



# Clicking into place:

The Rise of Small Business Digital advertising in 2021

# Introduction

Beneath the surface of the \$330 billion digital advertising sector is a vast underground market. On the dark web<sup>1</sup> or the open web are thousands of services, individuals and products offering ways to game the digital advertising system – increasing SEO through automated bot clicks, clicking competitor ads to drain budgets, solving captchas to bypass security measures, and inflating traffic.

This report highlights this underground ad economy. In fact, in the sector of paying for ad clicks through outsourced clickers, payouts have reached \$13.2 million based on 20 companies in this space. Such sites have seen increases in traffic of up to 40% in the past six months the face of global economic recession and COVID-19.

Most click fraud black market platforms and services barely hide activities. They offer customer support, have testimonials, and advertise on search engines. They provide incentives for workers who can earn \$100 per month. In the following pages we will analyze the offers from paying for autoclicker bots, to buying bot traffic to inflate traffic and hiring botnets. It emerges as a booming economy employing both sophisticated hackers to click operations in low-wage countries. However, the net effect from this activity is harming brands, wasting money, and damaging further the reputation of digital advertising.

<sup>1</sup>The dark web constitutes a small portion of the deep web and appeared as a result of the development by the United States of software known as Tor. It allowed internet users to encrypt their location and information they sent and received. This, in turn, ensured their anonymity and privacy. The dark web is often used by criminals for various malicious purposes, such as sales of guns, drugs and other illegal materials

# Autoclickers

Autoclickers simulate clicking on ads through a computing device. While they can have legitimate uses, threat actors have found several ways to improve and weaponize them.<sup>2</sup> These include inflating the number of visits to websites; draining competitors budgets by auto clicking ads; automating visits to paid-for-click websites; and cheats for gaming. This in clear breach of Google's advertising policies which prevents "automated, fraudulent or otherwise invalid impressions, inquiries, clicks or conversions."<sup>3</sup>

Prominent autoclicking solutions include The Bear Autoclicker (costing \$175) offering to generate traffic to a website. It employs several evasion techniques, including browser emulation (so the traffic appears to be originating from a browser). The Diabolic Traffic Bot (\$25) can interact with content on sites, such as downloading items and viewing videos.

Diabolic promises that activity will not be detected as bot traffic "because the bot changes the user agents, however, Google might know that you are using public proxies because many proxy IP are already blocked for searching in google due to abuse of scrapers." Such services also allow users to set the time for the bot to visit their site to appear human (one user says: "I set the minimum time that the bot would spend on my site to be 17 seconds and the max is 59 seconds - to make it look natural").

The platform also promises that "every 15 minutes you will have a new list of working proxies, new proxies added, and dead ones removed". Customers describe a range of needs fulfilled by autoclickers. One purchaser says: "I bought this traffic for helping my inbound marketing report client", while another needed to "push my article on a travel site".

## Gaming Hacks

Autoclickers are also used in gaming – with posts for instance offering autoclicking of Minecraft for only \$10. Dozens of websites, easily found on Google, sell code or services also automate the World of Warcraft Classic experience. This led leading to developer [Blizzard suspending](#) 74,000 accounts as bots upended the game's economy.

<sup>2</sup> Sixgill Report: Death by a Thousand Clicks; Autoclickers and Click Fraud on the Dark Web

<sup>3</sup> <https://www.google.com/intl/en/authorizedbuyers/terms/index.html>

# Click Fraud

Competitor click fraud services offer to exhaust the budget of rivals. GoodGoogle is one of the more infamous Google Ads players operating on Russian-language forums. Using a combination of custom software and hands-on customer service, GoodGoogle promises clients the ability to block the appearance of competitors' ads.

