A importância do MFA: O que é e como implementar?

Vivemos em uma era digital onde estamos cada vez mais conectados: redes sociais, e-mails, contas bancárias, lojas online... Com tanta informação circulando, manter seus dados protegidos é essencial. Contar apenas com uma senha já não é suficiente para garantir sua segurança. É aí que entra a autenticação multifator, ou simplesmente MFA.

Ela adiciona uma camada extra de proteção às suas contas e dificulta o acesso não autorizado, mesmo que alguém descubra sua senha. Mas o que exatamente é MFA e como você pode usá-la no seu dia a dia? Vamos explicar de forma simples.

O que é autenticação multifator?

A MFA é uma forma de proteger suas contas solicitando mais de uma etapa para confirmar sua identidade. Em vez de apenas digitar a senha, você também precisa validar com outra informação, como:

- Um código que chega por SMS ou aplicativo no celular;
- Um reconhecimento facial ou digital;
- Um token de segurança, entre outros.

Esse processo aumenta consideravelmente a segurança e reduz as chances de invasão, mesmo com a senha em mãos.

Por que só a senha não basta?

Senhas podem ser adivinhadas, copiadas ou roubadas em golpes — e o pior: muitas pessoas reutilizam a mesma senha em vários serviços. Em algumas situações, é difícil perceber que se caiu em um site falso ou clicou em algo malicioso. Nessas horas, confiar só na senha já não basta.

Com a MFA, mesmo que alguém descubra sua senha, ainda será necessário um segundo fator para acessar sua conta. Esse passo extra pode ser o que evita um vazamento de dados ou um golpe maior.

Casos reais reforçam a importância da MFA

Em novembro de 2024, o humorista e apresentador Fábio Porchat teve sua conta no Instagram invadida por golpistas, que utilizaram o perfil para aplicar fraudes financeiras. Com mais de 6 milhões de seguidores, o impacto poderia ter sido significativo, caso os seguidores não percebessem a tentativa de golpe. A rápida recuperação da conta e os alertas publicados por sua assessoria foram fundamentais para conter os danos.

Esse caso ilustra que, mesmo pessoas com acesso a equipes de tecnologia e comunicação, continuam vulneráveis quando medidas simples de segurança — como o uso consistente da autenticação multifator (MFA) — não estão ativas ou são burladas por engenharia social.

Mais do que uma exceção, esse tipo de incidente se tornou cada vez mais comum entre usuários populares e anônimos, demonstrando que a segurança digital é uma necessidade coletiva.

Como ativar a MFA nas suas contas?

A maioria dos serviços populares já oferecem essa opção, e ativar é simples.

Você encontra a opção nas configurações de segurança de:

- E-mails (Gmail, Outlook, etc.)
- Redes sociais (Instagram, Facebook, TikTok)
- Bancos e aplicativos de pagamento
- Lojas online e serviços de streaming (Amazon, etc.)

Abaixo estão os passos para ativar a MFA/2FA em alguns dos principais aplicativos:

WhatsApp (verificação em duas etapas):

1. Abra o **WhatsApp**.
2. Vá em **Configurações** (⚙️ no iPhone ou ⋮ > Configurações no Android).
3. Toque em **Conta**.
4. Selecione **Verificação em duas etapas**.
5. Toque em **Ativar**.
6. Crie um código PIN de 6 dígitos.
7. Adicione um **e-mail de recuperação** (opcional, mas recomendado).

8. Confirme o e-mail e finalize.

A verificação será exigida periodicamente e ao registrar o número em um novo aparelho.

Facebook (autenticação de dois fatores):

1. Abra o **Facebook** e vá em **Menu** (☰).
2. Vá em **Configurações e privacidade** > **Configurações**.
3. Toque em **Segurança e login**.
4. Role até **Usar autenticação de dois fatores**.
5. Escolha um método:
    - Aplicativo autenticador (ex: Google Authenticator, Authy)
    - Código via SMS
6. Siga as instruções e confirme com o código.

Após ativado, será exigido ao entrar em um novo dispositivo.

