INSTITUTION FOR SAVINGS

BUILDING STRONGER COMMUNITIES TOGETHER SINCE 1820.

Online Security for your Internet Banking Account

<u>The vast majority of cyber thefts begin with the thieves compromising your computer(s).</u> Perpetrators often monitor the customer's email messages and other activities for days or weeks prior to committing the crime. You should be vigilant in monitoring account activity. You have the ability to detect anomalies or potential fraud prior to or early into an electronic robbery.

Warning signs visible to a customer that their system/network may be compromised include:

1. Inability to log into online banking (thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money);
2. Dramatic loss of computer speed;
3. Changes in the way things appear on the screen;
4. Computer locks up so the user is unable to perform any functions;
5. Unexpected rebooting or restarting of the computer;
6. Unexpected request for a one time password (or token) in the middle of an online session;
7. Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.);
8. New or unexpected toolbars and/or icons; and
9. Inability to shut down or restart the computer.

Examples of Deceptive Ways Criminals Contact Account Holders:

1. The FDIC does not directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
2. Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.
3. Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent

statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

If you know or have any reason to suspect your computer may be compromised contact the Bank immediately to have your Internet Banking login disabled to avoid theft.

Additional information can be found on our website. From the home page click on **Security Alerts** at the bottom of the page. We encourage you also to review the slide show titled Corporate Account Takeover & Information Security Awareness.