

## **Phishing, Vishing, or Smishing, don't fall for it, just keep them wishing!**

Phishing is when someone sends out unwanted e-mail to lure people into fake Web sites to obtain personal information and commit identity theft. Victims receive fraudulent e-mails containing authentic looking logos and familiar graphics. They often lead to a "Spoofed", or fake site that looks authentic. You are asked to divulge account information or other personal data such as usernames, passwords, and Social Security numbers.

Vishing is the phone version attempt to steal information for identity theft. The thief will state that your information needs to be verified to keep your account from being "frozen", or they may give you some information that is slightly wrong hoping that you will "correct" them.

Smishing is the text message attempt to steal information for identity theft. The victim receives a text message usually "Urgent" and when they respond with sensitive information it is used for identity theft purposes. This is called Smishing due to the SMS communications protocol used to send text messages on wireless devices.

### **HOWEVER THIEVES ARE TRYING TO CON YOU, DON'T GIVE THEM ANY INFO!**

Studies show that most identity theft still occurs when thieves obtain information from paper, by digging through trashcans or stealing from mailboxes. Shredding your personal papers is an important step in protecting your identity.

Protect yourself, keep your information private. If a company needs to verify your information call them back at a number you know is legitimate, not a number they give you to call. Thieves are constantly looking for new ways to steal your information, be vigilant, don't give them a chance.

Bell Credit Union will never email, phone or text you asking for your personal information, we obtained that information from you when you came in to open your account with us.