

Security and Privacy

The Nashua Bank is committed to the security and privacy of your personal information. We take strong measures to verify the identities of customers and to authorize online banking activities. We maintain high standards to ensure that information is used only for appropriate business reasons in accordance with applicable laws and regulations.

Online Banking

The Nashua Bank uses firewall technology, encryption protocols, and custom-designed architecture to ensure the safety of your on-line banking sessions. Encryption is the process of scrambling private information to prevent unauthorized access. The Nashua Bank also utilizes multifactor authentication when customers login to their accounts. Multifactor authentication is a method of verifying identity through a combination of secret or unique identifiers linked to a specific customer (such as passwords and other means).

You must safeguard your online banking ID and password by keeping them private and secure. Memorization is preferable, as any written password is vulnerable to theft. To reduce the likelihood of password guessing, you will be locked out from the online banking system after three (3) unsuccessful login attempts. You are also responsible for preventing unauthorized viewing of or access to your computer during your online session. Your session will expire after ten (10) minutes of inactivity.

To provide you with better service we may place a "cookie" on your browser. A cookie is a mechanism that records your preferences when you visit a website. Cookies placed by Nashua Bank are commonly used and do not harm your system.

The Nashua Bank recommends that you also install and operate up-to-date anti-virus, anti-spyware, and firewall protection on your computer. Also make sure your computer has installed the latest security patches.

E-mail

Regular non-encrypted Internet e-mail is not secure. Please do not send confidential information such as social security or account numbers to The Nashua Bank via regular e-mail. We will not include any confidential information in an e-mail Internet response back to you since it will not be secure.

The Nashua Bank does not use email to request personal information, account numbers or passwords, etc. from customers. If you receive an email of this type purporting to be from The Nashua Bank – even with an official appearance and/or logos – please do not respond to it. Please notify us immediately at (603) 882 -2700 to report any activity of this nature.

Identity Theft

One of the most serious forms of financial fraud is identity theft - the unauthorized use of personal identifying information to establish new credit, conduct business, or commit other crimes in the name of a victim. This typically occurs without the victim's awareness. Identity Theft is an increasingly serious crime that impacts millions of Americans each year.

Identity thieves might use a variety of ways to steal your personal information. Some common tactics include rummaging through your trash, "skimming" account numbers when you process a card-based transaction, filing a "change of address" form in your name, or stealing your wallet, purse, mail, or employment records.

"Phishing" is another common identity theft tactic. To conduct this fraud, a perpetrator may send an email, text message, pop-up, or phone message pretending to be a legitimate company (perhaps your financial institution, your utility company, your doctor's office, etc.). The message may ask you to "update," "confirm," or "verify" certain information. Sometimes, these messages contain links connecting to fraudulent or "spoofed" websites. Spoofed websites may appear identical to legitimate websites. Phishing attempts will often appear very official or legitimate or may use various pressure tactics threatening serious consequences for failure to comply.

You should be aware that The Nashua Bank does not use email, text messages, or pop-ups to request personal information, account numbers or passwords, etc. from customers. If you receive a communication of this type purporting to be from The Nashua Bank – even with an official appearance and/or logos – please do not respond to it. Please notify us immediately at (603) 882 -2700 to report any activity of this nature.

Protecting Yourself from Identity Theft

To reduce the likelihood you will be impacted by identity theft, it is important to think about safeguarding your personal financial and identifying information on a regular basis. Below are some general steps you can take to help increase your security.

- **Never provide your personal information in response to an unsolicited request**, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
- **If you believe the contact may be legitimate, contact the sender yourself.** You can find phone numbers and Web sites on the monthly statements you receive from your financial institution or other company you do business with, or you can look them up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified.
- **Never provide your password, financial information, account numbers, or social security number over the phone or in response to an unsolicited Internet request.** Thieves armed with this information and your account number can help themselves to your savings. A financial institution would never ask you to verify your account information online.
- **Never click on the link provided in an e-mail you believe is fraudulent.** It may contain a virus that can contaminate your computer.
- **Do not be intimidated by an e-mail or caller** who suggests dire consequences if you do not immediately provide or verify financial information.
- **Review account statements regularly to ensure all charges are correct.** Pay attention to statement cycles. If an account statement is late in arriving, call promptly to find out why. If you have electronic account access, periodically review activity online to catch suspicious activity.
- **Order copies of your credit report from each of the three national credit reporting agencies every year.** Review your report for unauthorized activity. Instructions for ordering a free credit report can be found on the Federal Trade Commission official government website (see below).
- **Destroy (shred) sensitive documents prior to discarding them.** This also includes medical insurance forms, physician statements, and unused credit offers received through the mail.
- **Keep items with personal information in a secure place**, especially if you have roommates, employ outside help, or are having work done in your home.

