We are continually monitoring online threats and reviewing our security procedures to protect all Client information. Although the Internet is one of the most powerful communication tools available, criminals may use the Internet to defraud unsuspecting people. Scams to retrieve a Client's personal information can occur through many different channels, such as a phone call, email message or social engineering technique.

One of the most common methods used today to retrieve a Client's personal information is called "phishing." This is when fraudulent websites or emails are created in an attempt to steal personal information.

Important Information about "Phishing"

- Clients are advised to never give out confidential information or passwords by replying to an email or by going to a website through a link included in an email. Even if you click on the link in an email but don't actually provide confidential information, you could be exposing yourself to viruses, malware or other harmful pieces of software. Remember, Pilot Bank does not request confidential, personal or secure login information via email.
- Spammers have gotten creative by making spam email messages appear as though it came from a reputable company or government agency, thus creating a sense of urgency to respond. This is a technique frequently used to lure unsuspecting people to provide confidential information that may be used for identity theft.
- Be cautious of anyone calling you to ask for bank account or personal information over the phone.

How to Protect Yourself

- Clients are urged to protect their computer system through the use of anti-virus, anti-spyware and firewall hardware and/or software. If anti-virus software is used, it's very important to keep the virus definitions up-to-date so that the most recent threats may be detected.
- If you use an Operating System such as Microsoft® Windows XP or Vista, stay abreast of the many security updates Microsoft® releases. It is important that your computer is updated and contains the appropriate patches. You may choose to setup an automatic update at a certain time each day or week.

- Review your account statements when they arrive and report discrepancies to Pilot Bank.
- If you do not recognize the sender of an email message, delete the email without opening it.
- **Keep your passwords confidential**. Change passwords regularly using a complex combination of letters, numbers and special characters. Avoid using obvious passwords that may be easily guessed or hacked.
- Never dispose of a hard drive without thoroughly cleaning it to remove all personal information.
- When using an ATM or card machine at a gas pump, carefully inspect the device to ensure that no abnormal attachments have been added. If it doesn't look right, don't use it.

Reporting Fraud

If you believe you are a victim of fraud or need to report a suspicious email involving Pilot Bank's name, please forward it to us immediately at: reportfraud@pilot.bank. If you receive a suspicious phone call that uses Pilot Bank's name, please contact the bank at 813-349-4575.