



## Microsoft Online Safety

[Home](#)[Fraud Prevention](#)[Data Protection](#)[Resources](#)[Get Support](#)

### Create strong passwords

Strong passwords are important protections to help you have safer online transactions.

#### Keys to password strength: length and complexity

An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in your password, the better.
- Use the entire keyboard, not just the letters and characters you use or see most often.

#### Create a strong password you can remember

There are many ways to create a long, complex password. Here is one way that may make remembering it easier:

What to do	Suggestion	Example
Start with a sentence or two (about 10 words total).	Think of something meaningful to you.	Long and complex passwords are safest. I keep mine secret. (10 words)
Turn your sentences into a row of letters.	Use the first letter of each word.	lAcPasIkMs (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	IACpAsIkMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	IACpAs56IkMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?IACpAs56IkMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?IACpAs56IkMs" (14 characters)

#### Test your password with a password checker

A password checker evaluates your password's strength automatically. [Try our secure password checker.](#)

#### Protect your passwords from prying eyes

- **The easiest way to "remember" passwords is to write them down.**  
It is okay to write passwords down, but keep them secure. See [5 tips to keep your passwords secret.](#)

#### Common password pitfalls to avoid

Cyber criminals use sophisticated tools that can rapidly decipher passwords.

##### Avoid creating passwords using:

- **Dictionary words in any language.**  
Words in all languages are vulnerable.
- **Words spelled backwards, common misspellings, and abbreviations.**  
Words in all languages are vulnerable.
- **Sequences or repeated characters.**  
Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty).
- **Personal information.**  
Your name, birthday, driver's license, passport number, or similar information.

Share this page:

Print this page:

#### Search Online Safety Site

Submit

#### Related Links

[5 tips to keep your password secret](#)[Check your password. Is it strong?](#)[What is antispyware software?](#)[Top Tips for Internet Safety at Home](#)[Top Tips for Internet Safety at Work](#)