Password policy recommendations for Microsoft 365 passwords

Article • 06/15/2023

Check out all of our small business content on Small business help & learning .

As the admin of an organization, you're responsible for setting the password policy for users in your organization. Setting the password policy can be complicated and confusing, and this article provides recommendations to make your organization more secure against password attacks.

Microsoft cloud-only accounts have a pre-defined password policy that cannot be changed. The only items you can change are the number of days until a password expires and whether or not passwords expire at all.

To determine how often Microsoft 365 passwords expire in your organization, see Set password expiration policy for Microsoft 365.

For more information about Microsoft 365 passwords, see:

Reset passwords (article)

Set an individual user's password to never expire (article)

Let users reset their own passwords (article)

Resend a user's password (article)

Time to rethink mandatory password changes .

Understanding password recommendations

Good password practices fall into a few broad categories:

- **Resisting common attacks** This involves the choice of where users enter passwords (known and trusted devices with good malware detection, validated sites), and the choice of what password to choose (length and uniqueness).
- **Containing successful attacks** Containing successful hacker attacks is about

limiting exposure to a specific service, or preventing that damage altogether, if a user's password gets stolen. For example, ensuring that a breach of your social networking credentials doesn't make your bank account vulnerable, or not letting a poorly guarded account accept reset links for an important account.

- **Understanding human nature** Many valid password practices fail in the face of natural human behaviors. Understanding human nature is critical because research shows that almost every rule you impose on your users will result in a weakening of password quality. Length requirements, special character requirements, and password change requirements all result in normalization of passwords, which makes it easier for attackers to guess or crack passwords.

Password guidelines for administrators

The primary goal of a more secure password system is password diversity. You want your password policy to contain lots of different and hard to guess passwords. Here are a few recommendations for keeping your organization as secure as possible.

- Maintain an 8-character minimum length requirement
- Don't require character composition requirements. For example, *&(^%$
- Don't require mandatory periodic password resets for user accounts
- Ban common passwords, to keep the most vulnerable passwords out of your system
- Educate your users to not reuse their organization passwords for non-work related purposes
- Enforce registration for multi-factor authentication
- Enable risk based multi-factor authentication challenges

Password guidance for your users

Here's some password guidance for users in your organization. Make sure to let your users know about these recommendations and enforce the recommended password policies at the organizational level.

- Don't use a password that is the same or similar to one you use on any other websites
- Don't use a single word, for example, **password**, or a commonly used phrase like **Iloveyou**
- Make passwords hard to guess, even by those who know a lot about you, such as the names and birthdays of your friends and family, your favorite bands, and phrases you like to use

Some common approaches and their negative impacts

These are some of the most commonly used password management practices, but research warns us about the negative impacts of them.

Password expiration requirements for users

Password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous password. Password expiration requirements offer no containment benefits because cybercriminals almost always use credentials as soon as they compromise them.

Minimum password length requirements

To encourage users to think about a unique password, we recommend keeping a reasonable 8-character minimum length requirement.

Requiring the use of multiple character sets

Password complexity requirements reduce key space and cause users to act in predictable ways, doing more harm than good. Most systems enforce some level of password complexity requirements. For example, passwords need characters from all three of the following categories:

- uppercase characters
- lowercase characters
- non-alphanumeric characters

Most people use similar patterns, for example, a capital letter in the first position, a symbol in the last, and a number in the last 2. Cybercriminals know this, so they run their dictionary attacks using the most common substitutions, "$" for "s", "@" for "a," "1" for "l". Forcing your users to choose a combination of upper, lower, digits, special characters has a negative effect. Some complexity requirements even prevent users from using secure and memorable passwords, and force them into coming up with less secure and less memorable passwords.

Successful Patterns

In contrast, here are some recommendations in encouraging password diversity.

Ban common passwords

The most important password requirement you should put on your users when creating passwords is to ban the use of common passwords to reduce your organization's susceptibility to brute force password attacks. Common user passwords include: **abcdefg**, **password**, **monkey**.

Educate users to not reuse organization passwords anywhere else

One of the most important messages to get across to users in your organization is to not reuse their organization password anywhere else. The use of organization passwords in external websites greatly increases the likelihood that cybercriminals will compromise these passwords.

Enforce Multi-Factor Authentication registration

Make sure your users update contact and security information, like an alternate email address, phone number, or a device registered for push notifications, so they can

respond to security challenges and be notified of security events. Updated contact and security information helps users verify their identity if they ever forget their password, or if someone else tries to take over their account. It also provides an out of band notification channel in the case of security events such as login attempts or changed passwords.

To learn more, see Set up multi-factor authentication.

Enable risk based multi-factor authentication

Risk-based multi-factor authentication ensures that when our system detects suspicious activity, it can challenge the user to ensure that they are the legitimate account owner.

Next steps

Want to know more about managing passwords? Here is some recommended reading:

- Forget passwords, go passwordless
- Microsoft Password Guidance
- Do Strong Web Passwords Accomplish Anything?
- Password Portfolios and the Finite-Effort User
- Preventing Weak Passwords by Reading Users' Minds
- Choosing Secure Passwords
- Time to rethink mandatory password changes

Related content

Reset passwords (article)
Set an individual user's password to never expire (article)
Let users reset their own passwords (article)
Resend a user's password - Admin Help (article)

Feedback

Was this page helpful? Yes No

Provide product feedback