Beware of Fraudulent Emails and Phishing Attempts

What is “Phishing”?

“Phishing” (pronounced “fishing”) is the act of sending an e-mail that fraudulently represents a legitimate company and “lures” you (hence, the phishing name) into divulging personal and financial information that could then be used for identity theft.

Stay away from phishing

Your best line of defense against phishing is to not get lured. Unfortunately, thieves use creative tactics to trick you into providing your personal information. Do not reply to any e-mail that instructs you to enter any piece of personal information directly into the e-mail, such as:

- An urgent notice that your account will be closed or suspended if you do not provide personal information
- A survey that asks you to enter personal information
- An urgent notice that your account has been compromised and asks you to confirm your account information
- An e-mail that directs you to a non-secure webpage (http://) and asks you to enter your username, password or account numbers
- An e-mail that asks you to confirm, verify, or refresh your account, credit card, or billing information

What are some common phishing tactics that are used?

Many phishing emails are well designed and convincing and will even include a familiar company logo.

Signs of potential fraud with email phishing are:

- “Dear Borrower” (no customized salutation; this is a mass-mailing of a phishing e-mail).
- You receive an email stating “There Is a Problem With Your Account. Confirm your account number, password.”
- You receive an email stating “You Just Won a $100 Gift Certificate. Give us your name, address, and loan number.”

Phishing Avoidance:

- Double-check the internet address in your browser. It should say: https://www.seterus.com . The safe way to visit a website is by typing in the address you know to be authentic.
- Do not click on emails from unknown senders.
- Use caution when entering personal information including your account number, login name and especially credit card information and your social security number.
- Regularly review your online accounts to ensure no fraudulent activity has taken place. If anything suspicious appears contact your bank or service provider immediately.