MMO TẬP SỰ

Tại sao làm MMO cần ẩn danh tính thật?

02

BÍ MẬT ẨN DANH TRÌNH DUYỆT

oneADX

Hidemyacc

Mục Lục

Lời mở đầu

Chào bạn,

Nếu bạn đang cần tạo và nuôi tài khoản nhưng chưa biết làm thế nào để không bị nền tảng khóa một cách vô lý thì bạn nên bắt đầu lại bằng việc nghiên cứu nội dung trong cuốn ebook này.

Ở cuốn ebook 1, Hidemyacc đem đến cho bạn những kiến thức đầu tiên để bạn Hiểu ngành - Hiểu nghề - Hiểu chính bản thân mình khi bắt tay làm MMO thì cuốn ebook này sẽ tập trung vào giải thích các yếu tố ảnh hưởng đến việc một tài khoản của bạn "sống" và cách bạn giữ cho tài khoản hoạt động bền vững.

Hidemyacc không hướng dẫn chi tiết các mẹo để tạo và nuôi tài khoản thành công. Vì thực tế chúng tôi không nắm được những "tut", "trick" này. Dựa trên kinh nghiệm chuyên môn và những nghiên cứu để phát triển công nghệ ẩn danh trình duyệt, Hidemyacc sẽ giải thích cho bạn cách các website đang thu thập thông tin khi bạn truy cập website của họ và cách tạo "môi trường sạch" để tạo và nuôi số lượng lớn tài khoản an toàn.

CÁC YẾU TỐ ẢNH HƯỞNG ĐẾN QUÁ TRÌNH REG - NUÔI TÀI KHOẢN

Có một thực tế khá buồn khi rất nhiều website đưa Việt Nam vào danh sách quốc gia cần siết chặt chính sách. Nguyên nhân xuất phát từ những cá nhân, đôi nhóm lợi dụng những lỗ hổng của nền tảng để khai thác và trục lợi cá nhân hay còn gọi là "cheat" nền tảng khiến cách website phải bật "red flag" cho các truy cập đến từ Việt Nam.

Điều này vô tình khiến những ai làm ăn chân chính, đi theo con đường whitehat cũng bị ảnh hưởng. Rất nhiều tài khoản vốn không vi phạm chính sách cũng bị khóa vô tội vạ. Vậy nên, dù bạn có đang đi theo con đường whitehat thì bạn vẫn cần tìm hiểu những kiến thức về môi trường sạch, môi trường an toàn để bảo vệ tài khoản của mình. Hãy bắt đầu bằng việc tìm hiểu cách tạo một "môi trường sạch".

Vậy thế nào là "môi trường sạch" để reg- nuôi tài khoản?

Đầu tiên, hãy cùng định nghĩa về môi trường "không còn sạch" hay môi trường đã bị nền tảng cho vào blacklist.

Khi bạn truy cập vào bất kỳ nền tảng nào, ví dụ Facebook, thông qua công nghệ browser fingerprinting, Facebook sẽ biết được tài khoản của bạn hiện đang được login ở thiết bị và địa chỉ IP nào bằng cách thu thập các thông số browser fingerprint (Hidemyacc sẽ giải thích chi tiết về browser fingerprint là gì ở phần sau). Trong trường hợp bạn có 2 tài khoản trở lên, Facebook hoàn toàn xác định được những tài khoản này đều cùng một người dùng.

Nếu tài khoản thứ nhất có hành vi bất thường như thường xuyên spam, chạy quảng cáo sản phẩm/dịch vụ vi phạm chính sách,... Facebook sẽ khóa tài khoản này và đưa thông tin thiết bị cùng địa chỉ IP của bạn vào blacklist. Và khả năng cao, tài khoản thứ hai cũng sẽ bị checkpoint hoặc khóa. Dù có tạo thêm "n" tài khoản nữa trên thiết bị và địa chỉ IP đó, bạn vẫn sẽ bị đưa vào nghi vấn. Bạn không thể tạo thêm tài khoản trừ khi dùng một máy mới và địa chỉ IP khác.

Như vậy, môi trường đăng nhập các tài khoản Facebook trên của bạn "KHÔNG CÒN SẠCH". Một môi trường sạch để reg, nuôi tài khoản phải thỏa mãn hai yếu tố:

- Thiết bị chưa dùng để đăng nhập các tài khoản bị khóa hoặc bị đưa vào blacklist của nền tảng.
- Dải IP dùng để truy cập website chưa bị rơi vào blacklist của nền tảng đó.

Tuy nhiên, một "môi trường sạch" thôi là chưa đủ. Để reg- nuôi tài khoản thành công, bạn cần quan tâm 4 yếu tố sau:

- Thông tin cá nhân dùng để đăng ký tài khoản.
- Địa chỉ IP để truy cập vào nền tảng.
- Thông số thiết bị dùng để đăng nhập vào trình duyệt.
- Hành vi người dùng tuân thủ chính sách của nền tảng.

Trong quyển eBook này, Hidemyacc sẽ cung cấp đến bạn thông tin đầy đủ của bốn yếu tố và cách chúng ảnh hưởng đến quá trình reg, nuôi tài khoản.

Yếu tố 1:
Thông tin cá nhân

Để đăng ký tài khoản trên các website, bạn cần cung cấp thông tin cá nhân theo yêu cầu như địa chỉ email, số điện thoại, căn cước công dân, thẻ ngân hàng (khi đăng ký tài khoản seller trên các trang thương mại điện tử),... Những thông tin này giúp website liên hệ và xác minh danh tính người dùng.

Nếu tài khoản của bạn bị khóa, bộ thông tin người dùng gắn với tài khoản đó cũng bị đưa vào "danh sách đen" bên cạnh địa chỉ IP và thông số máy. Để đăng ký tài khoản mới, bạn phải dùng một bộ thông tin mới, có thể mượn từ người thân, bạn bè hoặc sử dụng thông tin chưa từng cung cấp cho website.

Ví dụ, khi đăng ký tài khoản Etsy seller, bạn có thể cung cấp bằng lái xe thay vì căn cước công dân được gắn với tài khoản bị khóa trước đó.

Với trường hợp bạn muốn đăng ký tài khoản Mỹ, Anh, Canada,... để mở store làm POD, dropshipping hay tham gia các chương trình bật kiếm tiền của TikTok, Twitter,... bạn có thể mua thông tin từ các bên cung cấp. Tuy nhiên việc mua bán thông tin luôn tồn tại nhiều rủi ro như thông tin đã bị rơi vào blacklist của các website, bị chính chủ report, bị scam, lừa đảo,... Rất khó để nói những thông tin này được lấy theo cách chính thống hay không. Bởi vậy, cách tốt nhất là sử dụng thông tin của mình hoặc bạn bè, người thân.

Hiện nay có nhiều bên cung cấp dịch vụ cho thuê bank, thẻ thanh toán quốc tế như Visa, Mastercard, PayPal, PingPong, Payoneer,... để giao dịch. Cách này tuy tiện nhưng dễ bị hack hoặc khóa tài khoản. Bạn nên sử dụng bank local chính chủ. Việc mở thẻ thanh toán quốc tế tại Việt Nam cũng rất đơn giản rồi.

