Cybersecurity Best Practices

PASSWORD AND PASSPHRASE MANAGEMENT

FBICYBER

We all use passwords to secure our phones, computers, email, and online accounts. Unfortunately, many of us use—and reuse—simple passwords because they are easier to remember. However, malicious cyber actors commonly exploit simple, weak passwords to obtain users' login information. Common types of attacks used to obtain login information include brute force attacks and credential stuffing.

Brute Force Attacks Short passwords or character patterns, such as Summer1993 and a1b2C#, are commonly used and relatively easy for an adversary's computer to crack with modern tools. As a result, it does not take long for a computer to guess all possible character combinations before the correct one is found.

Credential Stuffing Once your password is cracked, an attacker will take the password and any known usernames and emails to then try to gain access to other accounts under your name.

Organizations can implement the following best practices to prevent these types of attacks.

Prioritize password length over complexity. Complex passwords are hard to remember and easy to crack. Use long passphrases instead—combine multiple unrelated words into a string of 8-64 characters, such as Offend-H[o]rse-seA-Battery-5—and do not allow password hints. Review password protocols to ensure they align with the latest National Institute of Standards and Technology (NIST) guidelines.

Do not enforce routine password change requirements. Only require password changes when there is reason to believe the network has been compromised. This decreases the chance of employees recycling the same old, easy-to-crack passwords.

Screen employee passwords against dictionary words and known compromised passwords to prevent them from creating or reusing weak passwords.

Allow the use of password management programs. These programs, called password managers, store salted and hashed passwords for all your accounts in one place, under a single master password or passphrase. Be sure to identify a trusted password management program before using one.

Require Multi-Factor Authentication (MFA). Enabling MFA is easy and boosts security significantly as it requires an extra layer of identity verification before you can gain access to an account. There are three types of MFA credentials:

- Something you know (a password or PIN)
- Something you have (a token or fob)
- Something you are (e.g., your fingerprint)

Know website security questions are not a form of multi-factor authentication and SMS-based authentication is a significantly less secure MFA option—it is common for attackers to compromise your phone or text messages.

Monitor network access and activity. Using network tools to track account login activity will help you identify anyone who should not have access or that may be using accounts inappropriately. Ensure only a limited number of employees can use Admin credentials and that they are only using such access when necessary. Remove access for individuals who are no longer authorized (e.g., former employees).

Resources

NIST Special Publication 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management
https://csrc.nist.gov/publications/detail/sp/800-63b/final

CISA Tip: Choosing and Protecting Passwords
https://us-cert.cisa.gov/ncas/tips/ST04-002

CISA Tip: Supplementing Passwords
https://us-cert.cisa.gov/ncas/tips/ST05-012

CISA Tip: Understanding Denial-of-Service Attacks
https://us-cert.cisa.gov/ncas/tips/ST04-015