The company [says](#): "Are you tired of the competition in Google AdWords that take your first position and quality traffic?" "I will help you get rid once and for all competitors in Google AdWords." The prices range from \$100 to block between three to ten ad units for 24 hours to \$80 for 15 to 30 ad units. For a flat fee of \$1,000, small businesses can use GoodGoogle's software and service to sideline a handful of competitors' ads indefinitely. Nicholas Weaver, a researcher at the International Computer Science Institute (ICSI) suggests

it involves a "private botnet of hacked computers that do the clicking on ads, and advanced software that controls the clicking activity of the botted computers so that it appears to be done organically from search results. One satisfied user, "Alienstels", says on GoodGoogle's [forum](#): "The project was launched for several days, but after the launch, the competitor turned off direct advertising literally the next day (or he ran out of money)."

Another solution, Traffic Bot Pro (\$30) promises you can click your ad "to make fast money or beat your competitors by clicking their ad automatically." It says: "TrafficBot Pro can visit any page directly from a search, then click any ad you set on the page automatically. It can simulate real human operation by setting random page stay time, mouse move, scroll, inner link clicks, proxy, user agent and visit interval. You will make fast money by this ad click bot and your competitors will be crazy because of this."

# Buying Bot Traffic

The general buying of bot traffic represents a large slice of this underground market. Searches for 'buying traffic for website' yields tens of thousands of results.

Independent ad fraud investigator Dr Augustine Fou [says](#): "Traffic vendors can sell you all kinds of "traffic" and you can even select the "quality" level. Higher "quality" means the bots work harder and fake more things (like mouse movements, page scrolling, and clicks)"The implications for advertisers are clear.

Seif Khemaissia, group director, programmatic and analytics at Innocean Worldwide Canada, says: "Somebody would have a huge surge on a day that we launched a campaign and everybody's patting themselves on the back, saying 'Hey we did a really good campaign.

We ran all of these leads.' But when those leads come in and you find out that they are all fake, then it disrupts the entire reporting systems. The main characteristics of the fraud that Innocean saw was that 99% of it was coming from a Linux device and spending less than 00.01 seconds on the site.

Another traffic buyer [says](#): "These vendors offer a range of services and traffic types – everything from \$2.00 CPC traffic sourced from Google, Yahoo, and Bing, to \$0.002 CPC from god knows where.

When we told them we were looking for the cheapest traffic we could possibly buy there would be sort of a wink and a nod, and they'd make us aware that for that price the traffic would be of "unknown quality".

How much you pay determines how much bot traffic you're getting, so when you're paying \$0.002 a click, you're getting mostly bots. You can tell its bot traffic just by looking at the analytics. We'd see a traffic spike in our real-time analytics dashboard and then we would see all of our traffic for the day serve in a couple of hours."

# Developer Tools

Developer tools were created to help developers streamline web operations but have been engineered for click fraud. For their intended job, developer tools, such as Selenium and Puppeteer, monitor websites, aggregate online content, and automate repetitive tasks. But the same technology is also used to simulate human activity through visiting websites, consuming online media, writing social media posts, clicking on advertisements, installing applications, and filling out lead forms.

Browser bots use these automation tools for nefarious purposes, given their capabilities. Puppeteer (which can emulate 73 different types of device) has been downloaded [122 million times](#) in the last two years. Another developer advertises a \$100-a-month subscription to a browser called [Linken Sphere](#).

This is used according to the developers for penetration testing and privacy, but customers have used the software to get around fraud-detection tools employed by Google, Amazon, and Facebook. The browser allows users to harness hundreds of stolen online accounts, purchased on the dark web, to generate fake ad traffic or to boost online search rankings and shopping reviews, according to the Wall Street Journal.<sup>4</sup>

Tools mentioned on forums (such as BlackHat World) discuss means to hide fake clicks "using ZennoPoster, MultiLogin App or Selenium". Donat Voronin, chief executive of MultiLogin Software, based in Tallinn, Estonia, said his company's browser was primarily used for research by companies, nongovernmental organizations and universities but that, like any software service, there were "nonmainstream use cases."

<sup>4</sup>January 7 2020, Wall Street Journal: New Tactics Punch Holes in Big Tech's Ad-Fraud Defenses.

