

tellows magazine

the fight against dubious callers

Scam Method Overview

Information about how scams work plus reports based on user experiences and tips on how to protect yourself from scams

Legal Basics

Information about the current legal framework on nuisance calls and appropriate authorities and regulators

Solution

Protection methods in the fight against nuisance calls and fraudulent calls

Plus...

Statistics, real consumer experiences and information on how the scammers learned about your phone number

Are you a victim of telephone harassment?
tellows can help!



tellows

Who is calling?

Contents

1. General Info

Preface	3
Statistics says...	4
Who is the most harassed in US?	5

2. Why am I getting these calls?

How did the caller know my phone number?	6
Experience of consumers	7
Where do these dubious numbers come from?	8

3. What kind of phone scams are out there?

An Overview	9
Scam using Obamacare	10
Visa/Immigration Scam	11
Fake debt collector	12
Caribbean Numbers	13
Spoofing Verizon Wireless	14
Medical Alert Scam	14
Spoofing IRS	15
Job Offer Scam	15
Social Network Scam	16
PC Doctor	17
General Tips	17

4. Report a Scam

The National DNC Registry	18
FTC and FCC Links	18
The Telemarketing Sales Rules	19
The DNC and TPS	19

5. How can I protect myself?

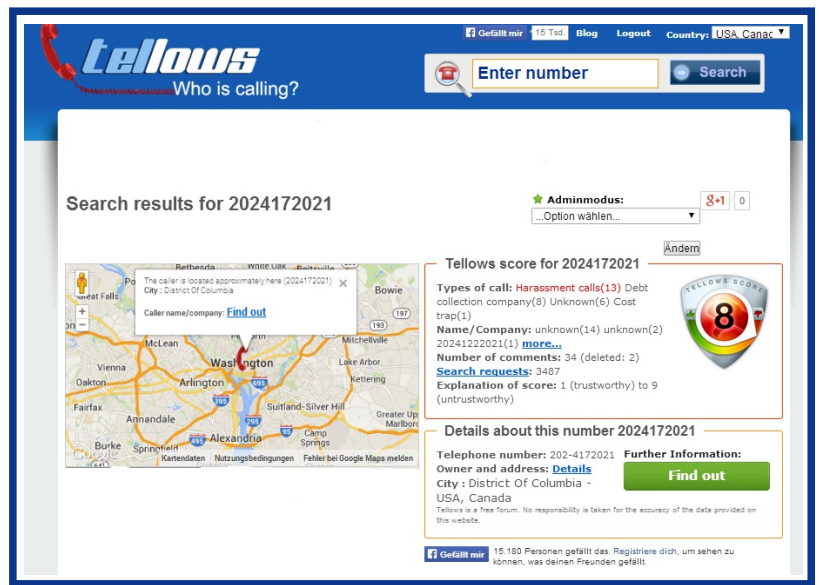
tellows helps!	20
tellows Score	21
Call Guideline	21
tellows App for Android und iPhone	23

6. And more.....

Still have questions?	24
Important Addresses	25
Imprint	25

Preface

Every week here at tellows.com, we receive various reports of phone scams that have cost their victims millions of dollars or caused anxiety and stress by robbing people of everything from their personal financial details to their good night's rest. Scammers are creative in finding ways to cheat people out of money. They may call you by your first name, ask about your situation to sound concerned, or make promising offers. They may say they are connected with the company you trust, or may send mails to convince you to call them back. In many cases, old scams are being reinvented with the use of advancing technology.



Criminals are ingenious and cruel, so read on - and beware. By knowing about these tricks you can help protect yourself and others from falling victim to the scammers.

It is the aim of the tellows magazine to raise awareness among consumers about this topic and protect you against telephone harassment. In this magazine you will receive information and solutions regarding nuisance calls and fraud. Recent reports from consumers serve as examples of how tellows works in over 50 countries with more than 75,000 phone numbers in its database worldwide. And as many consumers are not familiar with their legal rights and protection, the tellows magazine will provide an overview of the law and the respective public and private agencies. And of course, we have an app solution for your smartphone that will ease the burden of these annoying phone calls.

Our tellows Team wishes you good luck and success in the fight against telephone harassment!



Statistics says...

Increasing number of complaints and DNC subscribers

US government latest data show more than 80% increase in the monthly complaints submitted on phone fraud, as well as a two-fold increase in the complaints from people asking a telemarketer to stop calling them.

The National Do Not Call Registry now has more than 209 million phone numbers on it, considering that there are about 84 million landline subscribers plus plenty more people with cellphone numbers, which can also be registered in the DNC.

Identity Fraud

The 2013 Javelin Strategy & Research report shows that the number of identity fraud victims in the U.S. increased to a total of 12.6 million consumers, or more than 1 in every 20 consumers. Annual overall fraud reached \$20.9 billion.

More than 740 million credit cards and other records were exposed in 2013, making it the worst year in terms of data breaches recorded, which is still a very conservative estimate, according to the Online Trust Alliance.

