T2023_02 Why Is It Important to Have a Password Policy (20th February 2023)

What Is a Password Policy?

A password policy is a set of guidelines intended to improve computer security by enforcing the usage of stronger passwords by users. By creating a password policy, you may provide clear guidelines for how users should generate and use passwords on your online application password policy. Although you might not be able to completely regulate users' behavior, you can nevertheless direct them for their own safety.

Why Is a Password Policy Important

With a strong password policy, the organization may make it harder for cybercriminals to access its sensitive data. Promoting employee awareness of the risks they confront online can also help mitigate threats.

Cybercriminals frequently employ brute force assaults to guess passwords, and if they succeed in cracking your password, they might be able to access confidential data. They will damage your company in the following ways if they are successful in gaining access to this data:

- Financial Loss - Financial details about your business could be used by a cybercriminal to make illicit purchases or transfers.
- Loss of Customers - if your clients' confidential information is stolen, they might stop trusting you and do business somewhere else.
- Damage to Your Reputation - A data breach could harm your business's reputation and make it harder to bring in new clients or business partners.
- Compliance Issues - your firm can be held accountable and forced to pay a steep fine if the cybercriminal uses the data from your organization to perpetrate a crime.
- Permanent Closure - A data breach may, in some circumstances, force the permanent liquidation of your company.

How to Develop a Successful Password Policy

Your policy must have several elements in place to be effectively established. Let us look at a few of them.

1. Password Strength - The strength of your password is determined by its structure. Three factors influence a password's strength: the length of the character set used, the length of the password itself, and to a lesser extent, the variety in characters chosen. Example of a strong password "**m#P52s@ap$V"**

2. Password Expiry - Passwords with expiration dates are more likely to be changed frequently. Some users could unintentionally reveal their credentials to the incorrect parties. Whatever the situation, frequently changing passwords is a good cybersecurity practice since it renders exposed credentials useless when they are updated.

3. Password History - Cybercriminals frequently use outdated passwords in their attacks. Prevent users from using their previous passwords to avoid this from happening.

4. Password Change - Password changes should be possible at any moment for users. However, take precautions to guarantee that the owner, not an intruder, is the one initiating a password change. Using two-factor authentication to permit password changes is secure. Create additional means for users to validate their identity before continuing.

The Guyana National CIRT recommends that users and administrators review this tip and implement them where necessary.

References

- Renders, J. (2023, January 17). *Why Implementing a Strong Password Policy is Important for Your Business's Data - Brightline Technologies*. Brightline Technologies.https://brightlineit.com/why-implementing-a-strong-password-policy-is-important-for-your-businesss-data/#:~:text=By%20implementing%20a%20strong%20password,gain%20access%20to%20sensitive%20information.
- Odogwu, C. (2021, December 25). What Is a Password Policy and Why Is It Important. retrieved from make use of. https://www.makeuseof.com/