Instagram (verificação em duas etapas):

1. Vá até seu **perfil** > toque em ☰ **(menu)** > **Configurações e privacidade**.
2. Toque em **Central de contas** > **Senha e segurança** > **Autenticação de dois fatores**.
3. Selecione sua conta do Instagram.
4. Escolha o método:
    - Aplicativo autenticador
    - Código via SMS
    - Chave de segurança
5. Ative e confirme o código enviado ou gerado.

X (antigo Twitter):

- Toque em seu **ícone de perfil** > **Configurações e privacidade**.
- Vá em **Segurança e acesso à conta** > **Segurança**.
- Toque em **Autenticação em dois fatores**.
- Escolha o método:
    - Aplicativo de autenticação
    - Mensagem de texto (SMS)
    - Chave de segurança
- Siga os passos e confirme

- Acesse as configurações de segurança da conta.
- Procure por “verificação em duas etapas” ou “autenticação multifator”.
- Escolha como quer receber o segundo código (SMS, e-mail, aplicativo autenticador ou biometria).
- Siga as instruções do serviço e confirme a ativação.

A autenticação será solicitada em novos logins ou ao usar um novo dispositivo. Mesmo com alguns segundos a mais, esse cuidado aumenta significativamente sua proteção.

Dica extra: use um aplicativo autenticador

Para ainda mais segurança, opte por aplicativos como:

- Google Authenticator
- Microsoft Authenticator
- Authy

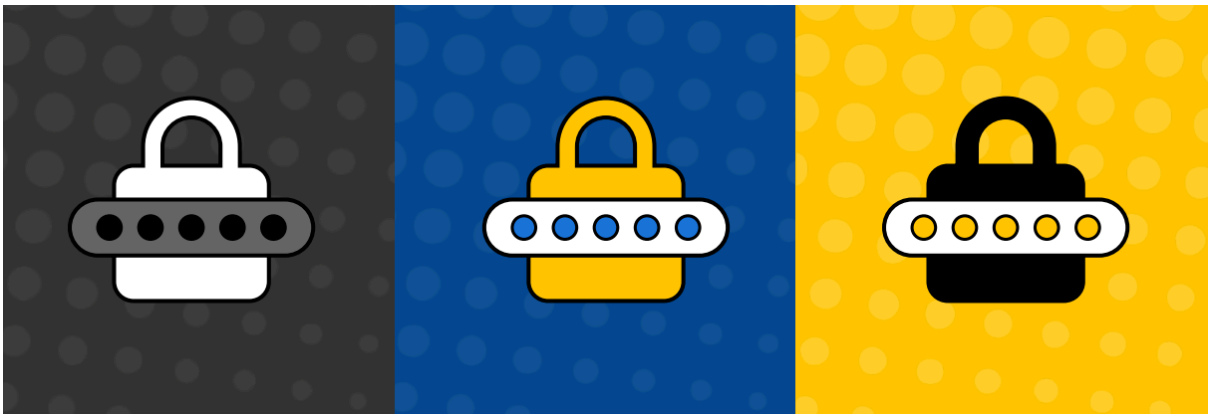
Esses aplicativos geram códigos que mudam a cada poucos segundos e funcionam mesmo sem internet.

Um lembrete importante

Habilitar a MFA é uma das formas mais eficazes de proteger suas contas.

Mesmo que sua senha vaze ou seja descoberta, essa camada adicional desencoraja invasores e bloqueia acessos indevidos.

Priorize a segurança das suas contas mais importantes. Com poucos minutos de configuração, você evita problemas maiores e mantém seus dados protegidos.



Referências:

10 benefícios da autenticação multifator (MFA). Disponível em: https://supertokens.com/blog/benefits-of-multi-factor-authentication

Fábio Porchat tem perfil no Instagram hackeado por golpistas. Disponível em: https://www.em.com.br/cultura/2024/11/6997590-fabio-porchat-tem-perfil-no-instagram-hackeado-por-golpistas.html?utm_source=chatgpt.com#google_vignette

Autora: Elisangela Silva de Mendonça