It's Phishing Season in Alaska!

Consumers beware! A new form of identity theft is tricking consumers into giving up personal information under the pretense of updating or providing corrected information to a company or organization with which they already have a relationship. "Phishing" or "spoofing" is a high-tech scam in which "phishers" use a company's trademarks or links to the company's actual website to appear legitimate, and ask consumers to reconfirm personal financial information. For example, victims receive an email that an account will be shut down unless the consumers reconfirm their billing information. Once the consumers respond to the email the phishers have set up the information goes to the phishers, not the company that holds the consumer's account. In March of this year, an Alaskan telephone company had to deal with phishers calling its customers asking for credit card numbers, Social Security numbers and birth dates under the guise of saving customers money on their monthly phone bills. Once the phishers get hold of this information they can either sell the information to third parties or make unauthorized charges to credit cards, changes in the billing address, or even open new lines of credit in their names. To protect yourself:

- Avoid emailing personal and financial information.
- Contact the company purporting to need the information using phone numbers you know to be genuine.
- Review credit card and bank account statements as soon as you receive them to determine if any unauthorized charges exist.
- Report suspicious activity to the FTC (http://www.ftc.gov/idtheft), the Alaska Attorney General's Office (http://www.law.state.ak.us/consumer/), and your financial institutions.
- For more information on ID theft please visit the FTC's website at http://www.ftc.gov/idtheft.