1.Multifactor authentication

A autenticação em sistemas e websites normalmente envolve um nome de usuário e uma senha, mas pode incluir outros fatores para aumentar a segurança. Esses fatores de autenticação são classificados em diferentes categorias: algo que você sabe, algo que você tem, algo que você é e onde você está.

O fator "***algo que você sabe***" inclui senhas, frases secretas, PINs e padrões de desbloqueio, informações que apenas o usuário deve conhecer. O fator "***algo que você tem***" envolve dispositivos físicos, como cartões inteligentes, chaves de segurança USB e tokens geradores de códigos, que garantem que apenas o detentor do dispositivo possa se autenticar. Esse fator pode ser implementado por meio de hardware dedicado ou de aplicativos em celulares que geram códigos temporários.

O fator "***algo que você é***" utiliza biometria, como impressões digitais, reconhecimento facial, voz ou padrões oculares. Esses dados são armazenados como representações matemáticas e não como imagens reais. Embora a biometria seja conveniente, não é infalível e pode ser complementada com outros fatores de autenticação.

Já o fator "***onde você está***" aproveita informações de localização para validar acessos. Um sistema pode bloquear tentativas de login de locais inesperados ou suspeitos. O rastreamento pode ser feito por meio de GPS, IP ou uma combinação de métodos para determinar a posição real do usuário.

A autenticação segura geralmente combina múltiplos fatores para aumentar a proteção. Quanto mais fatores forem usados, mais difícil será para um atacante obter acesso indevido.