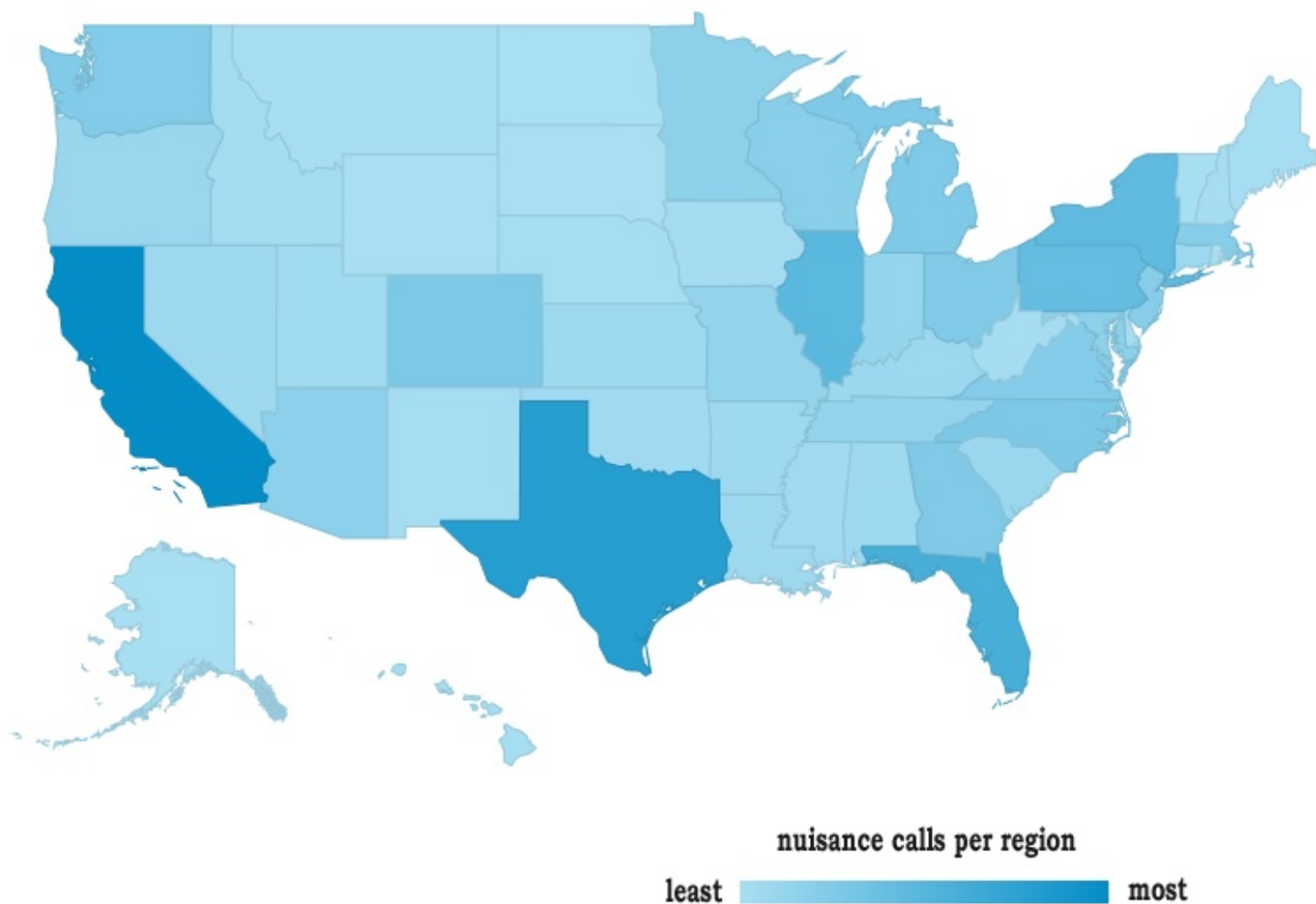
For instance, one kind of payday scam that was discovered in 2012 made more than 2.7 million calls to at least 600,000 phone numbers in the US, according to the Federal Trade Commission. The scammer allegedly collected \$5.2 million from consumers in less than two years.

IRS investigations

According to IRS, in the first three months of 2013, the agency worked with victims to resolve and close more than 200,000 cases. IRS Criminal Investigation tripled the number of identity theft investigations in fiscal year 2012, starting with 900 investigations. Nearly 500 people have been indicted across the country. From October 2012 through to March 2013, there have been more than 670 criminal identity theft investigations opened.

During 2012, the IRS prevented fraudulent refunds amounting to \$20 billion, including those related to identity theft, compared with \$14 billion in 2011. By late 2012, the IRS assigned more than 3,000 of its employees — double the number from 2011 — to work on identity theft-related issues. In addition, the IRS has trained 35,000 employees who work hand in glove with taxpayers to recognize identity theft indicators and help people victimized by identity theft.

Who is the most harassed in the US?



Based on the number of complaints submitted to tellows.com, this map highlights the regions which are subject to the most vehement of spam and scam calls. It displays hotspots the nuisance caller is focusing on. California came in as the region with the highest rate of unwanted calls received. Next is Texas and Florida, followed by New York and Pennsylvania. Illinois and Colorado receive less while Montana, North Dakota, Alabama and Mississippi are just some of the regions which reported the least number of complaints to tellows.

How did the caller know my phone number?

We often ask how and where the caller got our phone numbers. Here are some comments from tellows users asking the same question:

<i>(Anja)</i> <i>My number is not in the directory, whether online or in phone book, so how did these callers get my number?</i>	<i>(Anna)</i> <i>How come this caller knows my number? My friend said it's possible that my number is being sold to telemarketers, oh no...</i>	<i>(Ryan)</i> <i>This is getting crazier, I just changed my number and now I'm getting another annoying call!</i>
---	--	--

Quotes from tellows users

Primary sources for scammers would be the official directories and yellow pages containing names, addresses and telephone numbers. Fraudsters often choose those with old first names since they think old people are easy targets. Telephone numbers in newspaper ads are also abused. Disguised as tokens of gratitude for loyal costumer, fraudsters lure their victims with attractive offers, membership cards and discounts only to collect personal information. Sweepstakes and contests are another popular method of address collectors. Participants are tricked with the chance of quick money or prizes in exchange for their data. Some call centers also just try different combinations to call anyone randomly, the same as in the automatic sending of an SMS.

In the age of internet, it's even easier to spy out addresses and phone numbers. So-called bots browse the internet for phone numbers in classifieds or other publications. Social networks also offer an additional platform for scammers. Imagine the wealth of personal data stored in your Facebook account or Instagram. Fraudsters would also send website links and files which when clicked or downloaded would install malwares in your pc which can gather sensitive information, or gain access to your private computer systems.

The biggest problem lies in the business of data sharing. Companies earn a huge profit in the sales of personal info where price increases if the data gets more detailed. It is easy money since addresses and phone numbers can be sold several times.



This makes it impossible to prevent annoying calls because of the variety of ways available for companies to collect and sell contact details of individuals and firms. You may want to consider going ex-directory, and if you're online, look out for pop up boxes inviting you to receive a company's newsletter and make sure to choose the "tick here to opt-out" box.

2. Why am I getting these calls?

Experiences of consumers

If you ask the caller where and how he obtained your phone number, it is obviously a scam if you are fed with responses such as these below:

(hjk12)

The caller confirmed to me that he used the phone directory! Guess i should go ex-directory now.



(541zip)

caller told me it doesn't matter how he got my number, the important thing was that I listen to his message. duh!

(clips)

The telemarketer said they randomly generate numbers by a computer. This should be illegal! I am in the DNC!

(onno33)

The caller cld not tell me how he knew my number, I'm not even a customer of the company he's claiming he's connected with.

(turnip)

Caller was sarcastic and rude when I asked how he got my number and other personal info.

(maxx)

the caller just hung up without proper goodbye when i asked him politely how he knew my number!!!



(pines)

the guy said he got my number online. some random answer, obviously.

