DOES IGNORING ROBOCALLS MAKE THEM STOP? HERE'S WHAT WE LEARNED FROM GETTING 1.5 MILLION CALLS ON 66,000 PHONE LINES

Posted on February 23, 2021 by Sathvik Prasad, North Carolina State University and Bradley Reaves, North Carolina State University

New research aims to give phone companies tools to help curb robocalls.
Peter Dazeley/The Image Bank via Getty Images
Sathvik Prasad, *North Carolina State University* and Bradley Reaves, *North Carolina State University*

The Research Brief is a short take about interesting academic work.

The big idea

More than 80% of robocalls come from fake numbers – and answering these calls or not has no effect on how many more you'll get. Those are two key findings of an 11-month study into unsolicited phone calls that we conducted from February 2019 to January 2020.

To better understand how these unwanted callers operate, we monitored every phone call received to over 66,000 phone lines in our telephone security lab, the Robocall Observatory at North Carolina State University. We received 1.48 million unsolicited phone calls over the course of the study. Some of these calls we answered, while others we let ring. Contrary to popular wisdom, we found that answering calls makes no difference in the number of robocalls received by a phone number. The weekly volume of robocalls remained constant throughout the study.

As part of our study, we also developed the first method to identify robocalling campaigns responsible for a large number of these annoying, illegal and fraudulent robocalls. The main types of robocalling campaigns were about student loans, health insurance, Google business listings, general financial fraud, and a long-running Social Security scam.

Using these techniques, we learned that more than 80% of calls from an average robocalling campaign use fake or short-lived phone numbers to place their unwanted calls. Using these phone numbers, perpetrators deceive their victims and make it much more difficult to identify and prosecute unlawful robocallers.

We also saw that some fraudulent robocalling operations impersonated government agencies for many months without detection. They used messages in English and Mandarin and threatened the victims with dire consequences. These messages target vulnerable populations, including immigrants and seniors.

Why it matters

Providers can identify the true source of a call using a time-consuming, manual process called traceback. Today, there are too many robocalls for traceback to be a practical solution for every call. Our robocalling campaign identification technique is not just a powerful research tool. It can also be used by service providers to identify large-scale robocalling operations.

Using our methods, providers need to investigate only a small number of calls for each robocalling campaign. By targeting the source of abusive robocalls, service providers can block or shut down these operations and protect their subscribers from scams and unlawful telemarketing.

What still isn't known

Providers are deploying a new technology called STIR/SHAKEN, which may prevent robocallers from spoofing their phone numbers. When deployed, it will simplify traceback for calls, but it won't work for providers who use older technology. Robocallers also quickly adapt to new situations, so they may find a way around STIR/SHAKEN.

No one knows how robocallers interact with their victims and how often they change their strategies. For example, a rising number of robocalls and scammers are now using COVID-19 as a premise to defraud people.

What's next

Over the coming years, we will continue our research on robocalls. We will study whether STIR/SHAKEN reduces robocalls. We're also developing techniques to better identify, understand, and help providers and law enforcement target robocalling operations.

Sathvik Prasad, PhD Student, Department of Computer Science, *North Carolina State University* and Bradley Reaves, Assistant Professor of Computer Science, *North Carolina State University*