1.Password security

A escolha e o gerenciamento de senhas são fundamentais para a segurança digital. Um bom critério para criar senhas seguras é garantir alta entropia, ou seja, torná-las imprevisíveis para evitar ataques como força bruta ou "password spraying". Para isso, recomenda-se combinar letras maiúsculas e minúsculas, números e caracteres especiais, além de utilizar um comprimento mínimo de oito caracteres, embora padrões mais modernos surgiram senhas ainda mais longas. Uma alternativa segura é o uso de frases de acesso, que são mais fáceis de lembrar e oferecem maior complexidade.

Além da criação, a expiração da senha é um fator de segurança. Muitos sistemas exigem que as senhas sejam trocadas periodicamente, com prazos de 30, 60 ou 90 dias, e algumas organizações adotam ciclos ainda mais curtos para sistemas críticos. Para impedir o reaproveitamento de senhas antigas, é comum que os sistemas armazenem um histórico, forçando os usuários a escolherem novas combinações a cada alteração.

Uma prática recomendada é nunca reutilizar a mesma senha para diferentes contas. Isso evita que uma eventual violação comprometa múltiplos acessos do usuário. No entanto, lembrar de diversas senhas complexas pode ser difícil, por isso o uso de gerenciadores de senhas se tornou popular. Esses aplicativos armazenam todas as credenciais em um banco de dados criptografado, acessível mediante uma senha mestra e, muitas vezes, autenticação multifator. Além disso, oferecem funcionalidades como a geração automática de senhas fortes e a análise da saúde das credenciais, alertando sobre possíveis vazamentos.

Diante dos riscos associados ao uso de senhas, muitos sistemas estão migrando para métodos de autenticação sem senha. Isso pode incluir reconhecimento facial, biometria ou códigos temporários enviados a dispositivos confiáveis. Em alguns casos, uma senha ainda é usada na configuração inicial, mas o acesso posterior pode ser feito apenas com métodos alternativos.

Outra abordagem para minimizar riscos é a permissão temporária ***just-in-time*** (JIT), **especialmente útil em ambientes corporativos. Esse método concede credenciais administrativas apenas pelo tempo necessário para executar uma tarefa específica**, revogando automaticamente o acesso após a conclusão do trabalho. Isso reduz as chances de que contas comprometidas sejam usadas para ataques. O processo de JIT geralmente envolve um "cofre de senhas" centralizado, que gera credenciais temporárias sem expor as credenciais principais do sistema.

O gerenciamento de senhas e acessos continua evoluindo para equilibrar segurança e conveniência, e a adoção de práticas como o uso de gerenciadores de senhas, autenticação sem senha e permissões temporárias são medidas eficazes para reduzir vulnerabilidades.