THE ISSUE OF PASSWORD REUSE

Password reuse is a pervasive issue that affects all organizations.

Most people know better than to reuse passwords, but they struggle to recall unique passwords for all of their accounts. They also don't understand the risk when they use the same password across personal and work accounts.

The details below explain the issue and what organizations can do to mitigate the negative impacts of password reuse.

How many people reuse passwords?

65% of people **reuse passwords** across **multiple**, if not all, sites*

*Google

72% of individuals **reuse passwords** in their **personal life***

*Hypr

The **average person reuses each password** as many as **14 times.**

*LastPass

76% of **millennials recycle** their **passwords**

*Security.org

In 2020, Microsoft announced that a staggering **44 million accounts** were **VULNERABLE** to account takeover due to the use of **compromised or stolen passwords.**

It is not just personal accounts. Work accounts are impacted too.

73% of users DUPLICATE THEIR PASSWORDS in both their personal and work accounts.

*Microsoft

Bad actors prey upon the vulnerabilities caused by password reuse.

Compromised credentials and passwords are responsible for **81%** of **HACKING-RELATED BREACHES.**

*Verizon Data Breach Investigations Report.

What can organizations do to mitigate password reuse?

Add Another Authentication Factor

- Good option if the users are agreeable- less than 10% of Google users have turned it on MFA
- Users don't like it and/or may not have easy access to a 2nd factor
- If the password is exposed, you have just 1 factor

Password expiration policies

- Users will choose less secure passwords if they are forced to reset it regularly, according to the FTC
- 49% of employees change or add a digit or character to their password when updating their company password every 90 days *Hypr
- NIST and Microsoft both recommend against password expiration policies now

Free static password blacklists found online

- A static password blacklist off the internet will quickly become outdated
- They only have 10-20% of the common passwords that attackers use
- Blacklists don't account for similar or context-specific passwords
- Cracking dictionaries are not included

Compromised and weak password monitoring

- This solution screens passwords for weakness or compromise daily
- Filters for common, similar, and context-specific passwords
- Contains cracking dictionaries and root password detection
- It only impacts users who are using risky passwords, so it is low friction
- Required for compliance with NIST 800-63B and other security standards

Compromised and weak password monitoring in Active Directory is low-user friction, and it only impacts users who are using risky passwords. The rest of the users are unencumbered.

NIST Password Guidelines Supports Password Monitoring

NIST 800-63B Password Guidelines:

... verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised

- Passwords obtained from previous breaches
- Dictionary words
- Repetitive or sequential characters (e.g. 'aaaaaa,' '1234abcd')
- Context-specific words, such as the name of the service, the username, and derivatives thereof

Summary

Organizations are trying to reduce the negative impact of password reuse, and many are adopting the NIST 800-63b password requirements, but they often struggle with the workload associated with it.

Automated password policies can help simplify NIST password guidelines without creating a lot of additional burden on the IT team.

To learn more about tools that can help with password reuse by screening for risky and exposed passwords, visit **www.enzoic.com**

ENZOIC