# Brute Force Attack: Definition and Examples

### What's a Brute Force Attack?

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account(s).

This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

## What do hackers gain from Brute Force Attacks?

Brute force attackers have to put in a bit of effort to make these schemes pay off. While technology does make it easier, you might still question: why would someone do this?

**Here’s how hackers benefit from brute force attacks:**

- Profiting from ads or collecting activity data
- Stealing personal data and valuables
- Spreading malware to cause disruptions
- Hijacking your system for malicious activity
- Ruining a website’s reputation

**Profiting from ads or collecting activity data.**

Hackers can exploit a website alongside others to earn advertising commissions. Popular ways to do this include:

- Putting spam ads on a well-traveled site to make money each time an ad is clicked or viewed by visitors.
- Rerouting a website’s traffic to commissioned ad sites.
- Infecting a site or its visitors with activity-tracking malware — commonly spyware. Data is sold to advertisers without your consent to help them improve their marketing.

**Stealing personal data and valuables.**

Breaking into online accounts can be like cracking open a bank vault: everything from bank accounts to tax information can be found online. All it takes is the right break-in for a criminal to steal your identity, money, or sell your private credentials for profit. Sometimes, sensitive databases from entire organizations can be exposed in corporate-level data breaches.

**Spreading malware to cause disruptions for the sake of it.**

If a hacker wants to cause trouble or practice their skills, they might redirect a website's traffic to malicious sites. Alternatively, they may directly infect a site with concealed malware to be installed on visitor's computers.

**Hijacking your system for malicious activity.**

When one machine isn't enough, hackers enlist an army of unsuspecting devices called a botnet to speed up their efforts. Malware can infiltrate your computer, mobile device, or online accounts for spam phishing, enhanced brute force attacks and more. If you don't have an antivirus system, you may be more at risk of infection.

**Ruining a website's reputation.**

If you run a website and become a target of vandalism, a cybercriminal might decide to infest your site with obscene content. This might include text, images, and audio of a violent, pornographic, or racially offensive nature.

# Types of Brute Force Attacks

Each brute force attack can use different methods to uncover your sensitive data. You might be exposed to any of the following popular brute force methods:

- Simple Brute Force Attacks
- Dictionary Attacks
- Hybrid Brute Force Attacks
- Reverse Brute Force Attacks
- Credential Stuffing

**Simple brute force attacks:** hackers attempt to logically guess your credentials — completely unassisted from software tools or other means. These can reveal extremely simple passwords and PINs. For example, a password that is set as "guest12345".

**Dictionary attacks:** in a standard attack, a hacker chooses a target and runs possible passwords against that username. These are known as dictionary attacks. Dictionary attacks are the most basic tool in brute force attacks. While not necessarily being brute force attacks in themselves, these are often used as an important component for password cracking. Some hackers run through unabridged dictionaries and augment words with special characters and numerals or use special dictionaries of words, but this type of sequential attack is cumbersome.

**Hybrid brute force attacks:** these hackers blend outside means with their logical guesses to attempt a break-in. A hybrid attack usually mixes dictionary and brute force attacks. These attacks are used to figure out combo passwords that mix common words with random characters. A brute force attack example of this nature would include passwords such as NewYork1993 or Spike1234.

**Reverse brute force attacks:** just as the name implies, a reverse brute force attack reverses the attack strategy by starting with a known password. Then hackers search millions of usernames until they find a match. Many of these criminals start with leaked passwords that are available online from existing data breaches.

**Credential stuffing:** if a hacker has a username-password combo that works for one website, they'll try it in tons of others as well. Since users have been known to reuse login info across many websites, they are the exclusive targets of an attack like this.

## Tools Aid Brute Force Attempts

Guessing a password for a particular user or site can take a long time, so hackers have developed tools to do the job faster.

**Automated tools help with brute force attacks** These use rapid-fire guessing that is built to create every possible password and attempt to use them. Brute force hacking software can find a single dictionary word password within one second.

Tools like these have workarounds programmed in them to:

- Work against many computer protocols (like FTP, MySQL, SMPT, and Telnet)
- Allow hackers to crack wireless modems.
- Identify weak passwords
- Decrypt passwords in encrypted storage.
- Translate words into leetspeak — "don'thackme" becomes "d0n7H4cKm3," for example.
- Run all possible combinations of characters.
- Operate dictionary attacks.

**Some tools scan pre-compute rainbow tables** for the inputs and outputs of known hash functions. These “hash functions” are the algorithm-based encryption methods used to translate passwords into long, fixed-length series of letters and numerals. In other words, rainbow tables remove the hardest part of brute force attacking to speed up the process.

## GPU Speeds Brute Force Attempts

Tons of computer brainpower is needed to run brute force password software. Unfortunately, hackers have worked out hardware solutions to make this part of the job a lot easier.

Combining the CPU and graphics processing unit (GPU) accelerates computing power. By adding the thousands of computing cores in the GPU for processing, this enables the system to handle multiple tasks at once. GPU processing is used for analytics, engineering, and other computing-intensive applications. Hackers using this method can crack passwords about 250 times faster than a CPU alone.

So, how long would it take to crack a password? To put it in perspective, a six-character password that includes numbers has approximately 2 billion possible combinations. Cracking it with a powerful CPU that tries 30 passwords per second takes more than two years. Adding a single, powerful GPU card lets the same computer test 7,100 passwords per second and cracks the password in 3.5 days.