Quotes from tellows users

www.tellows.com/stats

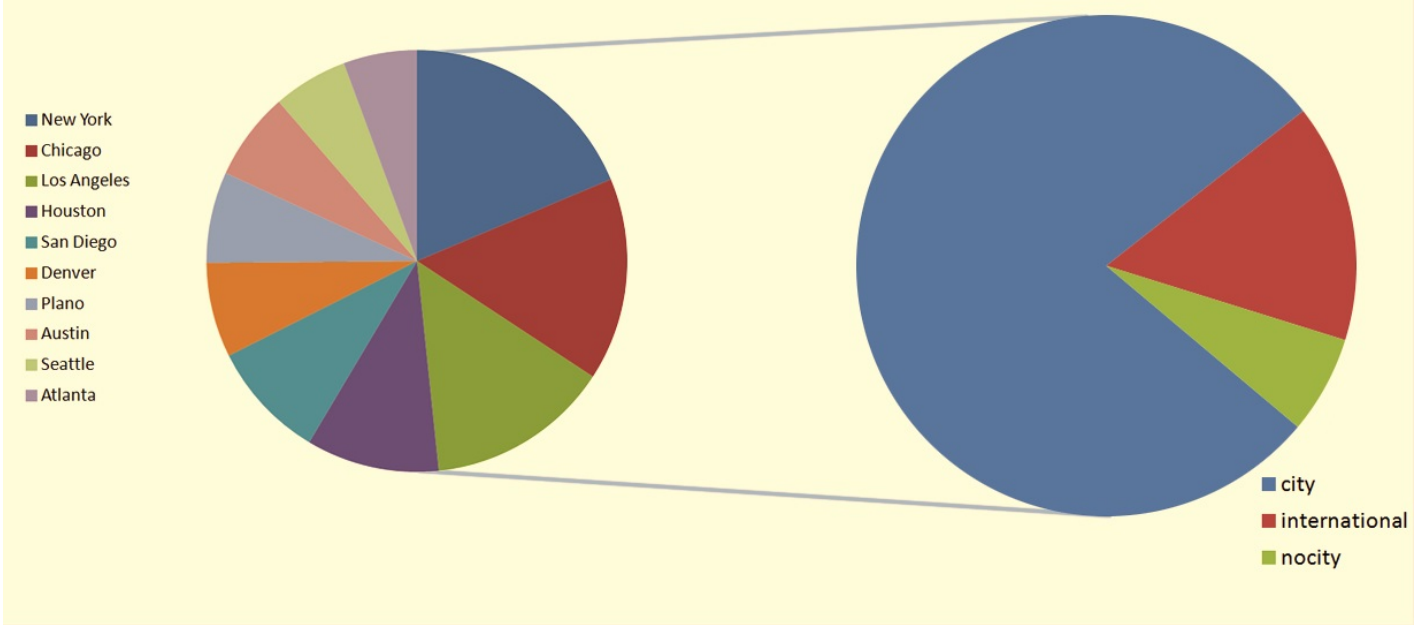
In the statistics page of the tellows US website, you will find a map that shows the location of people who have been using tellows within the last 24 hours. It is a "heatmap" that displays where numbers are mostly searched.

The page also lists the numbers with the most comments (last 5 days), those that are rated as untrustworthy, trustworthy, as well as the newly added numbers in tellows database.

2. Why am I getting these calls?

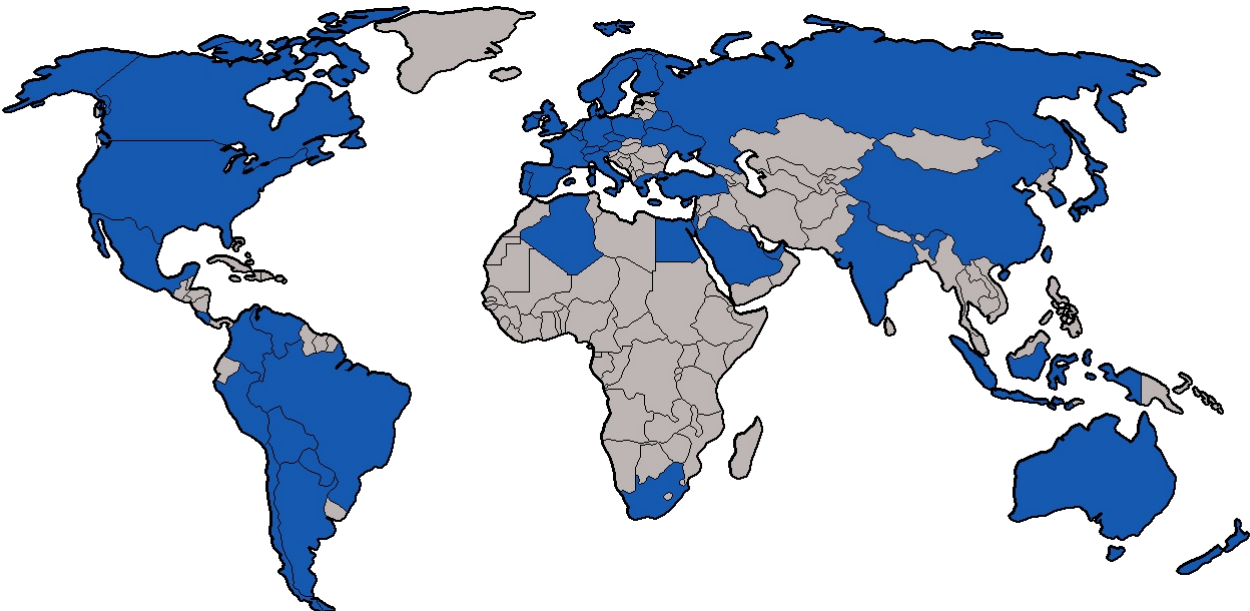
Where do these dubious numbers come from?

Neither do consumers usually have an idea why they receive the unwanted calls, nor where the calls originated from. Through tellows, the following chart classifies the numbers most searched according to whether they come from a particular city in the US, from a mobile source, or from an international location.



The chart shows that most calls were done using a landline service. New York is on the top of the list where most landline nuisance calls were conducted, followed by Chicago and Los Angeles. Seattle and Atlanta received less unwanted calls based on tellows data. On the other hand, more than 20% of the calls came from abroad.

Apart from US, tellows also contains a database of numbers in various countries. The following map shows where tellows is present based on the blue-marked countries.



