Password Do's and Don'ts

Here are a few tips for creating strong passwords. Take a moment to review these, and consider strengthening some of your passwords if they fall short.

-Create unique passwords that that use a combination of words, numbers, symbols, and both upper- and lower-case letters.

-Do not use your network username as your password.

-Don't use easily guessed passwords, such as "password" or "user."

-Do not choose passwords based upon details that may not be as confidential as you'd expect, such as your birth date, your Social Security or phone number, or names of family members.

-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. If you must use dictionary words, try adding a numeral to them, as well as punctuation at the beginning or end of the word (or both!).

-Avoid using simple adjacent keyboard combinations: For example, "qwerty" and "asdzxc" and "123456" are horrible passwords and that are trivial to crack.

-Some of the easiest-to-remember passwords aren't words at all but collections of words that form a phrase or sentence, perhaps the opening sentence to your favorite novel, or the opening line to a good joke. Complexity is nice, but length is key. It used to be the case that picking an alphanumeric password that was 8-10 characters in length was a pretty good practice. These days, it's increasingly affordable to build extremely powerful and fast password cracking tools that can try tens of millions of possible password combinations per second. Just remember that each character you add to a password or passphrase makes it an order of magnitude harder to attack via brute-force methods.

-Avoid using the same password at multiple Web sites. It's generally safe to re-use the same password at sites that do not store sensitive information about you (like a news Web site) provided you don't use this same password at sites that are sensitive.

-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 someone will be reading your e-mail soon.

-Whatever you do, don't store your list of passwords on your computer in plain text. My views on the advisability of keeping a written list of your passwords have evolved over time. I tend to agree with noted security experts **Bruce Schneier**, when he advises users not to worry about writing down passwords. Just make sure you don't store the information in plain sight. The most secure method for remembering your passwords is to create a list of every Web site for which you have a password and next to each one write your login name and a clue that has meaning only for you. If you forget your password, most Web sites will email it to you (assuming you can remember which email address you signed up with).

-One thing to note about password storage in Firefox: If you have not enabled and assigned a "master password" to manage your passwords in Firefox, anyone with physical access to your computer and user account can view the stored passwords in plain text, simply by clicking "Options," and then "Show Passwords." To protect your passwords from local prying eyes, drop a check mark into the box next to "Use Master Password" at the main Options page, and choose a strong password that only you can remember. You will then be prompted to enter the master password once per session when visiting a site that uses one of your stored passwords.

-There are several online third-party services that can help users safeguard sensitive passwords, including LastPass, DashLane, and 1Password that store passwords in the cloud and secure them all with a master password. If entrusting all your passwords to the cloud gives you the creeps, consider using a local password storage program on your computer, such as Roboform, PasswordSafe or Keepass. Again, take care to pick a strong master password, but one that you can remember; just as with the Firefox master password option, if you forget the master password you are pretty much out of luck.