INSTITUTION FOR SAVINGS
BUILDING STRONGER COMMUNITIES TOGETHER SINCE 1820.

"Do I really Need a Strong Password?"

In a word: YES!

Passwords are one of the critical problems in cybersecurity today. They are too easy to guess. They are too easy to break. A significant percentage of privacy breaches are caused by weak, stolen, or reused passwords. The following are security guidelines to help mitigate some of the risks.

DO:

- ✓ **Make Your Password Long**
  Minimum of 8 characters, 12 or more are better. Complexity is nice, but length is key – a longer simple password is better than a shorter complex one. Each character you add to a password makes it an order of magnitude harder to attack via brute-force methods.

- ✓ **Use Passphrases**
  Even better than passwords, are passphrases. A collection of words that form a phrase or sentence, perhaps the opening sentence to your favorite novel or the opening line to a good joke, as long as it's not too well known. Another option is to use the first one or two letters of each word in the phrase to form a password that is easy to remember but hard to guess.

- ✓ **Use a Password Manager**
  We hate to break it to you, but your brain may not be the best password manager. Trying to remember a unique password for each of your online accounts is nearly impossible. Password managers like LastPass, Dashlane or KeePass, allow you to have strong and unique passwords for every site. A password manager is an app or program that generates, encrypts and stores passwords for your online accounts. Different password managers may work slightly differently, but most of them use what's called a "master password." Entering this one password will allow you to retrieve or use the passwords associated with your various accounts on the password manager site.

- ✓ **Keep Your Password Secret**
  Never tell your password to anyone (this includes significant others, roommates, coworkers, etc.). Never write your password down, especially not anywhere near your computer.

- ✓ **Use Two-Factor Authentication**
  Two-factor provides for an extra layer of security. Dedicated authentication apps are a lot safer than just getting a code over SMS, but both are safer than a password alone.

DON'T:

- ✓ **Use Words That Can Be Found in the Dictionary**
  Password-cracking tools freely available online often come with dictionary lists that will try thousands of common names and passwords.

- ✓ **Use Unacceptable Passwords**
  Never use personal information, such as names and birth dates, or keyboard patterns, like qwerty and 12345. Particularly avoid sequences of number in order or repeating characters, such as mmmm3333.

- ✓ **Repeat Passwords**
  Don't use the same password in more than one place. A compromise at one site may make it that much easier to compromise your password on a completely different and unrelated site.

- ✓ **Never use the password you have picked for your email account at any online site.** If you do, and an e-commerce site you are registered at gets hacked, there's a good chance they will get access to your email. From reading emails, hackers can determine your banking and credit card accounts. They can then go to one of those sites and request that a password reset be sent to your now compromised email account.

Any password that has previously been compromised is no longer safe to use.

Questions? Call us at 978-462-3106 or email us at info@institutionforsavings.com.