

16 Bad Password Habits (and How to Solve Them)



According to the Verizon Data Breach Investigations Report, 85% of data breaches involve human vulnerabilities. Yet despite this, and the ever-increasing array of ransomware and malware attacks facing businesses, 65% of the 3,750 respondents from the LastPass 2021 Psychology of Passwords report revealed they use the same password or a variation for multiple accounts, despite knowing the risk.

Here are 16 of the most common bad password habits among employees that jeopardize the security of your business:



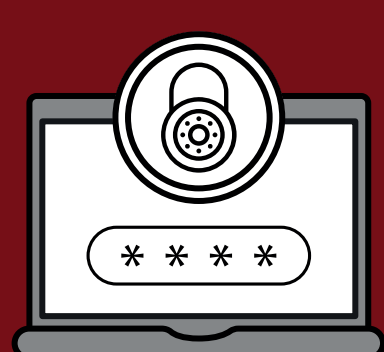
- 1 Using the same password for all your accounts
- 2 Cycling between a handful of the same passwords
- 3 Never updating your passwords
- 4 Using short passwords (less than 8 characters)
- 5 Storing passwords in browsers
- 6 Sharing passwords insecurely with other employees
- 7 Using “password” as your password
- 8 Using a row of characters from your keyboard, e.g. “qwerty”



- 9 Using all lowercase letters
- 10 Relying on memory to keep track of your passwords
- 11 Changing your password too frequently
- 12 Including any part of your name in your password
- 13 Including personal information in your password
- 14 Not changing your password after a breach
- 15 Writing passwords down or using sticky notes
- 16 Having too many passwords to keep track of

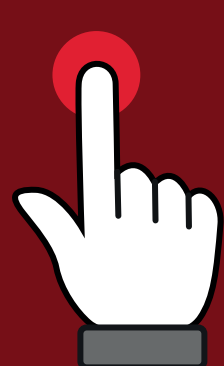


How to solve bad password habits: The three tools you need



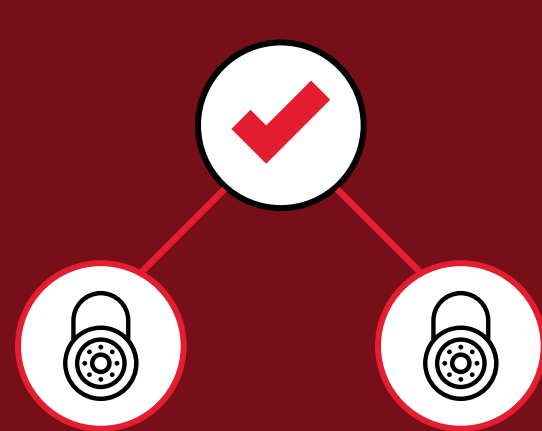
Password Management

A password manager remembers all your passwords for you. Once synced, you’ll only need one password, and the password manager will then automatically fill in your credentials.



Single Sign-On

Addressing today’s remote working needs, single sign-on makes authentication instant. It does this based on a user’s identity and permissions, rather than the use of multiple passwords.



Multifactor Authentication (MFA)

MFA uses biometric and contextual factors to protect your network, while also further securing the login process. It adds an extra authentication method to prevent unauthorized access to accounts while working in the background to facilitate productivity.

To learn more about the three pillars of effective password security, read the full guide [here](#).