Yếu tố 2:
Địa chỉ IP

Địa chỉ IP cung cấp thông tin về geolocation của bạn. Nếu địa chỉ IP đã bị rơi vào blacklist của nền tảng, bạn cần đổi địa chỉ IP mới để đăng ký tài khoản. Vậy có những cách nào để thay đổi địa chỉ IP trên thiết bị của bạn?

Có nhiều cách khác nhau để thay đổi địa chỉ IP. Mỗi cách lại có ưu và nhược điểm cũng như mức độ phù hợp với từng loại công việc. Bạn có thể xem xét chọn một trong các cách sau hoặc đôi khi kết hợp 2 cách để gia tăng bảo mật.

- Dùng proxy
- Dùng VPN
- Reset router, 3G/4G hotspot
- Dùng Dcom
- Đổi thủ công trên wifi thiết bị

Dùng proxy và VPN là hai cách phổ biến, được nhiều anh em làm MMO dùng nhất. Nếu muốn nuôi số lượng lớn và chạy đồng thời nhiều tài khoản thì bạn nên gắn một proxy riêng cho từng tài khoản để tiện quản lý và thao tác.

Trong cuốn eBook này, Hidemyacc sẽ cung cấp thêm cho bạn các kiến thức liên quan đến proxy, bao gồm cách phân biệt và kiểm tra chất lượng proxy. Đã dùng gì thì phải thực sự hiểu về nó mới có thể tiết kiệm được chi phí.

Hướng dẫn phân biệt proxy và cách chọn proxy phù hợp

Proxy là 1 server đứng giữa người dùng và Internet, có tác dụng thay đổi địa chỉ IP và truyền tải các request từ người dùng đến Internet và ngược lại. Proxy là một nguyên liệu không thể thiếu nếu bạn muốn che dấu danh tính thật khi online. Proxy có rất nhiều loại khác nhau. Sau đây là 5 cách phân loại proxy phổ biến nhất.

1. Phân loại theo nguồn gốc

Phân loại	Chi tiết
Datacenter proxy	Datacenter proxy hay proxy trung tâm dữ liệu/proxy máy chủ là proxy được tạo ra từ các trung tâm dữ liệu, thường có chung địa chỉ IP với nhau khi check vị trí trên bản đồ. Datacenter proxy có tốc độ load rất cao, phù hợp với những task cần access và trả request nhanh. Giá thành của proxy này khá rẻ do độ bảo mật kém, dễ bị website phát hiện.
Residential proxy	Residential proxy hay proxy dân cư là loại proxy được các nhà mạng cung cấp cho các hô dân cư theo từng khu vực. Residential proxy có IP sạch và trust hơn nên thường được dùng cho các kèo reg, nuôi tài khoản. Các bên cung cấp proxy dân cư thường cho bạn chọn chi tiết theo quốc gia, bang, thành phố, thậm chí là zipcode và ISP nên sẽ tự nhiên như người dùng thật và khó bị website phát hiện. Chính vì thế, dù tốc độ load khá chậm, residential proxy ngày càng đắt và khó tìm được nguồn proxy có dải IP sạch.
Mobile Proxy	Mobile proxy hay proxy di động thực chất cũng là proxy dân cư nhưng thay vì kết nối bằng Wifi, chúng sẽ sử dụng đường truyền và địa chỉ IP của các nhà cung cấp mạng như Viettel, Mobifone, Vinaphone,... Mobile proxy có giá thành cao và thường được tính theo dung lượng sử dụng. Mobile proxy được ưa chuộng cho các kèo nuôi tài khoản mạng xã hội như Instagram, TikTok,...
ISP Proxy	ISP Proxy là sự kết hợp giữa datacenter và proxy dân cư. Đây là proxy dân cư tĩnh, nghĩa là địa chỉ IP sẽ không đổi cho đến khi bạn đổi server. ISP Proxy có mọi đặc tính của proxy dân cư, giá thành cao và an toàn, tuy nhiên cũng khó tìm được proxy có dải IP sạch.

2. Phân loại theo trạng thái xoay/cố định của proxy

Phân loại	Chi tiết
Proxy tĩnh	Proxy tĩnh là loại proxy chỉ có một IP cố định, không thay đổi trong suốt quá trình bạn sử dụng. Proxy tĩnh thường là datacenter proxy hoặc ISP.
Proxy xoay	Proxy xoay là loại proxy có địa chỉ IP thay đổi theo mỗi lần request mới hoặc sau một khoảng thời gian nhất định. Người dùng cũng có thể reset thủ công để đổi IP. Proxy xoay thường là residential proxy hoặc mobile proxy, tốc độ load chậm hơn proxy tĩnh.

3. Phân loại theo version của proxy

Phân loại	Chi tiết
Proxy IPv4	IPv4 là phiên bản đầu tiên của IP, được sử dụng rộng rãi đến tận bây giờ. Hầu hết các website và ứng dụng đều hỗ trợ IPv4. Tuy nhiên, số lượng IPv4 có hạn và khó mua được proxy sạch. IPv4 không hỗ trợ sẵn tính năng bảo mật trong giao thức, vì vậy rất khó thực hiện bảo mật kết nối từ thiết bị gửi đến thiết bị nhận.
Proxy IPv6	IPv6 ra đời để giải quyết tình trạng tài nguyên IPV4 đang dần cạn kiệt. Đồng thời, IPv6 cũng được nâng cấp để khắc phục những nhược điểm về bảo mật của IPv4. Tuy nhiên, IPv6 có số lượng lớn, vượt quá khả năng kiểm soát traffic nên sẽ bị kiểm soát nguồn IP qua hành vi sử dụng. Do đó, không có nhiều web, ứng dụng hỗ trợ IPv6. Tính ứng dụng của IPv6 thấp hơn so với IPv4. Một số nền tảng như Gleam, Etsy, eBay,... không cho phép IPv6 truy cập nên bạn phải dùng IPv4 nếu muốn dùng proxy để vào các website này.

4. Phân loại theo giao thức của proxy

Phân loại	Chi tiết
HTTP Proxy	HTTP proxy là giao thức proxy phổ biến nhất nhưng độ bảo mật dữ liệu cá nhân không tốt vì nó sẽ gửi toàn bộ truy cập dưới dạng văn bản thuần túy.
HTTPs Proxy	Về mặt kỹ thuật thì proxy này giống loại HTTP nhưng có bảo mật dữ liệu cá nhân thông qua giao thức SSL nên còn được gọi là SSL Proxy.
SOCKS5 Proxy	SOCKS5 Proxy là một loại proxy cấp thấp, chuyển tiếp dữ liệu giữa client và server mà không thêm nhiều xử lý. Proxy này có thể mã hóa kết nối giữa client và proxy, nhưng không tự mã hóa dữ liệu được chuyển tiếp giữa proxy và server đích. Người dùng thường kết hợp SOCKS5 với các phương tiện bảo mật khác như TLS hoặc sử dụng VPN để tăng cường bảo mật.

5. Phân loại theo tính độc quyền sử dụng

Phân loại	Chi tiết
Shared proxy	Giá rẻ hơn nhưng phải chung với nhiều người nên nguy cơ dính blacklist cao hơn.
Private proxy	Đắt hơn nhưng được dùng riêng, không phải chung với nhiều người.

