

# ARE YOUR PASSWORD PRACTICES SECURE ENOUGH?

## THE THREAT OF POOR PASSWORD HYGIENE



86% of passwords are already compromised



29% of data breaches involve stolen credentials



Password-stealing malware increased by 60% last year



Brute force attacks occur roughly every 39 seconds

## PASSWORD FATIGUE AND BAD BEHAVIOR



The average business user has to manage logins for nearly 200 accounts. They're sick of it. That fatigue has created several bad habits that put both personal and professional data at risk.



51% Reuse passwords



69% Share with colleagues



67% Don't use 2FA



60.5% Update > 3 times a year



39% Write their passwords down

## THE SOLUTION TO PASSWORD FATIGUE

A password manager like LastPass eliminates the need to remember multiple passwords. Instead, you can focus on creating one strong set of login details, and let the software generate your other passwords.

## WHAT MAKES A PASSWORD SECURE?



12+ characters long



Complex & unique



No personal information



Easy to remember

## HOW TO CREATE A STRONG PASSWORD



Use a passphrase generator to create a random string of words



Add a few numbers, symbols, and capital letters



Memorize your passphrase using mnemonics



Use it as a master password