接收資訊。

## 二、端點星計劃

「Terminus 端點星計劃，是在 GitHub 開放平台搭建的一個站點，用於備份微信、微博等平台被刪文章。」

端點星已先後被微信和 GFW 屏蔽，在中國大陸需要翻牆才能訪問。

參見：[如何協作參與端點星計劃](#)

## 三、其他渠道

相關網站：[自由微博](#)、[自由微信](#)、[牆與書](#)

## 四、搜索引擎

在 Google 等不受中共審查的搜索引擎中搜索被刪文章、帖子的標題或關鍵詞查找他人的轉載和備份。

參見：[數字移民 | 如何找回被刪除的網頁/新聞](#) (2018-10-14)

## 第六章 番外

### 第十四講 去中心化網絡

- 一、ZeroNet
- 二、Mastodon
- 三、Steemit
- 四、IPFS
- 五、Matters
- 六、其他

### 第十五講 加密數字貨幣

- 一、加密數字錢包
- 二、如何獲取比特幣

## 第十四講 去中心化網絡

牆外的 Facebook、Instagram、Twitter 和牆內的微信、微博、豆瓣、知乎、貼吧等社交平台都是典型的中心化網絡的產物。用戶的數據統一存儲在中心服務器上，全操於平台服務商之手，因此網信辦等公權力機關可以肆無忌憚地刪帖銷號，或者通過惡法和行政命令要求騰訊、新浪等運營者自我審查，製造白色恐怖；Facebook 可以藉此分析用戶習慣、精準投送廣告和其他信息，將自己掌握的海量用戶數據變現。2018 年 Facebook 用戶數據洩露醜聞被曝光後人們逐漸開始對 Facebook 等互聯網巨頭主導的監控資本主義 (Surveillance Capitalism) 商業模式和傳統的中心化網絡有所警醒。

參見：

- [Solidot | Facebook 付費給青少年安裝它的 VPN 應用收集隱私，曝光之後宣佈將關閉](#)
- [The Verge | Apple blocks Facebook from running its internal iOS apps](#)

與中心化網絡相對應的去中心化網絡不再需要高度集中的中心服務器，每一個去中心化網絡的參與者都自動成為該網絡中的一個節點，數據將分布存放在參與網絡的每一台設備，從而避免了對數據享有絕對控制權的網絡巨頭濫用支配地位的可能。

去中心化網絡能夠彌補中心化網絡的若干弊病，有利於保障用戶的隱私權與信息自決權，但它目前仍不夠完善，現存的多個去中心化社交媒體的規模都無法與 Facebook 和 Twitter 相匹敵，在短期內顯然無法全面取代中心化網絡。編者對去中心化網絡所知十分有限，在此僅提供相關名詞和摘自維基百科的解釋，僅供讀者參考。

## 一、ZeroNet

「ZeroNet，中文被譯為「零網」，是一個以對等網絡用戶為基礎構成的類互聯網的分布式網絡。ZeroNet 的總部位於匈牙利的布達佩斯。ZeroNet 默認不提供匿名保護，但用戶可以使用 Tor 來隱藏 IP 地址以達到匿名效果。此軟件自帶的 Tor 網絡在中國大陸被封禁，用戶可能需要前置 VPN 才能正常下載初始配置文件。ZeroNet 使用了比特幣加密技術和 BitTorrent 網絡協議。現時該平台上托管了很多熱門網站，而郵件客戶端、文件管理器和新聞客戶端等專有功能也為 ZeroNet 的生態系統增加了價值。」

—— [ZeroNet - 維基百科](#)

參見：

- [ZeroNet 官網](#)
- [ZeroNet 工作原理](#)
- [如何使用 Tor 實現匿名](#)

## 二、Mastodon

「Mastodon（官方中文譯「萬象」，網民又稱「長毛象」）是一個免費開源的去中心化的分布式微博客社交網絡。它的用戶界面和操作方式跟推特類似，但是整個網絡並非

由單一機構運作，卻是由多個由不同營運者獨立運作的服務器以聯邦方式交換數據而組成的去中心化社交網絡。每個Mastodon的營運站點被稱為「實體 (Instance)」，用戶可到任何開放登記的實體登記，任何一個實體上的用戶可以與其他實體上的用戶溝通。用戶在推特中發佈的內容稱為「推文」，而在Mastodon中發佈的內容則稱為「啞文 (Toot)」，用戶可以調整隱私設置限制啞文被其他人或實體讀取或查看。Mastodon 吉祥物是一個棕色或灰色的長鼻目，描繪成正在使用平板電腦或智能手機。

此服務試圖通過定位成獨立運作的小型社區，而不是由上而下的審查。如同Twitter，Mastodon 支持用戶間直接、私密的消息，但與Twitter張貼的「推文」不同，Mastodon 的「啞文」可以是：對用戶、用戶的追蹤者私密，對特定實體、或通過實體網絡公開。聯邦式的 Mastodon 實體組成聯邦世界。」