Bạn có thể chọn mua loại proxy theo port hoặc theo băng thông (dung lượng - GB). Hidemy-acc phân tích một vài yếu tố để bạn có thể lựa chọn cách thức mua phù hợp với nhu cầu sử dụng của mình như sau:

Hình thức tính giá	Port	Băng thông
Shared proxy	• Thường là proxy tĩnh, hầu hết không giới hạn băng thông. • Hợp kèo cần IP cố định thời gian dài (ví dụ nuôi acc giá trị cao) hoặc tốn GB (ví dụ buff view Youtube).	• Thông thường các proxy xoay vòng không giới hạn số lượng cổng (chẳng hạn như Zeus Proxy hoặc Oxylabs). • Thích hợp cho các trường hợp yêu cầu số lượng IP lớn nhưng lại sử dụng trong thời gian ngắn (chẳng hạn như đăng ký tài khoản hoặc làm offer).
Private proxy	• Proxy tĩnh nếu IP không dùng được (die, dính blacklist,...) thì coi như bỏ, phải mua proxy mới. • Nếu làm số lượng lớn ví dụ như nuôi acc thì mỗi acc cần một proxy riêng, khá tốn kém.	• Một số tác vụ có thể tiêu tốn GB nhanh chóng, yêu cầu sử dụng các tool bypass các task tốn dung lượng hoặc mua các gói GB cao hơn để tối ưu hóa chi phí. • Không có IP cố định trong một thời gian dài. Nếu sử dụng nhiều tài khoản thì nên chọn nhà cung cấp xoay vòng IP theo vị trí đã chọn, thay vì xoay vòng IP ngẫu nhiên từ các quốc gia khác nhau.

Hướng dẫn kiểm tra chất lượng proxy

Sau khi chọn được loại proxy phù hợp bạn cần kiểm tra chất lượng proxy đó. Liệu IP của proxy bạn mua có dính blacklist của hệ thống nào không? Tốc độ của proxy này như thế nào, đã được cài đặt chuẩn chưa? Bạn hãy kiểm tra theo checklist 5 yếu tố sau:

1. Chuẩn geolocation

Đầu tiên, cần check xem location của proxy có đúng như bạn chọn mua không, ví dụ proxy US thì không thể có IP ở VN được. Bạn có thể kiểm tra bằng cách sử dụng các trang web check IP như IP Fighter, Pixelscan, Browserleaks,.... Hoặc bạn có thể lên Google và search cụm từ bất kỳ sau đó kéo xuống cuối trang để xem phần location hiển thị có khớp với location IP bạn mua không. Tương tự, các website bạn truy cập thường cũng có phần hiển thị location theo IP.

2. Chuẩn timezone

Bạn cần kiểm tra xem múi giờ của proxy có khớp với múi giờ thiết bị không, nếu không trùng thì sẽ bị website nghi vấn. Tương tự như khi kiểm tra geolocation, bạn cũng có thể kiểm tra timezone bằng 2 cách là sử dụng web check IP hoặc lên Google search “Time” xem kết quả trả về có khớp

không.

3. Không dính blacklist của hệ thống lớn

Bạn có thể check proxy mình dùng với 3 cách đơn giản sau:

- Search Google từ khóa bất kỳ thấy liên tục xuất hiện captcha.
- Truy cập vào 1 số forum lớn như blackhatworld.com bị check Cloudflare, đã verified human nhưng không thể bypass check secure.
- Check trên một số web check IP như IP Fighter, IP-score để check xem liệu IP của bạn có vào blacklist của nhiều hệ thống hay không.

Nếu không bypass được Google hay Cloudflare thì khả năng cao IP của bạn đã "nát" rồi. Tuy nhiên bạn vẫn có thể test trên kèo của mình (trừ các tài khoản quan trọng) vì chưa chắc website/ nền tảng đó sử dụng data từ các hệ thống này.

Lưu ý, dải IP ban đầu bạn check theo cách trên có thể trust nhưng khi có traffic lớn trong thời gian ngắn hoặc nhiều tài khoản dùng chung một IP thì sớm muộn gì cũng "nát" nên không có proxy nào là sạch mãi mãi, thường chỉ ngon trong thời gian đầu. Đó là lý do IP ở các khách sạn, quán cà phê, quán net đều không sạch do có nhiều người cùng sử dụng.

Sau một thời gian sử dụng, mặc dù cookie vẫn còn thời gian nhưng những tài khoản sử dụng địa chỉ IP bị detect sẽ bị out và bắt đăng nhập lại hoặc thậm chí không thể đăng nhập được, cần đổi lại địa chỉ IP thì mới đăng nhập được. Vậy nên, với những tài khoản giá trị cao, bạn nên mua proxy từ các nguồn uy tín, giá cao hơn nhưng an tâm.

Các nhà cung cấp, bán dịch vụ proxy có cơ chế để refresh IP (911 proxy là một ví dụ), không biết cơ chế cụ thể là gì, không loại trừ trường hợp bắt tay hay lobby cho các hệ thống lớn để xóa IP đó ra khỏi blacklist.

Trong các loại proxy thì proxy dân cư vẫn trust hơn proxy trung tâm dữ liệu do dải IP đó được nhà mạng bán riêng cho từng khu vực cho người dùng cuối cùng. Còn proxy IPv6, do số lượng IP quá lớn, vượt xa khỏi sự kiểm soát traffic của các hệ thống lớn nên đa phần các hệ thống sẽ kiểm soát nguồn IP qua hành vi hay một số website không hỗ trợ IPv6, ví dụ Gleam, Etsy, eBay.

4. Chuẩn địa chỉ đăng ký IP

Bạn có thể check thông tin IP Address Whois để xem thông tin của người đăng ký IP xem có khớp với location của proxy không. Nếu mua proxy US mà thông tin người đăng ký IP lại ở VN thì độ trust cũng thấp.

5. Không bị rò rỉ WebRTC/DNS

WebRTC cho phép giao tiếp giữa thiết bị và trình duyệt với nhau mà không cần cài plugin hay phần mềm hỗ trợ. Hiểu đơn giản thì WebRTC hỗ trợ bạn gọi điện, gọi video, gửi tài liệu,... trên web.

WebRTC leak (rò rỉ WebRTC) là tình trạng bị lộ thông tin IP thật qua WebRTC mặc dù đã sử dụng

proxy. Điều này là do web lấy được thông tin IP dựa trên giao thức WebRTC UDP. Vì đây là cơ chế hoạt động của trình duyệt nên kể cả có sử dụng proxy hay các cách khác để đổi IP thì chức năng WebRTC trên trình duyệt vẫn để lộ địa chỉ IP thực của bạn.

Tương tự như các yếu tố trên, bạn có thể kiểm tra WebRTC leak trên các trang như IP Fighter (https://ipfighter.com/), Whoer (https://whoer.net/) hay f.vision (http://f.vision/),...

