AUTENTICAÇÃO POR MÚLTIPLOS FATORES: POR QUE VOCÊ DEVE ADOTÁ-LA JÁ

Ao acrescentar camadas de autenticação, você acrescenta camadas de segurança às suas contas, dados e sistemas

A autenticação, no contexto da segurança, significa verificar a sua identidade. Você se autentica regularmente: ao entrar em contas e sistemas, você fornece informações para confirmar a sua condição de usuário autorizado. O problema da autenticação por um único fator — ou seja, aquela feita com senhas e PINs — é que ela constitui um único ponto de falha. Se uma senha é a única proteção em vigor e essa senha é comprometida… então, tudo fica comprometido.

A autenticação por múltiplos fatores (MFA) — também chamada frequentemente de autenticação por dois fatores (2FA) — está se tornando mais comum com o passar dos anos. Avanços tecnológicos tornaram relativamente simples a implementação de MFA em contas importantes, repositórios de dados e sistemas baseados em nuvem. Porém, há uma outra razão por trás da adoção da MFA: o roubo de senhas e os ataques bem-sucedidos de comprometimento de credenciais dispararam.

> "SEMPRE USE MFA QUANDO HOUVER ESSA OPÇÃO."

A MFA aumenta a segurança ao exigir dois ou mais elementos de informação — ou seja, múltiplos fatores — durante o processo de autenticação. Na MFA existem três fatores fundamentais:

1. **Algo que você sabe,** como uma senha, PIN ou frase.
2. **Algo que você tem,** como um código de verificação exclusivo, gerado em tempo real. Esses códigos de autenticação normalmente são gerados por um aplicativo móvel ou token de segurança ou são entregues a você por meio de uma mensagem de texto.
3. **Algo que você é,** em nível biométrico, conforme revelado por uma impressão digital, verificação de íris ou padrão de voz.

Sempre que houver opção, escolha MFA

Em alguns casos, a MFA não é opcional. As organizações frequentemente exigem que seus funcionários forneçam múltiplas formas de autenticação ao lidar com ativos como redes privadas virtuais (VPNs) e sistemas baseados em nuvem.

Em outros casos, porém, a escolha é sua. Muitos sites e aplicativos já implementaram a MFA — mas cabe a você ativá-la.

Veja a seguir três razões pelas quais você deve sempre aproveitar a MFA quando ela for oferecida:

1. **É fácil de acrescentar –** Sim, você precisa fazer algo para ativar a MFA nos seus logins, mas o processo não é difícil. Sites e aplicativos geralmente oferecem instruções simples, passo a passo, e explicam claramente quando esperar uma solicitação de MFA e como concluir um login.
2. **É fácil de usar –** Conforme observado, uma organização pode implementar a MFA de diversas maneiras. Porém, independentemente da tecnologia por trás do fator ou fatores de autenticação adicionais, a MFA acrescenta apenas alguns segundos ao seu processo de login (e esses segundos a mais valem a pena).
3. **É bem mais seguro que apenas uma senha –** Os criminosos cibernéticos têm acesso a bilhões de nomes de usuário e senhas roubadas em fóruns clandestinos. Imagine se o único obstáculo entre um criminoso e os seus dados, finanças e arquivos é uma senha comprometida? A MFA ajuda a limitar o dano que pode ser feito caso um perpetrador de ameaças roube (ou compre) credenciais de contas.