# How to Build Strong Passwords

**Thought exercise: which of these two passwords do you think is the strongest?**

**Asweaqf34$$a** **VS** **unclebudsbestcatfish**

Given its randomness and complexity, the first option must be the strongest of the two, right? Actually, no. The second password, though it doesn't contain random characters or upper and lowercase letters, is the superior option. Don't believe it? Head over to a password strength checker such as "How Secure Is My Password" or Kaspersky's "Secure Password Check" to see for yourself.

The truth is, both passwords offer elite strength and would serve as great options for any type of account. But which one is the easiest to remember? Which one is easiest to type? The key to strong password creation is not complexity, but length and memorability.

## Strong passwords in four easy steps:

### STEP ONE

Pick a passphrase like in the example above (*unclebudsbestcatfish*). You're welcome to add numbers or special characters to strengthen it (and some systems will require a variety of characters), but it's generally best to take an ***"easy to remember, hard to guess"*** approach.

### STEP TWO

Ensure it's at least 12 characters long. Of course, this may be limited by the requirements of by each login system but the longer, the better.

### STEP THREE

Never use it twice. Using the same password twice is a great way for multiple accounts to be compromised, especially if that password is associated with a username that is your email.

### STEP FOUR

Repeat for all accounts. Easy peasy. New passwords for each account that are easy to remember but hard to guess.

Please protect important information on the MIM portal.
Make sure your passwords are secure!