



BE SMART. BE SAFE. BE READY.

PASSWORD HYGIENE BASICS

STRONG PASSWORDS. SAFER ACCOUNTS.

Stronger
Passwords
=
Safer You

HOW TO MAKE A STRONG PASSWORD

A strong password is longer, harder to guess, and unique to each account.



Make it long

Use at least 12–16 characters.



Use a mix

Include upper & lowercase letters, numbers, and symbols.



Use a phrase

Try a mix of unrelated words. It's easier to remember and harder to guess.



Use a unique password

Don't reuse the same password across different accounts.



STRONG EXAMPLE

Maple!River7Sun

- ✓ Long (16 characters)
- ✓ Mix of letters, numbers, symbols
- ✓ Easy to remember
- ✓ Harder to guess



WEAK EXAMPLE

Password123

- ✗ Too short
- ✗ Only common words and numbers
- ✗ Easy to guess
- ✗ Often reused

WHAT IS MFA?

Multi-Factor Authentication (MFA) adds an extra layer of security to your accounts.



Adds a second step

After your password, you'll need a code from your phone or an authentication app.



Helps stop attackers

Even if someone gets your password, they can't access your account without the second step.



Used on important accounts

Turn on MFA for your email, banking, and any other accounts that offer it.



SIMPLE HABITS. BIGGER PROTECTION.

BE SMART. BE SAFE. BE READY.