PHISHING:
FACT OR FICTION?

Fraudsters continue to find new ways of using web sites, email and voice communications to scam innocent consumers, resulting in increasing fraud.

FACT: Identity Theft and Internet fraud go hand in hand. There continues to be a huge increase in types of frauds that gain personal information, which is then used or sold for the purpose of identity theft.

FACT: Fraud is a world-wide problem and is often part of organized crime rings with close to unlimited resources at their disposal.

FACT: Every person, from all walks of life, is susceptible to becoming a victim of fraud.

FACT: Fraud over the internet is popular because of its anonymity, ease of use, and its lack of borders. It used to be that fraudsters required cleverness to persuade people face-to- face. With an increase of internet access and email use comes an increase of fraud, as these fraudsters no longer need to be persuasive, just persistent and patient.

FACT: Fraud includes, but is not limited to: fake or compromised websites, fraudulent emails phishing (fishing) for personal information, phony buyers or sellers in online auction frauds, increased scams requesting an advance fee to deliver a prize or money, Business Opportunities and Work from Home Scams, International Modem Dialing and Cramming, and credit card fraud.

FACT: The ‘s’ in https:// indicates your communication with a site is secure. Always validate you are using secure communications before entering personal information, including user identification, passwords, and social security numbers.

FACT: Https protected web pages will include a lock icon. Clicking on the lock icon will show you which company validated the site and help you decide if the site is legitimate and trustworthy.

FACT: You can determine if you are on Seattle Bank’s secured online banking site by validating the URL as: https://www.pcsbanking.net/onlinebanking.

Seattle Bank

FACT: Seattle Bank cares about the security of your information and in educating all of our customers about protecting both your financial and personal information. Here are some ways to help protect your information:

- Never provide personal financial information in response to an unsolicited Internet or telephone request. Personal information includes your SSN, account numbers, log on IDs and passwords. A financial institution will never ask you to verify your account information online. Thieves armed with this information and your account number could steal your identity or gain access to your accounts. If you did not initiate the communication, you should not provide any information.

- Do not be intimidated by an e-mail or a caller who threatens actions based on failure to respond to their request. Thieves will often use the threat of dire consequences if you do not immediately provide or verify financial information.

- If you believe the contact may be legitimate, contact the financial institution yourself, instead of clicking a link provided in an email. Call the institution, or go to the company's web site by typing in the site address directly or using a page you have previously book marked.

- Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. Better yet, use Online Banking and eStatement to review activity online. It can help you catch suspicious activity early.

- Security experts advise that whenever possible use a combination of upper and lower case, numeric and special characters (for example !, @,$) for user IDs and passwords. A little extra complexity can prevent a fraudster from recreating your user ID and/or passwords.

- If your computer is more than five years old, its operating system (e.g. Windows 2000, Mac OS 9, etc.) may not offer the same level of protection as newer systems. Operating system manufacturers provide frequent updates to help make your system more secure. You can also check their web sites, including:
    - For Windows: microsoft.com/security
    - For Apple Mac OS: apple.com/support

- Virus protection software helps reduce the risk of contracting computer viruses that can compromise your security. Popular programs include:
    - McAfee VirusScan: mcafee.com
    - Symantec Norton Antivirus: norton.com

Seattle Bank will never send you unsolicited email asking for you to provide your password, account number, or other personal info. If you receive a communication that appears to be from us requesting personal information or are uncertain as to the authenticity of a communication, please notify us immediately by sending email to fraud@seattlebank.com or call us at 206-568-7800 or 1-888-500-BANK (2265).

FACT: We care!

Member FDIC

Seattle Bank