pindrop

2016 Top Consumer Phone Scams

FROM PINDROP LABS

Research Team: Aude Marzuoli, Valerie Bradford, McClain Talley

Top Consumer Phone Scams

Last year, 11% of U.S. consumers reported that they lost money to a telephone scam, according to a survey conducted by the Harris Poll. The survey estimates that 27 million U.S. consumers lost approximately $7.4 billion to phone scams, averaging $274 per victim. In an effort to understand the types of scams being conducted, the frequency and timing of their occurrence, and the methods and motives of the perpetrators behind these attacks, Pindrop Labs collected and analyzed more than 100,000 calls from the first half of 2016, of which about 30,000 were robocalls.

If you answer the phone and hear a recorded message instead of a live person, it's a robocall. You've probably gotten robocalls about candidates running for office, or charities asking for donations. These robocalls are legal. But if the recording is a sales message and you haven't given your written permission to get calls from the company on the other end, the call is illegal. In addition to the phone calls being illegal, their pitch most likely is a scam.It is unclear what percentage of robocalls are scam, but the top 40 scam campaigns account for more than 50% of robocalls.

A bigger problem with these consumer phone scams is that often they are just the first step in a larger attack. Scammers are looking for more than quick money from a consumer. They are also phishing for personal information that can then later be used to steal an identity and enable an account takeover attack at a financial institution, retailer, insurance provider, or other organization. Businesses must be aware of the role that consumer fraud plays in the larger threat landscape.

THE TOP 40 SCAM CAMPAIGNS ACCOUNT FOR MORE THAN 50% OF ROBOCALLS

Key Findings

Scammers target small business owners

As small businesses and homegrown side businesses continue to grow in popularity, fraudsters are finding these business owners to be a lucrative target. 29% of robocall scams this year actually target small business owners, taking advantage of their lack of knowledge about online search optimization.

News cycles drive scams

Fraudsters devise scams based on relevant news topics. For example, IRS scams gain popularity right before tax season and lose popularity afterwards, political scams are more common during and around election years, and since the implementation of the Affordable Care Act, four different types of robocalls have been discovered telling victims that they can lower their insurance rates or apply for Obamacare

Google is currently the top consumer phone scam.

In this scam, callers are told their business listings on Google are not up to date, or they're at risk of being removed from the top page of search results. "Consultants" who are not actually affiliated with Google promise to help business owners in return for a fee. However, usually the "consultants" are phishing for credit card information. While this type of scam first appeared in 2015, it's gained serious traction this year, and variations exist such as Yahoo and Bing-related scams, too.

PHONE SCAMS COMPLAINTS

	2016	2015	2014
1. Google	18%	4.4%	N/A
2. Loans	8%	12.5%	5.2%
3. Free Holiday	7%	3.0%	7.5%
4. Political Calls	6%	0.3%	N/A
5. Local Maps Verification	3%	N/A	N/A
6. Lower Your Electricity Bills	2%	N/A	N/A
7. Important Personal Business	2%	N/A	N/A
8. Credit Cards	1%	14.1%	18.5%
9. Home Security Systems	1%	6.6%	13.6%
10. Elderly Scams	1%	N/A	N/A

PERCENTAGE OF CALLS

1. Google/Business Listing Scams

18% of all ROBOCALLS | **1,250** SPOOFED phone numbers | ↑ from #9 in 2015

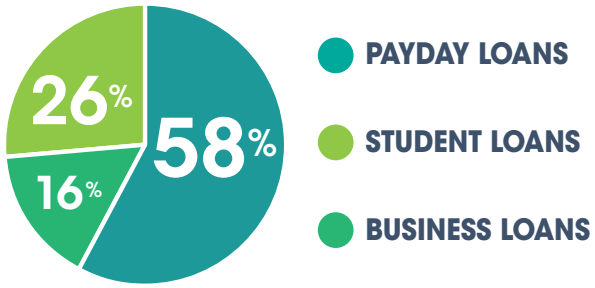
In this scam, callers are told that their business listings on Google are not up to date, or at risk of being removed from the top page of search results. "Consultants" who are not actually affiliated with Google promise to help the business owner in return for a fee. Though too often they are phishing for credit card information. Although the Google scam first appeared in 2015, it has gained serious traction this year. Variations on this scam include Yahoo and Bing search consultants as well. *https://soundcloud.com/pindrophq/business-verification*

2. Loan Related Scams

8% of all ROBOCALLS | **1,217** SPOOFED phone numbers | NO CHANGE from 2015

Victims of this scam pick up the phone to hear recordings offering help to lower interest rates, or threats that loans are past due. The steady popularity of this scam over the past year and a half may in part be due to an emerging trend around payday loans, which have recently become a new hook for scam artists. The National Consumer's League has received numerous complaints from consumers reporting that scammers claiming to represent payday loan companies, collection agencies and law enforcement have contacted them. The scammers frequently use information acquired from legitimate online loan applications to trick their victims into believing that the scammers are truly representatives of their loan providers. These scammers use the threat of being arrested to intimidate their victims into giving them money. *https://soundcloud.com/pindrophq/2-loan-related-scam*

BREAKDOWN OF PHONE LOAN SCAMS



3. Free Holidays

7% of all ROBOCALLS | **1,247** SPOOFED phone numbers | ↑ from #15 in 2015

Similar to the free cruise scam that peaked in 2014, the free holiday scam remains popular. Callers tell victims that they have been selected to receive a free vacation, hotel stay at a Marriott or Hilton, or trip to Disneyland. However, fraudsters use high-pressure sales tactics to spur victims to give them their credit card information to pay for "tax" or additional fees such as food and beverage packages.
https://soundcloud.com/pindrophq/3-free-holiday-scam

