# cam's guide to finding numbers

Each day, millions of automated scam calls are sent out to consumers around the world. However, coming across active numbers for these scams can be quite difficult. This guide is used to help scambaiters find the telephone numbers they need.

## Overview / The Basics

Most phone scammers work shifts that follow the eastern time zone, with call volumes increasing at around **11:00am through 3:00pm Eastern Standard Time**. Some may operate on weekends, but those robocall campaigns are much smaller in comparison to those on weekdays.

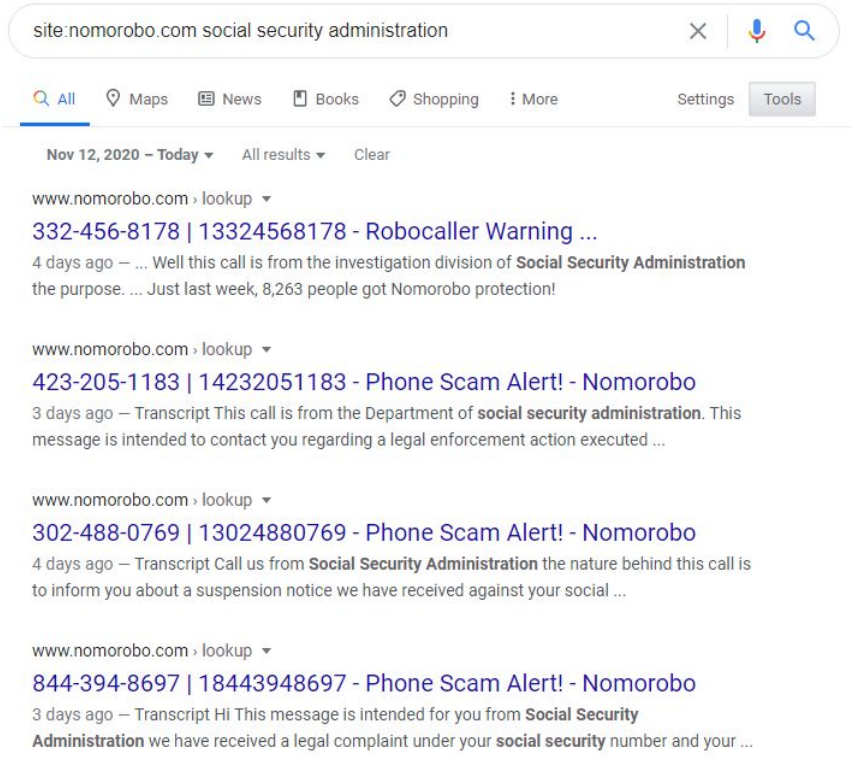
Social Security Administration robocalls are usually the first type of robocalls to be sent out, starting at around 9:00am EST. There are very few SSA scam call centers in the world, so the scammers working at these call centers may switch to the traditional refund scam during later hours.

Keep in mind that some of the methods explained may not work as expected, there's no guarantee that every single number you come across will be active. You may even find a few telephone numbers that have fallen victim to the act of **spoofing**. Spoofing is when someone uses a phony caller ID, typically masquerading numbers belonging to legitimate companies or organizations such as Microsoft, Amazon and Apple; or even innocent telephone subscribers who have no acknowledge of the scam. Many scammers spoof caller IDs in their robocall campaigns to appear more genuine.

If you plan on submitting the numbers you find to scambaiting platforms such as BobRTC or Scammer.info, make sure you always verify those numbers before posting them. Spoofed numbers are not allowed on these platforms as they do not directly lead to a scammer.

# Method 1 - RoboKiller and Nomorobo

This first method uses a combination of the two most popular robocall blockers on the market as well as search engine tools. With every number these platforms block, it is added to their respective lookup pages along with a recording and transcript which is all made public.