# Direct Revenue Schemes:

## Humans paid to click on millions of ads

Direct revenue schemes, or PTC (paid-to-click) sites are a key underground industry. This pays tens of thousands of people to click on ads, and complete CAPCHAs.

The business model of PTC sites is generally based on profiting from advertisements clicked on by visitors, that is generating payment for spoofed views of ads. Ryan Hildreth, discussing microworkers.com, says in a [video](#) watched 131,000 times on YouTube you can get paid "\$20,000 just to click on websites."

These people will pay you pay you a dollar to sign up and download an app, or \$9 to install an app. The easiest are the ones you have to click on a website."

## \$13.3 million dollars paid out to human clickers

Based on claims of 20 of the most well-known PTC sites, they have paid out \$13.2 million to people employed to click and view ads, at 5 cents a click. This equates to 266 million ads clicked. These ad views are not by desired customers, but paid workers with no intention or interest in the product or service, and most often, no geographic ability to access them.

These services are almost certainly against Google's own terms and conditions. Nevertheless, some vendors freely advertise on Google's own search service for keywords such as "organic clicks". For instance, Serpclick in its ad "discusses a pool of thousands of microworkers to optimize your organic CTRs and boost rankings."

<b>PTC service</b>	<b>Dollars paid</b> Out to member
PaidVerts	\$ 9.2 million
Scarlet clicks	\$ 2.4 million
PTCShare	\$ 434,000
GPTPlanet	\$ 423,262
Optimal bux	\$ 302,994
Adbazar	\$ 286,389
Investorclix	\$ 101,623
Indexclix	\$ 48,394
Fingersclix	\$ 31,526
Successbux	\$ 26,131
Adsbox	\$ 24,832
Grand Monopoly	\$ 24,470
Imajbux	\$ 9,624
Offersbux	\$ 8,055
Buxerclix	\$ 1,564
Studenbux	\$ 1,402
Indiaclix	\$ 747
LuckyPTC	\$ 577
Adsptc	\$ 26
Divbux	\$ 23
	<b>\$ 13.2 Million</b>

[All](#)
[Images](#)
[Videos](#)
[News](#)
[Maps](#)
[More](#)
[Settings](#)
[Tools](#)

About 19,600 results (0.37 seconds)

**Ad** · [www.serpclix.com/](http://www.serpclix.com/) ▾  
**SerpClix - Real Organic Clicks - Buy Real Traffic to Boost CTR**  
 Use our pool of 1000s of microworkers to optimize your organic CTRs and boost rankings! Buy real SEO traffic to improve your organic CTR and increase your rankings. Increase CTR to Boost SEO. Only Real Human Clickers. Offer Ends Soon. Better SEO Rankings.

**Ad** · [www.propellerads.com/](http://www.propellerads.com/) ▾  
**Buy High Quality Web Traffic - Quality Traffic That Converts**  
 Global Ad Network. 195+ Countries. High Quality Conversions. Start Today. Exclusive ad formats, **real** users, CPM/CPC bidding models. Join us. Auto-Optimization. **Live** Statistics. 24/7 Support. Desktop & Mobile. Flexible Targeting. **Buy** / Sell **Traffic**. Native Ad Formats. [How to Choose Vertical?](#) · [Traffic for CPA](#) · [Top 7 CPA Tracking Tools](#) · [Push Service](#)

**Ad** · [www.bestweb-traffic.com/](http://www.bestweb-traffic.com/) ▾  
**High Quality Website Traffic - 15 500+ Visitors for Only \$25**

In a testimonial video on the SerpClix site, one freelance clicker called Mohammad, says: "I have been clicking for Serpclix since it was founded in 2016. I am paid 5 cents for every click I make. I make about \$15 to \$20 a month from just a few minutes per day."

Google itself warns against using such sites. It [says](#): "To deliver the traffic levels that their customers expect, these services often generate clicks and impressions using click bots, or by providing users incentives to visit sites or click on ads. For this reason, we strongly urge you to use caution when partnering with third-party traffic services."

