CONSUMER ADVISORY

March 2009

By Attorney General Tom Miller

"Phishing" Scams Use New Tricks

Con-artists use text messages and phone calls as well as phony e-mails and web sites to steal victims' private financial information.

Identity thieves are constantly trying to trick people into giving them crucial information -- such as credit card numbers, bank account numbers, and private passwords. It's called "phishing." If they succeed in stealing your personal information, they may try to drain your account, run up credit card charges, or open new accounts in your name.

The most frequent form of "phishing" is by e-mail, but lately we've heard of other new tactics -- cell phone text messages supposedly from a bank or credit union, and phone calls claiming to offer better credit card rates. Text messages or calls may ask you to give information by phone. E-mail messages usually ask you to click on a link and enter your personal information for some reason. There are new kinds of "phishing" scams every day.

"Phishing" messages may say there is "suspicious activity" on your account, that they need to "validate" or "verify" your account or Social Security number, or even that they are the IRS and need your account info "to send your economic stimulus check." Phishing scams imitate banks, credit card companies, credit unions, the IRS, eBay, PayPal, UPS, your Internet provider -- just about any kind of institution or company.

How to avoid being hooked by a "phishing" telephone or e-mail scam:

- **Don't reply to e-mails, calls or text messages that ask for your info.** If there's any question, contact the company yourself at its *regular phone number*.
- **If you are tricked into providing your account information, notify your financial institution at once.** You may need to change your account or take other steps. Also report phishing to the U.S. Internet Crime Complaint Center – at www.ic3.gov.
- **Don't send sensitive information by ordinary e-mail** – it's just not safe. Use only *secure web sites* -- indicated by a padlock icon or "https" web address.
- **Examine your account statements each month for unauthorized charges.** Report any suspicious activity to the business. Put a security alert on your credit bureau files. See the AG's web site for more information on avoiding identity theft.

If you think you have given out personal account information, don't panic. Contact the Attorney General's Consumer Protection Div., Hoover Bldg., Des Moines, IA 50319. Call 515-281-5926 or 1-888-777-4590 toll-free. Web site: www.IowaAttorneyGeneral.org