



J.E. CHOSTNER
District Attorney
(719)583-6030

OFFICE OF THE DISTRICT ATTORNEY
TENTH JUDICIAL DISTRICT, COLORADO

STACIE HARRIS
Paralegal II
(719)583-6675

Scam Alert – Spoofing (High Tech Prank Calls)

by Stacie Harris, Economic Crimes Unit

Have you been spoofed? Would you know it if you had been?

You've been receiving phone calls constantly from a telemarketer and the same name and number keeps showing up on your caller ID. You decide you've had enough of them calling at all hours and decide to call the number back. Someone answers the phone and you give them a piece of your mind, only to discover that they have no clue what you're talking about or who you even are. You've been spoofed and the person you just called is just as much a victim as you are.

This really is not a "new" scam. It has been around for a number of years but has gone hi-tech. Caller ID Spoofing is when you receive a telephone call and your caller ID displays a name and phone number, but the caller has manipulated the information displayed and is not actually calling from that number.

With all the technology out there, Caller ID Spoofing seems to get easier everyday. Besides internet telephone equipment being used for this, there are many websites that provide caller ID spoofing services by selling a virtual calling card. The user is given directions on how to create a fake number and name they want to use to show up on your caller ID. Sometimes they don't even take the time to make one up. They just go to the phone book and pick a name at random.

But just when you think you may have started to figure all this out, there's another twist. Along with the technology that some of these websites provide is what is called "voice scrambling". The voice that you hear at the other end of the phone may sound like a male calling you, but it may actually be a female. Makes identifying the caller even more difficult.

Spoofers are also doing what is known as a "Pretext Call". This is when someone poses as an employee of a company to obtain your personal information and/or credit card numbers. The information obtained is then sold and your credit card number could be used to pick up cash transfers that have been ordered.

The Federal Communications Commission (FCC) Enforcement Bureau has been actively pursuing the issue of caller ID spoofing and has been investigating the issue since the summer of 2005, when it was brought to their attention. Although telephone companies can trace these calls to their origins, it is an extremely lengthy process. The calls being made sometimes are routed through several companies before reaching their destination. Some of the companies and websites have agreed to cooperate with the FCC by providing call logs to authorities when subpoenaed. The Enforcement Bureau continues to gather and analyze information about these companies and websites and is coordinating with the Federal Trade Commission and National Emergency Number Association for their assistance.

What does this all mean to you? It means you should be more cautious when doing business over the telephone with someone that has called you. Never give out personal identifying information over the phone. Remember, you are in charge of your own phone and who you talk to and always have the ability to stop the call and hang up.

IDENTIFY A SCAM
~ BEFORE A SCAM IDENTIFIES YOU! ~