<sup>4</sup>January 7 2020, Wall Street Journal: New Tactics Punch Holes in Big Tech's Ad-Fraud Defenses.

# COVID-rise in visits to click sites

Pay to click services have enjoyed rising traffic as COVID-19 requires new sources of income globally and human clicking is seen as a fast means to make money. Scarlet Clicks for instance achieved a 41% increase in traffic within six months, to 1.3 million visits a month in September 2020, according to SimilarWeb data. PTCShare has seen a 13% increase in traffic to 1.2 visits a month. NeoBux, one of the largest players hit a peak of 9m visits in May 2020.

Rank	Country	Username	Earnings	Rank	Country	Username	Earnings
1.	USA	partly	\$63,8804	3.	USA	valerian	\$8,5015
2.	USA	alman1212	\$8,4737	4.	USA	adrian	\$2,403
3.	USA	robert	\$7,0876	5.	USA	Lampard	\$6,21428
4.	USA	robert	\$7,0876	6.	USA	adrian	\$2,403
5.	USA	robert	\$7,0876	7.	USA	robert	\$2,2026
6.	USA	robert	\$2,2026	8.	USA	robert	\$4,93815
7.	USA	robert	\$2,2026	9.	USA	robert	\$4,2907
8.	USA	robert	\$2,2026	10.	USA	robert	\$3,9255
9.	USA	robert	\$2,2026	11.	USA	robert	\$3,9255
10.	USA	robert	\$2,2026	12.	USA	robert	\$3,8854
11.	USA	robert	\$2,2026	13.	USA	robert	\$3,7845
12.	USA	robert	\$2,2026	14.	USA	robert	\$3,7845
13.	USA	robert	\$2,2026	15.	USA	robert	\$3,7845

These sites have sales-type league leaderboards to encourage competition and boost earnings, and psychological techniques including showing how many other workers are online at any time during the day.

They also encourage posting of payouts to show the legitimacy of the service and remuneration achieved.

Other sites such as Fivesquid offer \$5 packages to give certain amounts of "safe" [Ad Sense Clicks](#) to sites.

This for instance sets out the terms of the clicks including real human visitors from the US. The offers set out "the minimum time that the visitor spend on your site" (in order not to attract attention), and ensures that the clicks are spaced out so customers achieve five clicks a day for seven days."

Sellers also offer monthly subscription to get regular visits.

## Captcha Solvers

Captcha solving is a core part of the PTC market. Captchas are verification tests in computing which are used to determine whether the user is a human or a robot.

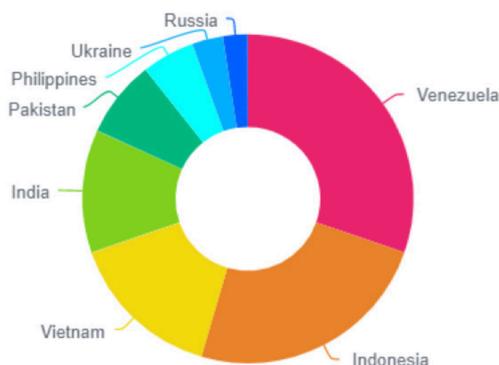
Captcha-solving farms provide armies of codebreakers to solve their captchas – which are deployed by companies to keep bots out from their funnel. Pricing for vendors including 2Captcha (\$0.77 per 1,000 Captchas) which also claims to have more than 2,000 workers online at any one time. Deathbycaptcha.com offers solving rates at \$1.39 per 1,000.

The combination of software and APIs allow for fast account creations or automated sign ups using bots and Captchas. For instance new accounts on Reddit can be created using dev ops software such as Puppeteer and captcha-solving leader, 2Captcha, [as shown in this study](#).

## The profile of Captcha solvers

One firm, Anti-captcha provide a profile of their Captcha solvers, and the importance of the industry in low-wage countries.

