Courtesy of
Connor & Gallagher OneSource

Mitigating Password Threats

Cybercrime continues to pose a serious threat to organizations of all sizes, highlighting the importance of strong cyber hygiene practices. While not the only line of defense against cyber threats, passwords remain a fundamental security control, and compromised credentials are among the most exploited entry points into business networks. As such, mitigating password threats is essential to reducing the likelihood of unauthorized access, protecting company data and strengthening overall cybersecurity resilience.

This article explains why passwords remain a common security threat, outlines current National Institute of Standards and Technology (NIST) guidance and describes the steps organizations can take to reduce credential-related risks.

Why Passwords Remain a Target

Organizations typically rely on passwords to secure email accounts, cloud platforms and other applications, making user credentials a valuable target for threat actors. Once obtained, these credentials provide a relatively straightforward path into business systems without the need to exploit software vulnerabilities.

Compounding security concerns, modern password-cracking tools have made it easier for attackers to identify short, predictable or commonly used passwords. In fact, a modern PC can attempt around 100 billion password guesses per second, according to NIST. Attackers can also obtain credentials through phishing, which is becoming increasingly difficult to identify as threat actors use AI and other technologies to craft more convincing emails, messages and other malicious communications.

Compromised credential risk is magnified if employees reuse passwords across accounts. When login details are exposed in a data breach, attackers often test them across other services, a tactic known as credential stuffing. As a result, a single compromised password may provide access to multiple business systems.

Tools such as multifactor authentication (MFA) and passkeys are helping to reduce reliance on passwords, but credentials remain a primary target for threat actors seeking access to business systems. As such, effective password management remains a key component of a strong cybersecurity strategy.

NIST Password Guidance

When developing passwords for workplace accounts, organizations should be aware of the following NIST guidelines:

- **Prioritize password length over special characters**—Employees should create passwords of at least 15 characters, as longer passwords increase the number of possible combinations a cybercriminal must guess to crack them. NIST no longer recommends mandating uppercase letters, numbers or symbols, as length is a more effective security measure, though some platforms may still enforce complexity requirements.
- **Check passwords against blocklists**—Employers should check newly created passwords against lists of commonly used or previously compromised credentials. If a password is rejected, employees should be told why and guided toward a stronger alternative.

- **Avoid mandatory password rotation**—Organizations should require password changes only when there is evidence of compromise. Routine resets can encourage weaker password choices and incremental changes to existing passwords that do little to improve security.
- **Encourage passphrase use**—Employees should use passphrases consisting of several unrelated words when setting passwords. Passphrases are typically easier to remember, reducing the temptation to write passwords down.

Strengthening Security Beyond Passwords

While strong passwords are an essential component of account security, organizations should not rely on them as their sole defense. Instead, they should supplement strong password practices with MFA, requiring users to provide a second form of authentication. Common verification methods include security keys, authenticator apps, fingerprint or facial recognition, and one-time codes delivered by text message or email.

Organizations should also consider using password managers that generate and store unique passwords for each account. These tools are recommended by NIST and automatically enter employee passwords, thereby removing the burden of memorizing complex combinations.

Coverage and Underwriting Implications

Cybersecurity controls, such as strong password practices and MFA, are increasingly expected by cyber insurers and may influence eligibility, premiums and policy terms. Insurers commonly expect MFA to be enabled across remote access systems, cloud platforms and administrative accounts at a minimum. Organizations should ensure that any security measures disclosed in insurance applications accurately reflect the controls they have in place, as discrepancies may affect underwriting outcomes and, in some circumstances, coverage following a claim. Carefully reviewing insurance applications and consulting with an experienced insurance professional can help organizations understand how these requirements apply to their policy and reduce the risk of coverage disputes.

Key Takeaways

Passwords remain a common target for attackers, and following recognized guidance, such as NIST's recommendations, is an important part of managing that risk. But passwords work best as one part of a broader access control strategy that includes MFA and password managers, both of which can also support favorable cyber insurance outcomes.

Contact us today for additional cybersecurity guidance and insurance solutions.