Myth #1: Atleast 1 digit, 1 uppercase letter, ...

Myth: Making safe looking short passwords which satisfies all the dumb rules set by a website somehow will provide protection.
Truth:
There are plenty of such rules, and they don't gurantee that a password is safe. https://dumbpasswordrules.com/sites/
To achieve true security, focus on entropy—the actual randomness and length of your credential. The longer and more unpredictable the string, the higher its entropy, and the harder it is to break.
Instead of traditional "8 characters with one capital, number, and symbol", aim for a minimum of **16 characters or more**. 8-9 character passwords are just not long enough.
A long string of 5 to 6 unrelated words is extremely difficult for brute-force tools to crack, yet easy for humans to remember. (e.g., Horse-Purple-Hat-Run-Bay or CorrectHorseBatteryStapleTrainAlien).
https://xkcd.com/936/
You can check how long it'll take for an hacker to crack your password: https://lowe.github.io/tryzxcvbn/
Don't worry, it's a webapp, stays in your browser, nothing is being transferred to the servers.

Myth #2: Never write down a password

Myth: Written passwords can be stolen.
Truth: Never fear writing your passwords down. Ironically, the dread of a physical thief causes people to create weak, easily hackable passwords.
Security professionals agree—it is vastly safer to write complex, 16-character passwords in a physical notebook kept secure at home than to memorize weak passwords

Myth #3: The Password Rotation

Myth: It's always a good idea to change the password after every few months.
Truth: Don't bother updating your password regularly. Sites that require 90-day -- or whatever -- password upgrades do more harm than good. **Unless you think your password might be compromised, don't change it.**
Check if your password is already been leaked in a historical data leak: https://haveibeenpwned.com/Passwords
A survey of 200 people conducted by security outfit HYPR has some alarming findings.
For instance, not only did 72% of users admit that they reused the same passwords in their personal life, but also 49% admitted that when forced to update their passwords in the workplace they reused the same one with a minor change.
Forced changes don't trick hackers; they just exhaust users into creating predictable patterns that automated cracking tools guess.
Keep a strong password until a breach actually demands a change.

How Passwords Get Compromised

Phishing: Attackers don't always hack their way in; often, they just ask. Phishing involves deceptive emails, fake login pages, or spoofed messages designed to trick you into voluntarily typing your credentials directly into a hacker's database.
Network Sniffers: If you connect to insecure or unencrypted Wi-Fi (like public hotspot networks), attackers can deploy "sniffers". This software intercepts data moving through the airwaves, capturing any passwords transmitted in plain text.
Keyloggers: This malicious software or hardware silently infects a device to record every single keystroke you type. It captures your master passwords and PINs in real-time, completely bypassing browser encryption.
Brute force or Cracking: Using specialized software, hackers cycle through millions of character combinations or known common phrase lists per second until they guess the correct match.
Weak passwords: Short, predictable passwords that are just too easy to guess. Here's a list of some of the most common and unsafe passwords: https://en.wikipedia.org/wiki/List_of_the_most_common_-passwords
Reuse of passwords and use of compromised passwords: Reusing identical combinations across multiple platforms, or continuing to use a phrase after it has appeared in a known public data leak.
Clear text passwords in code and config. files: Leaving passwords written in plain, unencrypted text inside software source code or system configuration files where anyone with server access can read them.

Diceware method

Diceware method ensures that the words you're picking are actually random rather than what you think is random. The passwords are also super easy to remember.

When using this method, make sure that the passwords are **atleast 6 words long**.

Passphrases of six words or more are considered safe for online banking, or high-security applications.

Four words only provide about the same entropy as an 8 character password made up of random ASCII characters.

According to the creator of Diceware Reinhold, six words may be breakable by an organization with a very large budget, such as a large country's security agency. Seven words and longer are unbreakable with any known technology, but may be within the range of large organizations by around 2030. Eight words should be completely secure through 2050.