They explain: *"An average worker makes about \$100 per month which is a very good salary in such countries like India, Pakistan, Vietnam and others. With your help they now have a choice between working in polluted industries and working in front of a computer."* In this case the largest share of employees come from Venezuela, followed by Indonesia, Vietnam and India.



# Click Farms

Strictly, a click farm is any kind of operation intended to fraudulently interact with a website. They continue to migrate to online platforms, as seen above. However physically located mass click farms remain housed in low-cost regions like South East Asia or India, where the authorities have run crackdowns on click farm operations, sometimes recovering hundreds of thousands of SIM cards used to validate accounts.

Former click farms workers have reported working 12-hour shifts for very little money, and even some form of PTSD related to hearing an incessant clicking sound for hours on end.

| \$10 | THE ONLY SEO TOOL YOU NEED | GOOGLE ADS BOT | ON-SITE CLICK

08-10-2020, 09:53 PM (This post was last modified: 08-14-2020, 06:12 PM by waytoclashy)

♥ #1

**CURRENT PRICE: \$10** (x more orders until price increases!) (this is my first tool I am selling on HF hence the low price.)

## Lone wolves

Smart motivated and capable people also cause harm in this underground market by manipulating online advertising. Black hat forums regularly host [questions](#) about click operations and services.

Jason Yim, a platform specialist says his [24-year-old friend](#) created their own software to click on ads. He says: "Running a startup a few years ago only had a limited budget to spend on ads. Knowing there was no way he could outbid his competitors on paid search, he decided to drain their ad budget.

He devised an algorithm to search for the keyword he was going for and to click on his competitor's ad. Once their ad budget is drained, he proceeded to launch his ads to capture the market. The algorithm had some sophisticated rules behind the scenes It will only click the ad 20% of the time to maintain the CTR so the competitors couldn't detect something was wrong. It had IP rotation to ensure Google wasn't able to flag it as bot traffic."

# VPNs

Readily available virtual private network (VPNs) are a vital part of the click fraud economy despite, once again, having many legitimate uses. The VPN market has grown exponentially over the past 10 years, generating more than [\\$15 billion in revenue](#).

The virtual location uses a unique new IP address every time the VPN is activated. So, if you're in India, a clicker could use a VPN to show your location as the USA. This hurts campaigns targeting the US which receives irrelevant clicks masked by this privacy-protecting software.

This type of location obfuscation is used by organized setups such as click farms or botnets. With a bank of servers pre-loaded with VPNs, fraudsters can route bot traffic and hide their actual location.

Based on billions of impressions analyzed for enterprise clients, we have found that more than one in five invalid clicks (21%) include location obfuscation, whether via emulators or VPN proxies.

## Fake review bots

It has [been shown](#) how easy it is for bots to mimic human reviews. Fake reviews services are common on the dark web, including generating fake app ratings.

# Enforcement

Enforcement against this underground market is rare despite the numerous challenges they face to legitimate advertisers. Google lists the "*generating or receiving automated traffic*" as one of the main "*violations that lead to account closure*."

In other cases, court enforcement is taken against fake traffic buying or misrepresentation. For instance, Amazon subsidiary, Kindle Direct Published took court action against a British book publisher who breached [Amazon's terms](#) by using click farms to manipulate their rankings.

The US Securities and Exchange Commission (SEC) has taken enforcement action against Paid-to-Click vendors offering [scam "ad packs"](#) or other advertising products.

# Conclusion

The flourishing underground ad click economy is diverse, thriving and continues to grow. However, its impact on advertising is clear.

Persistent automated clicking of ads remains an hourly feature across the client accounts [ClickCease](#) analyzes, representing more than 2000 clients across all industries.

The use of readily available tools and platforms discussed in this paper is the engine of a click fraud problem that can account for up to 15% of interaction on paid campaigns.

Based on the upper end of advertising on paid search, the average small business can lose more than \$15,000 a year to click fraud, perpetrated using the readily available options available. More must be done to ensure that only viable leads and clicks are captured. This will improve the fortunes of businesses and the reputation of online advertising in general.