Phishing, Vishing, & Smishing
Avoid getting taken, hook, line, and sinker

Phishing, Vishing, and Smishing are scams that use new technology in an attempt to obtain personal, non-public information from consumers to be used for fraudulent purposes, most notably identity theft. The following information provides you with background on how these scams work, and tips to help you avoid becoming a victim.

Phishing
Phishing is probably the most common scam in which unsolicited, seemingly legitimate, e-mails are sent to consumers luring them to click on a link to verify account information. The scammer may request such information such as account numbers, social security numbers, passwords, and debit/credit card numbers, and expiration dates. The e-mails and phony websites realistically mimic the branding of a company by using similar colors, graphics, etc. They often use language to the effect that if the consumer does not perform the verification, their account will be subject to closure, suspension, denial of services, or other account restrictions.

Vishing
A consumer receives a call with a recorded message that states the consumer's credit card has been breached and to call the following phone number immediately. When the consumer calls the number, another message tells them that they have called account verification and please enter your 16-digit card number. This is an example of Vishing, short for voice-phishing, which uses a combination of phishing e-mails and Voice over Internet Protocol (VoIP). Through broadcast e-mails or random dialers, consumers are contacted and asked to "verify" information. Instead of clicking on a web link to verify their personal information, consumers are asked to call an 800 number. The 800 number is linked to an automated answering service/recorded message that directs the caller to input account information.

Smishing
This brings us to Smishing, a phishing attack sent by Short Message Service (SMS). SMS is a service that allows the transmission of text messages between mobile phones and handheld devices. An example message: "We're confirming you've signed up for our dating service. You will be charged $2/day unless you cancel your order." The message includes a link that, when accessed, takes the recipient to a phishing site where they are prompted to download a program - a Trojan horse.

Tips to safeguard yourself from Phishing, Vishing and Smishing:

- Never respond to unsolicited e-mails or text messages; especially coming from people or companies that you do not have a relationship with or regarding services you have not contracted for. Remember to contact Plumas Bank or any merchant via the regular channels you use to communicate with them.
- When you are accessing secure accounts online, make it a habit to check for the small yellow lock in your browser window. If it's unlocked - you are not in a secure area of the website.
- If you receive a Vishing message, and you do want to check your account, disregard the recorded number and contact Plumas Bank through the customer service phone number on your statement or credit card.

- Pay attention to the URL. Fraudsters cannot exactly mimic a company's website URL, but will often insert one letter or symbol to make it appear legitimate.
- Keep a record of services you sign up for on your mobile devices. If you receive a Smishing message for a service you don't think you signed up for - you probably didn't. Disregard the message.
- When in doubt, do not respond to an email, voicemail or text message regarding an account. Contact your financial institution through regular channels.
- If you receive multiple phishing, vishing or smishing messages from any financial institution, bring it to their attention to help them uncover the fraud.

Although these scams differ slightly in delivery and execution, they all use advances in technology and social engineering skills to hook you, they all give you a line about needing to "verify" your account or personal information, and, if you fall victim, the sinker is they will steal your identity and/or empty your accounts.

Remember, Plumas Bank will never contact you via text message, e-mail, phone or any other way to ask for your account numbers or passwords. If you suspect you've been a victim of phishing, vishing, and smishing or any other form of ID theft, contact Plumas Bank at 1.888.375.8627.