Here's a good explanation of how this method works by Computerphile:

Diceware & Passwords - https://www.youtube.com/watch?v=Pe_3-cFuSw1E

Interested in learning more about Diceware: https://theworld.com/reinhold/dicewarefaq.html

Diceware method is even recommended by EFF. https://www.eff.org/dice

Here are some Diceware lists you can use:

https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt

https://www.eff.org/files/2016/09/08/eff_short_wordlist_1.txt

https://www.eff.org/files/2016/09/08/eff_short_wordlist_2_0.txt

https://www.rubin.ch/pgp/diceware.doc

https://theworld.com/%7Ereinhold/beale.wordlist.asc

https://docs.google.com/spreadsheets/d/1KzFglmCKr4Q8AWOFE-5QFywOuSdRA_DDFs1M9BFXGZL4/edit?usp=sharing

Diceware method (cont)

https://web.archive.org/web/20080312042519/https://www.ibm.com/developerworks/library/s-pass2/index.html

If you are lazy, or just don't want to manage the effort to roll the dice, use these alternatives: https://www.mouseware.org/ https://diceware.rempe.us/#eff

Passwords and their strengths

elephant1234	58
cat-walrus_traiN	100
/*-+.\][-	44
doggo007	35
9452718465	26
trainNo.#4886	84
123@9	19
!smartkittly99%	91
sId	7
Fast&furiou$	75
*daydreamer	61

Myth #4: The Passwordless

Myth: One can completely eliminate passwords by switching to FaceID or fingerprint readers.

Truth: **Biometrics replace usernames, not passwords**. Your face or fingerprint identifies who you are, but your biometrics aren't a secret. Passwords are secrets.

Passwordless means passwords will be used less. It doesn't mean they disappear completely

Password cracking

There are commercial programs that do password cracking, sold primarily to police departments. There are also hacker tools that do the same thing like https://openwall.com/john/

As computers have become faster, they're able to test more passwords per second, *10s of millions per second*. These crackers might run for days, on many machines simultaneously. For a high-profile police case, they might run for months.

The efficiency of password cracking depends on two largely independent things: **computing power** and **efficiency**(ability to guess passwords cleverly, e.g. try the most common passwords first).

How to Choose a Password - Computerphile

Video: http://youtu.be/3NjQ9b3pgIg

Use Password generators

Use these password generators (make sure to **change password length to atleast 16 characters**): https://www.intuitivepassword.com/en/Tools/PasswordGenerator
https://us.norton.com/feature/password-generator#password_generator
Password generation **using abbreviated phrases**: https://rmmh.github.io/abbrase/
Password generator android app: https://play.google.com/store/apps/details?id=de.aregel.advancedpasswordgenerator

How to store Passwords

A **password manager** is a software program that prevents password fatigue by automatically generating, autofilling, and storing passwords. Here are some you can download and use for free:
RoboForm: It has been a reliable name in password management since 1999. Its free version offers great value with unlimited logins on a single device, and college students can even grab a full year of premium for free. For users on the move, it features a unique portability option that lets you run the app directly from a USB drive across different computers.
Bitwarden: Offers a transparent, community-vetted architecture ideal for modern, secure syncing across devices.
KeePass: Provides total isolation by storing passwords strictly in a local, encrypted database (no automatic syncing). As FOSS, its massive ecosystem of third-party plugins allows endless functionality extensions across almost any device, browser, or platform.

Definitely use MFA

If a site offers **multi-factor authentication(MFA)**, seriously consider using it. It adds a critical extra layer of defense by requiring multiple pieces of evidence to prove your identity:
What you know: Passwords, PINs, or security questions.
What you have: Mobile apps (software tokens), hardware keys, OTP SMSs, emails, or digital certificates.
Who you are: Biometrics like fingerprints or facial recognition.
Where you are: Location-based checks like your IP address or GPS.

Sources

https://cypressdatadefense.com/blog/password-security-risks/
https://web.archive.org/web/20220214162332/https://outline.com/-dqfuqL
https://grahamcluley.com/49-of-workers-when-forced-to-update-their-password-reuse-the-same-one-with-just-a-minor-change/
College students can get Roboform free for an year: https://www.roboform.com/promotions/college-verify
Check the strength of your password: http://password-checker.online-domain-tools.com/
Making a secure password by the security expert Bruce Schneier: https://web.archive.org/web/20190825152420mp_/https://boingboing.net/2014/02/25/choosing-a-secure-password.html
https://web.archive.org/web/20211228191634/https://arstechnica.com/information-technology/2014/03/diceware-passwords-now-need--six-random-words-to-thwart-hackers/