**How To Create Secure Passwords (PassPhrases)**

**Test your password at:**

[**https://aenigma10computers.com/security/**](https://aenigma10computers.com/security/)

**Five reasons why a passphrase is better**

1. Passphrases are easier to remember than passwords. A random collection of numbers and symbols can be difficult to keep track of, which can mean that users often make it simpler to remember them. A passphrase is usually not as hard to remember.
2. Passphrases are difficult to crack through brute force. Many password-cracking tools work to break down 10-character passwords. Since passphrases are longer, they can be much more secure and safe from these tools.
3. Passwords are easily hacked by password-cracking tools and robots as well as by humans. People do not like to change passwords and tend to stick to things that they can remember, making them more easily guessed.
4. Most major applications and OS (operating systems) allow for up to 127 characters and the use of passphrases for optimal security.
5. A passphrase can easily satisfy complex rules and requirements for passwords, as most allow for punctuation and uppercase and lowercase letters.

## **Passphrases: Supported by Industry Standards**

Passphrases are supported by industry standards such as the [NIST](https://www.fbi.gov/contact-us/field-offices/elpaso/news/fbi-tech-tuesday-strong-passphrases-and-account-protection#:~:text=Recent%20guidance%20from%20the%20National,For%20example%20TechTuesday2023Strengthen!) and the FBI, who both recommend the use of passphrases instead of passwords.

If you weren’t satisfied in your password strength rating, it’s time to create new and stronger passwords. Here are the best practices:

* A password should be at least 12 characters long (ideally 16 characters or more); our password-related research has found that 45 percent of Americans use passwords of eight characters or less, which are not as secure as longer passwords.
* A password should include a combination of letters (both uppercase and lowercase), numbers, and characters.
* **You must have a unique password for each online account.**
* A password shouldn’t include any of your personal information like your birthday or address, as [identity theft](https://www.security.org/identity-theft/) and [data breaches](https://www.security.org/identity-theft/what-is-a-data-breach/) can compromise such information. It’s also best not to include any information that can be accessed on social media like kids’ or pets’ names.
* A password shouldn’t contain any consecutive letters or numbers (i.e. ABCD, 1234, etc.)
* A password shouldn’t be the word “password” or the same letter or number repeated.

**Why Is Password Security Important?**

Not having secure passwords has its consequences, which include but are not limited to:

* After gaining access to a user’s credentials, many hackers will log into their accounts to steal more of their [personally identifiable information (PII)](https://www.security.org/identity-theft/what-is-pii/) like their names, addresses, and bank account information. They will use this information either to steal money from the user directly or to steal their identity. Identity theft can result in further financial losses or difficulty getting loans or employment.
* A hacker breaking into your accounts due to a weak password can compromise your privacy. For example, if you don’t change the default password of your IP security cameras, hackers may be able to log into your user account and watch you in your own home.
* For businesses, [hackers](https://www.security.org/antivirus/hackers/) can start disinformation campaigns against companies, sharing their data with competitors and storing it for a ransom1.

**Other Ways To Protect Yourself Online**

Aside from creating secure and unique passwords for all web accounts, there are other best practices to increase one’s [digital security](https://www.security.org/digital-safety/).

1. Use a **VPN**: While passwords keep unauthorized users out of accounts, Internet Service Providers can still track a user’s online activity as well as their devices’ private IP addresses. The only way to [hide web activity](https://www.security.org/vpn/browsing-history/) and IP addresses is to connect not directly to a public Wi-Fi network, but instead to [a VPN](https://www.security.org/vpn/), which stands for Virtual Private Network. Learn more about some of the [best VPNs](https://www.security.org/vpn/best/) such as [NordVPN](https://www.security.org/vpn/nordvpn/review/), all tested by our digital security experts.
2. Get **identity theft protection**: While a strong password can go a long way in protecting online accounts, there’s no single action that can protect a user’s personally identifiable information from identity theft. Rather, [top identity theft protection](https://www.security.org/identity-theft/best/) software monitors key criminal and financial areas for users’ personal information.
3. Use **antivirus software**: [The best antivirus software](https://www.security.org/antivirus/best/) can scan computers, phones, and tablets for malware, [ransomware](https://www.security.org/antivirus/ransomware/), viruses, [spyware](https://www.security.org/antivirus/spyware/), and other cyber threats.
4. Use a **password manager**: [The best password managers](https://www.security.org/password-manager/best/) store users’ usernames and passwords in encrypted vaults, requiring only master passwords or biometrics to log into accounts. Memorizing dozens of secure passwords is tedious, so we strongly recommend using a reliable [password manager to store all your passwords](https://www.security.org/password-manager/).
5. **Only change passwords when needed**: While digital security experts used to recommend changing passwords in regular intervals, it’s a myth that doing so keeps your accounts more secure. The prevailing train of thought now among experts like ourselves is that if you change your password often, there’s a greater chance you’ll use weaker passwords that are easier to remember or succumb to a pattern that will make your passwords more predictable. Rather, it’s only necessary to change passwords if the account itself is compromised.

**How Our Tool Works: Methodology**

Our “how secure is your password” tool above checks users’ passwords against a database of common weak passwords. It evaluates each password based on key factors such as:

* **Number of characters**: The password should have at least eight to 10 passwords, but 16 to 20 characters is ideal.
* **Combinations:** The password should include a combination of letters, numbers, and symbols rather than a phrase. Each character has an associated numerical value, and these characters are summed to create a grand total.
* **Uniqueness**: The password shouldn’t be repetitive in terms of its characters, with unique combinations instead.

Using these factors, the tool scores each password and converts this score into the amount of time it would take a computer to crack this password. For example, the password “f0JB^B5sjmXl” would take a computer 34,000 years to crack.

The guidelines state that “memorized secrets should be 64 characters or longer” and that “simple or common phrases, including idioms, are not recommended.” By following industry standards, organizations can ensure that their cybersecurity practices are up-to-date and effective.

Customer privacy laws such as [HIPAA](https://www.impactmybiz.com/blog/what-is-hipaa-compliance-what-hipaa-means/), [CCPA](https://www.impactmybiz.com/blog/blog-what-is-ccpa-and-what-does-it-mean-for-business/), and CMMC also require organizations to protect their customers’ sensitive data such as personal information, patient data, or patent information from being exposed due to a data breach. Using a complex passphrase is an easy yet effective way to do so.

The main strength of passphrases is that they use unrelated words to create a unique phrase. Here are a few examples of passphrases:

* I am a cowboy who hates horses
* 1 am a cowboy who hate$ horses
* Correct Horse Battery Staple
* Sunshine Rainbows Butterflies
* Jazz Music Coffee Lover
* Purple Monkey Dishwasher Carrot
* Guitar Pizza Football Tacos

it’s important to avoid common phrases