Protect your private information from Internet and e-mail scams.

At Ft Sill Federal Credit Union, your privacy is very important to us. That's why we want to let you know about a e-mail scams on the Internet called "phishing", pronounced "fishing", a technique hackers use to lure online consumers to fake corporate Web sites through links sent to consumers by e-mail.

The message in the e-mail often warns consumers that their account will be closed if their information is not updated or verified or that something has happened and it is necessary that account information be verified. The links within the e-mail are often pointed to Web forms that ask for bank account information such as routing numbers, account numbers, PIN numbers, passwords and Social Security numbers.

It is a Ft Sill Federal Credit Union policy to not send or request confidential account information through e-mail because it is not a secure form of communication. **You should never enter private, personal information in a form that was sent to you by e-mail.**

Here are a few ways you can protect yourself from Internet and e-mail fraud (phishing):

1. Never click on links in an unexpected e-mail that request confidential information. If updates to information are needed, always type in the address to the Web site in the browser.

2. Before submitting confidential information through forms, make sure that you are using a secure internet connection. There are two ways of determining if your connection to a website is secure. First, look at the address bar at the top of your browser. If the website address begins with "https://", then you have established a secure connection to the website, but if it begins with "http://", then the connection is unsecured. Second, look for a "lock" icon in your browser's status bar in the bottom right hand corner. The lock verifies that your connection to the website is secure.

3. Make sure that you have installed and run updated anti-virus and anti-spyware software. Both viruses and spyware can leave your computer vulnerable to attack and intrusion. Anti-virus and anti-spyware software will keep your computer safe from malicious software that might have installed itself or tries to install itself onto your computer. Anti-virus & anti-spyware software is especially important if you are using a broadband internet connection like DSL, cable or satellite.

4. Install a Firewall, either software or hardware. A firewall will prevent attacks on your computer from the internet by determining if a requested connection is malicious or not. A firewall is especially important if you are using a broadband internet connection like DSL, cable or satellite.

5. Keep your internet browser, anti-virus, anti-spyware and firewall up to date by visiting the manufacturer’s website and check for software and security upgrades.

6. Check and monitor your checking account, debit card, credit card statements and your credit report regularly to be sure all transactions are legitimate.

7. Watch for misspelling or grammatical errors on forms requesting confidential information. Hackers often make errors while rushing to get bogus Web sites in place. If something doesn't look right, there is a good chance that it's not.

Ft Sill Federal Credit Union will *never* request a customer's personal, confidential information (bank card number, account number, social security number, personal identification number or password) through e-mail. If you should ever receive an e-mail requesting your personal, confidential information that appears to be from Ft Sill Federal Credit Union, do not respond to the e-mail and contact us immediately at webmaster@ftsillfcu.com and if possible, forward us a copy of the e-mail you received or contact us by telephone at 800-654-9885.