What is a “smart” password? A smart password strikes a balance between being **easy-to-remember** and **hard-to-guess**. The best practices below will help you create smart passwords, but remember to refer to your firm’s password policy for specific guidance on the number of characters required and any restrictions to keep in mind.

# Easy-to-Remember

|  |  |
| --- | --- |
| Step 1 | Instead of using a pass*word*, create a pass*phrase.* For example, **sink or swim** or **once upon a time**.  To make it easy to remember, choose a passphrase that has personal meaning for you but isn’t something that could be easily guessed by walking into your office.  **Twist and shout** |
| Step 2 | Once you’ve chosen a passphrase, use letter substitutions to incorporate numbers, capital letters, and special characters into your passphrase. Remember to refer to the requirements specifically outlined in your firm’s password policy.  First, add capital letters:  **TwistAndShout** |
| Step 3 | Next, add numbers:  **Tw1stAndSh0ut** |
| Step 4 | Finally, add special characters:  **Tw1st&Sh0ut!** |

# Hard-to-Guess

Here are a few best practices to help keep your password hard to guess:

|  |  |
| --- | --- |
|  | Don’t use information that is easily accessible or easy to guess, such as your pet’s name, your children’s names, addresses, or birthdates. |
|  | Don’t use the same password for every system. |
|  | Don’t store your password in an unsecured location, including paper on your desk! |