7 Sm@rt Th1n9s Ab0ut Pas$w*Rds

1. The average password is … pretty terrible. “The overwhelming majority of users choose passwords that contain lower case letters only (i.e. no uppercase, digits, or special characters) unless forced to do otherwise,” say Microsoft researchers. What’s worse, there’s a high statistical likelihood that a password is either ‘password’ or ‘123456’ or ‘qwerty’.

2. Security experts generally agree that a strong password must have four components: length (longer = stronger), a variety of character types and cases, randomness, and uniqueness. "Every password you use can be thought of as a needle hiding in a haystack,” says data security expert Steve Gibson. “After all searches of common passwords and dictionaries have failed, an attacker must resort to a ‘brute force’ search— ultimately trying every possible combination of letters, numbers and then symbols until the combination you chose, is discovered.”

3. According to research from Microsoft, the average computer user has 6.5 passwords, each of which is shared across 3.9 different sites. Each user has about 25 accounts that require passwords, and types an average of eight passwords per day.

4. The average password has a bit strength of 40.54. A password with 40 bits of strength would require 240 attempts to exhaust all possibilities during a brute force search. However, a hacker using a brute force search will typically have to try half the possible passwords before finding the correct one. (Password-detection programs can run several billion password guesses per second.) Adding one bit of entropy (i.e. one character) to a password doubles the number of guesses required, which is why longer passwords are far more secure. The National Institute for Standards and Technology recommends a password strength of 80 bits.

5. You don’t need a strong password for every site. Just for the important ones. Slate.com tech writer Farhad Manjoo says four or five passwords will suffice, as long as your strong and unique ones are used for the important accounts. “It's perfectly OK to repeat passwords on sites that don't need to be kept very secure,” says Manjoo.

6. Manjoo has a helpful shortcut for creating passwords that are both strong and easy to remember. “Start with an original but memorable phrase … and turn [it] into an acronym. Be sure to use some numbers and symbols and capital letters, too. I like to eat bagels at the airport becomes Ilteb@ta, and My first Cadillac was a real lemon so I bought a Toyota is M1stCwarlsIbaT.”

7. Owners of web-based services and apps have—and should be pressured to use—additional tools to ensure the security of user data. As far as preventing brute force attacks, a simple and effective solution is to have an auto-lockdown system in place when the wrong password is entered multiple times in a row.