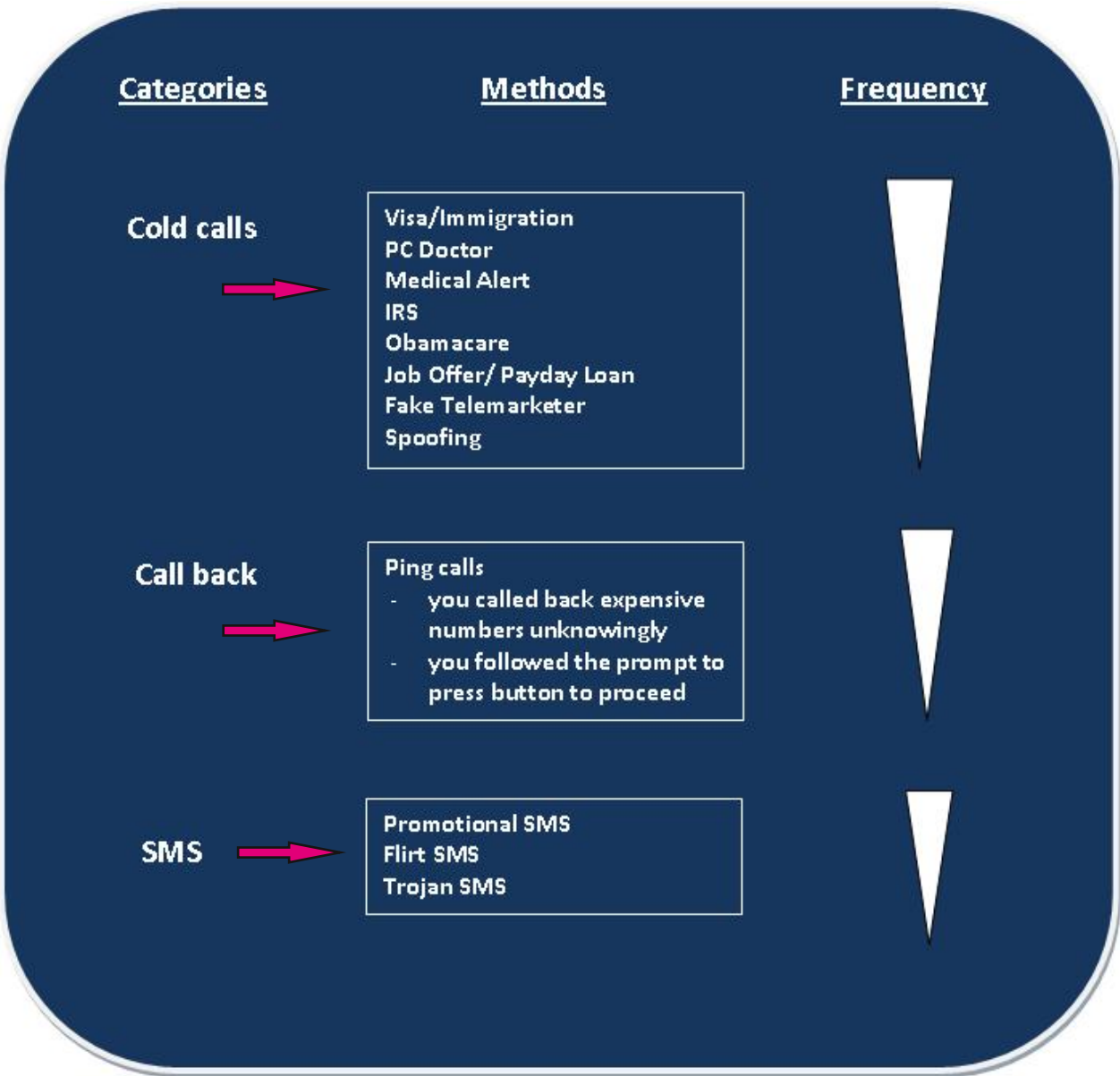
3. What kind of phone scams are out there?

An Overview

The best protection against a scam is to become aware of the method.

The fraud methods on the phone are of different nature. Scammers use ingenious and creative ways to surprise their victims with various tactics. Some old tricks are being updated with new twists and technology. Some are already overused, but never tire to find new targets.

tellows gives you the ten most common phone scam methods in the US as reported in our website. One type of strategy would ask you to pay fees in advance so they can process your visa, health insurance, loan, tax refund, job and training application. Another kind would send out messages that sound like an emergency or would ring your phone incessantly just to make you call them back. While the last type would pretend to be calling from a valid number, or would use the name of a legit company and brand, as if offering their products and services. All these are just baits so they can leach your purse out and account information.



3. What kind of phone scams are out there?

Scam using Obamacare

The complexity behind the newly approved Affordable Care Act brought a lot of confusion among Americans, which in turn, opened a lot of doors to scammers and fraudsters as a way to fool citizens into sharing their personal information, and stealing their money.

Scammers would:

- Claim that they are connected with federal government
- Inform the target victim that he needs a new insurance card for the Obamacare
- Ask for personal information like bank account number, credit card number, social security, medicare ID
- Charge fees as high as \$100 to help people understand the new policies
- Target older people, or those above 65 years old, by falsely claiming that they need to buy a supplemental coverage



Reports in tellows:

(Lis): *I don't know how to place this number, but I just received a call from it and a pre-recorded message said that they were from America's Next Generation and then they went on to talk about Obamacare. I don't know exactly what their agenda is, but I didn't wait to figure it out. After a minute or so I hung up because whatever they were trying to sell me (literally or metaphorically) I wasn't going to buy!*

(Lois): *Recently received a call from this number. It was a political call, although I'm not quite sure what kind of political movement or group they belong to. An automated message identified the caller as America's Next Generation (even though I never heard of the group nor am I aware of what I ever did to "deserve" these kind of calls). They just kept talking about Obama care.*



- Tips:
- never pay upfront fees. Real advisers provide information about the ACA (Affordable Care Act) for free.
 - never click any links provided in e-mails. Even if it appears to be a legitimate link from a trustworthy source, type in the URL yourself.
 - be suspicious of anyone claiming to represent the government. Government agencies typically communicate only by mail.
 - go to www.healthcare.gov. It's the official shopping place for qualified health plans.
 - report scams or suspicious activity. You can file a complaint with the Federal Trade Commission at www.ftc.gov/complaint or call 1-877-FTC-HELP.
 - if you think your identity has been stolen, visit www.ftc.gov/idtheft or call 1-877-ID-THEFT.

3. What kind of phone scams are out there?

Visa/Immigration Scam

Scammers would claim they are connected with the United States Citizenship and Immigration Services (USCIS), “spoof” the victim’s telephone Caller ID system to display that the call originated from USCIS, ask for the social security and passport numbers, dates of birth, etc., and scare the victim by saying that there are some problems in their immigration records. The perpetrator would then convince the victim to pay a certain fee to process his records and threaten them with deportation or application/petition denial if the victim refuses to pay.

Those applying for visas, green cards and employment authorization are also being scammed by "businesses" promising faster and a more sure way of getting applications approved. Scammers also use fake websites offering step by step guidance on completing a USCIS application or petition that claim to be affiliated with USCIS. Others even ask for payment to download forms, instructions or other information.