Nếu kết quả cho thấy bạn đang bị WebRTC IP leak thì bạn có thể xử lý theo các cách sau:

- **Dùng VPN làm nền:** Bạn có thể kết hợp dùng cả VPN và proxy để tránh bị leak. Đầu tiên bạn bật VPN (chọn location càng giống với proxy càng tốt), sau đó kết nối proxy để truy cập website như bình thường. Như vậy thì dù treo máy hay F5 cũng không sợ bị lộ IP gốc. Tuy nhiên, dù IP location giống nhau thì dãy IP của VPN và proxy cũng không giống nhau 100% nên đây chưa phải giải pháp tối ưu nhất.
- **Disable WebRTC (Tắt WebRTC):** Một cách đơn giản để tránh bị detect IP qua WebRTC là tắt chức năng WebRTC của trình duyệt đi để website không detect được. Tuy nhiên, cách này sẽ ảnh hưởng đến tính năng hoạt động của trình duyệt, đồng thời khiến web nghi ngờ bạn đang muốn giấu diếm thông tin, và xử lý bằng cách chặn truy cập hoặc bắt bạn verify liên tục.
- **Làm nhiễu kết quả detect IP từ WebRTC:** Để tránh bị web nghi ngờ, bạn có thể làm nhiễu để website không lấy được kết quả IP từ WebRTC. Website sẽ thấy không lấy được thông số này vì nguyên nhân khác chứ không phải do bạn cố ý ngăn cản.
- **Trả kết quả IP của proxy khi web detect IP từ WebRTC:** Cách làm này tự nhiên giống người dùng thật nhất, tuy nhiên chỉ áp dụng được với các proxy có hỗ trợ UDP.

Yếu tố 3:
Thông số thiết bị

Trong ví dụ Facebook đầu tiên, Hidemyacc đã đề cập đến việc nền tảng có thể thu thập thông số browser fingerprint để định danh người dùng. Không chỉ Facebook mà tất cả các website hay nền tảng đều thu thập thông số này.

Browser fingerprint là gì?

Browser fingerprint (có thể còn gọi là device fingerprinting) là dấu vân tay trình duyệt. Khi người dùng truy cập bất kỳ một website nào, trang web đó sẽ thu thập mọi thông tin dữ liệu mà người sử dụng để lại trên website.

Browser fingerprint bao gồm các thông số về phần cứng, user-agent, hệ điều hành, cấu hình thiết bị, vị trí, múi giờ, ngôn ngữ, độ phân giải màn hình và nhiều yếu tố khác. Giống với dấu vân tay thực của chúng ta, browser fingerprint của mỗi thiết bị là duy nhất. Điều này giúp các trang web xác định "khách" ghé thăm website của họ là cùng một người. Và nếu có hành vi đáng ngờ, các chủ website có thể cấm hoặc không cho người đó truy cập website của mình.

Nếu trình duyệt web chỉ thu thập các thông tin như lịch sử duyệt web, dữ liệu tải xuống và lịch sử tìm kiếm thì browser fingerprint có thể thu thập được nhiều thông tin hơn.

Dưới đây là danh sách các thông số mà một website có thể thu thập được khi bạn truy cập:

- User-agent: User-agent chứa các thông tin về trình duyệt và thiết bị của người dùng khi truy cập website, bao gồm: Hệ điều hành, phiên bản của hệ điều hành, trình duyệt, phiên bản trình duyệt,...
- IP Address: Địa chỉ IP cung cấp thông tin về geolocation của bạn. Dựa vào địa chỉ IP, website có

thể biết được vị trí thực của bạn ở đâu.

- Timezone: Múi giờ được lấy theo IP của bạn.
- WebRTC: WebRTC cũng được dùng để thu thập thông tin trình duyệt của người dùng. Khi bị rò rỉ WebRTC, website có thể phát hiện được địa chỉ IP thật dù bạn đã sử dụng proxy hay VPN.
- Cookie: Cookies giúp website ghi nhớ các tùy chọn của bạn, ví dụ như thông tin đăng nhập, các cài đặt trên website, lịch sử duyệt web, số lượt truy cập, thời lượng phiên, vị trí địa chỉ,... Nếu bạn chấp nhận cookies từ một trang web, bạn đã cho phép chủ sở hữu trang hoặc các nhà quảng cáo thu thập và lưu trữ thông tin của bạn. Cookies có giới hạn lưu trữ là 4Kb và có thời gian hết hạn.
- Local storage: Local storage lưu trữ các thông tin người dùng như tên đăng nhập, mật khẩu, trình thiết lập cá nhân,... Local storage có dung lượng lưu trữ khoảng 5Mb. Khi đóng tab hoặc tắt trình duyệt thì dữ liệu ở local storage vẫn tồn tại. Nó chỉ bị mất đi khi user xóa cache hoặc xóa dữ liệu trên website.
- Plugins: Plugins là các phần mở rộng hoặc thành phần bổ sung được thiết kế để mở rộng chức năng của ứng dụng hoặc hệ thống nào đó.
- Hardware concurrency: Hardware concurrency cho biết có bao nhiêu CPU (CPU processor) được phân bổ trên trình duyệt của người dùng để chạy các chuỗi. Một số thông tin có thể thu thập như số lượng bộ xử lý/nhân xử lý trên CPU hoặc GPU, độ phân giải GPU, băng thông,...
- Device memory: Bộ nhớ trong của thiết bị.
- Language, Fonts: Ngôn ngữ và font chữ bạn cài đặt trên thiết bị.
- Screen Resolution: Kích thước màn hình.
- Media devices: Các thiết bị ngoại vi được kết nối vào máy như loa. headphone, camera micro,... Website sẽ thu thập thông tin số lượng các thiết bị ngoại vi này.
- Browser history: Lịch sử duyệt web.
- WebGL Fingerprint: Điểm ảnh trên website hoặc Google Maps giúp hiển thị đồ họa 3D trên trang web.
- Audio Context: Đây là một API của trình duyệt web được sử dụng để xử lý và tạo ra âm thanh trong ứng dụng web.

FACT

Chế độ trình duyệt ẩn danh không giúp bạn ẩn danh trên môi trường Internet

Chế độ trình duyệt ẩn danh Private Browser (trên Firefox) hoặc Incognito (trên Chrome) không thật sự ẩn danh như bạn nghĩ. Chế độ này chỉ không lưu lại cookies, lịch sử trình duyệt hay local storage của phiên đăng nhập đó, còn các thông số browser fingerprint như hệ điều hành, trình duyệt, thông tin máy,... vẫn bị lưu lại và website có thể dựa vào các thông số này để xác định danh tính của bạn. Do đó nếu bạn thay đổi IP và sử dụng trình duyệt ẩn danh để reg, nuôi số lượng lớn tài khoản thì vẫn bị website phát hiện.

Các cách để thay đổi thông số thiết bị

1. Dùng extension

Có nhiều loại extension hỗ trợ thay đổi các thông số browser fingerprint như extension đổi User Agent, chặn WebRTC,... Mặc dù dễ sử dụng và đa phần miễn phí nhưng chưa có extension nào có thể fake được tất cả các thông số thiết bị. Chính vì vậy, extension không phải lựa chọn tối ưu khi truy cập các website detect sâu.

2. Thuê máy ảo

Thuê máy ảo là dịch vụ cho thuê máy tính mới và được điều khiển từ xa trên máy thật. Về độ tự nhiên thì hình thức này gần tương đương với bạn sở hữu một bộ PC mới. Thế nhưng, với những nền tảng detect sâu thì máy ảo không xử lý được triệt để các vấn đề. Bởi, các giải pháp như VMware hay Virtualbox đều không có card đồ họa. Vì thế, khi các website thu thập thông số WebGL thì ngay lập tức bạn bị phát hiện đang dùng máy ảo.

3. Dùng antidetect browser

Antidetect browser là phần mềm hỗ trợ tạo ra các profile trình duyệt có các thông số browser fingerprint khác nhau. Mỗi profile sẽ có các thông số về trình duyệt, hệ điều hành, phần cứng, phần mềm khác nhau tương đương các máy tính riêng biệt.

