Strong Password Rules

A quick printable guide from capybaranet.com

The Core Rules of Password Strength

To protect your accounts from automated hacking tools, every password must follow three strict criteria:

1

Length

Use at least 16 characters. Length is the most critical factor — it exponentially increases the time required to guess your credentials.

2

Randomness

Avoid predictable patterns, dictionary words, and personal details like birthdays or pet names.

3

Uniqueness

Never reuse a password. If one site suffers a breach, hackers will immediately try that password elsewhere.

Two Methods for Creating Strong Passwords

Method 1: The Passphrase Method

(Best for manual memory)

Combine several completely unrelated words instead of a chaotic string of characters.

`LaughingPurpleHorseHatBathing`

Why it works: 29 characters — long, secure against guessing, yet easy for a human to visualize and remember.

What to avoid:

- Famous quotes, song lyrics, or common phrases — hackers use lists of these.
- Basic substitutions like "password" becoming P@ssw0rd! — cracking tools bypass this easily.

Method 2: The Random Method

(Best for automated tools)

Generate a completely chaotic string of uppercase, lowercase, numbers, and symbols.

`cXmnZK65rf*&DaaD`

Why it works: maximizes randomness and leaves zero predictable patterns for software to exploit.

Essential Security Add-Ons

Use a Password Manager

Tools like Bitwarden or 1Password securely store hundreds of unique, complex passwords so you only have to remember one master password.

Turn on Multi-Factor Authentication

Always enable MFA (an authenticator app or fingerprint scan) on your important accounts. If a hacker steals your password, MFA acts as a secondary shield to keep them out.

The single most important rule: never reuse a password.

A password manager makes unique, strong passwords effortless for every account.