Password Management Best Practices Checklist

Password management is often your first line of security to prevent network and data breaches. Following these best practices will help prevent and mitigate data breaches due to compromised passwords.

☑ Use Two-Factor or Multi-Factor Authentication

This adds a layer of protection when employees sign-in to the network. An additional layer can require identity verification such as entering a code received via text message or scanning a fingerprint before granting users access to network data.

☑ Train Employees

Periodic training for employees is essential for protecting companies against a breach. The three goals of employee training are to empower with tips and tactics, raise awareness of the importance for protecting data, and set expectations based on corporate policies.

☑ Encourage Passphrases

Encouraging employees to use passphrases that contain multiple words, characters and spaces, instead of single-word passwords will help make it more difficult to guess employee passwords.

☑ Limit Password Attempts

Locking an account after a specific number of attempts helps deter cyber attacks because cyber attackers will attempt to log in again and again until they figure out the right password the original hash.

☑ Simplify Password Security

Keep password access on a need-to-know basis. For small businesses, passwords can be configured with role-based access control that allows management of password permissions for multiple users.

☑ Periodic Resets

The National Institute of Standards and Technology says that periodic password changes are no longer necessary because of the improved computer environment, however, this extra layer of protection can guard against other ways that passwords are lost or stolen aside from hacking.

☑ Implement Password Hashing

Password hashing is a one-way function that turns readable data into scrambled information. This process creates a hash when a password is created and each time it's entered for login, the system creates the same hash and checks it against the original hash.

☑ Breached Password Protection

Check new passwords against a list that includes dictionary words, repetitive or sequential strings, passwords from previous breaches, variations on the site name, commonly used passphrases, and other words and patters that cyber criminals would likely guess.

Visual Edge IT™

SECURE TECHNOLOGY SOLUTIONS