calleridspoofing.info

The definitive resource on Caller ID spoofing

What is Caller ID Spoofing?

Caller ID Spoofing: Changing the Caller ID to show any desired number on a recipients Caller ID display.

The Real History of Caller ID Spoofing

The Early Days

Many people do not realize that Caller ID spoofing has been around since Caller ID was created. For over a decade Caller ID spoofing was used mainly by businesses with access to expensive PRI (Primary Rate Interface) telephone lines provided by local telephone carriers. A single PRI line can provided businesses with up to 23 telephone lines and all of these lines are capable of having unique telephone numbers. Caller ID spoofing, in it's most basic form, was typically used by businesses to display one main telephone number on all outgoing calls, even though those calls were not really originating from those numbers.

Around the late 90's and early 2000's Private Investigators took notice of Caller ID spoofing in it's most basic form and began purchasing these expensive PRI lines with the intent of selling access to other Private Investigators for a fee. These services were typically referred to as "blind lines" at that time. Private Investigators, concerned with their anonymity, would regularly use these blind line services to guarantee that their real telephone number would not be shown to the called party. Private Investigators knew first hand that Caller ID was not 100% blockable, and that toll free 800 numbers would typically be able to see their real Caller ID number, even if *67 (Caller ID Blocking) was used. Some of the providers that offered a blind line service were: US Tracers, Skip Tracey, Universal Communications, and IISNet. The services provided by these companies were marketed very discretely and only people with the P.I. industry typically knew about these services.

In the early 2000's phone hackers, also known as "phone phreaks" or "phreaks", began using Orange boxing to attempt to spoof Caller ID. Orange boxing is done by using a device, usually special computer software, to send a series of tones down the line during the first few seconds of a phone call, attempting to emulate the Caller ID signal sent from the telephone office. Orange boxing is very crude and unreliable, as it has to be done within a short timeframe at the beginning of a call. Phone phreaks, without access to PRI lines or blind line services at the time, thought the technique was clever.

2003-2004

In late 2003 and early 2004 the same phone phreaks began to explore a relatively new platform for developing voice applications, known as VoiceXML or VXML, which was offered by companies such as Voxeo. VoiceXML offers interactive voice applications, which are programmed in a similar fashion to HTML web sites. VoiceXML applications can easily be created to mimic functions of a normal PBX and typically these VXML providers are connected to PRI lines. Word began to spread around the phreaking underground that someone had created a VoiceXML application using Voxeo that let you change your Caller ID number. The Caller ID spoofing application worked, however it was somewhat crude, as the spoofed number had to be entered into the applications code and then re-uploaded to the VXML server before each use. Within a few days, phone phreaks figured out how to program these applications to allow you to enter the numbers you wanted to spoof over the phone, allowing you to fake your Caller ID on the fly, and began sharing the code on the Internet for others to use. To this day it's still possible to spoof Caller ID with various VXML services, however people seemed to have found it easier to use other services and methods.

At the same time that people were discovering VoiceXML, VoIP (Voice Over IP) telephony started to become popular with savvy phone and Internet users and phone phreaks took notice very quickly. In 2003, phone phreak Lucky225 discovered a flaw with the VoIP provider Vonage that allowed users to send a fake Caller ID number by initiating a request to port your existing number to Vonage, but giving them any valid telephone number that you wanted to show as your Caller ID. At the same time, other phone phreaks began to use a new open source PBX software application, named Asterisk, to manipulate their Caller ID number. Phone phreaks and software developers figured out that Asterisk allowed users to set their Caller ID within the application and then pass the spoofed Caller ID number to their outbound VoIP provider or telco, in the same fashion that businesses had been setting their Caller ID with PRI lines for over a decade.

In August 2004 an entrepreneur named Jason Jepson announced that he would be launching and actively marketing a new Caller ID spoofing service for Private Investigators and Law Enforcement, using VoIP and Asterisk, named Star38. On September 1st, 2004 Star38.com officially launched and gained attention from mainstream media around the world after USA Today published a front-page article in its paper about the service. For the next few days Star38 was featured in newspapers and web sites around the world.

A week later, Jason Jepson announced that he would be selling Star38, as he claims to have been receiving death threats by hackers and phone phreaks. Many who have met Mr. Jepson since then claim that he made this story up to get even more attention and never really ended up selling Star38.

On October 27, 2004 Kevin Poulsen of SecurityFocus.com reported on Camophone launching the first public Caller ID spoofing site. While Star38 gained mass mainstream

attention, it still only catered to Private Investigators and Law Enforcement officials. Camophone.com stepped in and was the first service to offer its service to anyone who was willing to purchase a prepaid calling card from its site. That same day, Telespoof launched its Caller ID spoofing service to compete with Star38. At the times of launch, Camophone.com only offered Caller ID spoofing by utilizing a web site callback interface, which Star38 also offered, however Telespoof.com offered service by using a toll free 800 number. Before the end of 2004, another Caller ID spoofing site named CovertCall would launch at CovertCall.com with both a web interface and toll free access. Both Camophone and CovertCall's websites were very basic, with nothing more than a few lines of text and a login section.

2005

In 2005 a handful of new sites allowing you to spoof your Caller ID were quietly launched. Some of the sites were PiPhone.com, CallNotes.net, SecretCalls.net, StayUnknown.com, SpoofTech.com, SpoofTel.com, and SpoofCard.com. During the same time Covertcall and then Camophone shut down, after they were hacked and their users information was traded around the Internet. Camophone even posted a note on their site that they were for sale, however no one seemed interested in buying the company. By the end of 2005, PiPhone closed down and even Star38, the company that started the mass marketing of Caller ID spoofing, closed down. During this time SpoofCard emerged as the dominant Caller ID spoofing provider with the most mass appeal. SpoofCard also was the first service to offer free call recording and a voice changer that allowed users to sound like a man or a woman, making it even more appealing to the public.

