Information Security

Today's technology has changed the way we bank. It's faster, easier and more convenient than ever. With the benefits come the potential for our most personal information to fall into the wrong hands. That's why it's important to develop safe habits to ensure that your personal information remains your personal information.

At Newtown Savings Bank, the privacy and confidentiality of your personal and banking information is top priority. As your trusted banking partner, we provide you with the facts, the tools and the know-how you need to keep your confidential information secure and protected.

ATM SECURITY

We encourage all of our customers to consider the following ATM safety guidelines:

- Always pay close attention to the ATM and your surroundings. Use ATMs in familiar, public, well-lit locations.
- Maintain an awareness of your surroundings throughout the entire transaction.
- Be wary of strangers trying to help you with ATM transactions. Newtown Savings Bank representatives will have identification.
- Shield the keypad with your hand when entering your PIN. Never share your PIN with anyone.
- Be aware of anyone sitting in a parked car nearby.
- Do not use an ATM that appears unusual looking or offers unfamiliar options.
- Never count cash at the machine or in public. Wait until you are in the safety of your car or another secure place.
- Make sure you retain your transaction receipt, if you chose to receive a printed receipt. Do not throw the receipt away at the ATM site.
- Always remember to take your card with you after completing your transaction.

DEBIT CARD FRAUD MONITORING

We offer a comprehensive fraud monitoring solution for your Debit Card. If we detect an unusual transaction, you may receive one or more notifications to alert you of potential fraud on your debit card. Each notification will enable you to either verify the transaction or let us know you do not recognize the transaction.

We will send you notifications in the following order:

1. An email notification, with the option to reply with "fraud" or "no fraud."
2. A text alert, which also has the "fraud" or "no fraud" option.
3. If we do not receive a response, we will initiate automated calls (8 am to 9 pm ET). The call will also give you the option of speaking to a fraud analyst.

In order to receive the three notifications described above, please be sure that we have all your current information such as email address, cell phone and home phone numbers on file. You may update your information by visiting any branch or by calling Customer Service Center at 800.461.0672.

VISA DEBIT CARD ALERTS

You can set up Visa® alerts at Visa.com/PurchaseAlerts. Choose notifications when purchases reach or exceed the dollar amount you set up; when your card is used outside the U.S.; and when purchased are made online or by phone.

Information Security

INTERNATIONAL TRAVEL AND YOUR DEBIT CARD

If you are planning international travel, contact us one week prior so that we will know the dates you are away and in what countries you will be traveling. This will help us monitor any suspicious activity and protect you against fraudulent use of your card.

INTERNET SECURITY

While online banking is an easy and convenient way to manage your Newtown Savings Bank account, there is the potential for fraudulent activity. To maximize your security:

- Never share your password, account numbers, PIN or other account data with anyone.
- Make sure that your online password is long and complex - using letters, numbers and symbols.
- Never leave your computer unattended while engaging in online banking.
- Notify Newtown Savings Bank immediately regarding lost or stolen information, or suspected fraudulent activity.
- Protect your hardware by installing a security suite containing automatic updates on your computer (antivirus, antispyware and firewall).
- Always keep your operating system, web browser and other computer software current. Back up your computer files on a regular basis.
- Be very cautious before providing any personal information online.
- Be absolutely sure of the validity of a site before providing an account number or social security number. When in doubt, don't provide it.
- When logged on to a public wireless network, do not use online banking.
- Newtown Savings Bank will never contact you to request your personal electronic banking credentials on an unsolicited basis.

EMAIL SECURITY

To protect your personal information passing through email servers, Newtown Savings Bank suggests that customers refrain from including any account numbers and financial information in a standard email. Instead, we offer our customers communicating with us a safer option through Secure Email*, a free alternative service which uses encryption technology to protect against identity theft and fraud. This service allows documents containing confidential information such as social security numbers, tax identification numbers, account and credit card numbers, and financial records to be securely transferred electronically.

To register for, or to access Secure Email, visit NSBonline.com and click "Contact Us." Never reply to an email that requests your account number or social security number.

**Secure Email and Secure Messaging through Online Banking are only available on a full screen device.*

Information Security

SOCIAL NETWORKING SECURITY

Social networking is a great way to stay in touch and connected to your friends and family. However, it's important to be smart about what you post on these channels. To stay safe in the online social world, we encourage the following precautions:

- Review the privacy and security settings on each social networking sit in order to control who has access to your posting activity.
- Be aware of how much personal information you share on social networking sites and who is viewing it.
- Carefully review all incoming messages that contain links. Even links that look like they come from friends can sometimes contain malware or be part of a phishing attack (attempts to collect personal information such as your login, password and other identifying information, by appearing to look like they've been sent by a friend or a business). In these situations, if you are at all suspicious about the message, avoid clicking on the link entirely and contact the sender directly to verify the validity of the message.

SHREDDING

For your protection, we recommend shredding all documents that include signatures, account numbers, social security numbers, medical or legal information. For information on upcoming Shred Events, where you can shred and destroy your unwanted confidential documents and personal files, visit NSBonline.com.

EMPLOYEE SECURITY TRAINING

Newtown Savings Bank conducts on-going security training with all employees. This ensures that every individual that you interact with throughout your banking relationship with Newtown Savings Bank is educated, knowledgeable and up to date on the most current banking security measures.

CREDIT REPORTS

It is always a good idea to check your credit report at least once a year. To request a free online credit report, we recommend you visit www.annualcreditreport.com, which, according to the FTC, is the only website that provides free annual credit reports under Federal Law. For more information regarding privacy and security from Newtown Savings Bank, visit the security page on NSBonline.com by clicking the security text link on the bottom of every page or directly at http://www.nsbonline.com/about-us/privacy-statement.aspx. View our full policy, including how the Bank collects, shares and uses your personal and banking information.

Newtown Savings Bank
The Power of Local

800.461.0672 • NSBonline.com