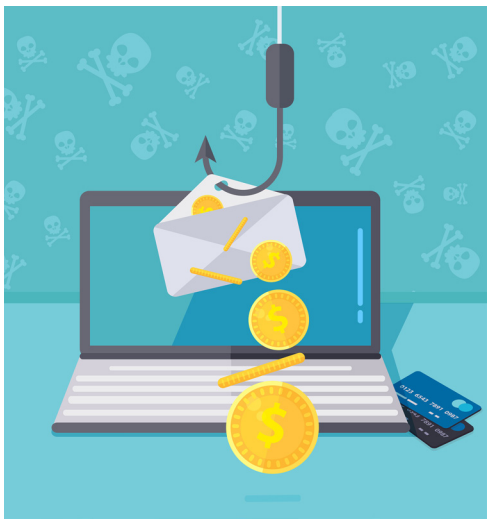
Spotting the Spoofers

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE



There probably is nothing much more annoying than having dinner interrupted by a telemarketer trying to sell you a "free" vacation. Even worse, they may purport to be from a government or law enforcement agency, and tell you that you are in big trouble (www.fbi.gov). Spoofing masks the true identity of the caller and can lead to identity theft or financial loss. Helping clients understand the risk, as well as ways to avoid getting "spoofed", is another value-added service of the professional insurance agent.

The last two decades have seen the rise of caller ID spoofing. The actual act of spoofing caller ID is not illegal. The process to spoof the caller ID is easy. After buying a certain amount of credits from a spoofing service, you dial a number provided and enter a code or PIN, the number you want to call and your fake caller ID and number (https://lifehacker.com). The Caller ID Act of 2009 considers it a crime only if it causes harm or defrauds someone. The spoofing companies market it as a way for businesses and professionals to protect their identity, i.e. their real phone numbers and names. This is very helpful for robocalls and sales calls. It has also been useful for private detectives and bill collectors. Even law enforcement, (FBI, CIA etc.) has used spoofed caller ID in various undercover investigations (www.calleridspoofing.info).

Spoofing is also used by spammers who are marketing some item or service. For the most part this is merely an unwanted and annoying practice. They will use a technique called neighborhood spoofing, where the spoofed caller ID is the same area code and first three digits as the unsuspecting recipient, making it more likely they will pick up.

The serious trouble is when those with intent to defraud use the spoofing tools to their advantage. A scary feature about caller ID spoofing is the ability by scammers to insert legitimate phone numbers. The FBI reports a scam where college students received calls that showed the FBI caller ID and the actual FBI number. The message said they were delinquent on student loan debt, taxes and even parking tickets and demanded immediate payment. A scam targeting home owners showed the caller ID and number of their town hall and demanded immediate payment for past due property taxes. By showing the actual numbers and caller ID a false sense of legitimacy was established in the minds of the victims.

The FTC, (Federal Trade Commission) recently reported scams targeting older citizens. A caller with the ID from a well-known company claims to be from technical support. They then sell `necessary' support that requires immediate payment. Another scam is bogus sweepstake winnings. The victim will be asked to pay a small fee in order to receive the bogus winnings (www.consumer.ftc.gov).

The IRS and DEA also report on similar scams where fraudulent caller ID is used and some type of immediate payment is demanded. The IRS stresses they do not ask for immediate payment over the phone, use of a specific payment method, or for credit card numbers over the phone or via e-mail. Their communication is always by regular mail. They will never threaten to send law enforcement to arrest you (www.irs.gov).

When the scammers are able to obtain personal information, social security numbers, bank account numbers, or even login information to retirement accounts, very serious identity theft damage can also occur. Bank and retirement accounts can be drained, as well as credit cards and mortgages taken out in the victim's name.

There are defenses against caller ID spoofing. For cell phones, apps are available that will recognize and block spoofed caller IDs. Landline call blockers are also on the market and easily accessible (www.trapcall.com). In any case, personal information such as social security number or bank or credit account numbers should never be given out over the phone, or to an unsolicited e-mail. Request that all demands be sent via regular mail.

It is important to note that spoofing is not limited to phone numbers. Hackers also like to send e-mails that appear to be from an employer, friend, bank or government institution. These often include requests to transfer money or provide personal information. They may tell you to click on a link, which can lead to virus or malware infections on your computer.

Spoofing can lead to identity theft, or significant financial loss, and can be done either on the phone or via e-mail. Helping clients understand how spoofing works, and ways to protect themselves from becoming victims, is another sign of the true insurance professional.

Previously published in the Insurance Advocate®