- **Guard your mail from theft.**
- **Give your Social Security number only when absolutely necessary.** Ask to use other identifiers when possible.
- **Find out how your personal identifying information will be used** and whether it will be shared with others before you reveal it.
- **Limit identification information and carry only those cards you will need.**
- **Protect your account access with passwords;** be sure to use passwords that are difficult to guess. Do not use readily identifiable formats such as your mother's maiden name, your birth date, the last four digits of your social security number, or your phone number. The Federal Trade Commission offers the following recommendations for passwords:
 - Passwords should have at least eight characters and include numbers or symbols. The longer the password, the tougher it is to crack. A twelve-character password is stronger than one with eight characters.
 - Avoid common words: some hackers use programs that can try every word in the dictionary.
 - Don't use your personal information, your login name, or adjacent keys on the keyboard as passwords.
 - Change your passwords regularly (at a minimum, every 90 days).
 - Don't use the same password for each online account you access.
- **Protect yourself from fraudulent or copycat Web sites** that deliberately use a name or Web address very similar to, but not the same as, that of a real financial institution or other company. The intent is to lure you into entering your personal information or passwords onto the fraudulent site. Always check to see that you have typed the correct Web site address before entering information or conducting a transaction. Consider installing and maintaining updated anti-phishing software on your computer.

What to Do If You Fall Victim to Identity Theft

If you believe you have been the victim of identity theft, notify The Nashua Bank immediately at (603) 882-2700 and alert us to the situation.

The NH Department of Justice web site offers a step-by-step "toolkit" detailing what to do and who to contact (see links below). The toolkit will also instruct you to notify law enforcement if you believe you are a victim of identity theft. In addition, you should report all suspicious contacts to the Federal Trade Commission by calling **1-877-**

IDTHEFT. You can help fight identity theft by reporting suspicious contacts and phishing attempts even when no information is believed stolen.

You should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name.

Here is the contact information for each major credit bureau's fraud division:

Equifax

800-525-6285

P.O. Box 740250

Atlanta, GA 30374

Experian

888-397-3742

P.O. Box 1017

Allen, TX 75013

TransUnion

800-680-7289

P.O. Box 6790

Fullerton, CA 92634

Additional Information

When it comes to identity theft and protecting your personal information, constant education and awareness are your best defenses. Below are websites sponsored by state and federal agencies with important information on how to deter, detect, and defend from identity theft and related fraud. *Please be aware that The Nashua Bank accepts no liability or responsibility for websites not our own.*

State of NH Department of Justice - Office of Attorney General

<http://doj.nh.gov/consumer/index.html>

Believing that “the best consumer protection is widespread public awareness,” the NH Attorney General offers this extensive site. It features an identity theft “toolkit” for use if you believe you are a victim of identity theft. There is also a link to identity theft prevention resources and recent ID theft warnings. The site also contains a “Don’t Cash That Check” link explaining various check and

lottery scams. Also included is also a link to the highly informative “NH Attorney General’s Consumer Sourcebook.”

http://doj.nh.gov/consumer/credit_freeze.html

Also with the NH Department of Justice, this site describes the difference between a “fraud alert” and a “credit freeze.” Instructions are given for initiating a “credit freeze” to prevent your credit file from being shared with potential creditors.

State of Massachusetts – Office of Attorney General

<http://www.mass.gov/?pageID=cagosubtopic&L=3&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&sid=Cago>

Provides in-depth information regarding consumer scams and identity theft. There is also a step-by-step guide for Massachusetts victims of identity theft.

United States Federal Trade Commission

<http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm>

This site contains information on phishing, identity theft, and internet security & safety including a link to obtain your free credit report. This site also contains information about the sale and purchase of identity theft protection products and services.

Federal Deposit Insurance Corporation (FDIC)

<http://www.fdic.gov/bank/individual/online/safe.html>

This site contains tips for safe banking over the Internet.

Acknowledgement: the information on these pages is developed in part from materials produced by the Federal Deposit Insurance Corporation (FDIC), the US Federal Trade Commission, State of NH Department of Justice, State of Massachusetts Office of Attorney General, and the Federal Reserve Bank of Philadelphia.