

Phishing Scams

Recently, fraudulent emails, telephone calls and cell phone text messages were sent to First National Bank of Chester County customers and non - customers by phishing scammers. The phishing scammers were attempting to obtain confidential information such as account numbers, an ATM card number, passwords, Social Security numbers and other personal and confidential information. With information received from a successful phishing scam, thieves can withdraw funds from your accounts, take out loans, and obtain credit cards and even a driver's license in your name. Phishing scams can harm your financial history and personal reputation. Understanding what phishing is and how it works is the key to protecting yourself against this crime.

What is Phishing?

Phishing, pronounced "fishing" is exactly what thieves are doing. They are fishing for any type of personal financial information. Phishing scams take many forms. It can be an email, a telephone message to your home or cell phone and even a cell phone text message. These scammers will use various ways to contact you, phishing for one thing – your personal information.

How Phishing Works

- Typically, you will receive an email or telephone call that appears to be from a company that you regularly do business with such as your financial institution, credit card company or even a government agency.
- The email or phone message will warn you of a problem with your account and to contact them immediately.
- The email will then ask you to click on a link to go to the institution's web site. Unfortunately, that link takes you to a counterfeit web site that looks exactly like the real one.
- The phone call will ask you to call a number, different from any number associated with the institution.
- In either case, it asks you to update your account or verify who you are with information such as your account numbers, an ATM card number, passwords or a PIN number, Social Security number. Sometimes they even ask for your mother's maiden name or place of birth.

Should you provide any of the requested information, you may become a victim of identity theft.

How to Protect Yourself from Phishing

- **Never provide your personal information to an unsolicited email, telephone call or a text message.** Remember, if you did not initiate the call, text or email, do not give out any personal information.
- **If you believe that it may be a legitimate telephone call or email, visit or contact the institution directly, by using a telephone number or web site you**

have verified yourself. Verify those numbers through published numbers found in a telephone directory or on a web site. A monthly statement, such as your bank statement, is another source for verifying legitimate telephone numbers and web sites.

- **Never provide your password or PIN number over the telephone or when replying to an unsolicited email.** Institutions, especially financial institutions, will never ask you to verify any account or personal information online or over the telephone.
- **Review your account statements regularly.** Checking your accounts through an online Internet banking program gives you the ability to view your accounts on a daily basis to catch any suspicious activity, rather than waiting for your monthly statement.
- **Do not be intimidated by an email or caller.** Be suspicious of an email or caller suggesting that if you do not respond immediately with account information or verify account information, your account will be in jeopardy.
- **If you receive a suspicious email, text or telephone call, report it to the business or institution immediately.** If it is an email, forward the email to the business or institution. Provide the fraudulent telephone number that you have been directed to contact, if you received a text message or telephone call.
- **Report all suspicious contacts to the Federal Trade Commission at www.consumer.gov/idtheft or by calling 1-877-IDTHEFT.**

What to Do If You Suspect You Have Been a Victim of Phishing

- ◆ Contact the business or institution immediately to alert them to the situation. If necessary close accounts and open new ones.
- ◆ If you disclosed any personal or confidential information in a phishing scam, contact one of the three major credit bureaus to place a fraud alert on your file. This will prevent the scammers from opening new accounts in your name. Below is the contact information for the three major credit bureaus.

Equifax
800-525-6285
P.O. Box 740250
Atlanta, GA 30374

Experian
888-397-3742
P.O. Box 1017
Allen, TX 75013

TransUnion
800-680-7289
P.O. Box 6790
Fullerton, CA 92634