

# STRENGTHEN YOUR PASSWORDS: KEEP YOUR ACCOUNTS SECURE!

STAY ONE STEP AHEAD OF HACKERS!



Learn how to create strong passwords, avoid common mistakes, and enhance security with multi-factor authentication.

## WHY STRONG PASSWORDS MATTER?

- 80% of cyber breaches are due to weak passwords.
- 123456 and Password123 are still the most commonly used passwords!
- A hacker can crack an 8-character password in less than 8 hours!

No of characters	Time Duration
6	Instantly cracked
8	8 hours
10	1 week
12	5 years
16	Over 1,000 years!

## BAD VS. GOOD PASSWORD HABITS

Bad Passwords	Strong Passwords
123456	T@bl3Ch@ir\$un5et!
password	D0gRun\$5Mil3s.
qwerty123	`9Rain&CloudSky`
companyname123	Xy#73&Zqw\$@8



## THE DO'S & DON'TS OF PASSWORD SECURITY

	DO		DON'T
✓	Use long passwords (at least 12+ characters)	✗	Use the same password for multiple accounts.
✓	Include uppercase, lowercase, numbers, and symbols	✗	Share your password with anyone.
✓	Use passphrases (e.g., HorseBattery\$Tabl e123!)	✗	Use easily guessable passwords (e.g., yourname123)
✓	Enable multi-factor authentication (MFA)	✗	Write down passwords on sticky notes
✓	Use <b>password managers</b> to store complex passwords	✗	Click on links in emails asking you to reset your password unless verified

# COMPANY PASSWORD POLICY

## (QUICK OVERVIEW)

Minimum 12-character passwords required.

Passwords must be updated every 90 days.

Multi-factor authentication (MFA) is mandatory for all accounts.

Company-issued password managers must be used for storing credentials.

Report any suspicious password reset requests to IT immediately.



## BEST PRACTICES FOR PASSWORD SAFETY

Use MFA whenever available

Change compromised passwords immediately

Use unique passwords for every account

Be cautious of phishing attempts asking for password resets

Use company-approved security tools to store passwords securely

## PASSWORD POWER-UP: CROSSWORD CHALLENGE!

Think you know your password best practices? Put your knowledge to the test with this fun crossword puzzle!

Each word is a clue to keeping your accounts secure. From must-know terms to common mistakes, this game is your chance to brush up on what makes a strong, safe password.

Complexity, TwoFactor, Unique, Passphrase, Breach, Lockout, Manager, Authentication, Credential, Secure, Update, Symbols, Length, Guessing, Reuse, Encryption

U	Y	T	T	N	Y	T	M	M	J	Z	E	S	M	P
N	H	C	U	W	C	D	E	W	D	O	A	E	U	E
I	D	T	R	O	O	H	C	A	E	R	B	C	S	S
Q	C	P	G	E	K	F	N	I	L	T	I	U	S	R
U	J	W	H	N	D	C	A	S	P	D	E	R	V	P
E	G	L	I	W	E	E	O	C	V	R	S	E	A	G
T	T	W	W	K	M	L	N	L	T	X	B	S	C	N
C	O	M	P	L	E	X	I	T	Y	O	S	R	T	I
P	B	U	K	E	G	H	M	U	I	P	R	E	U	S
M	U	B	L	G	A	I	P	S	H	A	R	G	N	S
O	U	B	J	P	J	D	U	R	K	G	L	A	Q	E
G	H	B	B	M	A	T	A	J	L	C	W	N	P	U
P	G	A	K	T	B	S	V	U	D	G	S	A	R	G
M	N	D	E	I	E	S	U	S	L	O	B	M	Y	S
A	U	T	H	E	N	T	I	C	A	T	I	O	N	N

Let's #LockDownPasswords!