Protecting Your Financial Security

At Citizens Savings Bank, we want to help ensure you don't become a victim of a scam that could result in financial loss. Listed below are just a few of the various types of fraud that are currently prevalent; please take a moment to read and become familiar with them.

- **Account Compromise.** You receive a call (usually from an automated system) that claims to be from your bank, stating that your account has been compromised, deactivated or suspended. It instructs you to provide personal information in order to reactivate the account. Never provide this information, especially if you did not initiate the call. If you are still concerned about the validity of the call, phone or visit the bank personally.

- **Check scams.** These come in many forms; the most prevalent are those from someone you don't know. You are directed to deposit a check, retain a small portion for yourself, and send the remaining funds via wire transfer. Just a few of these situations include:

    - Inheritance – from a relative you never heard of before. These may state that a portion of the inheritance tax is payable in advance.
    - Lottery winnings – from a ticket you never purchased – and usually from a foreign country. These ask you to send a payment to cover a portion of the taxes on the winnings.
    - Mystery shopping – where you are enlisted to do some shopping at a large retailer and complete a survey, which you return along with most of the funds.
    - Overpayment for the purchase of a large item (such as a car) – you are asked to return the funds along with the item itself, to the "purchaser".

Never accept these checks and more importantly, never negotiate them. When the check is determined to be bad, *you* will be responsible for repayment of the funds to the bank.

- **Phishing.** By posing as an individual or organization that you may know and trust, criminals gain access to your personal information from your computer. Through the use of fake emails and websites, phishers attempt to obtain your bank account information, credit card numbers, and passwords. Once obtained, these pieces of information can be used fraudulently to make purchases or obtain credit in your name.

- **Pharming**. This redirects web traffic away from one site, to another that looks identical – but is in reality a phony site designed to obtain your personal information.

- **Telephone Solicitations –** Work the same way as other frauds. Posing as an individual or firm that you may do business with, criminals begin with friendly small talk to gain the trust of unsuspecting persons. Once that has been obtained, they proceed to look for important personal information. Just as in phishing, once obtained it is possible to make purchases or obtain credit in your name.

What can you do to protect yourself?

- Protect your Social Security Number, credit & debit card numbers, passwords, personal identification numbers (PINS) and any other personal information; particularly to those unsolicited contacts. Never give these out in response to an unsolicited email or telephone call.
- Change passwords and PINS on a regular basis.
- Keep a close watch on your bank account statements and credit card bills. Review these statements in a timely manner, and immediately contact the bank if there is any discrepancy or something unusual.
- Obtain copies of your credit report, on no less than an annual basis. This should also be checked for accuracy.
- Never simply dispose of documents that may include confidential information; these should be properly shredded before placing in the trash.
- Be aware of anything that pressures you to act immediately, guarantees success or requires an up-front investment on your part. If it sounds too good to be true, most likely it is.
- Don't click on a link inside of an email; type the address into your internet browser.