Reports in tellows:

- (iceman): *they called me up also in asked my credit card no. for legal fee for immigration lawyer, and they talk very fast and persistent. i give them my old credit card no. anyway thank you for knowing it...*
- (bai): *I got a call from this number saying she is processing a visa. she is asking for any debit card or credit card last 4 digit number in order to open the application.*
- (Irish Hazel): *after clicking that website, 10 minutes ago I receive a phone call from this no. and asking me if I am serious in applying for Canadian Immigration, firstly she asked about my job, etc. and after that she congratulate me for I am qualified for Visa in Canada, and then finally she ask my last digit of my credit card number. Like the hell? why should I give her my card no. by that time I knew it's a scam. SO PLEASE BE CAREFUL*



- Tips:
- seek assistance from the National Visa Center through (603) 334-0700.
 - applying directly with USCIS can give you the same result without extra charges and fees. Trust only the official website of USCIS with free downloadable documents.
 - report such scams to the Federal Trade Commission at www.ftccomplaintassistant.gov and your appropriate state authorities.

3. What kind of phone scams are out there?

Fake debt collector Scam

“This is the Civil Investigations Unit. We are contacting you in regards to a complaint being filed against you, pursuant to claim and affidavit number D00D-2932, where you have been named a respondent in a court action and must appear... You or your attorney will have 24 to 48 hours to oppose this matter... Call xxx-xxx”.

The message sounds official, only that it is a bluff from a fake debt collector. These scammers use fictitious names that imply they are affiliated with a law firm. They threaten that if you don't pay, you could be sued, arrested at work, or forced to appear in court. The end goal is for you to pay them through a bank transfer as soon as possible.



Reports in tellows:

- (Evelyn): *They threaten me if I don't make a payment 1200 within 10 min, they will send sheriff out and arrest me right away .I was so scared don't know what to do. Because I had no money at all .I just let it it be .Now I realized this is America. I wish F.b.I or police will to something about this.p.s they also call me with the sheriff tel ID # showing*
- (Tadd): *Told me that if I don't paid they will send sheriff out and arrested me for 7 years prison. I almost got trap,and very scare panic . Don't know what to do . Luckily my lawyer said just hang up their phone and call police .They said. It's totally a scam.I felt much better.I hope someone out there will do something about this scam . Otherwise more victims will fall into their trap*
- (Joyce): *Phone rang. Picked up. No answer. Called number back. Phone rang for quite some time. Hung up and retried. Waited several minutes until someone finally picked up. Asked for someone who used our number. Said our number would be removed. We will see. Asked where they were calling from. First response was “Midland Credit Management.” Repeated, “Where are you calling from?” Response, “From one of our offices in India.” “India?” I asked. Response, “Yes.”*



- Tips:
- ask the debt collector to provide official “validation notice” of the debt, i.e., in writing. The notice must include the amount of the debt, the name of the creditor and a statement of your rights under the Fair Debt Collection Practices Act.
 - ask for the caller's name, company, street address, and telephone number. Then, do some research to know if the collection agency is real.
 - do not provide or confirm any bank account, credit card or other personal information over the phone until you have verified the call.
 - check your credit report by going to www.annualcreditreport.com or calling (877) 322-8228 to know if you have outstanding debts or if there has been suspicious activity under your name.
 - file a complaint with the Federal Trade Commission if the caller uses threats. The Fair Debt Collection Practices Act prohibits debt collections from being abusive, unfair or deceptive.

3. What kind of phone scams are out there?

Caribbean Numbers

The scam starts by calling anyone, usually during late hours, so one would think that it is an emergency and would then make a return call. Unfortunately, it is often just a recording generated by a computer system with the purpose of making the victim stay on hold for a longer time. Apparently, it is coming from a "pay-per-call" line (similar to area code 900 numbers in the US) that charges high fees including international rates.

This scam has been going on since the 90's and because it is not a US-based number, it is not under US regulations. It would be difficult for those people who were scammed to get assistance and ask for a credit or refund from its local phone carriers since for one, they did make the call, and second, it is already another foreign company in the Caribbean that they should be dealing with.

The pay-per-call scammer, unlike the 900 number in the US, also does not inform the caller about charges and rates, nor provide a time limit during which the call can be terminated without being charged.

Reports in tellows:

- (Pimmelkowski): *didn't manage to get on the phone in time. No wonder when they call me in the middle of the night.
I did some internet research on this and they don't want you to answer the phone.
They want you to call them back so they'll earn money.*
- (Danglt): *Seems to be a ping call from grenada. Even without any fees for a service number the reaming fee will be high enough to cost you some dollars*
- (Dave Mindstrange): *decided to call them back, immediately someone answered on the other end and sounded like they were having hardcore sex. Then decided to call it from my land line, the number then states it is disconnected. Go figure, every time I call back it starts the sex over.*
- (reamimi): *That number rang at 2:00 a.m. didn't managed to get out of bed in time so I don't know who it was. I read on google it's an old lady with technomusic in the background though(???)*
- (bibiblocksberg): *Caller from tha caribbean islands. Don't call them back! They will charge a fortune on you just for dialing that number*
- (mont): *calling at 2 in the morning?? seriously?? i wont call back as ive heard about this scam!!! you cant fool me guys!*



Tips: - if your telephone does not employ a call blocker, the least thing you should take into consideration is filing a complaint with the NANPA (the organization that holds responsibility for the whole North American Numbering Plan which includes Grenada). More information on how to file a complaint with NANPA can be found here: http://www.nanpa.com/complaint_process/index.html

3. What kind of phone scams are out there?

Spoofing Verizon Wireless

- 1) You'll receive a call from someone claiming to be from Verizon.
- 2) The automated voice will inform you that you are owed an obscure amount of money (usually amounting to a couple of hundred dollars) as a bill rebate and instruct you to log in at www.vzw***.com (** being the 3-digit figure you're supposedly owed) to collect it.
- 3) You go online and type in the web address provided, which will look, incidentally, exactly like Verizon's own site.
- 4) You tap in your log-in credentials, hit Enter, and now the scammers have your vital account details.



Reports in tellows:

(Duh): *They have called me several times telling me I have a \$331 credit to my account. Only problem is, I don't have a Verizon account. Maybe they will just send me the cash. Should be close to 10 grand by now.*



Tips: - if you feel your account is being threatened by any type of fraud or similar abuse, send Verizon an email at abuse@verizon.com

IRS Scam



The scheme: scammer uses the Internal Revenue Service's caller ID to make threatening calls demanding that their victims pay their 'overdue tax'. The caller will casually request that the tax be paid via debit card or a wire transfer, both methods conspicuous by their untraceability.

Not only are they calling from what appears to be the IRS's number (spoofed), they also know the last 4 digits of your social security number and make it sound valid by providing staff names, badge numbers and emails with the IRS logo and format.

Reports in tellows:

(Dumbo): *A man with a thick accent said his name barely audible and claimed to be from the IRS and said that this call was regarding some debt I allegedly had. He got very rude and threatened to freeze my accounts and credit cards. The thing is, I don't have any debt and I'm VERY sure of it. So I told him not to call anymore and, still hearing his protests through the phone, I just hung up.*



Tips: - call the IRS directly on 800-829-1040.
- or go to the official IRS 'scam-alert' web page

3. What kind of phone scams are out there?

Medical Alert Scam

Often living at home alone, senior citizens may feel isolated or vulnerable; so when a scammer comes calling from 'Senior Safety Alert' with an offer of a cheap in-house alarm system for break-ins or medical emergencies, they will probably jump at the chance.

