How Passwords are Cracked

Dictionary

This isn't a dictionary like Webster's. It's a list of character sequences commonly used in passwords including standard dictionary words, foreign language words, dates, and keyboard patterns.

Keyboard

Alphanumeric

Transformations

People often try to strengthen passwords by transforming a seed word — e.g., replacing "a" with "@" and "e" with "3". But, attackers know these tricks too and the same transformations are built into cracking tools.

Padding

Mixing Cases

Substitution

Combine

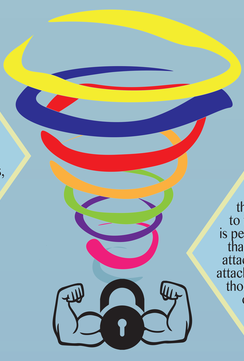
Combine several words and transformations into a longer password. Attackers can search for multi-word combinations also, of course, but the difficulty increases exponentially with the password length.

	Time to guess
toaster	1 sec
tOaSTer	2 min
t0@$t3r	4 min
Toast5!	15 min
toaster51!	28 hours
toa56p*%%%ster	15,000 centuries

*These times were obtained by running John the Ripper software ont he md5 hashes of these passwords, the final time was estimated assuming 100 trillion guesses/second

Should I use a passphrase?

Phrases of several words are better than short passwords. But, beware of common phrases. Cracking tools know about song lyrics, poems, movie quotes, and the rules of language grammar too!



Longer is better

Every character you add to your password multiplies the number of guesses needed to find it. Even if your password is perfectly random, if it is shorter than 12 characters, a powerful attacker can crack is using brute attack. With 16 random characters, though, even all the computers on Earth couldn't crack it in a century.

Things to Avoid

Names: Spouse, Friends, Kids, Pets

Words and Phrases: Dictionary, Patterns

Personal Information: Phone, SSN, Birthday, Address, License Plate, Bank Pin

Should I write down my password?

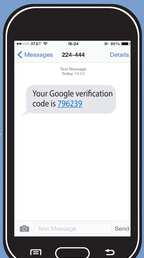
A strong password needs to be long & complex enough that you probably can't remember it! Writing down your passwords on a post-it stuck to your monitor is a bad idea. You should write down your passwords, but in some way that leaves out a part of the password that you can remember and store the written password in a safe place.

Multifactor Authentication

Adds a second layer of protection to access your information

1. Requires something you know (password)
2. Something you have (ID Card, verification code)

Need both of these to break into account



University of Virginia

For more information, visit www. suretysecurity.org

NSF
BY NC