Passwords

A password (or pass phrase) is a sequence of letters, numbers, and/or characters used to protect your account or device from access by another entity.

Take a look at the list below.

Bad Passwords 2022

Password	Crack Time	Password	Crack Time	Password	Crack Time
password	< 1 second	666666	< 1 second	159753	< 1 second
123456	< 1 second	123321	< 1 second	1q2w3e4r	< 1 second
123456789	< 1 second	654321	< 1 second	54321	< 1 second
guest	10 seconds	7777777	< 1 second	pass@123	2 seconds
qwerty	< 1 second	123	< 1 second	222222	< 1 second
12345678	< 1 second	d1lakiss	3 hours	qwertyuiop	< 1 second
111111	< 1 second	777777	< 1 second	qwerty123	< 1 second
12345	< 1 second	110110jp	3 seconds	qazwsx	< 1 second
col123456	11 seconds	1111	< 1 second	vip	< 1 second
123123	< 1 second	987654321	< 1 second	asdasd	< 1 second
1234567	< 1 second	121212	< 1 second	123qwe	< 1 second
1234	< 1 second	gizli	10 seconds	123654	< 1 second
1234567890	< 1 second	abc123	< 1 second	iloveyou	< 1 second
000000	< 1 second	112233	< 1 second	a1b2c3	< 1 second
555555	< 1 second	azerty	< 1 second	999999	< 1 second

That is a list of the most common passwords pulled from hacked user databases, and beside each, the amount of time it would take a computer to break that password.

If you see your password(s) here, assume hackers have all information you have put on the web.

Why, you may ask, does it matter if someone hacks into my social media account, or my Shopping Rewards account, or even my phone? It matters for several reasons.

First, in many cases your information is not the only data at risk. Your phone is full of email addresses and phone numbers. Your Facebook account is linked to every single person you are friends with.

Secondly, your Shopping Rewards account has personal information that might help someone break into a different, more important, account. It is especially a problem if you reuse passwords on multiple sites.

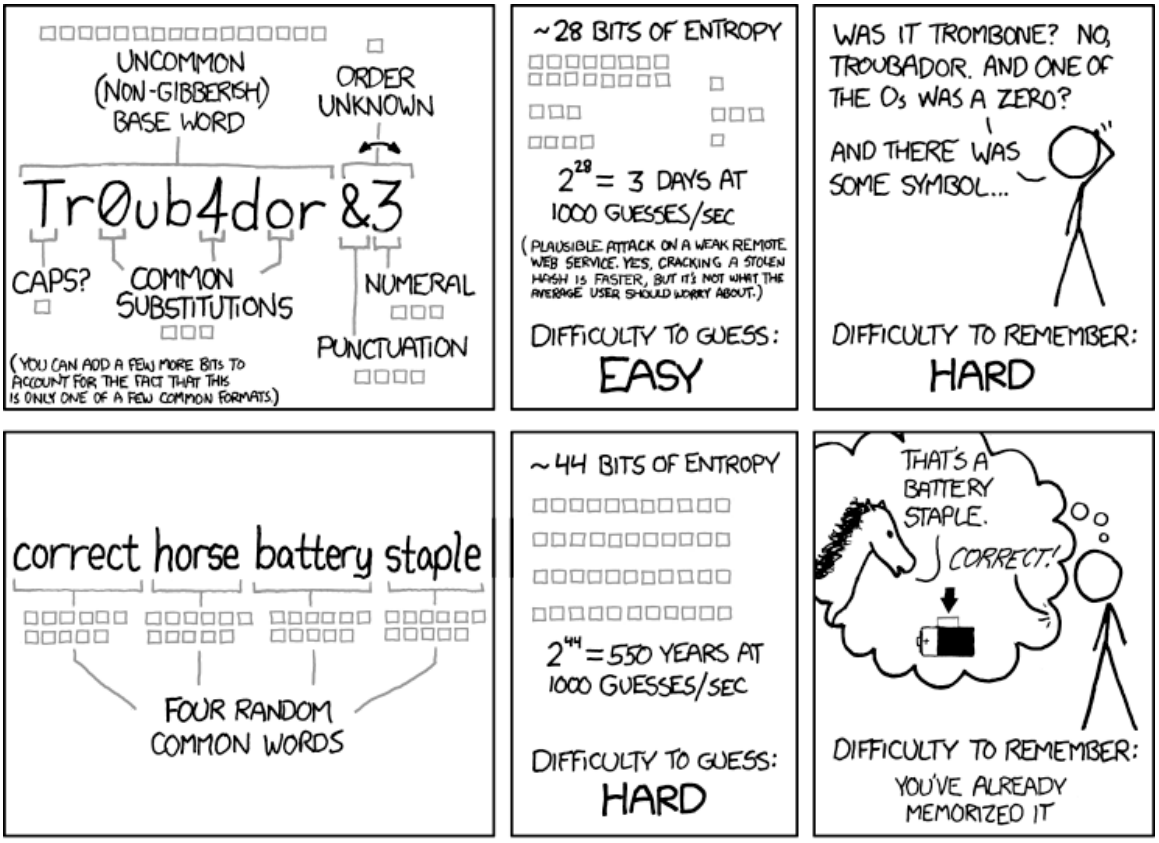
If a website is hacked and user information stolen, the first thing that thieves will do is try your usename / email address with your password on a variety of websites--including bank, credit card, and shopping websites.

