Create strong passwords

If someone steals your passwords, they can use your name to open new credit card accounts, apply for a mortgage, or pose as you in online transactions. To prevent this, you can do the following

- Follow 6 steps to build a strong password
- Learn what makes strong passwords
- Avoid common password strategies that fail

6 steps to build a strong password

The strongest passwords look like a random string of characters to attackers. But random strings of characters are hard to remember.

Make a random string of characters based on a sentence that is memorable to you but is difficult for others to guess.

1. **Think of a sentence that you will remember**
   Example: "My son Aiden is three years old."
2. **Turn your sentence into a password**
   Use the first letter of each word of your memorable sentence to create a string, in this case: "msaityo".
3. **Add complexity to your password or pass phrase**
   Mix uppercase and lowercase letters and numbers. Introduce intentional misspellings.
   For example, in the sentence above, you might substitute the number 3 for the word "three", so a password might be "MsAi3yo".
4. **Substitute some special characters**
   Use symbols that look like letters, combine words, or replace letters with numbers to make the password complex.
   Using these strategies, you might end up with the password "M$8ni3y0."
5. **Test your new password with Password Checker**
   Password Checker evaluates your password's strength as you type.
6. **Keep your password a secret**
   Treat your passwords with as much care as the information that they protect. For more information, see 5 tips to help keep your passwords secret.

Qualities of strong passwords

Length

- Each character you add to your password increases the protection it provides.
- 8 or more characters are the minimum for a strong password; 14 characters or longer are ideal.

Complexity

- The greater variety of characters that you have in your password, the harder it is to guess.
- An ideal password combines both length and different types of symbols.
- Use the entire keyboard.

Easy to remember, hard to guess

- The easiest way to remember your passwords is to write them down.
- It is OK to write passwords down, but keep them secret so they remain secure and effective.

Password strategies to avoid

To avoid weak, easy-to-guess passwords:

- **Avoid sequences or repeated characters**
  "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not make secure passwords.
- **Avoid using only look-alike substitutions of numbers or symbols**
  Criminals will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0$0ft" or "P@ssw0rd".

  These substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case.
- **Avoid your login name**
  Don't use any part of your name, birthday, social security number, or similar information for your loved ones.

  This type of information is one of the first things criminals will try, and they can find it easily online from social networking sites, online resumes, and other public sources of data.
- **Avoid dictionary words in any language**
  Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, profanity, and substitutions.
- **Avoid using only one password for all your accounts**
  If your password is compromised on any one of the computers or online systems that use it, you should consider all of your other information protected by that password compromised as well.

  It is critical to use different passwords for different systems.
- **Be careful with password recovery questions**
  Many Web sites offer a "password " service that lets you provide the answer to a secret question. If you forget your password, the service will send it to you if you can remember the answer to your secret question.

  The questions are often random, but sometimes the answers to these questions are freely available on the Web. Choose your questions carefully or make up the answers.
- **Avoid using online storage**
  If criminals find your passwords stored online or on a networked computer, they have access to all your information.