

# Strong passwords

## Creating strong passwords

You'll need to **create a password** to do just about everything on the Internet, from checking your email to online banking, and while it's simpler to use a short, easy-to-remember password, this can also pose **serious risks** to your online security. To protect yourself and your information, you'll want to use passwords that are **long, strong, and difficult for someone else to guess** while still keeping them relatively **easy for you to remember**.

## Why do I need a strong password?

At this point, you may be wondering, **why do I even need a strong password anyway?** The truth is that even though most websites are secure, there is always a small chance someone may try to access or steal your information. This is commonly known as **hacking**. A strong password is one of the best ways to defend your accounts and private information from hackers.

## Tips for creating strong passwords

A strong password is one that's easy for you to remember but difficult for others to guess. Let's take a look at some of the most important things to consider when creating a password.

- **Never use personal information** such as your name, birthday, username, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.

- **Use a longer password.** Your password should be at least six characters long, although for extra security it should be even longer.
- **Don't use the same password for each account.** If someone discovers your password for one account, all of your other accounts will be vulnerable.
- Try to include a combination of **numbers, symbols,** and both **uppercase** and **lowercase** letters.
- Avoid using simple words that can be found in the dictionary, for example, **swimming1** would be a **weak password**.
- **Random passwords are the strongest.** If you're having trouble creating one, you can also use a **password generator** instead to give you some additional ideas.
- Remember to update and change your passwords on occasion, but especially whenever you believe an account may have been compromised.



## Creating strong passwords

Some of the most commonly used passwords are based on **family names, hobbies**, or just a **simple pattern**. While these types of passwords are easy to remember, they're also some of the least secure. Let's take a look at some of the most common password mistakes and how to fix them.

### Scenario 1



Password: **123abccba321**

*“My password follows a simple pattern, so it’s easy to remember and type on my keyboard”*

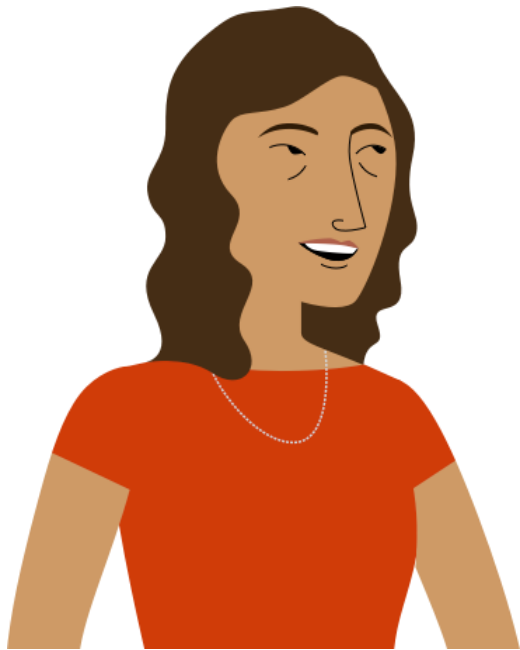
**Problem:** While patterns like this are easy to remember, they are also some of the first things a hacker might guess when attempting to access your account.

**Solution:** Remember that **random passwords** are much stronger than simple patterns. If you're having trouble creating a new password, try using a password generator instead. There are many free to use online password generators available.

Here's an example of a generated password: **#eV\$plg&qf**.

If you use a password generator, you may also want to create a **mnemonic** to make the password easier to remember. A mnemonic is essentially a system which utilises a pattern of letters, ideas, or associations which assists you in remembering something. For example, the password **H=jNp2#** could be remembered as **HARRY = jessica NORTH paris 2 #**. This may still feel pretty random, but with a bit of practice it becomes relatively easy to memorise.

## Scenario 2



Password: **W3St!**

*"My password is so simple! It's just the beginning of my street address with a few extra characters."*

**Problem:** At only five characters, this password is way too short. It also includes part of her address, which is publicly available information.

**Solution:** A stronger version of this password would be **much longer**, ideally more than 10 characters. We could also substitute a nearby street name instead of her current address. For example, Pemberly Ave could become **p3MberLY%Av.**

## Scenario 3



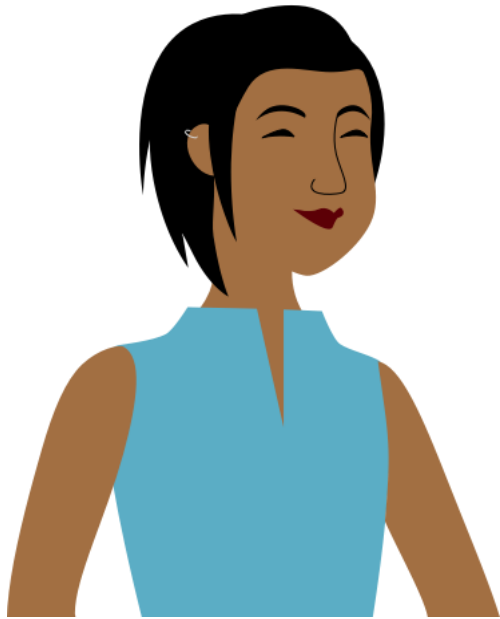
Password: **brian12kate5**

*"I doubt anyone could guess my password! It's my childrens' names and ages. Who else would know that?"*

**Problem:** This password uses far too much personal information, along with common words. Furthermore, a password that includes something like a child's name, especially in a community as small as Gibraltar is not secure.

**Solution:** A stronger version of this password would use symbols, uppercase letters, and a more random order and rather than using family names, you could combine a character from a film with a type of food. For example, Chewbacca and pizza could become **chEwbAccAp!ZZa.**

## Scenario 4



Password: **BrAveZ!2**

*"I use the same passwords for all my accounts. This way, I only have to remember one password!"*

**Problem:** There's nothing really wrong with this password but remember that you should **never use the same password with different accounts.**

**Solution:** Create a unique password for each of your online accounts.

### Unique password managers

Instead of writing your passwords on paper where someone might find them, you can use a **password manager** to store them securely online. Password managers can remember and enter your password on different websites, which means you won't have to remember longer passwords.



Password: **m#P52s@ap\$V**

*"I use a password generator to create all of my passwords. They're not super easy to remember, but that's OK; I also use a password manager to keep track of them."*

This is a great example of a **strong password**. It's strong, long, and difficult for someone else to guess. It uses **more than 10 characters** with letters (both uppercase and lowercase), **numbers**, and **symbols**, and includes no obvious personal information or common words. This password might even be a bit too complicated to remember **without a password manager**, which highlights why they're so helpful when creating a strong password.

**Remember to use these tips whenever you create a password to keep your online information safe and secure.**