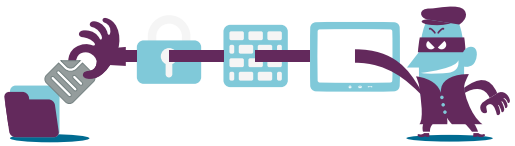
SPECOPS PASSWORD POLICY

Hackers are finding new ways to exploit password-protected systems. Organizations must stop relying on failing password complexity requirements, and blacklist weak passwords instead.

To stand up to these attacks, passwords must overcome the standard structure and character profile. Attackers search for predictable patterns in user behavior, including character substitutions, leetspeak, and popular compositions. The task not only falls on users, but also on organizations and password policies that encourage predictability.

- 1.9 billion usernames and passwords exposed via data breaches and traded on black-market forums, *Google Report: Data breaches, phishing, or malware? Understanding the risk of stolen credentials*
- Hacked passwords cause 81% of data breaches, *Verizon: Data Breach Investigations Report, 2017*
- Average cost of a data breach globally is $3.86 million, *Ponemon Institute: 2018 Cost of a Data Breach Study* (Average cost for data breaches of 2,500-100,000 lost or stolen records)



Brute-force: A trial and error method, generating a large quantity of password guesses, until the right one is found.

Dictionary: A computerized list of high-probability passwords to uncover target passwords.

Specops Password Policy enables stronger passwords by blacklisting known weak passwords. Even with character complexity requirements enabled, Specops Password Policy can block leetspeak, keyboard patterns, and even appending old passwords with a number or symbol.

Requirements	Specops Password Policy	Microsoft on-premises password policy
1 Billion Blacklist	✓	×
Customizable Blacklist	✓	×
Blocks keyboard patterns	✓	×
Blocks leetspeak	✓	×
Blocks incremental characters	✓	×
Passphrases	✓	×