



# Password Best Practices Guide

## Tips For Password Security

- ✓ Enable phishing-resistant multifactor authentication (MFA) whenever possible
- ✓ If you can, use a password manager and protect it with MFA and/or a long password/passphrase
- ✓ Use a password generator to create truly random passwords with a minimum of 12 characters
- ✓ If you must create a password, use a passphrase with a minimum of 20 characters
- ✓ Never share passwords between accounts
- ✓ Keep your passwords private – never share a password with anyone else
- ✓ Do not write down your passwords

## How To Create A Strong, Complex Password

If you must create a password, here's a way to make a strong password that's difficult to crack:

USE ONE OF THESE TWO METHODS	EXAMPLE
1 Create passwords with at least 12 characters that are truly random, ideally using a password generator.	<b>R#Yv&amp;ZCAojrX ELv!2MibAb&gt;RC?ru a!#+dH)vvLykijhu</b>
2 Think of a random phrase with at least 20 characters that is easy to remember.	<b>I went to 7-11 earlier today. rogerjumpedoverthepurplefox 2belivingtherockandrolllifeforever</b>

## Why This Matters

Traditional passwords can be cracked by hackers in less than a minute! Follow this guide for password best practices to create passwords that would take centuries to crack.

[DOWNLOAD](#)

For more advice on what your Password Policy should be, download our e-book.