INSTITUTION FOR SAVINGS

BUILDING STRONGER COMMUNITIES TOGETHER SINCE 1820.

CHOOSING A SECURE PASSWORD

A significant percentage of 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**
  Password managers, like LastPass or 1PAssword, allow you to have strong and unique passwords for each and every 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:

- **Do not 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.

MORE---

- Unacceptable Passwords
  Never use personal information, such as names, and birth dates, keyboard patterns, like qwerty or 12345. Particularly avoid sequences of numbers in order. 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've 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 a password reset be sent to your now compromised email account.

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