7. How to create a secure password?

For almost every account that you make online, you are required to make a *secure* password. Choosing one that's difficult for others to figure out requires the creation of unlikely letter and number combinations. Fortunately, crafting hard-to-crack and easy-to-remember passwords is pretty straightforward.

In this article we would like to introduce 4 different methods to choose a secure password.

Method 1 of 4:
Applying Password Basics

Choose a password that no one will easily guess or hack. Don't use a word or phrase of special importance to you—like a birthday or family member. That's the kind of information that can be discovered by someone doing a little digging.
→ Also, do not use default passwords, as they are easily cracked. Some default passwords include *password*, *password123*, *1234*, *admin*, and *guest*, among others. These can be found across the internet.

Do not share passwords. This is an open invitation to your online accounts, and it's often exploited to accomplish online identity theft.

Make sure your password is long. It should be at least eight-to-10 characters long, and longer passwords are even more secure. Some sites or applications may limit the password length, however.

Use at least one capital letter and one lowercase letter in your password. The capital and lowercase letters should not be grouped together. Mixing them up makes the password more difficult to predict. This kind of strategy might lead to "JeCaMiJe_" in the first example or "HouseOnSpooner#1500" in the second example.

Use spaces in your password. Many password systems don't allow actual spaces, but it can be useful to insert one into the middle of a password with systems that do. Alternatively, an underscore "_" or two can serve a similar function.

Generate similar but distinct passwords for separate accounts. You can use similar base words to help you remember your passwords easily without making them too easy to crack. So "JeCaMiJe_" might be modified as "my kids JeCaMiJe," "HouseOnSpooner#1500" might become "1500*my first House On Snooper."

Make sure your password is written down and kept in a safe place. Choose a location away from your computer (and from prying eyes), but make sure you can easily access it. If you forget your password, you can retrieve it without much trouble.

- When writing your password down, consider coding it with an offset pattern to make your password more difficult for others to decipher. Thus ri7%Gi6_ll might be written as 2tk9&Ik8_nn (where the offset for the coding is indicated by the first character, in this case +2). This would mean that each subsequent coded

character is two alphabetical letters or numbers greater than the actual password character.

Method 2 of 4:
Creating a Secure Password

Create a sentence or phrase as the basis for your password. This is a useful starting point for making a password that's complex and difficult to guess while easy for you to remember. Also remember that your password should ultimately be lengthy (at least eight to 10 characters) and include a wide variety of character types (upper and lower-case letters, numbers, spaces or underscores, etc.). While you should stay away from personally relevant information that others could easily identify, it's still convenient to create a password that you can recall without much trouble. Crafting a statement or sentence that will stick with you can serve as a useful basis for your password.

- One example of a mnemonic device is the Person-Action-Object (PAO) method developed by Carnegie Mellon computer scientists. Simply select an image or photograph of a memorable person performing an action with or to an object—and then put them all together to construct a phrase (however amusing or nonsensical). By selecting characters (e.g. the first three letters of each word) from said phrase, you can develop a password that's readily recalled.

Use your sentence or statement to craft an easily memorable password. By taking certain letters from your phrase, you can assemble a password that's easy to remember (e.g. by using the first two or three letters from each word in your phrase and putting them together in order). Make sure your statement or sentence includes upper and lower case letters, numbers and special characters.

Create a complex but memorable sequence of words and/or letters. You can use a phrase or series of letters that is seemingly random but nevertheless easy to remember. The easily memorized series of letters can form a "base word" to which you should add symbols or numbers.

- If your children are Jessie, Cassey, Michael and Jenny, your base word might be "jecamije"—the first two letters of each name combined. If your first house was on Spooner Street, a base word might be "houseonspooner."

Use at least one letter, number and special character in your password. So, you could add an underscore (or other random punctuation) and numbers to create "jecamije_." Or you can add a symbol to the word to make "houseonspooner#1500."

Memorize your secure password. For example, a sentence like "My mother was born in Kansas City, Missouri on January 27th" might become a password like MmwbiKC,MOoJ27. Or a sentence like "The radio show begins at 9:10 AM on Mondays, Wednesdays and Fridays" could become "Trsb@0910oM,W&F."

Consider using your computer's Character Map/Character Palette to (optionally) insert special characters into your password. Windows can find these options under the Start Menu by clicking All Programs, clicking Accessories, clicking System Tools and finally selecting Character Map. Mac users simply need to select Edit at the top of their browser menu and subsequently select Special Characters at the bottom of the Edit menu. You can then replace some of your letters with special symbols to make your password more difficult to guess.

- These symbols can replace more commonly used characters, but it's worth noting that some sites' password system won't accept all of the available symbols. By way of example, "SüΠSƮıηξ" could be used to replace "Sunshine."
- Remember that you'll have to actually re-enter this password when attempting to access a website or application, so consider the difficulty associated with repeatedly accessing your character map when entering passwords. You may decide it's too much of a hassle.

Remember to update and vary passwords. You shouldn't be using the same passwords across your various logins, and you shouldn't use the same password for more than a few months at a time.

Method 3 of 4:
Using Password Managers

Select a password management program. This software will generally allow you to automatically handle a wide variety of passwords (for applications and websites) by simply entering one "master" password—significantly simplifying your memorization and organization responsibilities. Password managers will generate, remember and audit a variety of distinct, complex and secure passwords for each of your requested logins while allowing you to simply remember that one master password. Some of the most popular options include LastPass, Dashlane, KeePass, 1Password and RoboForm. A number of articles and websites offer thorough reviews of these and other programs.

Download and install a password manager. Specific instructions will vary depending on which program you select, so be sure to follow instructions carefully. Generally speaking, you'll need to visit the appropriate vendor website and click a "download" button before following the installation instructions associated with your operating system.

Set up your password manager. Again, the process will vary depending on the specific program. But the basic idea is to set up a complex master password that allows the production and/or maintenance of multiple, site and application-specific passwords to access their destinations. Most popular programs are pretty user-friendly when it comes to core functionality.

Customize your preferences. Most of the best password managers will give you the option to either use your master password locally or synced across a variety of devices, so be prepared to determine what works best for you. You can also generally decide whether you wish the program to automatically log you in to sites

and whether it audits your distinct passwords to ensure they're sufficiently different and changed on a regular basis.

Methods 4 of 4:
Passwords to Avoid

Avoid default passwords. Some of them are: password, guest, user, admin. They are widely available on the internet, and are disallowed by many computer systems.

Avoid number sequences. Sequences such as 1234, 911, 112, 31415, 27183, or 0000 can be easily guessed because they are very common sequences.

Use more complex obfuscation. Instead of using the password "pr0d@dmin" (a password compromised during the DigiNotar attack), use an anagram such as "0@imdndpr".