

## Top 10 Tips for Password Security.



### Know your guidelines.

Your organization has its own policies for password security. Know them and push them to the limits! If they allow passwords of 8-20 characters, always make it 20.



### Longer is better.

New research says longer passwords are harder to guess. "Wine" is short; "1998dontdrinkwinewithbadchee\$e-2002worstweddingEVER" is long.

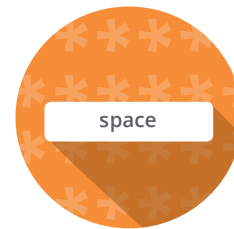
### Use uncommon sense.

Substitute uncommon words for common ones. Try to avoid words found in dictionaries, if possible.



### Think phrases, not words.

A space is just another character in a string, so long phrases with spaces are effectively single unsearchable words. A phrase like "dinosaurs don't dance disco" is unique and memorable.



### Choose something only you know.

Think of something that makes sense only to you. This could be a private joke, a childhood nickname, or an association only you would make.



### Do not write it down.

Put down the Post-Its! Choose a password you can remember without writing it down. If you must, write down a hint that would only make sense to you.

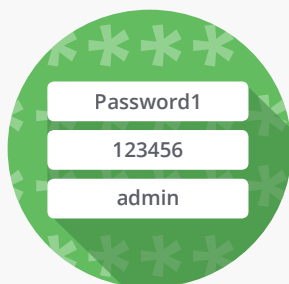
### Never repeat.

Do not reuse passwords. If you already used a password for another account, or used it previously for the same account, invent a new password.



### Never share passwords.

Passwords are like toothbrushes. Change them regularly and never share them with anyone!



### If it has not worked before ...

Know your common passwords. "Password1," "123456," "admin," and "qwerty" are all common passwords that hackers will always guess.



### Avoid using common substitutions.

It has become common practice to replace letters with similar-looking numbers and symbols. These are known substitutions and will not help make a password stronger.