Reported Theft of 1.2 Billion Passwords

Click here for the New York Times article for more information.

Consumers who may have used the same username and password for their online financial accounts as they used for other online websites should consider changing those credentials. Although initial reports say that financial institutions were not the target of the hackers who stole 1.2 billion passwords from over 420,000 websites, consumers tend to use the same username and passwords for multiple accounts. This potentially leaves them vulnerable to unauthorized access to their funds.

We also encourage consumers to be vigilant and review their accounts. Any unusual activity should be reported to their bank as soon as possible.

Consumers need to be aware of phishing scams that may try to take advantage of the security concerns that usually occur with news of data breaches, especially breaches of this scale. Do not respond to emails with links claiming that your account is in jeopardy. If you do have concerns with any service provider due to the possibility of a compromised account, SNBT encourages you to contact those businesses directly to avoid becoming a victim of a scam.

SNBT offers the following five tips for proactively protecting your online accounts:

1. Use a passphrase rather than a password. For example, you might create a passphrase such as "GroceryShoppingOnSaturdays".
2. Create strong passwords by substituting numbers for letters: for example, "1" for "L," "3" for "E," or "5" for "S." (0ct0b3r 13av35).
3. Consider using the first line of a song or rhyme such as "If you give a moose a muffin," which becomes "IUgaM00saMuf1n."
4. Password complexity and length are important. Most websites require at least 8 characters, but 12 is now recommended.
5. Avoid using the same credentials for multiple systems or websites. If you must, periodically change your password for financial sites or those that store your credit card information.

Advice about Changing Passwords After a Breach - If you have been notified that your information has been compromised, the first step you should take is securing your e-mail account by changing that password. Your e-mail is typically where all password resets for other accounts are sent. If a hacker has compromised those other accounts, it's possible they may have gained access to your e-mail as well. So the best advice is to secure the most critical account first, then all your other accounts.

Heartbleed FAQs - Answers to commonly asked questions regarding the Heartbleed bug with an emphasis for bank customers.