2006

Everything seemed to be going smoothly for the Caller ID spoofing industry, but then in late February 2006, SpoofCard and Telespoof both received letters from the FCC notifying them of investigations into their services. It is believed other Caller ID spoofing services received the same letter from the FCC in the first round of the FCC's investigations. However, SpoofTel, SpoofCom, and SpoofTech was able to dismiss the investigations as it is headquartered in Canada. Shortly after the FCC's letters, the Florida Attorney General began their own investigation into SpoofCard, SpoofTel, SpoofTech, SpoofCom and TrickTel.com. Not a lot of information was released about the Florida Attorney Generals investigation and exactly what they were interested in finding out.

Later in 2006, Caller ID spoofing became a target within the House of Representatives and the Senate, with several bills popping up attempting to stop Caller ID spoofing from being used for fraudulent purposes. As of this time, none of these bills have actually been passed and a few of them seem to have just disappeared.

On August 22nd 2006, Caller ID spoofing once again gained the attention of the mainstream media as SpoofCard announced it had canceled an account belonging to Paris Hilton which was being used to harass Lindsay Lohan, and to help break into her voicemail.

Word of the FCC's probe into Caller ID spoofing seemed to slow down the launch of new services for the majority of 2006, but late in the year CIDSpoof.com, CovertCard.com and Itellas.com all quietly launched their own Caller ID spoofing services. By this time SpoofCard had already firmly cemented its position as the largest and most feature packed Caller ID spoofing provider, so the launch of these new sites did not shake up the Caller ID spoofing industry much.

2007

As spoofing seems to be getting closer and closer to being regulated by the US government, the Caller ID spoofing industry seems to have slowed down and the only new site that has appeared in 2007 was SpoofEm.com, a white-label version of SpoofTel.com. In later April, SecretCalls.net was shut down and the domain name was renewed by someone other than its original owner. The domain is now parked and only displaying advertisements. A few weeks later, a new site called "PhoneGangster" launched it's own Caller ID spoofing service. However the service looks rather amateurish. Towards the end of May, another site, TheZeroGroup.com, launched offering Caller ID spoofing, amongst it's other phone related services. TheZeroGroup's site claims they are hosted off-shore to avoid any legal issues that may arise.

On June 13th the U.S. House of Representatives passed the "Truth in Caller ID Act of 2007" which would make it "unlawful for any person within the United States, in connection with any telecommunications service or VOIP service, to cause any caller identification service to transmit misleading or inaccurate caller identification information with the intent to defraud or cause harm." A similiar bill was passed onto the Senate in April, but the Senate hasn't acted on either of the bills yet.

Around June 19th a new site popped up called Call Condom. Call Condom is run by CDYNE, a company who for some time now has offered developers access to a web based application that allows spoofing. Call Condom claims they spoof ANI unlike, which they also claim no other company does, but we believe that this is just used as a sales pitch, and that they do not even truly understand ANI/BTN.

On June 27th the US Senate's Committee on Commerce, Science, and Transportation passed the "Truth In Caller ID Act of 2007" meaning that the bill will now actually go in front of the Senate for a vote. The bill previously stated that Caller ID may not be spoofed for fraudulent purposes, but now only states that Caller ID may not be spoofed to be intentionally misleading or inaccurate, which is very vague. Is Caller ID spoofing about to be made illegal? This bill would now inadvertently affect millions of businesses across the country.

On July 2nd we noticed a new Caller ID spoofing provider for the first time, called FakeYourID. However, FakeYourID.com's checkout system appears to be down, so we're not sure if the site is live or not. On July 3rd we received an exclusive one-on-one interview with the creator of a commercial Caller ID spoofing service. The complete interview can be found here.

This summer the first Caller ID spoofing company located outside of North America was launched in Germany. VisuKom Deutschland, located in Germany, is now offering what they call a "Call ID spoofing" service. It's unknown at this time if they work across Europe or only in Germany.

In August SpoofCard, followed by Telespoof, began offering free Caller ID spoofing trials on their respective web sites for the first time, allowing users to place free calls up to two minutes in length. In August SpoofCard also launched an affiliate program at Commission Junction, one of the largest global affiliate networks.

In late August a new phoney Caller ID service was spotted at TheSpoofer.com. TheSpoofer appears to be another amateurish attempt to enter the Caller ID spoofing market, with very basic and unprofessional looking website that currently reads "The Spoofer allows you to change what someone sees on their call display when they receive a phone call. With your spoof card make personal and business calls with complete privacy. We currently provide local service spoofing in the 213 and 415 area codes."

In October OfficialSpoofCard.com released an iPhone app for free Caller ID spoofing trial calls. The iPhone application uses SpoofCard's free trial form and turns it into a lightweight AJAX interface for iPhone users. OfficialSpoofCard's Caller ID spoofing iPhone application is located at http://www.officialspoofcard.com/iphone/. A screenshot of the app is on Flickr and can be seen by clicking here.

Just a few weeks later, SpoofCardWidget.com released a downloadable SpoofCard Widget for Mac OS X users, also taking advantage of the free sample calls offer from SpoofCard. This is the first time Caller ID spoofing has been been brought to the desktop computer as a downloadable and installable application. A screenshot of the SpoofCard Widget can be seen by clicking here.

Last Update: October 14th, 2007