IMPORTANT SECURITY INFORMATION

PHISHING

Protect Yourself and
Your Accounts

Important Security Information

At Century Savings Bank, security and privacy of your financial information is a top priority. In addition to our many thorough security features, we want to keep our customers aware of how to best protect their accounts. Please review the information below to learn about protecting the security of your personal and private customer information as well as information on frequently used Internet and e-mail scams.

❖ DISCLOSING PERSONAL INFORMATION

It is often necessary to ask for certain personal information when a customer calls or visits a branch or logs into our Web site. Requiring the disclosure of personal information before beginning a transaction is a valuable security tool to verify and protect a customer's identity. Unfortunately, personal information shared on the Internet or telephone may be used to commit fraud, so provide this information only to businesses you know and trust.

Century Savings Bank will NEVER independently call a customer or send an e-mail asking a customer to disclose account numbers, ATM or debit card numbers, passwords, or other personal information. If at any time you receive an unsolicited telephone call or e-mail from a person claiming to be a representative of Century Savings Bank asking for personal or identifying account information, do not respond. Instead, please call our Operation Department at 856-451-3300 to verify that you are communicating with a Century Savings Bank representative.

PHISHING

Be Alert for Potential Email Scams

Century Savings Bank cautions consumers to be on the lookout for phishing scams in which various fraudulent emails claiming to come from Century Savings Bank ask recipients to click on hyperlinks to update account information, unlock debit cards, receive a tax rebate or refund, or complete a survey to receive a fee. These are not legitimate emails from the bank; instead, they are fraudulent emails sent as part of a scam in which criminals try to trick people into divulging their confidential information. Recipients should not click on any links in these emails or respond with any confidential information such as account numbers, debit card numbers or Social Security Numbers. Clicking on a link in this type of email could expose a computer to malicious software that could track keystrokes, potentially giving the scammers private information such as account passwords. Fraudulent emails such as these may look official, sometimes including the company logo. Century Savings Bank does not send out unsolicited emails asking its customers to click on a hyperlink and input confidential account or debit card information.

If you have questions about whether a communication you've received is legitimate, please contact the bank using a phone number you know is reliable, such as the customer service number found on your account statements or in the upper right corner of each page on our website. If you receive an email that you believe may be fraudulent, you can notify us by emailing **customerservice@centurysb.com** or calling the Operation Department at 856-451-3300.

Phishing Scams Using Phones

There is a variant of traditional phishing scams that uses telephone calls (instead of email) to gather confidential information. Customers may receive an automated phone call or an email saying their account or debit card has been compromised and giving them a phone number to call to resolve the issue. When they call, they reach an automated answering program that asks them for their account number (or debit card number) to verify their account. Customers should not give confidential information in response to suspicious requests like this. These types of phone-phishing scams, sometimes called "vishing," have become more common with the increasing popularity of Voice over Internet Protocol (VoIP), which allows telephone calls to be made from computers instead of from traditional phones.

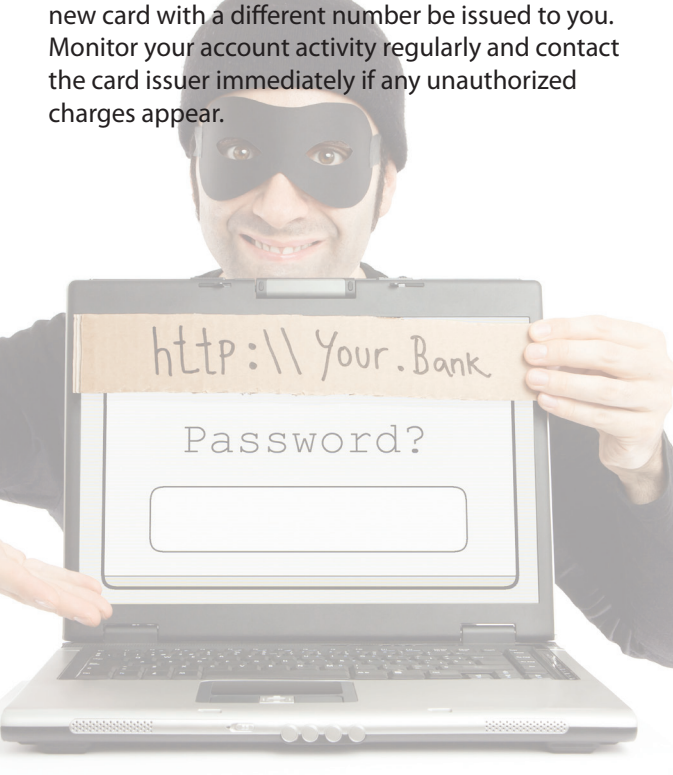
We recommend the following actions if you think you are a victim of a phishing scam.

- **If you have given out your bank account information:**

Contact your local branch as soon as possible so we may close your account and reopen a like account with a different account number.

- **If you have given out your credit, debit, or ATM card information:**

Report the incident to the card issuer as soon as possible and request that your card be closed and a new card with a different number be issued to you. Monitor your account activity regularly and contact the card issuer immediately if any unauthorized charges appear.



Main Office – Vineland
1376 W. Sherman Ave.
856.690.9100

Upper Deerfield
53 Cornwell Dr., Bridgeton
856.451.3300

Elmer
121 N. Main St.
856.358.2100

Gibbstown
800 E. Broad St.
856.423.1616

Mullica Hill
100 N. Main St.
856.478.6200

Vineland
1005 E. Landis Ave.
856.691.9600

CENTURY
SAVINGS BANK
Since 1865
community banking *plus*

www.**centurysb**.com

MEMBER
FDIC

02/2014

EQUAL HOUSING
LENDER