Citizens State Bank
Confident. Courteous. Close By.

Phishing Scams: Don't Take the Bait!

As a courtesy for our new and existing customers, Citizens State Bank would like to provide the following information to help you avoid falling victim to phishing scams.

What is phishing?

Phishing occurs when someone is contacted by a scammer posing as a legitimate institution for the purpose of acquiring personal information, such as social security numbers, PIN numbers and user names and passwords. Phishing can occur via email, text message and even by phone. If successful, the scammer then uses the victim's information for personal gain, either by accessing the victim's bank and credit card accounts, or using the victim's personal information to create new accounts that can be exploited by the scammer.

Phishing scams continue to be problematic for businesses and consumers alike; a report published by the data security firm RSA noted that in 2013 there were nearly 450,000 phishing attacks, resulting in losses of more than $5.9 billion!

How does phishing work?

Phishing emails, text messages, websites and phone calls are designed to mimic well-known and trusted businesses, financial institutions and government agencies. Scammers usually employ one of three tactics:

- *An Attractive Offer* – the scammer informs the victim that they've won a contest or can benefit from a limited-time offer; to claim the prize or redeem the offer, the victim is instructed to click a link and provide the personal information required.
- *A Sense of Urgency* – the scammer poses as an authority figure or agency and contacts the victim, warning them that their account will be canceled or that they will be penalized unless they immediately verify their personal information.
- *Confirmation Required* – the scammer contacts the victim and informs then that they are required to update or confirm their account number, password or other personal information.

How can I avoid becoming a phishing victim?

Citizens State Bank has compiled the following tips to help you avoid falling victim to phishing scams:

1) Learn to identify and ignore suspicious emails, text messages and phone calls.
2) Understand the policies of organizations with which you do business, and know that they will never request sensitive information via phone, text or email.
3) Never click on a link included in a suspicious email.
4) Protect your computer by utilizing a reputable antivirus program, and keep your software up to date.
5) Verify you are using a secure website before entering sensitive information – look for a lock icon or a web address that begins with https://
6) Review your account activity regularly and check for any unusual or unidentifiable transactions.
7) Do not allow yourself to be pressured into providing personal information to someone claiming to represent a business or government agency.

Lastly, please know that Citizens State Bank will *never* ask you to provide your password, account number, social security number or any other personal information by phone, text message or email. NEVER respond to any such requests. If you have the slightest doubt, contact a Citizens State Bank representative and ask for clarification.