CNET News: FAQ on vishing

What is vishing?
The term "vishing" is a socially engineered technique for stealing information or money from consumers using the telephone network. The term comes from combining "voice" with "phishing," which are online scams that get people to give up personal information.

How does it work?
Typically attackers use a technique called caller ID spoofing to make it look like calls are coming from a legitimate or known phone number. It's a very similar technique to email spoofing, which makes e-mail addresses look like they are coming from a trusted source. But because people typically trust the phone service and caller ID, spoofing phone numbers can be particularly damaging.

And just like with online phishing attacks, which direct consumers to phony Web sites, vishing attacks usually have a recorded message that tells users to call a toll-free number. The caller is then typically asked to punch in a credit card number or other personal information. In the case of the warranty scams, users are asked to buy a bogus extended warranty for their car, which can cost anywhere between $2,000 and $3,000.

How easy is it to spoof a phone number?
With voice over IP phone technology, caller ID spoofing is very easy to do. The traditional phone network works by connecting one circuit to another. Each circuit on either end of the call is assigned a phone number by the phone company. So changing the phone number of a caller was more difficult. Of course, there were people who had figured out ways to hack into the old phone network to do this, but it wasn't as easy as it is today with voice over IP technology. With VoIP services, there is no circuit. These services use the Internet, which assigns different devices on the network IP addresses instead of actual phone numbers. Phone numbers are actually assigned by the users themselves.

There are several companies offering commercial spoofing services, such as SpoofCard. And even VoIP services, such as Skype, allow people to pick an area code and even the prefix number they want when they set up a new phone number. These numbers can be used to disguise where calls originate. Of course, Skype is built for individual use, but other services like Flowroute provide VoIP services for businesses using PBXs. A PBX, or private branch exchange system, makes connections among the internal telephones of a private organization, such as a business, and it also connects them to the public switched telephone network (PSTN). These services allow companies to pick any phone number for caller ID they want. And some telemarketers use the service to spoof telephone numbers.

The practice of caller ID spoofing is so widespread and common that one of the telemarketers accused in the FTC lawsuit supposedly bragged to a prospective client that he could call the entire United States in just a few hours and would not get caught calling people on the Do Not Call List.

Is caller ID spoofing illegal?
No it's not. But there is proposed legislation that could make manipulating a phone number to look like it's coming from someone else illegal.

Are there legitimate uses for caller ID spoofing?
Yes, there are some legitimate uses for spoofing. Voice over IP providers by definition must use spoofing, or some kind of number manipulation, to create phone numbers. But there are other legitimate uses. For example, doctors who might want to call back patients from their home may use spoofing to conceal their their home numbers. Some online dating services use spoofing to let people talk to potential matches without revealing their real phone numbers. And some lawyers involved in domestic violence cases may use caller ID spoofing to protect the whereabouts of abused clients.

Even though there are some legitimate uses for caller ID spoofing, Lance James, co-founder of Secure Science, which specializes in fraud protection, says 75 percent of all caller ID spoofing is likely for illegitimate purposes. Still, he believes that any new laws written that make caller ID spoofing illegal, should distinguish between people using spoofing for legitimate purposes and those looking to harm or scam people out of money.

Who typically uses caller ID spoofing and vishing scams?
Most of the vishing attacks have been from nefarious individuals or crime rings who are stealing credit card numbers or other personal information in identity theft. But telemarketers are also using the technique to get people to buy bogus products. Because the costs are so low for to spoof caller ID numbers using a voice over IP service, it means that companies using the technique only have to get a few people to buy a phony product or hand over personal or financial information to make the efforts profitable.

How do the scams usually work?
Scammers often use either a war dialer, which is software that identifies numbers that can be used to make calls, to call phone numbers in a given region, or they access a legitimate voice messaging company with a list of phone numbers stolen from a financial institution. Usually they set up an automated recording to call individuals telling them that their credit cards have been flagged for fraudulent activity. Then they either ask people to provide credit card numbers, PIN codes, and/or Social Security numbers to verify their account or they provide another number where the consumer is to call to provide account details.

Some sophisticated attacks combine vishing and phishing. These scams typically start with a phishing e-mail that says there has been a problem with an online account from a known Web site, such as a bank, credit card company, or online retailer, and it directs users to call a number and enter information to verify their account.

Is it hard for authorities to catch vishers?
Yes and no. Because all calls originate and terminate somewhere, there are billing records that law enforcement officials can use to trace calls to their sources. But this often takes several subpoenas to get access to the right information, which takes time and costs money.

Are there any technologies that can be used to identify vishing attacks?
The biggest vulnerabilities in the communications network occur where older technologies meet new technologies, according to Secure Science's James. As a result, he believes that a coordinated effort by traditional phone companies and newer VoIP companies can help stop many attacks. Essentially, traditional phone companies and VoIP providers can verify and authenticate calls to ensure people making calls are who they say they are. This practice should cut down on much of the illegal activity that is done by spoofing caller ID numbers, James said.

Carriers could also add clauses to their terms of use that would prohibit customers from using spoofed IDs to commit fraudulent acts. And if these users are caught doing something illegal, they could have their service terminated.

Some companies are offering blacklist software that blocks certain caller ID phone numbers. Of course, blacklisting can be tricky since scammers and telemarketers can numbers can change the pool of numbers they use to conceal their identities. For example, Google will offer a feature in its Google Voice product that will allow phone calls to be filtered like email so that users can block calls or send some calls from certain phone numbers to a "spam" folder.

And finally caller ID spoof providers like SpoofCard, which handles the large majority of spoofed numbers on the market, can work with service providers and law enforcement to flag suspicious spoofers.

What can consumers do to protect themselves?
Here is some advice from security experts:

• Be aware. Consumers need to know that these scams exist. To find out more information, go to the FTC Website.

• Be suspicious of all unknown callers. People should be just as suspicious of phone calls as they are of e-mails asking for personal information. And some experts suggest letting all calls from unknown callers go to voicemail.

• Don't trust caller ID. Just because your caller ID displays a phone number or name of a legitimate company you might recognize, it doesn't guarantee the call is really coming from that number or company. As explained earlier, caller ID spoofing is easy.

• Ask questions. If someone is trying to sell you something or asking for your personal or financial information, ask them to identify who they work for, and then check them out to see if they are legitimate.

• Call them back. Again if someone is selling you something or asking for information, tell them you will call them back and then either verify the company is legitimate, or if it's a bank or credit card company, call them back using a number from your bill or your card. Never provide credit card information or other private information to anyone who calls you.

• Register your number with the National Do Not Call registry at donotcall.gov. Even though criminals and unscrupulous telemarketers may ignore the list, if you are on the list and get a call from a supposed telemarketer, that could be a tip that the offer is bogus. Most legitimate telemarketers obey the rules and laws about contacting consumers. Also, the Website provides a place where complaints can be filed.

• Report incidents. Report vishing calls to www.ftc.gov or call (888) 382-1222. The FTC wants the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message. If you think you've been a victim of a vishing attack you can also contact, the Internet Crime Complaint Center.

 *Marguerite Reardon has been a CNET News reporter since 2004, covering cell phone services, broadband, citywide Wi-Fi, the Net neutrality debate, as well as the ongoing consolidation of the phone companies. E-mail Maggie.*
http://news.cnet.com/8301-1035_3-10244200-94.html