You can take advantage of search engine tools to find numbers for certain types of scams that do outbound campaigns. This includes SSA, refund, Amazon customer support and more. Here are some commands and keywords you may want to use:

- **site:robokiller.com** - Pulls numbers from RoboKiller's lookup page
- **site:nomorobo.com** - Pulls numbers from Nomorobo's lookup page
- **"computer", "renewal", subscription", "antivirus"** - Finds computer related scam numbers, usually refund
- **"social security administration", "legal", "law enforcement"** - Finds SSA scam numbers
- **"amazon"** - Finds Amazon scam numbers, sometimes business listing scams

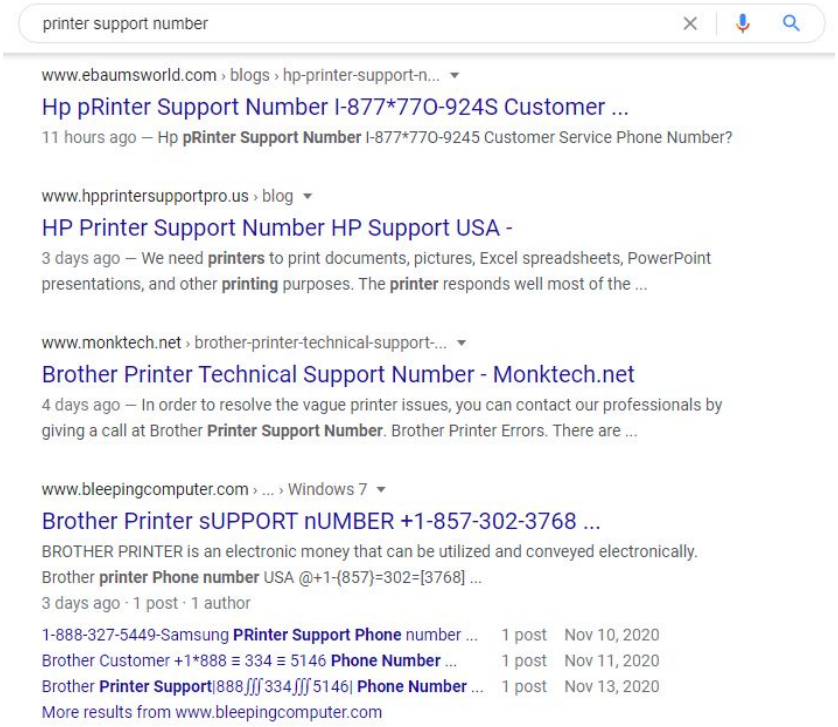
...and so on. You can always use different keywords relating to scams I haven't mentioned here, these are just ones that will give you the most numbers as they're the most popular forms of phone scams. Most importantly, make sure you select "Past hour" for recent numbers. Otherwise, you'll be stuck with old numbers that are no longer in service and will not work.

Make sure you verify which numbers are the scams you're searching for. For example SSDI robocalls may show when searching for SSA robocalls; those numbers are useless for scambaiting because they are typically outbound only.

## Method 2 - Search Engine Spam

This next method also uses search engine tools to find numbers. To bring victims in need of urgent technical support, scammers will spam their phony support numbers on various discussion forums, online guest books/memorials and other websites that offer a form of communication. This is for search engine optimization (SEO) purposes, and it helps bring those telephone numbers to the top of search engines.

Scammers sometimes create custom websites with platforms like Wix and Weebly to boost SEO. This is also used to make victims believe they are visiting the official contact/support pages for these companies and products and will prompt them to dial the support number listed.




An example of various tech support scammers advertising their inbound telephone numbers onto forums or their own custom websites to boost search engine optimization.

## Method 3 - The PopupDB generator

PopupDB hosts a website and Discord server used to research fraudulent tech support pop-ups, they also have a great tool to find these pop-ups (and their telephone numbers) at https://popupdb.org/generator/.

These fake pop-ups work just like robocalls, you'll need to look for them during peak hours when people are using their computers. Also remember that most pop-ups will not appear if you are using a VPN. Some of the pop-ups you find may feature content deemed not safe for work as well as phishing scams and pages demanding you to download a malicious browser extension or software update, disregard these.

## Method 4 - Online Telephone Directories (800notes, WhoCallsMe, etc.)

While it's the weakest of all methods and should be treated as a last resort if you can't find any numbers, these websites and its many contributors can be quite helpful for finding scam telephone numbers.

This method is very simple. Just go to 800notes.com and/or whocallsme.com and use the search tool to find certain types of scams. Use keywords previously mentioned in Method 1 and try sorting by recent ranges of time, not by relevance which often showcases old and outdated numbers.

## Resources

- Scammer.info, the largest scambaiting forum on the internet
- BobRTC, a free calling service with a great database of scam numbers
- The PopupDB generator, a useful way to gather scam pop-ups
- 800notes and WhoCallsMe, a pair of free phone directories