Đến thời điểm hiện tại, antidetect browser là giải pháp ưu việt nhất với nhiệm vụ tạo các new device với chi phí rẻ và thuận tiện khi quản lý và sử dụng.

Antidetect browser Hidemyacc - Giải pháp tạo môi trường sạch an toàn và hiệu quả nhất

Hidemyacc là phần mềm chống phát hiện trình duyệt (antidetect browser) giúp người dùng ẩn danh tính thật trên môi trường Internet bằng cách tạo ra các profile tương tự Chrome nhưng mỗi profile sẽ có một bộ thông số browser fingerprint khác nhau, tương đương với một máy tính thật.

Hidemyacc được sử dụng cho mục đích tăng cường bảo mật danh tính và tài khoản của người dùng. Những trường hợp sử dụng Hidemyacc cho mục đích xấu như giả mạo danh tính, lừa đảo, chiếm đoạt tài sản hay các hành vi vi phạm pháp luật khác không bao giờ được chúng tôi ủng hộ.

Antidetect browser Hidemyacc chỉ thay đổi thông số browser fingerprint cho từng profile. Nếu muốn đổi địa chỉ IP, bạn cần sử dụng thêm proxy hoặc VPN. Sau khi đổi địa chỉ IP, các profile này tương đương các máy tính thật được lắp đường truyền mạng mới, hoàn toàn riêng biệt và không liên quan với nhau.

Hidemyacc sở hữu nhân trình duyệt Marco được phát triển trên công nghệ mới, có thể dễ dàng bypass được nhiều webcheck browser fingerprint như Pixelscan, IPhey và cho điểm số cao trên

Creepjs. Kho dữ liệu của Hidemyacc cũng liên tục cập nhật các thông số mới nhất trên thị trường.

Bạn có thể sử dụng Hidemyacc cho nhiều nhu cầu reg, nuôi số lượng lớn tài khoản trên các nền tảng khác nhau:

- Tạo và nuôi nhiều tài khoản để bán hàng, POD, dropshiping, affiliate, checkout trên các sàn thương mại điện tử như Amazon, Etsy, eBay, Rebubble, Walmart,...
- Tạo, nuôi nhiều tài khoản chạy quảng cáo, seeding, spam, tăng tương tác trên các nền tảng mạng xã hội như Facebook, Tiktok, Youtube, Instagram, Twitter, Linkedin,...
- Tạo các bộ tài khoản airdrop, webgame,...
- Tạo số lượng lớn tài khoản web scraping, crawl data cho các tool spy ads, spy sản phẩm,...

Khi sử dụng antidetect browser Hidemyacc, bạn không cần phải thiết lập các thông số browser fingerprint vì hệ thống sẽ tự động cài đặt cho bạn, đảm bảo mỗi profile đều có một bộ thông số riêng. Bạn cũng có thể tùy chỉnh các thông số này theo nhu cầu của mình. Hướng dẫn setup chi tiết bạn tham khảo ở phần Phụ lục.

Yếu tố 4:
Hành vi người dùng

Hành vi người dùng là cách bạn tương tác và hoạt động trên website/nền tảng. Nếu bạn có những hành vi không "chuẩn mực" hay vi phạm chính sách, website có thể khóa tài khoản và cấm bạn truy cập. Những tài khoản được tạo dưới danh nghĩa của bạn (cùng địa chỉ IP, thông số máy hay thông tin người dùng) đều không được chấp nhận.

Thế nào là hành vi bất thường?

Hành vi bất thường là những hành động, tương tác không tuân theo các tiêu chí thông thường khi người dùng sử dụng tài khoản trên website hay nền tảng đó. Những hành vi này khiến website nghi ngờ tài khoản của bạn và liệt chúng vào danh sách những tài khoản cần xem xét.

Một số ví dụ về hành vi người dùng bất thường:

- Đăng nhập từ địa điểm lạ: Tài khoản được đăng nhập ở quốc gia, khu vực khác với vị trí thường đăng nhập.
- Đăng nhập sai nhiều lần: Người dùng liên tục đăng nhập sai tài khoản.
- Tài khoản được đăng nhập từ nhiều thiết bị khác nhau: Một tài khoản nhưng lại được ghi nhận đăng nhập từ nhiều thiết bị ở nhiều khu vực khác nhau, khác với thiết bị và vị trí thường đăng nhập.
- Đăng nội dung, chạy quảng cáo vi phạm chính sách, đả kích chính trị, phản cảm,...
- Spam tương tác, comment, link,...
- Dùng bot chạy automation.
- ...

Những hành vi này thường dẫn đến tình trạng khóa tài khoản, đặc biệt với những tài khoản

mới tạo hoặc đã vi phạm nhiều lần. Việc này ảnh hưởng rất lớn đến quá trình đăng ký tài khoản mới vì địa chỉ IP, thông tin người dùng hay thông số máy đều bị đưa vào blacklist của website.

Nhiều anh em làm MMO muốn sử dụng tool để tự động hóa công việc nhưng lo sợ tình trạng khóa tài khoản vì website phát hiện sử dụng bot. Lí do là vì các website detect rất sâu nhưng công nghệ của tool không đủ đáp ứng. Sử dụng tool kém chất lượng thì sớm hay muộn website cũng detect ra được. Do đó, nếu muốn dùng tool automation thì bạn nên lựa chọn những bên uy tín.

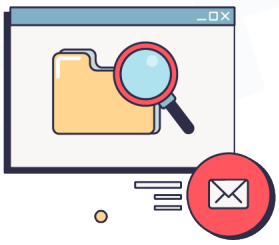
Tạo hàng loạt kịch bản nuôi tài khoản với Hidemyacc Automation

Automation là tính năng được tích hợp sẵn trong antidetect browser Hidemyacc giúp người dùng tạo các kịch bản automation, tự động hóa quy trình nuôi tài khoản với nhiều loại kịch bản trên nhiều nền tảng khác nhau.

Có 3 cách để bạn có thể tạo kịch bản automation trên Hidemyacc:

- **Kéo thả câu lệnh:** Hidemyacc cung cấp các câu lệnh có sẵn, bạn chỉ cần kéo thả và sắp xếp chúng thành một kịch bản automation hoàn chỉnh.
- **Record thao tác thực trên website:** Hidemyacc là antidetect browser đầu tiên trên thị trường có tính năng record thao tác người dùng. Bạn chỉ cần ấn nút Record, thao tác trực tiếp trên website rồi export ra kịch bản automation. Hệ thống sẽ lấy chính xác các thao tác của bạn trên website đó.
- **Import kịch bản tự code trên JSON hoặc Pupepteer:** Bạn có thể import kịch bản tự code trên JSON hoặc Pupepteer để chạy cho các profile Hidemyacc. Ngoài ra, bạn có thể export kịch bản automation và chia sẻ cho các tài khoản Hidemyacc khác.

Câu chuyện bên lề



Một chia sẻ thực tế từ người dùng biết cách kết hợp cả 4 yếu tố kể trên để đăng ký và nuôi tài khoản Etsy thành công.