Even if you use unique passwords for your important accounts, when you reuse passwords, you've given a hacker access to another account, where they can then collect *more* information about you—including information that could be used to reset your passwords.

Password Rules

Every website you log into should have a unique password. And those passwords should never be kept somewhere a person with bad intent could easily find them.

Unfortunately, the problem with computer passwords is that we have implemented a system that creates passwords that are hard to remember, but easy to crack.



The best password is the one in your password manager you never type, however, device passwords/passcodes *do* have to be typed, so you want one that is easy to remember, easy to type, but to guess.

My favorite method is to take objects in front of my computer and combine them into a password:

T-Rex Star Trek Shuttle
or
T-R3x_$tarTrek_Shuttle
or
TR3x-$tarTrek-Shuttle

If you're new to making strong passwords, I highly recommend going to a Password Strength Checker. These sites will help you learn what does—and does not—make a strong password.

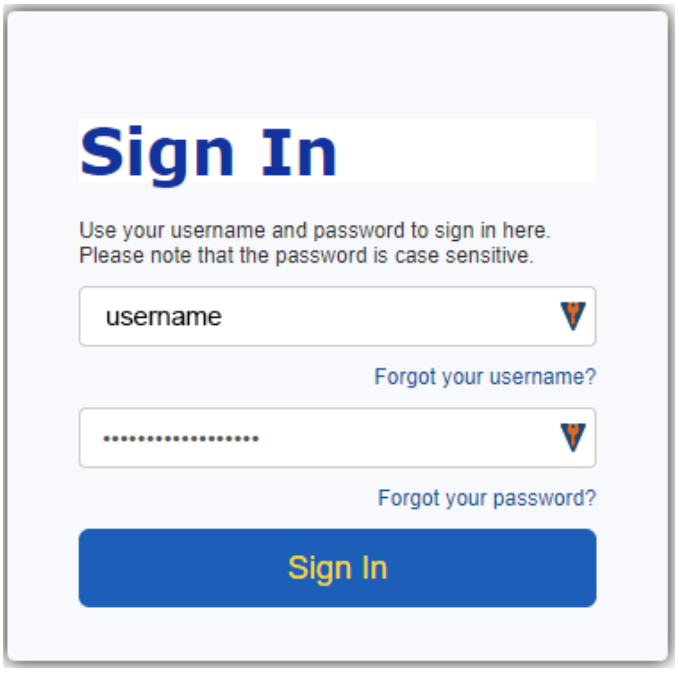
https://lastpass.com/howsecure.php
https://www.security.org/how-secure-is-my-password

Password Managers

A password manager is an encrypted, secure program that stores user names, passwords, and other information for websites, apps, and programs. Most password managers have browser add-ins that will make a logins completely painless.

How does a password manager work?

You enter your usernames and passwords into an encrypted "safe". Those login credentials are then saved so you can copy and paste or auto enter them as needed. You can also store additional information, such as account numbers and security questions.



Once you have set up your password manager and browser Add-In, when you visit a site you will be prompted to automatically inserting your information.

You should also have the ability to save new credentials to your password managers from your web browser, as you create them.