Title:
Is There Something Sinister About Caller ID Spoofing?

Word Count:
441

Summary:
Proponents of this technology laud its uses for law enforcement and private investigators. They claim the technology protects agents from being discovered in undercover operations. Agents can freely make pretext calls to criminal elements by using caller ID spoofing. A pretext call is one that allows law enforcement to solicit information over the telephone by representing themselves as someone else.

Keywords:
CLID, CALL ACCOUNTING, TELEMANAGEMENT, CALLER ID, TELEPHONE REPORTING

Article Body:
Spoofing refers to the ability to disguise the originating caller identification number when placing a telephone call. The calling party may select an alias or dummy number to appear on the called party telephone display.

Proponents of this technology laud its uses for law enforcement and private investigators. They claim the technology protects agents from being discovered in undercover operations. Agents can freely make pretext calls to criminal elements by using caller ID spoofing. A pretext call is one that allows law enforcement to solicit information over the telephone by representing themselves as someone else.

Caller ID spoofing is now marketed by a number of websites to any business or individual who wishes to subscribe to the service. Individuals can hide or mask the call origin with whatever number they desire. This guarantees anonymity. Collection agencies or government tax agencies often find it difficult to reach defaulters. This service could help these companies contact an individual using call screening.

Critics of the caller ID spoofing claim that using this VoIP phone service makes it easy for scam artists to make it appear that they are calling from another phone number.

Jokesters could masquerade their caller ID as The Oval Office, Ed McMahon or

Paris Hilton. Hackers and con artists could utilize spoofing to break into unsecured voice mail boxes that rely on caller identification for authentication. For example, Secure Science Corporation discovered that hackers could use caller ID spoofing to break into the voice mailboxes of over 15 million subscribers of wireless service provider T-Mobile. The company scrambled to add an optional pin code authentication to thwart tampering.

Criminal elements could utilize caller ID spoofing to reverse the tables on law enforcement, harass victims and break into interactive voice response systems that use the caller's phone number as authentication. A child molester could contact a home and disguise number as a parent's work number. An alarm company or emergency response dispatch could be contacted and reassured of false alarm by a burglar breaking into a premise.

Methods and kits on how to emulate and display spoofed caller ID messages are now available on the Internet. Anyone with a general understanding of the concept and a compatible modem can construct a device that will provide caller ID spoofing.

In the end, caller ID spoofing, like any other technology does have some merit especially for law enforcement. However this technology is very easy to use unethically and perhaps criminally. The lesson here is don't trust caller id display. If you are unsure of the caller id information of a suspicious caller, take the number down, return the call or alert authorities.