HƯỚNG DẪN KÈO REG - NUÔI TÀI KHOẢN BÁN HÀNG TRÊN ETSY

Tình trạng chết tài khoản, thậm chí là chết theo giàn ko chỉ xảy ra với acc mới reg mà kể cả những acc đã có nhiều lượt mua bán cũng vẫn có thể dính.

Mình share vài tut mình tự thử và đúc ra được từ quá trình làm Etsy cho ae newbie, mấy anh em làm lâu năm đừng có comment "biết rồi khổ lắm nói mãi" nhé. Ngày xưa lúc mới bắt đầu làm cũng chỉ mong có ai nói những thứ cơ bản này cho mình.

Vấn đề về fake IP, hay cụ thể là dùng proxy

Bác nào newbie, chưa bao giờ reg acc Etsy, IP sạch + máy sạch thì cứ tự tin reg bằng mạng nhà thôi không cần đổi IP. Còn nếu đổi IP thì bác có thể dùng proxy, IPv4, proxy dân cư, lúc reg số lượng lớn muốn tiết kiệm thì dùng proxy xoay, nhưng lúc nuôi thì nhất định phải dùng tĩnh.

Mua proxy ở đâu thì các bác phải tự test, chắc chắn mình sẽ ko nói đâu (miếng cơm manh áo mà). Ít người biết thì ngon mà nhiều người biết lại thành nát. Nên ae cứ tự mua tự trải ở phần này.

Test IP thì các ae check location xem country, city chuẩn chưa, check black list, điểm chất lượng... trên Whoer.net, IPfighter.com, IP-score.com sẽ chấm điểm. Nhưng cũng chỉ để tham khảo, vì dữ liệu của các site này còn hạn chế, vào blacklist của các site này chưa chắc đã bị black-list của Etsy.

Nếu đi mua info để reg thì phải test info

Các bác mua info ở nguồn nào cũng phải test kĩ xem đã bị dùng để reg trước chưa. Cứ test từng ít một trước. Đừng tham rẻ mà mua số lượng lớn ngay. Chẳng may gặp phải lô info đã bị vào blacklist thì lại mất tiền ngu (mình đã từng). Lưu ý là mấy giao dịch mua bán thì nên qua trung gian, có chính sách bảo hành rõ ràng.

Tips nuôi tài khoản

Nuôi tài khoản thì mình nuôi từ buyer trước rồi mới lên seller. Giai đoạn buyer cơ bản là lướt, order, review như mình đi mua hàng thật. Reg acc rồi lên mấy group thuê người buff đơn, trả tiền cho mình order để có review, vừa trust acc vừa có tiền mua hàng một công đôi việc. Muốn lên seller thì phải email, chat hỏi support cách lên seller cho tự nhiên như người dùng thật.

Etsy ưu tiên sản phẩm handmade nên ở giai đoạn listing, ae ưu tiên list các sản phẩm hand-made hình tự chụp, list sản phẩm digital mình thấy tỷ lệ live cực thấp.

Nuôi acc thì ae cứ tư duy nuôi làm sao giống người dùng thật nhất có thể. Hành vi của người dùng bình thường như thế nào thì cứ theo đó. Chứ cũng chẳng có công thức nào chung.

Bán hàng và chăm sóc khách hàng

Sản phẩm phải 100% sạch. Tốt nhất tự chụp, tự làm video sản phẩm, hoặc nếu có copy thì phải thay mockup và redesign. Ship phải nhanh, còn nếu bị chậm quá thời gian thông báo thì phải email xin lỗi khách ngay.

Dành riêng cho anh em chơi số lượng lớn tài khoản

Nếu ae chỉ tập trung vào 1 hay 1 vài shop, đại loại là ít tài khoản thì cứ dùng VPS, hay dùng profile Chrome, Firefox cũng oke.

Nhưng nếu là team lớn hay chuyên reg acc để bán thì nên đầu tư vào tool. Những con acc mình reg đời đầu đang login trên VPS vẫn đang ổn định, mới 1 năm gần đây thì mình dùng thêm Multilogin. Anh em nào chưa biết thì antidetect là tool dùng để tạo ra nhiều profile trình duyệt có thông số khác nhau, giống như sắm dàn máy tính mới. Gắn thêm proxy nữa là các acc sẽ ko bị liên quan đến nhau, ko bị chết chùm, chết giàn.

Mức độ giống máy tính mới tới đâu thì còn phụ thuộc độ ngon của tool. Ngoài Multi của Nga thì mình có test qua Hidemyacc với Omni của người Việt. Về cơ bản cũng giống Multi, được cái rẻ hơn với lại ae người Việt dễ nói chuyện, support tốt. Nhưng mình xác định đã là tool thì sẽ có nhược điểm. Tool có tốt đến mấy thì cũng phải reg với nuôi chuẩn thì acc mới sống lâu.

Mình thấy reg nuôi acc hơn thua nhau ở tỉ mỉ, cẩn thận, kiên trì. Chứ cũng ko đến nỗi bán tut vài chục, vài trăm củ. Cẩn thận nên cứ kiên trì rút kinh nghiệm liên tục sau mỗi lần die acc thôi. Cứ die cả giàn vài ba bữa sẽ tự đúc rút ra được kinh nghiệm.

Nguyễn Nhất Thương - Chia sẻ trong group Etsy to Go

HÀNH TRÌNH PHÁT TRIỂN ANTIDETECT BROWSER HIDEMYACC

Chào các bạn, mình là Tiến, founder của OneADX, chủ sở hữu phần mềm antidetect browser Hidemyacc.

Tính đến nay mình đã có 12 năm kinh nghiệm trong lĩnh vực kiếm tiền online (MMO). Quay lại thời điểm hơn 10 năm trước, khái niệm kiếm tiền online còn khá mới mẻ, không phổ biến như bây giờ. Các thông tin về quy trình tạo và nuôi tài khoản để làm MMO hầu như không có. Nếu có cũng chỉ là anh em quen biết giới thiệu cho nhau.

Giải pháp phổ biến nhất ở thời điểm đó là dùng VPS, dùng máy ảo hay cài extension để thay đổi user agent, địa chỉ IP và block WebRTC. Ai biết thủ thuật này là đã ở tầm hiểu biết kha khá rồi. Nhưng thực tế, cách này chỉ làm được các kèo đơn giản, không kiểm soát hết các yếu tố khiến website khóa tài khoản và khi gặp các website khó thì chắc chắn không bypass. Đặc biệt, nếu ai muốn chạy đồng thời số lượng lớn tài khoản thì các giải pháp cũ này đều không thể đáp ứng được.

Mình từng làm app, game, xây rất nhiều chợ ứng dụng. Mình cũng có thời gian làm nhiều trên các sàn ecommerce như eBay và Etsy. Việc khóa tài khoản là chuyện hàng ngày. Có rất nhiều tài khoản quan trọng cố gắng kháng mãi cũng không được. Mình nhận ra, nếu cứ tiếp tục mua nguyên liệu như thế này sẽ tốn rất nhiều chi phí, dẫn đến thua lỗ. Và ngoài kia cũng có rất nhiều anh em đang gặp cùng vấn đề này.

Tồn tại một vấn đề lớn như vậy thì chắc chắn sẽ phải có giải pháp để giải quyết nó. Mình bắt đầu tìm hiểu sâu hơn về nguyên nhân nào hay làm cách nào để website có thể ra quyết định có khóa một tài khoản hay không?

