ONLINE SAFETY AND PRIVACY
FEB 25, 2026 | 5 MIN READ

How To Create Strong Passwords (And Remember Them!)

Passwords protect every part of your online life, from email and banking to shopping, streaming, and work accounts.

They’re still your first line of defense against criminals, so knowing how to create and manage strong passwords is one of the most important everyday cybersecurity habits – it’s

the first of our Core 4 behaviors!

Embracing good password habits doesn't have to be stressful or technical. With today's tools like password managers, creating and using strong passwords is easier than ever.

THE THREE RULES OF STRONG PASSWORDS

When it comes to passwords, three rules matter more than everything else: length, uniqueness, and complexity. You might also think of complexity as "randomness."

1.

Long passwords are the most secure!

Your passwords should be at least 16 characters long.

Length significantly increases the time it takes attackers to guess a password using automated tools. Short passwords – even complicated-looking ones – can be cracked quickly if they are less than 16 characters long. It is a difference of hours and days to millions of years for 16-character passwords. Longer passwords slow attackers down so much that most will give up and move on. How are you expected to remember these long passwords? A password manager – more on this below.

1.

Every account needs a unique password

Each account should have its own password. No exceptions!

Reusing passwords is incredibly common, so don't beat yourself up if you've done it. But here's the risk: if one account is breached, attackers will try that same password everywhere else (software and AI can help them do this). Email, banking, social media...everything becomes vulnerable when you reuse passwords. Also, small changes, such as adding a number or symbol, don't make each password unique enough. Each password should be unique, which is where password managers excel. Are you recognizing a pattern (we love password managers!)?

1.

Make each password random and unrecognizable.

Strong passwords are random strings of letters, numbers, and symbols. Avoid recognizable

words, names, keyboard patterns, or dates. Complexity matters less than length and randomness. A long, random password is far stronger than a short, “clever” one with substitutions like P@ssw0rd!. Some sites even allow spaces, which can make passwords longer and harder to crack. Along with letters, throw in a number and special character for each password – many websites will require complexity. But every password should be 16 characters long! Password managers can create a great blend of complexity and randomness in generating strong passwords for you.

So what makes a strong password?

Every password should be:

- At least 16 characters long
- Unique to that account
- A random mix of letters, numbers, and symbols

Strong password examples

Here are some samples of strong passwords that follow our principles – but don't use these examples as passwords! These should be a guide for creating your own unique passwords.

- VYffnxK9O$VuL59k
- 8&QpP3SdsPzUf5P6
- 2kwe-85o5-LPFYz8

ADD AN EXTRA LAYER: USE MULTIFACTOR AUTHENTICATION (MFA)

Even the strongest password benefits from backup.

Multifactor authentication (MFA) requires an additional step when you log in. The extra step might be an app-generated code, a code texted to your phone, a fingerprint, or a facial scan. If someone steals your password, MFA can still stop them from getting in...as long as you don't share the MFA code!

Turn on MFA for any account that offers it, especially email, financial, and work-related

accounts. MFA may add a few seconds to your digital flow, but the added protection is well worth the time.

HOW OFTEN SHOULD YOU CHANGE YOUR PASSWORDS?

If your passwords are already long, unique, and random, you don't need to change them regularly. This is older advice that is no longer necessary if you follow our three guidelines.

You should change a password if:

- You suspect unauthorized access
- You're notified that the account was part of a data breach

Modern guidance, including recommendations from NIST, indicates that unnecessary changes often lead to weaker habits, such as reusing old passwords or choosing simpler ones.

Strong passwords work best when they're changed only when there's a reason.

WHY YOU SHOULD USE A PASSWORD MANAGER

Keeping track of hundreds of strong, unique passwords isn't realistic without help – we know the guidelines would be impossible to follow if you were expected to remember all your passwords. Today's technology can help immensely.

Password managers securely store your passwords in an encrypted vault. You only need to remember one strong master password, and the manager does the rest.

Benefits of password managers

- No more memorizing, reusing, or constantly resetting passwords
- Automatically generate long, random passwords
- Autofill logins on websites and apps
- Quickly generates and stores new strong passwords

Encrypted vaults are far safer than notes, spreadsheets, or reused passwords

Modern password managers use strong encryption and zero-knowledge designs, meaning even the provider can't see your passwords. Always enable MFA for your password managers!

Password managers are a game-changer

The average person has over 100 online accounts. Reusing passwords across them creates a single point of failure, meaning one breach can unlock everything.

Password managers eliminate that risk by making unique passwords effortless. Many are free or low-cost, easy to use, and work across phones, tablets, and computers.

Once you start using one, managing passwords becomes simpler, not harder!

If you still want to use your physical password notebook, we understand. Just remember to follow our three guidelines for strong passwords, and treat your notebook like cash – don't leave it in your car or on your desk at work.

WHAT ABOUT PASSKEYS?

Passkeys are a newer login option that can replace passwords entirely on some sites. Instead of typing a password, you authenticate using a trusted device and biometrics, like a fingerprint or facial scan. They're convenient, phishing-resistant, and worth using when available – and they are very quick to set up. Try passkeys if prompted, and check whether the services you use support them.

However, know that passwords are still essential for many accounts today. Also, many password managers securely store passkeys today!

GET STARTED TODAY – AND YOU CAN START SMALL!

You don't need to fix everything at once.

Start by choosing a reputable password manager (see our guide for options). Update your most important accounts first, like email, banking, and work services. From there, replace weak or reused passwords a few at a time. Many password managers (did we mention there are many free options?) will help you reset weak passwords quickly and alert you to which