Protect Yourself from Fraud

Safeguarding customer financial and personal data is not only the responsibility of Newtown Savings Bank but also the responsibility of every customer. Common cyber threats include phishing (a high-tech scam that uses email to deceive customers into disclosing personal information) and spear phishing (targeted phishing directed towards a specific individual or group of individuals), malicious code (any type of harmful code or script that is intended to cause system vulnerabilities, back doors, security breaches, data theft, etc.), unpatched or outdated software and weak and default passwords. In this article, we'd like to advise you of some of the things you can do to protect your financial and personal data.

There are a number of simple steps you can take to protect yourself from the potential loss of your personal and financial information. Some tips to protect your online security include:

Protecting Your Online Identity

- For online access to your bank account or other sensitive financial information, you should choose strong passwords or even use a passphrase instead of a password. Weak passwords include words found in the dictionary and readily available personal information (*e.g.* social security numbers, phone numbers, addresses, etc.). The best passwords contain uppercase and lowercase letters, numbers and special characters. If you need help, there are also online tools you can use to generate a password for you.

- Try using a passphrase instead of a password. Passphrases create much longer passwords and can be a song lyric, quote from your favorite novel or movie, or even the punchline to a joke. For example, you could use the phrase "I love my '09 Honda Civic" and derive a easy to remember unique password - Ilm'09hc.

- Change your password regularly and NEVER share it!

- Don't keep a written list of passwords on your computer, mobile device or on a sticky note. Doing so makes you an extremely attractive target for hackers.

- Don't use the same password for multiple accounts or services. Commercially available password manager tools are available to help you keep track of them.

- Organize your passwords in separate groups by using a different system for creating passwords for different types of websites, such as banking, social networking and other sites. Should a hacker crack one password, they won't immediately be able to crack all of them.

- When available, you should always use two factor authentication which provides an extra layer of security known as "multi factor authentication". This authentication method requires not only a password and username but also something that only the user knows or has on them.

- If you have been the victim of a data breach, you should contact the Bank and immediately change your passwords.

Some Other Tips to Protect Yourself

- You should use a firewall at all times, especially when performing banking activities. A firewall is a network device which blocks certain network traffic, forming a barrier between a trusted and an untrusted network. Firewalls also block dangerous programs, viruses or spyware before they can infect your system.

- Encrypt and Back Up your Data (including your email and files) for your desktop, laptop or mobile device. Data can be encrypted on a USB drive or a SIM card and backed up on the cloud. Also, don't forget to delete old files from cloud backups.

- Secure your wireless network using a password to prevent an unauthorized individual from gaining access.

- When finished using your computer, laptop or other device, you should always remember to turn it off. Leaving them on and connected to the internet leads to the possibility of a rogue attack.

- Don't perform financial transactions on an unsecured network (*i.e.* airport Wi-Fi or a coffee shop).

For additional information, we recommend that you take a look at some recent advice from the FDIC on *A Bank Customer's Guide to Cybersecurity*.