—— Mastodon - 維基百科

參見：

- Mastodon 項目官網

- 長毛象中文站

長毛象中文站維護者 海啞督 的 一張圖看懂長毛象項目

\* Instance 也譯為「實例」，編者注

### 三、Steemit

Steemit 是一個基於 Steem 區塊鏈為內容發佈者提供獎勵的博客和社交網站。用戶可以通過發佈、發現和評論來獲得 Steem 區塊鏈提供的 Steem 和 Steem Dollars 兩種可交易的代幣。運行 Steemit 的 Steemit, Inc. 是一家設在紐約，總部位於弗吉尼亞州的私人公司。

Steemit 的亮點在於發佈在該平台上的內容會被存儲在區塊鏈中，理論上可以永久保存（同時一經發佈後就無法刪除）；作者可以根據讀者的「點贊」數量來獲得相應的代幣獎勵。（V2Ray 項目已將其官方博客遷移到了 Steemit 上—— <https://steemit.com/@v2ray>）

目前獲取 Steemit 帳號的方式主要有免費註冊、使用比特幣等加密數字貨幣付費購買和從已有賬號者手中購買賬號。免費註冊 Steemit 賬號這種方式對中國大陸的用戶不是很友好，往往申請就石沈大海杳無音訊。如果你只是想要一個賬號來給別人的文章點贊幫她/他創收，用支付寶從已有賬號者那裡買一個倒也無妨；如果你想將 Steemit 作為發佈原



創內容的博客平台，編者建議通過 <https://anon.steem.network> 支持加密數字貨幣的方式購買一個 Steemit 賬號，以保證賬號的相對匿名性和自身安全。

參見：[Steemit 註冊頁面](#)

## 四、IPFS

星際文件系統（InterPlanetary File System，縮寫 IPFS）是一個旨在創建持久且分布式存儲和共享文件的網絡傳輸協議。它是一種內容可尋址的對等超媒體分發協議。在 IPFS 網絡中的節點將構成一個分布式文件系統。它是一個開放源代碼項目，自 2014 年開始由 Protocol Labs 在開源社區的幫助下發展。其最初由 Juan Benet 設計。

IPFS 是一個對等的分布式文件系統，它嘗試為所有計算設備連接同一個文件系統。在某些方面，IPFS 類似於萬維網，但它也可以被視作一個獨立的 BitTorrent 群、在同一個 Git 倉庫中交換對象。換種說法，IPFS 提供了一個高吞吐量、按內容尋址的塊存儲模型，及與內容相關超鏈接。這形成了一個廣義的 Merkle 有向無環圖（DAG）。IPFS 結合了分布式散列表、鼓勵塊交換和一個自我認證的名字空間。IPFS 沒有單點故障，並且節點不需要相互信任。分布式內容傳遞可以節約帶寬，和防止 HTTP 方案可能遇到的 DDoS 攻擊。

該文件系統可以通過多種方式訪問，包括 FUSE 與 HTTP。將本地文件添加到 IPFS 文件系統可使其面向全世界可用。文件表示基於其哈希，因此有利於緩存。文件的分發採用一個基於 BitTorrent 的協議。其他查看內容的用戶也有助於將內容提供給網絡上的其他人。IPFS 有一個稱為 IPNS 的名稱服務，它是一個基於 PKI 的全局名字空間，用於構築信任鏈，這與其他 NS 兼容，並可以映射 DNS、.onion、.bit 等到 IPNS。

—— [星際文件系統 - 維基百科](#)

相比於中心化網絡下的 Google Drive、Dropbox 等網盤，基於 P2P 的 IPFS 更難為 GFW 所封殺，V2Ray 就已開始使用 IPFS 來分發安裝包和客戶端應用：

目前對於文件分享，P2P 的一個主流方案是 IPFS。和 BT 類似，IPFS 沒有中心服務器，你可以連接到其它的 IPFS 節點來下載所指定的文件。文件名（或目錄名）就是一個字符串，有了這個字符串，你就可以下載到 V2Ray 的安裝包。

—— [v2ray：嘗試使用 IPFS 來分發 V2Ray 安裝包](#)

原理與使用方法參見 [IPFS 官網](#)

## 五、Matters

[Matters](#) 是端傳媒前總編輯張潔平 (Annie Zhang Jie Ping) 離職後創辦的內容生態系統。[Matters](#) 以區塊鏈作為底層技術，以去中心化方式連接社群，以 IPFS 存儲信息，鼓勵用戶創造優質內容並予以回報，目前尚在內測中。

參見：

- [Matters Lab: 社交媒體的另一種可能：Arendt的桌子](#) (2018-04-02)
- [Matters Lab: Matters 項目草案：重塑內容價值鏈](#) (2018-05-31)
- [Matters Lab: 給Matters朋友們的一封信：向星際啟航](#) (2018-11-09)