The call starts with a recording offering the deal: a system worth hundreds of dollars, fitted for you, on a \$30 per month contract. The potential victim will then need to press a number to indicate their interest and will be transferred to a 'customer advisor', who will take their credit card numbers and personal information.

Other warning signs include a refusal to disclose any details about the company (e.g. address) or an unwillingness to provide any authentication documents.

Report in tellows:

(vanity-affair): *I'm not a senior but the calls are still annoying. I'm not interested in buying something over the phone.*



Tips: - don't make any transactions over the phone, no matter how good the deal is
- be wary of requests to call them back even if they claim it is for you to check their authenticity (they could keep your phone line open by not hanging up)

Job Offer Scam

This scheme takes advantage of the situation of people on low incomes, such as students, the unemployed, or those on benefits. Usually they offer paid training programs with the promise of a job in the end.

You receive an email from Wilfred Adams (this name was a favourite of theirs) from Ghana Gold Corporation with a job offer, which seems to fit you perfectly and also happens to pay pretty nicely. (It's always an email, never a call or a letter). Although you may initially have some doubts, they'll provide you with ample information on their projects, give you access to their webpage (<http://ghgoldcorp.com/projects.html>) and provide their contact information.

However, the catch will inevitably become visible when formalities are discussed; the job is, after all, in Ghana and there will be a fair few administrative points to consider.

(john): *when you come to the "formalities" of the job offer they start asking for money, like for the courier services, medical clearances and custo clearances and so on. They never really answer your questions and the offer comes out of the blue, without any calls. You would believe that a big company like that doesn't make you pay for something like courier services but this is the first hint.*



Tips: - check the legitimacy of the company first
- don't divulge any confidential information such as your bank account, credit card or Social Security numbers.

3. What kind of phone scams are out there?

Social Network Scam

Often using a rather common name like Amanda, Ashley, Jennifer, Jessica, Lisa or Nicole, the scammer contacts people on Facebook with a friend request, sometimes even sharing a mutual facebook “friend”.

Once added, the person contacts you again, often asking some random questions or engaging in a little small talk before ending the conversation quickly with the excuse that they supposedly have to log off of facebook and stating that the other person should text or call at a certain number.



Scammer would want you to call for various reasons:

- to get your number
- to verify your number (to be used or sold to call centers, telemarketers etc.)
- to charge you for the call
- to forward your call to another number

Reports in tellows:

(Gary): *This actually didn't just happen to me but some friends of mine as well. A Jennifer/Lisa/Ashley/Amanda or what have you tries to befriend you, sending a friend request, then striking up a conversation only to quickly log off again, asking you to call "her" at number xy. This is not the only number they try to get you to call or text to, but it's all I've got so far. I guess that really teaches you a lesson about "befriending" strangers on facebook.*

(Stan W.): *[...] It seemed odd to me – who gives out their number to strangers like that? [...] I just wonder what they are trying to accomplish by it?*

(Peter): *[...]I don't know how it works and what they have to gain from this, but do not under any circumstance respond to their requests!*



- Tips:
- if you have been contacted by a stranger asking you to call an unknown number – especially without giving you a very good and plausible reason why, it is perhaps the most sensible thing not to react and to rather be safe than sorry.
 - be wary when a message on your Wall contains short links from friends who don't usually post links on your Wall. This also is another form of the message being "out of character" for your Facebook friend.
 - look in your Facebook news feed. If you are suddenly seeing this message appear multiple times, it could a scam that is being sent through automated means.

3. What kind of phone scams are out there?

PC Doctor

In most instances, the scammer posed as a representative of Microsoft or Windows Microsoft, claiming that the computer of the person has been infected with malware causing the operating browser or computer to send a critical error message to the supposed tech support of the corporation. The goal, to gain access to the computer and subsequently other sensitive personal information about its owner or users, is achieved by instructing the target to change current computer settings or to download rogue security software to leave the computer vulnerable.

In some cases, they also attempt to charge a fee for supposedly fixing your computer



Reports in tellows:

(Mr. Swanson): *Total scam! The caller said he was calling from "Microsoft" and that it had come to their attention that my computer had been infected with a dangerous virus. Of course, they had the solution for my "problem" and, yes, while it might cost nearly \$300, it would be a good investment and apparently really the only way to save my computer. I figured I humored them long enough, said they should go to hell and hung up. So if you're not in the mood for playing with some scammers, don't pick up!*



- Tips:
- if you have already given away information and think you might be a victim of scammers, change the password on your computer as well as for other user accounts they may try to access such as email account, bank or credit card account.
 - run a trustworthy and reliable scan program on your computer – Microsoft recommends the Microsoft Safety Scanner.

General Tips

The diversity of the listed methods of fraud has no end. Scammers are always on the look out for new ventures and would seize any opportunity that presents itself. You should always be one step ahead and remember to think twice before you put yourself into the trap. Always ask questions to confirm the validity of the call.



- Tips:
- Never give out contact details or financial information to strangers or to businesses that should already know your details
 - Never send money to someone you don't know
 - Check bank and credit card statements regularly and let your bank know immediately if there are any entries you don't recognise

The National Do-Not-Call Registry

The National do-not-call Registry was created by the Federal Trade Commission (FTC) in 2003, in conjunction with the Federal Communications Commission (FCC), allowing consumers to place their telephone numbers in a central DNC registry to prevent sales solicitation calls from telemarketers. The following exceptions are allowed:

- Customers may be called for up to eighteen months after a customer’s purchase, rental, or lease of the seller’s goods or services or any other financial transaction between the customer and seller. For a magazine publisher, this exemption runs for 18 months from the delivery of the last magazine issue;
- Consumers may be called for up to three months after the consumer contacts the seller with an inquiry; and,
- Consumers may be called if they have given written consent to receive telemarketing calls.

Telemarketers are supposed to check the list at least every 31 days for numbers they can't call.



Company-specific DNC lists

In addition to complying with the National DNC list, companies must establish and maintain company-specific DNC lists and must not call consumers on this list, even during the 3 and 18 month exception periods described above. Publishers must also ensure compliance with the company-specific DNC list by telemarketing agents working on their behalf.

FCC Online Complaint regarding:	www.fcc.gov/complaints
Telemarketing, pre-recorded messages, Caller ID Spoofing, and Do-Not-Call	
FTC Online Complaint regarding:	www.ftc.gov/complaint
Identity theft	Sweepstakes, lotteries, and prizes
National Do Not Call Registry violations	Business opportunities and work-at-home schemes
Computers, the internet and online privacy	Health and weight loss products
Telemarketing scams	Debt collection, credit reports, and financial matters
Credit scams	
Immigration services	

The Telemarketing Sales Rules

The federal response to increased telemarketing has been to regulate commercial callers in order to protect privacy. Noncommercial callers, however, such as charities and political groups, have been consistently exempted.

