SEJA CIBERESPERTO
#CyberMonth

MÊS DA CONSCIENTIZAÇÃO EM CIBERSEGURANÇA 2021: FAÇA SUA PARTE. #BECYBERSMART

AUTENTICAÇÃO MULTIFATOR

Você já reparou na frequência com que violações de segurança, dados roubados e roubo de identidade estão na primeira página do jornal hoje em dia? Talvez você, ou alguém que você conheça, seja vítima de cibercriminosos que roubam informações pessoais, credenciais bancárias ou pior. Com o aumento da prevalência desses incidentes, você deve pensar em usar a autenticação multifator, também conhecida como autenticação forte ou autenticação de dois fatores. Você já pode ter familiaridade com essa tecnologia, já que muitos bancos e instituições financeiras exigem uma senha e um dos métodos a seguir para fazer o login: um telefonema, e-mail ou SMS com um código. Se você aplicar esses princípios de verificação a uma ou mais das suas contas pessoais, como e-mail e redes sociais, por exemplo, vai conseguir proteger melhor suas informações e a sua identidade on-line!

O QUE É

A autenticação multifator (MFA, do inglês multifactor authentication) é definida como um processo de segurança que requer mais de um método de autenticação, de fontes independentes, para confirmar a identidade do usuário. Em outras palavras, uma pessoa que queira usar o sistema só recebe o acesso após fornecer duas ou mais informações que identificam essa pessoa de forma única.

COMO FUNCIONA

Existem três categorias de credenciais: algo que você sabe, tem ou é. Eis alguns exemplos de cada categoria.

ALGO QUE VOCÊ SABE
- Senha/frase secreta
- Número de PIN

ALGO QUE VOCÊ TEM
- Token ou aplicativo de segurança
- SMS, telefonema ou e-mail de verificação
- Cartão inteligente

ALGO QUE VOCÊ É
- Impressão digital
- Reconhecimento do rosto
- Reconhecimento de voz

Para obter acesso, suas credenciais devem vir de pelo menos duas categorias diferentes. Um dos métodos mais comuns é fazer o login usando seu nome de usuário e senha. Em seguida, um código exclusivo de uso único é gerado e enviado para seu telefone ou e-mail, e esse código deve ser inserido dentro do período de tempo estabelecido. Esse código único é o segundo fator.

QUANDO UTILIZAR

A MFA deve ser usada para adicionar uma camada extra de segurança em sites que contenham informações sigilosas ou sempre que se desejar segurança reforçada. A MFA significa que pessoas não autorizadas têm mais dificuldade em fazer

o login como se fossem o proprietário da conta. Segundo o Instituto Nacional de Padrões e Tecnologia (NIST), a MFA deve ser utilizada sempre que possível, principalmente no que diz respeito aos dados mais sensíveis, como seu e-mail primário, contas financeiras e registros de saúde. Algumas organizações exigem que você use MFA; em outras, isso é opcional. Se você tiver a opção de habilitá-la, tome a iniciativa de fazê-lo para proteger seus dados e sua identidade.

ATIVE IMEDIATAMENTE A MFA NAS SUAS CONTAS

Para aprender a ativar a MFA nas suas contas, vá para o site Bloqueie seu login, que oferece instruções sobre como para aplicar essa forma mais robusta de segurança a muitos sites e produtos comuns de software que você pode estar usando. Se alguma das suas contas não estiver listada nesse site de recursos, consulte as configurações ou o perfil de usuário da conta e verifique se a opção de MFA está disponível. Se ela estiver lá, cogite ativá-la imediatamente! Nomes de usuário e senhas não são mais suficientes para proteger contas que têm informações sigilosas. Usando a autenticação multifator, você pode proteger essas contas e reduzir o risco de fraude e roubo de identidade on-line. Pense em ativar esse recurso também nas suas contas nas redes sociais!

ENTRE EM CONTATO COM A EQUIPE DO MÊS DA CONSCIENTIZAÇÃO EM CIBERSEGURANÇA DA CISA

Agradecemos o seu contínuo apoio e compromisso com o Mês da Conscientização em Cibersegurança e sua ajuda para manter todos os americanos seguros e protegidos on-line. Envie um e-mail para nossa equipe no endereço CyberAwareness@cisa.dhs.gov ou acesse www.cisa.gov/cybersecurity-awareness-month ou https://staysafeonline.org/cybersecurity-awareness-month/ para saber mais.