Khi "browser fingerprint" trở nên phổ biến hơn

Mình đọc được khái niệm về browser fingerprint hay dấu vân tay trình duyệt do các bên cung cấp dịch vụ Bot detection giới thiệu. Mỗi thiết bị khi mở trình duyệt sẽ có một bộ thông số để "định danh" họ là duy nhất. Không chỉ đơn giản ở việc thay bằng một địa chỉ IP cư dân mới hay đổi user agent là có thể đổi thông số máy. Thông tin này như khai sáng những bế tắc trước đây. Mình bắt đầu chia sẻ về khái niệm này cho mọi người và có thể tự tin nói mình là người đầu tiên giới thiệu khái niệm "browser fingerprint" đến với cộng đồng anh em làm MMO tại Việt Nam.

Nhưng nếu chỉ biết nguyên nhân thôi thì chưa đủ, cần có một giải pháp để giải quyết được bài toán này. Mình tìm hiểu thêm thì trên thị trường đã có các bên cung cấp các giải pháp antidetect browser rồi. Nhiệm vụ của tool này là tạo ra được các browser profile có các bộ thông số browser fingerprint khác nhau mà không cần phải mua thiết bị mới hay không cần phải thuê VPS và máy ảo. Antidetect browser là "cuộc cách mạng" về cách tạo và nuôi số lượng lớn tài khoản. Rất đơn giản, dễ dung, chạy mượt mà, về độ tự nhiên thi chỉ sau việc mua một thiết bị mới hoàn toàn, còn lại antidetect browser đã khắc phục hết được các nhược điểm của các giải pháp như VPS, Vm-ware, Virtualbox,...

Multilogin và Gologin là những cái tên tiên phong trong phát triển phần mềm này. Khi chưa phát triển Hidemyacc, mình đã từng có thời gian dài dung Gologin và Multilogin. Gologin có mức độ ổn định ở mức trung bình thấp. Còn Multilogin giá lại khá cao.

Bắt tay vào phát triển antidetect browser

Mình quyết định sẽ phát triển một tool tương tự để team tự dùng. Hiểu về nhu cầu, nghiệp vụ lại nắm chắc được công nghệ, phát triển một phần mềm antidetect browser không khó. Mình chỉ mất một tháng tập trung code để hoàn thiện sản phẩm bao gồm cả giao diện app và giao diện website. Tính đến nay đã được hơn 3 năm kể từ khi Hidemyacc chính thức ra mắt, trải qua rất nhiều phiên bản, đồng hành cùng rất nhiều team lớn ở Hà Nội, Đà Nẵng, Thái Nguyên,... Hidemyacc giờ có thể tự tin đứng ngang hàng về chất lượng với cả những bên tiên phong, thậm chí số lượng thông số thiết bị còn lớn và tự nhiên hơn rất nhiều.

Thế nhưng, mặc dù mình đang cung cấp tool antidetect browser nhưng mình muốn nhắc nhở bạn đừng thần thánh hóa nó vì thông số thiết bị chỉ là 1 trong các yếu tố. Nếu bạn đã đọc chi tiết cuốn ebook này, có tất cả 4 yếu tố quan trọng ảnh hưởng đến quá trình bạn reg – nuôi tài khoản.

Kiến thức trong cuốn ebook này có thể bạn đã đọc một thứ một ít ở đâu đó, nghe ai đó chia sẻ rồi. Nhưng để tổng hợp lại thành một cuốn sổ tay đầy đủ như vậy thì chắc chắn chưa có trên thị trường. Đây là sản phẩm team của mình muốn chia sẻ rộng rãi đến với những ai đã, đang và có ý định muốn làm MMO. Khi mọi thứ đều tỏ tường, mọi người sẽ không bị hoang mang, chọn được đúng thứ mình cần, không phải đi đường vòng và tốn nhiều chi phí như mình trước kia.

Các bạn có thể chọn cuốn ebook này như sổ tay để mở ra xem bất cứ lúc nào. Và cũng đừng tiếc một lời khen cho đội ngũ biên tập từ team marketing của mình nhé. Cảm ơn mọi người và chúc mọi người thành công!

Nguyễn Mạnh Tiến - Founder OneADX và antidetect browser Hidemyacc

Tổng kết

Tạo tài khoản nghe qua tưởng chừng là một việc rất đơn giản vì bạn có thể dễ dàng tìm kiếm các bài viết, video hướng dẫn trên Internet. Nhưng tạo tài khoản thành công và xây dựng hệ thống các loại tài khoản "khỏe mạnh" luôn là một bài toán khó đối với những người làm MMO.

Một máy tính mới, một địa chỉ IP mới chỉ là điều kiện cần để tạo ra môi trường sạch. Để duy trì các tài khoản này và tương tác sao cho giống người dùng thật nhất đòi hỏi bạn phải hiểu rõ về những hành vi sử dụng, tương tác trên website.

Quyển eBook này đã giới thiệu đến bạn chi tiết bốn yếu tố ảnh hưởng trực tiếp đến quá trình reg, nuôi tài khoản. Như chúng tôi đã nói, đây không phải là quyển sách hướng dẫn bạn cách đăng ký tài khoản thành công trên từng nền tảng. Quyển sách này cung cấp cho bạn kiến thức để bạn, dù dùng website hay nền tảng nào, đều hiểu và biết cách đăng ký tài khoản thành công.

Hy vọng bạn đã tìm thấy những kiến thức bổ ích khi đọc quyển sách này.

Cảm ơn tất cả các bạn đã ủng hộ quyển eBook này của chúng tôi. Hidemyacc dành tặng mã giảm giá độc quyền 10% "HIDEMYBOOK" cho khách hàng lần đầu tiên thanh toán các gói Hidemyacc. Bạn hãy liên hệ đội ngũ support của Hidemyacc để được hỗ trợ.

Phụ Lục

HƯỚNG DẪN SETUP CÁC THÔNG SỐ BROWSER FINGERPRINT CHO PROFILE HIDEMYACC

1. Overview

Operating System (OS)

Hidemyacc cung cấp 5 hệ điều hành là Window, MacOS, Linux, Android, iOS với các phiên bản mới nhất. Hidemyacc khuyến khích bạn chọn hệ điều hành tương tự như máy thật để có hiệu suất hoạt động tốt nhất.

Browser

Bạn có thể tùy chọn 5 loại trình duyệt khác nhau với các phiên bản update mới nhất là Chrome, Brave, Opera, Edge và Yandex.

2. Proxy

Hidemyacc không thể thay đổi địa chỉ IP nên bạn cần thêm proxy cho các profile này.

- Free Proxy: Sử dụng proxy miễn phí của Hidemyacc.
- Your Proxy: Thêm proxy của bạn. Hidemyacc hỗ trợ các loại proxy như HTTP, Socks 4, Socks 5, SSH, Tinsoft, TM theo định dạng IP:Port:Username:Password. Để kiểm tra tình trạng của proxy, bạn click vào Check Proxy. Nếu hiển thị "Can't connect to server" thì proxy của bạn bị lỗi. Nếu hiển thị địa chỉ IP cùng quốc gia của proxy đó thì proxy của bạn hoạt động bình thường.
- Without Proxy: Không thêm proxy vào profile. Lúc này profile sẽ có cùng địa chỉ IP như máy thật của bạn.

