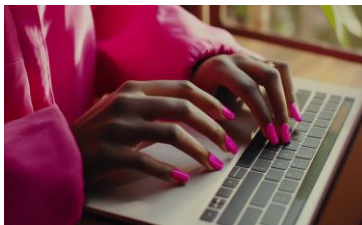




Create and Use Strong Passwords and Passphrases



Create and Use Strong Passwords and Passphrases

Passwords are the keys to safeguarding your digital and online life. Even though passwords have been “going away” for the past two decades, they are still your first line of defense. And knowing how to create and store strong passwords is one of the most critical aspects of everyday cybersecurity.

Protect your passwords like you'd protect your house keys. Of course, maintaining your password collection is frustrating for many of us (until you start using a password manager).

While creating, storing, and remembering passwords can feel overwhelming, they remain your first line of defense against cybercriminals and data breaches. Fortunately, free, secure, and user-friendly password managers have made it easier than ever to maintain strong passwords. You can work to secure your online presence with just a few simple steps today.

The power of long, unique, and complex passwords

For maximum security, remember three principles:

- 1. Long :** Passwords should be at least **12 characters long**. The longer your password, the longer it takes for hackers to crack it using brute force techniques. Right now, an eight-character password takes a few minutes for hacker software to guess by trying every combination of letters, numbers, and symbols. A 16-character password takes a **billion years** to guess!
- 2. Unique:** Each account should have a **unique password**. If you reuse passwords, don't feel ashamed! Reusing passwords is a bad habit many of us are guilty of, but you can start changing your habits today! Reusing passwords across multiple accounts can cause huge headaches. If one account is compromised, unique passwords ensure your other accounts remain secure. Small tweaks like adding a number or a special character aren't enough; each password should be entirely distinct. You can use a password manager to create and store unique passwords for all your accounts!
- 3. Complex:** Passwords should include a mix of **uppercase and lowercase letters, numbers, and special characters** (like @, !, or \$). Some platforms even allow spaces. The strongest passwords are a long string of random characters, not identifiable words, names, or dates. However, even if your passwords are random, you must ensure they are each at least 16 characters long!

Let's review!

Each of your passwords should be:

- Unique to the account
- At least 12 characters long
- A random jumble of letters, numbers, and symbols.

By using strong passwords, you're taking a crucial step toward protecting your digital identity.

What about using a passphrase?

A passphrase is basically a more secure form of a password. People use passphrases for the same reasons and in the same way as a password. A passphrase is typically longer and contains spaces or underlines where spaces would occur. A passphrase can also contain symbols, and it does not need to be grammatically correct.

It is often best if the words in the passphrase are completely random. The passphrase meaning should not be easy to guess or a typical or common phrase. Using a random phrase makes a [passphrase stronger](#). An example of a passphrase for your Netflix account can be "Lazy cat snores Netflix!" A passphrase should be easy to remember but hard for hackers to crack and guess.

When to use a passphrase vs. a password

Both a password and a passphrase can be made secure. But generally speaking, a strong, random passphrase is said to have more [entropy](#) and therefore be more secure than a regular password. Longer passwords (**16 characters or more**) can also have a high level of entropy, making them more difficult to crack through brute force, but they are also harder to remember.

Most passcode rules and security standards allow for the use of passphrases instead of passwords. Overall, using a passphrase is more secure and offers better peace of mind. In either case, the [FBI](#) recommends making passwords or passphrases as long as a system will allow for optimal security. When creating a strong passphrase, follow these rules:

- Do not choose a popular phrase or saying.
- Avoid song lyrics.
- Consider nonsense words.
- Make the phrase at least 16 characters long.
- Five words are better than four.
- Add in symbols and letters.
- Choose random words.
- Use a different phrase for each account.

Remember that a [passphrase](#) does not need to be a proper sentence or even follow basic grammar rules.

MFA takes your security beyond the password

Multi-factor authentication (MFA) adds a whole new layer of security to each of your accounts. When you turn on MFA, you use more than a password to log in, which might mean a facial scan, a text message, or a special app. We recommend turning on MFA for every account that permits it. Find out more in [this guide to MFA!](#)

How often should you change your passwords?

If your passwords are already long, unique, and complex, there's no need to change them unless:

- You suspect unauthorized access to your account.
- You receive notification of a data breach involving your account.
- Doing so is required by certain regulatory, statutory or contractual obligations.

Why you should use a password manager

This advice about unique, strong, and complex passwords probably seems overwhelming if you've never used a password manager before. However, modern services can help you breathe a lot more easily. A password manager will become your favorite tool as you navigate the digital world. With a password manager, you only need to **remember one master password** to unlock your secure vault of stored passwords.

Benefits of using a password manager

- **Convenience:** No more struggling to remember dozens of passwords.
- **Enhanced security:** Automatically generate and store long, unique, and complex passwords.
- **Time-saving:** Browser extensions and smartphone apps autofill credentials for quick and secure logins.
- **Safe vaults:** You might be wary of storing all your passwords in one place, but high-quality password managers use encryption and zero-knowledge architecture to keep you secure. Password managers are safer than notebooks, sticky notes, spreadsheets, or reusing passwords because you're trying to remember them all.

Why password managers are a game-changer

According to [surveys](#), the average person manages over 160 accounts. Using the same password across accounts means that hackers can access all linked accounts if one gets compromised. Password managers eliminate this risk by enabling you to maintain unique passwords for every account without the hassle of remembering them all.

Many password managers are free or affordable, simple to use, and work seamlessly across devices. Adopting a password manager can significantly reduce your vulnerability to cyber threats and make your online experience more secure and stress-free. Check out [this guide to password managers!](#)

What about passkeys?

Passkeys are exciting new technology that remove the need for passwords. Instead of entering a password, with passkeys you typically log in by having a secure device handy (like a phone) and using biometrics, like a facial scan. They are easy to set up and [worth checking out!](#)

You can get started today

Start protecting your digital life by creating long, unique, and complex passwords for your accounts. If changing all your passwords at once seems daunting, go slow. Find a trusted password manager and start changing weak passwords one batch at a time. Becoming a password aficionado is your strongest defense against cybercriminals.



The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.