

Details: Fake Caller ID Numbers

In a new phishing scam, con artists are using phony caller ID numbers to solicit personal information and money. Thanks to the phony caller IDs, the "spoofers" are able to convince victims that they're receiving a call from a bank, credit union or credit card company. The scammers use this technique to acquire sensitive personal and financial information, or even money, from their victims.

The frightening aspect of this scam is that few people would ever think that the names and phone numbers appearing on their caller ID screens were not genuine. However, scammers are already using phony caller IDs and are posing as representatives of banks, credit card companies and government agencies. The problem has reached the point where Senator Bill Nelson from Florida is sponsoring legislation to ban the transmission of false caller ID numbers. "A similar bill has already sailed through the house," reports ABCnews.go.com.

Unfortunately, anyone with Internet access and a few dollars can find a number of legal online services that supply fake caller ID numbers. ScamBusters.org reports that in just a few minutes of research revealed several services that tout the "benefits" of caller ID spoofing, including:

- Maintaining the privacy of your caller ID number.
- Changing your voice to sound like a male or female.
- Fooling friends and business associates (or business competitors).
- One firm claims its technology is suited to individuals in certain law-enforcement-related professions, while another advertises its services as inexpensive, easy to use, and great for "business or fun."

Loss Prevention Recommendations:

- Do not assume that the information displayed on your phone, regarding who the caller is, is accurate. It can easily be spoofed.
- Never give out personal or financial information over the telephone unless you know EXACTLY whom you're dealing with.
- If you have doubts about who's on the phone, call back the number of record at your financial institution or credit card company.
- Educate your membership on **"Phishing"** and **"Vishing."**
 - Post "phishing/vishing warnings" on your web site, in newsletters and in your lobby.
 - Post a warning on your credit union's web site that you will never solicit personal/private information via e-mail.
 - Make it very clear to your members what to expect from your credit union with regard to official communication.
 - What does it look like?
 - Will they be addressed by name?

- Use the FTC (Federal Trade Commission) web site www.onguardonline.gov
 - Consumers can take interactive quizzes designed to enlighten them about identity theft, phishing, spam and online-shopping scams.
 - Elsewhere on the site, consumers can find detailed guidance on how to monitor their credit histories, use effective passwords and recover from identity theft.
- If a member is a victim of phishing/vishing, take appropriate steps to help protect him/her.
 - Block and reissue the compromised credit/debit cards
 - Report to credit bureau
 - Order a credit report