Here are the highlights of the 2003 Telemarketing Sales Rules.

- 1. Telemarketers are required to give his or her name, company, telephone number or address where he or she can be contacted. You should expect these details on the initial part of the call.
- 2. No phone solicitation/ telemarketing is allowed before 8 am or after 9 pm.
- 3. As soon as you ask the telemarketer to include you in the do-not-call list, they should comply and you shouldn't be receiving any more calls from them. At least for the next 5 years.
- 4. The telemarketer must honor your do-not-call request for five years and you must repeat your request once you get the same call after the period.
- 5. The national DNC only applies for home voice or personal wireless phone numbers, and does not make telephone solicitations unlawful when it comes to a business number, although the latter can still register under the national DNC.
- 6. Check if your state also has its state do-not-call lists.
- 7. You will definitely receive a call from an entity if you have made an inquiry, application, purchase or transaction regarding their products or service. This is already called an established business relationship (EBR). They should stop calling though as soon as you requested for it.
- 8. Autodialers and any prerecorded voice messages must not be used to contact number assigned to any emergency telephone line.
- 9. Autodialers should provide a phone number (which should not be a 900 number or any number with charges) which you can call to ask that the entity no longer call you.
- 10. If you have a caller ID, a telemarketer should display its phone number, the name of the company, and/or another phone number for a call back.

Differences between the National do-not-call register and the TPS

USA DNC

- Consumers must renew their registration every 5 years.
- Even if a consumer puts their number on the National do-not-call Registry, a company may call them for up to 18 months after their last purchase or delivery from it unless they ask the company not to call again.

UK TPS

- Numbers remain on the register indefinitely or until the phone number is re-allocated.
- If a consumer is registered with the TPS then a company must be able to show that they have a clear opt-in before they can call.

5. How can I protect myself?

tellows helps!

With www.tellows.com, we have created a platform that helps to better classify unknown phone numbers, as well as unwanted calls. It is a community where members help each other by sharing their experiences about nuisance telephone and mobile numbers. Unlike a phone book reverse lookup, the website contains more information on the caller. In addition to testimonials, a tellows score is also provided, 7 to 9 being the most annoying and untrustworthy ratings. You can also find information on the latest scam methods and ways on how you can protect yourself against unwanted callers through the tellows blog and www.facebook.com/tellows that contains the most current and interesting contributions regarding telephone fraud and related topics.



With 150,000 site visits each day and over 80,000 phone numbers on its database, tellows offers consumers a perfect platform to bring down annoying callers, spammers and scammers. Let's hear it from the tellows users:

(Petra): *As a mother, this website is very helpful in protecting my family from scammers.*

(Rob): *It's nice to have discovered this website. It saved me from calling back a potential fraudster!*

(kol21): *tellows blog is always up-to-date, very professional and reliable.*

(hizzy): *Good job tellows. It's a good complement for the DNC.*

(Paul): *The actual reports from this site submitted by target victims really helped me a lot.*



tellows Score

tellows aims to provide a free platform to all those who are looking for information on unknown callers. To achieve this, the focus rests on the special feature called the tellows Score. Thanks to the tellows Score, you are now able to spot the trustworthiness of the calling number at the first ring of your phone.

Reliable phone numbers are represented by scores less than 5 and highlighted in green, whereas dubious numbers are those greater than 5 up to 9 highlighted in red. Hence, the more dubious the number is, the higher is the rating.

Interesting fact: tellows is available in over 50 countries and is used by millions to rate incoming calls!



Positive
score

This is a trustworthy caller. Most people rated this number positively.



Neutral
score

Either this number is still unknown to tellows or there are not enough information available to categorize the caller adequately. However, there is the chance that both negative as well positive comments balance each other.



Dubious
score

Attention! The majority of tellows users rated this number untrustworthy. Please make sure to deal with this caller cautiously.

