

## 10 Easy Tricks to Create Unhackable Passwords

*Passwords are the lifeblood of online activity. With all that is available on the Internet, it's possible to have tens if not hundreds of sites to which you need credentials for. If you put a great deal of your business online, the risk potential is even greater. So, how can you create strong passwords that will keep unwanted guests out of your accounts? This all depends on how creative you are. Here are several ideas that can help you implement credentials to protect your data.*

### 1. Eight Characters Minimum

Many experts believe that passwords should be approximately eight characters long. In fact, a lot of websites you come across will require this as a minimum.

Two reasons why this is a magical number are because: 1) it makes it easier to remember and 2) more difficult to crack. Each character beyond eight increases difficulty for hackers as well as yourself.

You could have a 24-character password so long as you have the capacity to remember it a few months down the road.

Bear in mind that not all systems can utilize spaces in the password. Filling in the blanks can be done using special characters or numbers.

### 2. Keep Away from Dictionary Words



Using properly spelled words from the dictionary is considered a poor practice. For example, you wouldn't want to have a password as, "default" or "analytical." These are much easier to hack.

A lot of programs are designed to force a word into the credentials starting with every one of them that is in the dictionary. Something you thought was once clever may give someone access to your information.

This is especially true if the word you chose was somehow related to your business or personal lifestyle.

### 3. No Family Names

Names of kids, spouses and pets should be avoided at all costs. This is another form of easy-to-guess information. It's also one of the first things many people will try when attempting to gain access to your data.

While this may be easier for you to remember, it may also be your undoing if someone knows you or your family. If you truly want to use the name of someone you'll remember, go back in time.

Find an ancestor from more than a hundred years ago who is obscure.

### 4. Use Special Characters in Words



One trick that many people utilize is special characters to fill in for letters of words. For example: If used the name "Charles" as your password, you would change it to, "Ch4r!3\$."

Replace the letters with characters that look similar, such as "S" and "\$". This makes remembering the name or word easier, especially if you're familiar with recognizing numbers and characters.

Type out the word, then look at your keyboard. Several letters can easily be swapped out making the password much more secure.

### 5. Using Passphrases, Not Passwords

A passphrase is often easier to remember and much more difficult to crack than just a word. Phrases are favorite sayings, titles of books or anything else that involves more than a single word.

Once you start replacing letters with numbers and adding characters, the phrase becomes nearly impossible to guess or hack. Just make sure it's a phrase that you're fond of to make it memorable.

For instance, a bank password could be, "1\$l0v3\$m0n3y!" One glance and you can see the text, "I love money" with dollar signs filling in the blanks.

## 6. Using Numbers to Finish Words



You can use numbers and special characters to finish certain words of the password to help you remember it. For instance, “I hate olive oil” could look like: “lh80liv30i!” How about, “ll0v3B33fS2!” in place of “I love beef stew?”

Although you are somewhat limited to what words you can formulate, you’re only limited by your imagination. The more creative you are, the harder it will be for others to crack the phrase.

## 7. Condensing Favorite Sayings

You can condense your favorite phrase or quote that uses a number to help you create strong passwords. For example, the song, “Wake me up before you go” could look like: “WkMeUpB4UGo!” The exclamation point signifies the song is by “Wham!”

Bible verses are also a common method among many as you use the actual verse of the scripture.

Condensing may take a bit of imagination depending on the word you’re using. However, this form of password generation is very effective.

## 8. Removing the Vowels and Add Numbers

If you want to use a word that is easier for you to remember, remove the vowels and add a few numbers. Take a topic that you’re interested in and create a memorable factoid.

For instance if you like horses, the winner of the Kentucky Derby in 2009 was “Mine That Bird.” This could look like, “mnhthbrd2009” or perhaps “20mnhthbrd09” as your password.

As there are so many facts regarding any topic, it would be extremely unlikely for someone to figure it out.

## 9. Reversing the Website Name

Reversing the name of the website you're using can help you remember the password that goes to the account. Once you add in memorable characters, the password could be very difficult to crack.

For example, a password for a Google Gmail account could be "Elg00g!2016." This is Google backwards, using "0" for "o," an "!" as a special character and a significant year.

This may be an effective process because it helps you generate a new memorable password for each site you use.

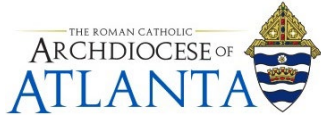
## 10. Using a Password Generator



Many websites today have a method of generating a password for you. There are also apps you can download for your computers and mobile devices. Usually, these will generate a completely random structure to use that creates a secure login credential.

Since many of these tools base the creation on random lengths and characters, it's one of the best forms of developing a password. However, they are usually not that easy to remember without writing them down.

With most of these systems, you'd have a better chance of winning the lottery than seeing the same password twice.



## Keep it Complex

The more complex the password is, the more difficult it is to hack. Unfortunately, this may also make it much more difficult to remember. It's the price you pay if you want to create strong passwords to keep your sites and accounts safe.

Take measures to protect yourself as well as the organization. If you care about the security of your online business, [you should read our earlier article on the 7 deeply upsetting signs your data has been tampered with and how to prevent it](#). The last thing you'll want is someone gaining access to your data and stealing identities, financial information or confidential business data.

