KnowBe4
Human error. Conquered.

What Your Password Policy Should Be

Table of Contents

INTRODUCTION

Passwords are part of every organization's security risk profile that should be taken seriously by IT security professionals like you. Just one weak password with access to an organization's critical systems can cause a breach, take down a network or worse. Whether we like it or not, passwords are here to stay as a form of authentication for at least another decade or so. There is no time like the present to review your organization's password policy and update it for the betterment of your organization's overall security.

This whitepaper will cover the critical components of a recommended password policy for any organization around the world. It will also summarize the advantages and disadvantages of using passwords, provide a detailed breakdown of the various types of passwords attacks and defenses, as well as KnowBe4 tools that you can utilize to implement better passwords throughout your organization.

RECOMMENDED PASSWORD POLICY SUMMARY

Your personal and enterprise passwords and policies should follow these recommendations.

The reasons your passwords and password policies should follow these recommendations are due to the methods attackers commonly use to compromise passwords and the defenses it takes to mitigate those threats.

This whitepaper will discuss the various password attacks that justify the recommended password policies. If you do not have time to read this entire whitepaper, just implement the recommended password policy to the right. But if you read this whitepaper, you will gain a good understanding of why these specific policies are recommended and why you should follow them (or not, if you decide to make a different risk decision).