

## **Advanced password Tips and Tricks**

by Whitney Merrill

Legal Fellow, Division of Privacy and Identity Protection, FTC

Time to create another password? Make it a secure one. A little extra attention when you create a strong password can prevent an attacker from getting access to your account.

Your password should be long, complex, and unique. Here are additional steps you can take to help create strong passwords and secure your accounts:

- Avoid common words, phrases, or information. Don't use information available to others like your birthday, phone number, or Social Security number. Attackers often use a dictionary of previously exposed passwords and information gathered from the internet to help them guess a password.
- Change passwords quickly if there is a breach. Attackers who steal data from companies often obtain password information. If you receive a notification from a company about a possible breach, change that password and any account that uses a similar password immediately.
- Consider a password manager. Most people have trouble keeping track of all their passwords. Consider storing your passwords and security questions in a password manager, an easy-to-access application that allows you store all your valuable password information in one place. Use a strong password to secure the information in your password manager.

What about security questions? If you forget your password, many companies require you to answer security questions to regain access. Here are some tips to make sure an attacker can't use your security questions as a way to get into your account:

- Select security questions where only you know the answer. Many security questions ask for answers to information available in public records or online, like your zip code, mother's maiden name, birth place. That is information a motivated attacker can obtain.
- Don't use answers to security questions that can be guessed. An attacker can guess the answer to a security question that has a limited number of responses (dates, colors, states, countries). Avoid questions like "What state were you born in?" or "What color was your first car?" which allow an attacker to guess all possible answers.
- Don't give a generic answer to a security question. Find an answer to a security question that you will remember but is also more complicated than a generic word. For example, if the security question asks "What is your favorite childhood memory?" the answer "watching the Dodgers with my mom" is more secure than "baseball."