Your credit union is committed to protecting your personal information and your financial accounts. A part of that commitment is to provide timely information on the many scams and fraud schemes that criminals use in an attempt to steal your money or your identity. Having that knowledge will help each member avoid being a victim of fraud.

NAFCU

Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

SF78-807

VISHING ...
A NEW IDENTITY THEFT THREAT

VISHING: A RISING FORM OF IDENTITY THEFT

Identity thieves often use fake Web sites and e-mails that appear so realistic they have tricked many people into providing their private financial information. But many identity thieves are also using a computer technology called Voice over Internet Protocol (VoIP) that enables them to make anonymous calls to your phone for a crime called "vishing."

For example, you may get a call from an identity thief saying that your credit card has been used illegally. You're asked to dial a fake toll-free number in order to "confirm" your account details and credit card number. Once you provide this information to the thief, it is used to run up charges on your account and leave you with a financial mess to clean up. Your credit rating may also be affected.

Tips To Protect Yourself

It can be hard to determine when you are the target of a vishing scam and when your credit card provider is making a genuine attempt to contact you because of a problem with your account. But following these tips can help:

- If you receive a phone call asking you to "confirm," "update" or "verify" credit card account numbers or other financial information, hang up even if the person claims to be from your credit card provider. Then, call the customer service number on the back of your card or your statement to check if the call was legitimate. If it was, they will know it.
- When a caller asks for the three-digit security code on the back of your credit card, do not provide it unless you made the call, using the customer service number on your credit card or account statement.
- Some telephone numbers can be faked with VoIP. Even if your Caller ID shows that a caller is using a number in your area, you should be suspicious of any caller who wants you to "confirm," "update" or "verify" your financial information over the phone.
- If you're notified by e-mail that there is a problem with your account and you're asked to respond to the e-mail or call a toll-free phone number, don't do it. Instead, use the toll-free number on your credit card or account statement.
- Be wary if the caller does not address you by your first or last name.
- Report any vishing attempts to your credit union or credit card provider as soon as possible.