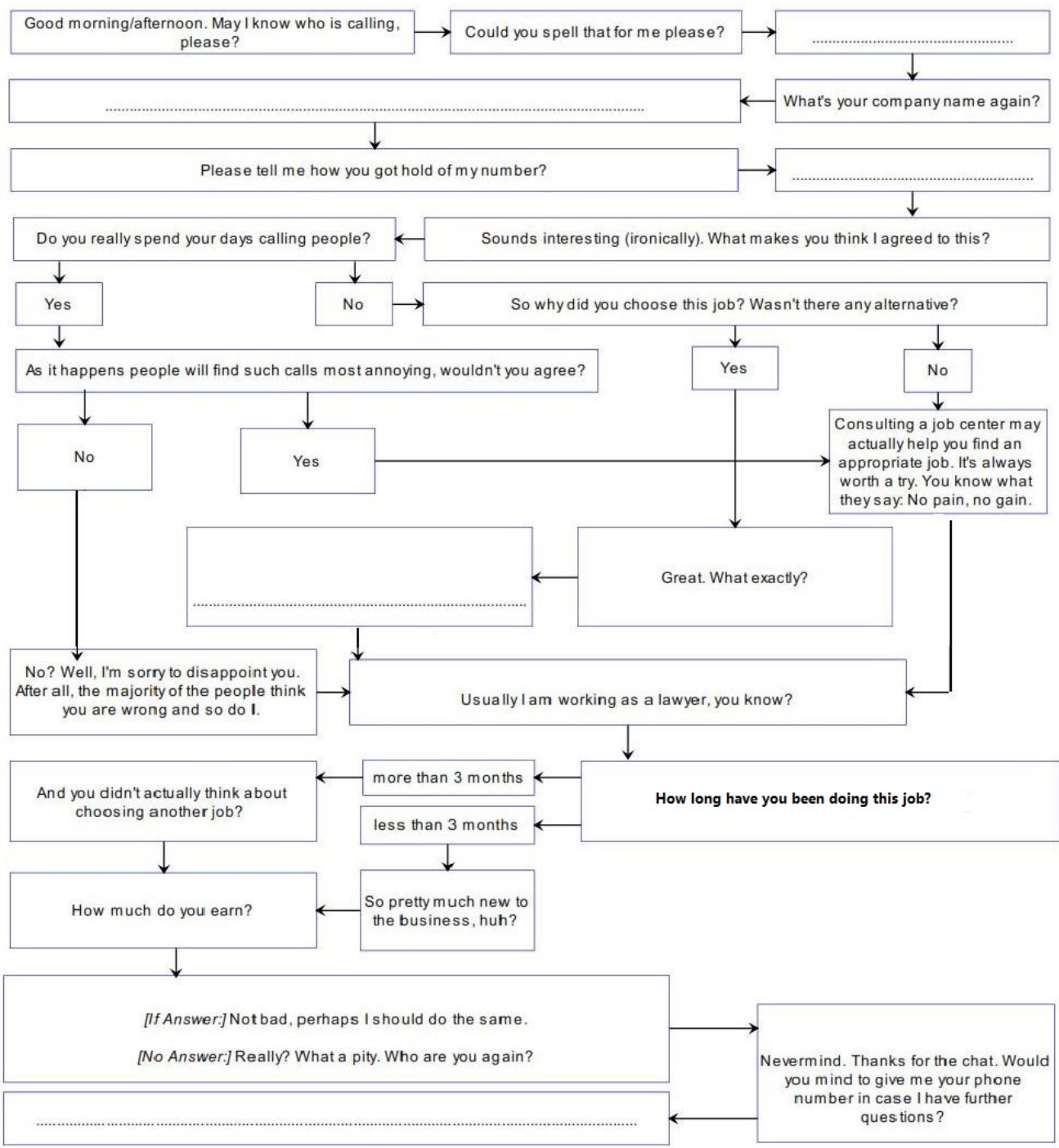
tellows Call Guideline

Everyone who has already been called by telemarketers knows how annoying such a call can be. Their only objective is to sell their products. They achieve this by asking cleverly formulated questions, or by following a script usually supplied by a software.

By using the tellows Call Guideline, you are well prepared for those nuisance calls. With these questions you turn the tables around and give the call center agents a hard time. In addition to the questions, there are also blank spaces for you to write down the caller's answers. Print the guideline and use it as a support whenever you receive unsolicited calls.

5. How can I protect myself?

Call guideline for annoying telemarketing calls and phone surveys



Please send the completed guideline to: kontakt@tellows.de

5. How can I protect myself?

The tellows App for Android und iPhone a caller id for your Smartphone

With the tellows app, you can now identify unknown callers!

The app will tell you real-time if the call is trustworthy or not. On the first ring of your phone, the tellows Score will automatically appear in order to help you decide whether to answer the phone or cancel it – 7 to 9 being the most untrustworthy numbers. The app also allows you to read the comments of users about this number. Post your own complaints through this app so you can also warn others. The service is completely free of charge.



Features of the App:

- Classification of incoming calls using the tellows scores
- Import function of address and name of unknown numbers in the contact list
- Comment function
- Direct search of unknown numbers
- Call log of incoming calls
- Lists more than 80,000 dubious telephone numbers
- Uses over 1 million information about individual phone numbers
- Real-time spam warnings

iPhone

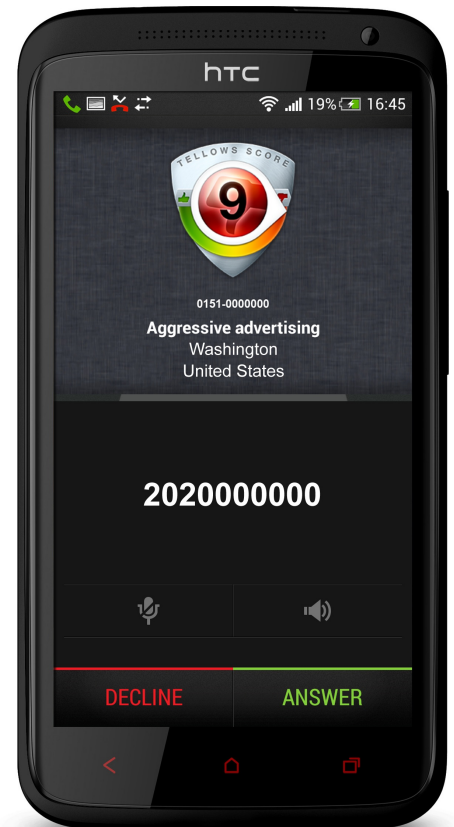


(Martin):
„This app really helped me filter unwanted calls! I was already scammed, and i cant let them fool me again“

(Max):
„Very helpful app, and it's free!“

(Peter):
„You'll never know when the scammer would attack, so better be safe than sorry. This app is very useful for these kinds of situations.“

Android



More questions?

The entire tellows team hopes that the magazine will help as many consumers as possible in the fight against telephone terror. Of course a nuisance on the phone can never fully be prevented, but the knowledge about scams and legal protection are good starting points to defend yourselves adequately. If you still have questions or you want to express your opinion, please contact us through any of the the following:



Do you have comments about the magazine? Any opinion on the subjects presented? Then write to us!

kontakt@tellows.de

Your feedback is appreciated and helps to more effectively combat telephone scams.



Experienced the same telephone harassment? Or were you wise enough to outwit the scammers on the phone? How about a new fraud method you know of? Then register the phone number with us!

www.tellows.com

This way, you get to warn other people and maybe even help others know how to deal with the situation.



Would you like to remain up-to-date and be informed of legislative changes or new fraud methods? Then visit our blog or our Facebook page!

www.facebook.com/tellows

blog.tellows.com

Get news and participate in discussions about dubious numbers or current topics.

Important Addresses

Federal Communications
Commission
Consumer and Governmental
Affairs Bureau
Consumer Inquiries and
Complaints Division
445 12th Street, SW
Washington, DC 20554
Tel.: 1-888-CALL-FCC
Website: www.fcc.gov

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
Website:
www.ftccomplaintassistant.gov

National Do Not Call
Registry
Attn: DNC Program Manager
Federal Trade Commission
600 Pennsylvania Avenue,
N.W.
Washington, DC 20580
Tel: 1-888-382-1222
Website: www.donotcall.gov

Imprint

tellows Magazine is a Project of
tellows UG
Eschenring 6
D-04828 Bennewitz,
Germany

1st Edition, 2014

Note

Despite careful content-wise control, mistakes cannot be ruled out.
Thus, a guarantee of actuality, accuracy and comprehensiveness cannot be applied.

Photos

Title: ©iStockphoto.com/delihayat
Page 7, Phone number: ©iStockphoto.com/vuifah
Page 7, Phone handset: ©iStockphoto.com/asbe
Page 10, Dice: ©iStockphoto.com/RaminKhojasteh
Page 11, Newspaper: ©iStockphoto.com/koun
Page 12, Job Offer: ©iStockphoto.com/Bet_Noire
Page 14, Key: ©iStockphoto.com/RaminKhojasteh
Page 14, Paragraph: ©iStockphoto.com/froxx
Page 16, Dollar sign: ©iStockphoto.com/Kuklev
Page 17, SMS: ©iStockphoto.com/fractalgr
Page 18, Phone: ©iStockphoto.com/ZU_09
Page 24, Check sign: ©iStockphoto.com/ISerg