3. Extension

Hidemyacc cung cấp gần 800 extensions khác nhau, bạn chỉ cần tìm kiếm extension phù hợp

rồi Install vào profile. Nếu extensions bạn muốn không có sẵn trên hệ thống, bạn có thể tải lên từ máy tính.

4. Timezone

Thông tin timezone sẽ được lấy tự động theo proxy bạn đang dùng. Nếu không dùng proxy thì timezone sẽ được lấy theo địa chỉ IP máy tính thật của bạn.

Bạn cũng có thể tắt phần "Thiết lập múi giờ dựa trên IP thực" và chọn timezone theo mong muốn của mình.

5. WebRTC

Với Hidemyacc, địa chỉ IP qua WebRTC sẽ nhận diện IP sau mỗi lần Run profile. Vì vậy, khi sử dụng proxy, bạn cần chú ý khi nào cần bật hoặc tắt WebRTC như sau:

- Altered: Khi bật Alter, website sẽ lấy IP theo địa chỉ IP của proxy gắn trên profile. Áp dụng trong trường hợp proxy tĩnh hoặc proxy có địa chỉ IP không đổi trong mỗi lần sử dụng profile.
- Disable: Khi chọn disable, hệ thống sẽ làm nhiễu để website không lấy được địa chỉ IP. Lúc này, website sẽ nhận định rằng do quá trình truyền thông tin bị lỗi dẫn đến việc không lấy được địa chỉ IP chứ không phải do người dùng cố tình disable WebRTC. Áp dụng trong trường hợp proxy xoay, địa chỉ IP thay đổi liên tục trong khi sử dụng profile.
- Real: Nếu bạn chọn Real, website sẽ lấy theo IP gốc của máy, dù bạn có đang sử dụng proxy hay không.

6. Geolocation

Geolocation sẽ được thiết lập theo proxy bạn đang sử dụng. Bạn có thể tùy chỉnh theo 3 tùy chọn sau:

- Prompt: Điền thông tin vị trí mong muốn theo kinh độ, vĩ độ và chọn độ chính xác (tính theo mét).
- Allow: Cho phép website lấy thông tin geolocation của bạn.
- Block: Từ chối website lấy thông tin geolocation của bạn. Khi chọn tùy chọn này website không thể thu được thông tin về vị trí thực của bạn.

7. Advanced

Đây là những phần thiết lập nâng cao khi tạo profile mới trên Hidemyacc.

- Mục Security: Nếu bạn không muốn đồng bộ data với máy chủ của Hidemyacc, hãy tắt Đồng bộ hóa dữ liệu trình duyệt lên đám mây.
- Mục Hardware:
  + Mask Canvas: Yêu cầu trình duyệt vẽ một hình ảnh Canvas ẩn, sau đó chuyển về định dạng chuỗi hash để giúp nhận diện browser fingerprint. Thông số này có thể không độc nhất vì có một tập hợp những bản sao của phần cứng thiết bị của bạn ở đâu đó trên thế giới.
  + Audio Context: Đây là thông số tần số âm thanh của thiết bị. Trang web sẽ yêu cầu trình duyệt mô phỏng cách phát các tệp âm thanh dựa trên cài đặt âm thanh và phần cứng bạn đã cài đặt. Thông số này có thể không độc nhất.
  + WebGL Image: Đây là thông số điểm ảnh trên web hoặc Google Maps và cách hiển thị đồ họa 3D trên các trang web.
  + WebGL Metadata: Đây là thông số về card đồ họa. Nếu bạn sử dụng máy ảo thì sẽ không có thông số về card đồ họa nên website có thể dễ dàng phát hiện ra bạn đang không dùng

thiết bị thật. Ngược lại thì các antidetect browser như Hidemyacc sẽ luôn có thông số về card đồ họa, đảm bảo website luôn nhận diện như một thiết bị thật.

+ Client Rects: Đây là thông tin về khoảng cách giữa các điểm ảnh, cho phép website thu thập các thông tin về font chữ cũng như độ phân giải màn hình.

- Mục Khác:
  + Xóa Cache sau khi tắt trình duyệt: Xóa bộ nhớ đệm mỗi khi tắt profile.
  + Phục hồi phiên trình duyệt trước đó: Khi run profile sẽ hiển thị lại các tab đã mở trước đó.
  + Không hiển thị hình ảnh các trang web: Nếu bật thì profile sẽ không hiển thị hình ảnh trên các website được truy cập.
  + Tắt âm: Nếu bật thì profile sẽ không bật tiếng trên website đó.
  + Ghi chú: Nhập các ghi chú cho profile của mình.
  + URL khởi tạo: Khi run profile, hệ thống sẽ tự động mở các URL này. Bạn có thể thêm bao nhiêu URL cũng được. Nếu không muốn mở các URL này nữa, bạn có thể sửa thành URL khác hoặc xóa chúng đi.
- Mục Navigator:
  + Ngôn ngữ: Ở đây là ngôn ngữ trình duyệt. Bạn có thể thay đổi ngôn ngữ trình duyệt theo nhu cầu của mình.
  + Các thông số như độ phân giải màn hình, bộ nhớ phần cứng, bộ nhớ thiết bị bạn có thể để như mặc định hoặc tùy chỉnh lại theo nhu cầu của mình.
- Mục Mask Media Device: Đây là các thông số về thiết bị ngoại vi kết nối với máy tính của bạn. Nếu bạn tắt thì hệ thống sẽ tự động lấy thông tin theo máy tính thật của bạn. Nếu bạn bật lên thì Hidemyacc sẽ random hoặc bạn có thể tùy chỉnh các thông số này:
  + Video inputs - Đầu vào video (số lượng camera): Số lượng từ 1-5.
  + Audio Inputs - Đầu vào âm thanh (số lượng micro): Số lượng từ 1-5.
  + Audio outputs - Đầu ra âm thanh (số lượng loa): Số lượng từ 1-5.

Thông tin về thiết bị ngoại vi mặc dù không đủ để định danh người dùng nhưng nó vẫn đóng một vai trò nhất định để xác định các thông số browser fingerprint.

Lưu ý: Không phải thông số nào cũng là độc nhất nên việc các profile có trùng thông số cũng là điều bình thường, ví dụ như trùng Mask Canvas (các máy tính được sản xuất cùng một thời điểm thì sẽ có khả năng trùng Mask Canvas với nhau), Audio Context, kích thước màn hình,...

8. Cookies

- Nếu bạn muốn sử dụng cookies cũ từ các trình duyệt trước, bạn có thể:
- Tải lên cookies theo định dạng trên JSON hoặc Netscape.
- Nhập cookies thủ công.

9. Bookmarks

Lưu lại dấu trang trên trình duyệt theo 3 định dạng khác nhau:

- Folder::Name::URL
- Name::URL
- URL

Lưu ý: Folder và Name ở đây là thư mục và tên hiển thị trên Bookmarks.

Hidemyacc

Cảm ơn tất cả các bạn đã ủng hộ quyển eBook này của chúng tôi.
Hidemyacc dành tặng mã giảm giá độc quyền 10%

HIDEMYBOOK

(Đến hết ngày 31/03/2024)

cho khách hàng lần đầu tiên thanh toán các gói Hidemyacc.

Bạn hãy liên hệ đội ngũ support của Hidemyacc để được hỗ trợ.

Website:
https://hidemyacc.com

Support: Hidemyacc