Your password

The key to your personal information

Passphrases, passwords and PINs help protect your personal information from potential online threats. And the stronger they are, the more secure your information will be.

We recommend that you use passphrases, as they are longer yet easier to remember than a password of random, mixed characters. A passphrase is a memorized phrase consisting of mixed words with or without spaces.

If a passphrase isn't an option, complex passwords that are unique to every account and device can also make it more difficult for cyber criminals to access your accounts and devices. Discover the steps you can take to create the best passwords possible – and how to keep them safe once you've made them.

Protect your password

Always use a strong password or passphrase
Passwords that are easy to remember, like a pet's name or family member's birthday, are also easy for attackers to guess. Instead, follow these tips to create a strong passphrase or password:

- When possible, create a passphrase: a combination of four or more random words, and a minimum of 15 characters

- For traditional passwords:
  - Use at least twelve characters
  - Use a combination of upper- and lower-case letters and at least one number
  - Include at least one character that isn't a letter or number, like: !, # or $.
  - Use a series of letters that only make sense to you, like the first letters of each word in a sentence

Use unique passwords for everything
Many people use the same password for multiple accounts and devices. Unfortunately, this has one major problem: if a cyber criminal gets access to one of your accounts, they get access to all of them.

Using unique passwords is the easiest way to protect all of your accounts in the event of a breach. Plus, you can always try a password manager if you're having trouble remembering multiple passwords.

Only log in from trusted sources
Legitimate websites will never ask you to send your personal information or to log in via email or text message.

If you're unsure if a message you receive is a phishing scam, try logging in from the home page of the organization you're dealing with – never click a link in a suspicious message or respond to any message asking for your password.

Never share your password
This one should be obvious, but just in case it's not: never, ever, ever share your passwords with anyone. Ever.