## Steps to Protect Passwords for Professionals

To keep yourself and your network safe, you'll want to take your precautions and help others do so as well. User behavior and network security systems will both need reinforcement.

For IT specialists and users alike, you’ll want to take a few general pieces of advice to heart:

- **Use an advanced username and password.** Protect yourself with credentials that are stronger than admin and password1234 to keep out these attackers. The stronger this combination is, the harder it will be for anyone to penetrate it.
- **Remove any unused accounts with high-level permissions**. These are the cyber equivalent of doors with weak locks that make breaking in easy. Unmaintained accounts are a vulnerability you can’t risk. Throw them away as soon as possible.

# Passive Backend Protections for Passwords

**High encryption rates:** to make it harder for brute force attacks to succeed, system administrators should ensure that passwords for their systems are encrypted with the highest encryption rates possible, such as 256-bit encryption. The more bits in the encryption scheme, the harder the password is to crack.

**Salt the hash:** administrators should also randomize password hashes by adding a random string of letters and numbers (called salt) to the password itself. This string should be stored in a separate database and retrieved and added to the password before it's hashed. By salting the hash, users with the same password have different hashes.

**Two-factor authentication (2FA):** additionally, administrators can require two-step authentication and install an intrusion detection system that detects brute force attacks. This requires users to follow-up a login attempt with a second factor, like a physical USB key or fingerprint biometrics scan.

**Limit number of login re-tries:** limiting the number of attempts also reduces susceptibility to brute-force attacks. For example, allowing three attempts to enter the correct password before locking out the user for several minutes can cause significant delays and cause hackers to move on to easier targets.

**Account lockdown after excessive login attempts:** if a hacker can endlessly keep retrying passwords even after a temporary lockout, they can return to try again. Locking the account and requiring the user to contact IT for an unlock will deter this activity. Short lockout timers are more convenient for users, but convenience can be vulnerability. To balance this, you might consider using the long-term lockdown if there are excessive failed logins after the short one.

**Throttle rate of repeated logins:** you can further slow an attacker’s efforts by creating space between each single login attempt. Once a login fails, a timer can deny login until a short amount of time has passed. This will leave lag-time for your real-time monitoring team to spot and work on stopping this threat. Some hackers might stop trying if the wait is not worth it.

**Required Captcha after repeated login attempts:** manual verification does stop robots from brute-forcing their way into your data. Captcha comes in many types, including retyping the text in an image, checking a checkbox, or identifying objects in pictures. Regardless of what you use, you can use this before the first login and after each failed attempt to protect further.

**Use an IP deny list to block known attackers**. Be sure that this list is constantly updated by those who manage it.

**Active IT Support Protections for Passwords**

**Password education:** user behavior is essential to password security. Educate users on safe practices and tools to help them keep track of their passwords. Services like Password Manager allow users to save their complex, hard-to-remember passwords in an encrypted "vault" instead of unsafely writing them down on sticky notes. Since users tend to compromise their safety for the sake of convenience, be sure to help them put convenient tools in their hands that will keep them safe.

**Watch accounts in real-time for strange activity:** Odd login locations, excessive login attempts etc. Work to find trends in unusual activity and take measures to block any potential attackers in real-time. Look out for IP address blocks, account lockdown, and contact users to determine if account activity is legitimate (if it looks suspicious).

## How Users Can Strengthen Passwords against Brute Force Attacks

As a user, you can do a lot to support your protection in the digital world. The best defense against password attacks is ensuring that your passwords are as strong as they can be.

Brute force attacks rely on time to crack your password. So, your goal is to make sure your password slows down these attacks as much as possible, because if it takes too long for the breach to be worthwhile… most hackers will give up and move on.

Here are a few ways you can strength passwords against brute attacks:

**Longer passwords with varied character types**. When possible, users should choose 10-character passwords that include symbols or numerals. Doing so creates 171.3 quintillion (1.71 x 1020) possibilities. Using a GPU processor that tries 10.3 billion hashes per second, cracking the password would take approximately 526 years. Although, a supercomputer could crack it within a few weeks. By this logic, including more characters makes your password even harder to solve.

**Elaborate passphrases**. Not all sites accept such long passwords, which mean you should choose complex passphrases rather than single words. Dictionary attacks are built specifically for single word phrases and make a breach nearly effortless. Passphrases — passwords composed of multiple words or segments — should be sprinkled with extra characters and special character types.

**Create rules for building your passwords.** The best passwords are those you can remember but won't make sense to anyone else reading them. When taking the passphrase route, consider using truncated words, like replacing "wood" with "wd" to create a string that makes sense only to you. Other examples might include dropping vowels or using only the first two letters of each word.

**Stay away from frequently used passwords.** It's important to avoid the most common passwords and to change them frequently.

**Use unique passwords for every site you use.** To avoid being a victim of credential stuffing, you should never reuse a password. If you want to take your security up a notch, use a different username for every site as well. You can keep other accounts from getting compromised if one of yours is breached.

**Use a password manager.** Installing a password manager automates creating and keeping track of your online login info. These allow you to access all your accounts by first logging into the password manager. You can then create extremely long and complex passwords for all the sites you visit, store them safely, and you only have to remember the one primary password.