4. Political Calls

6% of all ROBOCALLS | **1,341** SPOOFED phone numbers | ↑ from #17 in 2015

With the Presidential election scheduled for this coming November, fraudsters are employing politically- geared robocalls to pique consumers' interest. According to the Better Business Bureau, fraudsters claim to be pollsters with survey companies and gain the trust of their victims by agreeing with their political sentiments and claiming that your donation will help the cause/candidate that you care about. They also ask for donations, phish for personal information by claiming that you need to re-register to vote, and offer to take your vote over the phone.
https://soundcloud.com/pindrophq/4-political-calls

5. Local Maps Verification

3% of all ROBOCALLS | **106** SPOOFED phone numbers | NEW in 2016

This scam is a robocall informing consumers that their local business has been flagged by online maps verification and they must confirm personal information. With the personal information gained via this scam, fraudsters can commit account takeover in various multiple channels.
https://soundcloud.com/pindrophq/5-local-maps-verification-scam

6. Lower Your Electricity Bill

2%	of all ROBOCALLS	102	SPOOFED phone numbers	NEW in 2016

In this scam, consumers are offered the opportunity to lower their monthly electricity bill and then prompted to disclose personal information. Fraudsters claim to be a representative from your electric company in this particular scam, earning a consumer's trust before stealing their personal information. This scam is often presented as a "now or never" or "limited time" offer. *https://soundcloud.com/pindrophq/6-lower-your-electricity-bill-scam*

7. Important Personal Business

2%	of all ROBOCALLS	102	SPOOFED phone numbers	NEW in 2016

This non-descript consumer scam only states that the caller has an urgent message concerning "important personal business" and prompts the victim to press 1 to hear the message. Because nothing more than "important personal business" is specified, many consumers fall victim to curiosity and are exploited by this scam. Pindrop Labs researchers believe this scam to actually be a fake debt collection scam. When victims press 1, they hear a message claiming that victims owe money to the state or certain scholastic departments.
https://soundcloud.com/pindrophq/important-personal-business

8. Credit Card Related Scams

1%	of all ROBOCALLS	59	SPOOFED phone numbers	↓	from #1 in 2015

Falling in popularity this year due to stricter surveillance and many shutdowns by the FTC, are credit card related scams. Here, fraudsters claim that they will be able to help you pay off your credit card debt faster, lower the interest rate on your bills, and save you thousands of dollars. Most illustrate a need for the victim to act now as they are offering a one-time opportunity. These "programs" rarely do anything to help the victims with their credit card. To make matters worse, the callers may try to "confirm" personal and financial information, including existing credit card numbers in order to "process" the rate reductions. Fraudsters can then use this information to steal a victim's identity. *https://soundcloud.com/pindrophq/8-credit-card-scam*

9. Free Home Security System

1%	of all ROBOCALLS	291	SPOOFED phone numbers	↓	from #7 in 2015

This scam was the second most popular scam of 2014, but is still swindling many callers today. In the scam, callers are warned that crime has been increasing in their neighborhood, and a friend or neighbor has suggested they would be interested in a free security system.

The “free” system is often tied to a pricey long-term system-monitoring contract that includes hefty administrative fees. In many cases, scammers convince victims to give them their credit card information resulting in account takeover and identity theft. *https://soundcloud.com/pindrophq/9-home-security-robocall-scam*

10. Elderly Scams

1%	of all ROBOCALLS	83	SPOOFED phone numbers	NEW in 2016

Senior citizens are frequently the targets of consumer scams because fraudsters consider them easy victims. These scams cover everything from Medicare and health insurance to faulty anti aging products and even funeral and cemetery plots. Fraudsters believe the elderly to be lucrative targets because they often have a significant amount of money in their accounts or retirement funds. *https://soundcloud.com/pindrophq/10-elderly-scam*

Tips For Consumers

The first step in stopping unsolicited calls is to register all phone numbers with the **National Do Not Call Registry.** Once listed, you number is protected and you should be suspicious of any unwanted caller because they are likely breaking the law. It is also wise to remain conscious of fraudsters using free tools to change the number that appears on your Caller ID. These tools are highly accessible and ID alone cannot be trusted these days.

Don’t Wire Money

In 2015, the FTC banned all wire transfers, reloadable cash cards, and payment orders for phone transactions. If a caller asks you to pay using one of these methods, it is definitely a scam.

Don’t Answer, Don’t Interact, Don’t Request to be Removed

Fraudsters keep lists of “live” contacts. If they detect a human is on the other end of the line, they will only start calling you more often.

Call-blocking apps

Use a call-blocking service. Consumers have access to several apps like Hiya, and Truecaller that can alert them when a call they are receiving is from a scammer by checking the number against databases of phone numbers commonly used by illegal robocallers. These services are not perfect, but are improving over time.

Call them back.

If you are concerned that a robocall could be legitimate, ask to call them back. If the caller says this is not possible, they are likely a fraudster. When calling back, do not use the number the initial caller gives you or the Caller ID, but rather ask for a case number for your scenario and then look up the number for the specific organization on your own – for example, on the back of your credit card.

Methodology: *Pindrop Labs collected phone scam data using their proprietary PhoneypotTM tool.The Phoneypot is the largest telephony honeypot in the worlds, and it allows researchers to collect data from millions of calls to unlisted numbers. Pindrop uses the phoneypot to analyze phoneprints and detect calling patterns for unwanted callers, such as robocallers, debt collectors and telemarketers. This provides researchers with new insights into telephony abuse and attack patterns.*