## 六、其他

「[diaspora](#) 基於三大核心哲學：去中心化、自由和隱私。它希望能引起大家關切由中心所控制社交網站下的隱私問題，所以可以讓用戶自行架設服務器（或稱"pod"）來控制內容，而各個服務器可以再自行互動分享動態更新、照片或其它的資料。

[Friendica](#) 強調在隱私控制上的仔細設置，它是一個容易安裝在服務器上的軟件，以期待盡可能出現更多其它的社交網絡聯邦。[Friendica](#) 用戶可以從 Facebook, Twitter, Diaspora, GNU social, App.net, Pump.io 等等多項社交網絡服務來整合其聯繫人的名單到自己的社交時間流。

[GNU social](#) 的功能有點類似推特，但希望能為微博客社群，提供更開放、互相扶持的分散式溝通功能。企業或個人可以自行安裝 GNU social 在自家機器上，以控管自己的服務與資料數據。著名的公共網站如：[quitter.se](#) 和 [gnusocial.no](#)。」

——[iYouPort | 安全手冊：這裡是你需要的幾乎所有安全上網工具；以及為什麼建議不要使用以美國為基地的網絡服務](#)

## 第十五講 加密數字貨幣

編者對於加密數字貨幣所知有限，只能幫助入門者解決從無到有的問題，幣圈玩家請忽視本講內容。

### 一、加密數字錢包

Blockchain是業界領先的數字貨幣軟件平台，提供在線數字貨幣錢包服務。由平台在線托管數字貨幣的優點在於用戶只需要記住自己的比特幣地址和密鑰就可登錄管理，無需下載高達數百 GB 的完整交易列表而使電腦本地磁盤不堪重負。

為了確保資產安全，Blockchain 提供了多重安全驗證機制（層級數可由用戶決定），除了錢包 ID 和密碼外，每次登錄時都需要登錄驗證郵箱在驗證郵件中點擊確認鏈接；此外用戶還可以選擇加入兩步驗證、關聯手機號和備份恢復字串等方式增強賬戶的安全性。

建議使用端對端加密的匿名郵箱作為 Blockchain 的驗證郵箱，不要使用國內郵箱

關於兩步驗證 (2FA)，你需要在移動設備上安裝 Google Authenticator 或類似應用（請從 App Store、Google Play 等官方應用商店搜索下載），對相應網站進行關聯設置。之後每次登錄時你在輸入密碼後需要額外填寫 2FA 應用實時顯示的 6 位數驗證碼，該驗證碼會在設定的時間間隔內自動更新。

參考教程：

Velaciela: 比特幣錢包安全指南 (2018)

### 二、如何獲取比特幣

#### （一）交易平台

提供兩個加密數字貨幣交易平台，僅供參考。

LocalBitcoins：線下/線上交易比特幣

CoinCola：線下交易 BTC、ETH、BCH、USDT 等貨幣。

不推薦使用國內的交易平台。

## （二）購買流程

——以在 LocalBitcoins 購買比特幣為例

1. 買家可以根據賣家所在地區、標價、最低/最高購買額度、支付方式（支付寶、微信支付、國內銀行卡轉賬、PayPal……）等標準篩選賣家
2. 確定賣家後輸入需要購買的比特幣金額，開始交易
3. 按照賣家的要求付款
4. 賣家確認收到款項後釋放比特幣，由平台暫時托管
5. 稍後平台會將比特幣轉移到你的賬戶上
- \*6. 你可以將其比特幣轉移到自己的數字貨幣錢包中（需要支付一定手續費）

\*使用支付寶、國內銀行卡轉賬等支付手段進行比特幣交易會被中國政府監控，請謹慎使用這類交易手段，不要進行大額交易。

\*編者在自學加密數字貨幣的過程中從 Project V 官網處獲益良多，特此向小薇姐姐表示感謝🙏。

## 附錄

### 推薦閱讀

Security in-a-box 數據安全工具及策略 (中文版) (網頁)

數字安全實用手冊 (網頁, 內含三部 pdf 電子書)

人權捍衛者的數據安全與隱私 (電子書)

公民實驗室: 如何繞過互聯網審查 (電子書)

Citizen Lab: EVERYONE'S GUIDE TO BY-PASSING INTERNET CENSORSHIP

privacytools.io (網頁)

Electronic Frontier Foundation 電子前哨基金會 (網站)

數字移民 (網站)

https://medium.com/@iyouport (博客)

https://steemit.com/@iyouport (博客)

有關密碼學的科普內容 (博客)

【編程隨想】收藏的電子書清單 (多個學科, 含下載鏈接) (網頁)

鳴謝

(按首字母順序排序)

Baye

編程隨想

破娃醬

clowwindy

聰聰 (印象筆記 | 科技 NEWS)

Cryptoboy404

iYouPort

Telegram Messenger

PSA-安全公告專欄

泡泡

Shadowrocket News

Solidot

Telegram 新手指南

Victoria Raymond

網絡公民安全指南

信息極權社會的生存手冊 (已刪號)