Brattleboro Savings & Loan

A Guide to Online Banking Security Practices and Procedures

For a safer online experience, it is important to understand the threats that exist on the internet. While Brattleboro Savings & Loan has implemented many security features to make your online banking experience as safe as possible, it is important that you as a consumer do your part to keep your information safe as well. This means you need to be vigilant in protecting yourself against account fraud and identity theft. Working together we will help keep your internet transactions secure. This guide has a number of ideas to assist you in this endeavor.

When you "visit" our bank on the internet whether it's to learn about rates, to review your accounts or to pay your bills, you are entering a secure area. Measures we have taken include:

The Use of Passwords and PINs – Your password and PIN (personal identification number) is your first line of defense and a unique identifier. Be sure not to share them with anyone—most frauds involving hijacked accounts originate with someone the victim knows. Security begins with a strong password, which only you, the user, knows. Experts advise a combination of letters and numbers avoiding dictionary words, especially the names of your spouses, children, pets, birthdays, home addresses, etc. totaling 8-12 characters.

Multifactor Authentication – This form of identity verification provides added security by requiring multiple forms of identification, such as something you know (password or PIN) and something you have (Debit card, IP address of your computer). When an online session is started from a computer(s) that isn't the one you usually use, a request for the answers to the security questions you have already established will occur.

Anti-virus Protection – Make sure the anti-virus software on your computer is current and scans your e-mail as it is received. This simple step is critical to personal safety and security when online.

Encryption – Once online with our online banking application, your transactions and personal information are secured by encryption software that converts the information into code that is readable only between you and us.

Privacy Policies – All banks are required to have privacy policies which require them to protect your information. Your confidential information is treated with the utmost care, meeting or exceeding federal and state mandates.

E-mail Communication – E-mail is generally not encrypted so be wary of sending and sensitive information such as account numbers or other personal information in this manner. If you receive an unscheduled or unsolicited e-mail purporting to be from us be cautious—take the time to call us and make sure the e-mail was sent from us. We do have a secure e-mail system which can only be initiated from within the bank. You will be prompted to create an account, password and security question. Once created, you can use this account whenever you receive a secure e-mail from us. If our system

determines your e-mail account is hosted on a secure server, you will not be prompted to log in to obtain the e-mail.

Signing Off – Always log off by using the online banking "logout" selection to ensure the protection of your personal information.

Be Aware – Crooks are trying to get your personal information—and they employ some ingenious methods. Don't respond to any unusual request for personal information—when you opened your bank accounts you already gave it. When in doubt, call us.

Identifying the Most Common Online Threats Understanding what criminals are trying to do over the internet is the first step in building a good defense. Most electronic fraud falls into one of these three categories. Experts advise: understand these to understand how best to protect yourself.

Phishing—Fraudulent e-mails purporting to be from your bank or a similar trusted source lures you to a copycat website (one that may look just like our web site. Once there you are instructed to "verify" certain personal information, which is then used to hijack your accounts and your identity. If you receive a suspicious e-mail, do not respond to the message and call us to inform us of the phishing scam. You may be asked to attach the fraudulent e-mail to one from you to the bank so that forensic work may be done to determine the actual sender.

Pharming—Also called "domain spoofing," this cybercrime intercepts internet traffic and re-routes it to a fraudulent site. Once there, the victim is asked to enter personal information, just as with Phishing.

Malware—This is software designed to infiltrate or damage a computer system without the owner's knowledge. Examples of malware (malicious software) include computer viruses, worms, Trojan horses, spyware and adware.

Learning More:
Drop by any of our branches to learn more about online banking and the security measures that are in place for your protection. Or contact any of these financial industry regulators.

Federal Deposit Insurance Corporation
http://www.fdic.gov
Board of Governors of the Federal Reserve System
http://www.federalreserve.gov
Federal Trade Commission
http://www.ftc.gov

The Federal Trade Commission's web site also has an educational pamphlet called **"Take Charge: Fighting Back against Identity Theft".**

The State of Vermont also maintains a list of recent phishing scams on its web site. Go to www.bisca.state.vt.us and click on **"Consumer Alerts"**.