Manual de Segurança Digital

FASCÍCULO

AUTENTICAÇÃO DE DOIS FATORES

Secretaria de Segurança da Informação e Cibernética/GSI/PR

2024

ATUALMENTE, UTILIZAR SOMENTE UMA SENHA NÃO É SUFICIENTE PARA ALCANÇAR UM BOM GRAU DE SEGURANÇA NO SEU ACESSO AOS MAIS DIVERSOS SISTEMAS (*WEBMAIL*, CONTA BANCÁRIA, REDE SOCIAL, ETC).

Tópicos abordados:

- métodos de autenticação;
- o que é autenticação de dois fatores ou 2FA;
- como funciona a 2FA;
- quem disponibiliza a autenticação de dois fatores;
- utilize senhas fortes; e
- como a 2FA melhora a sua segurança.

Se for utilizada em dispositivo infectado por *malware*, ou em rede sem segurança, a senha torna-se alvo fácil de ataque, ou de ações de engenharia social. Neste fascículo vamos aprender a como deixar suas contas mais seguras através da 2FA!

MÉTODOS DE AUTENTICAÇÃO

Métodos de autenticação são processos usados para confirmar a identidade de um usuário, dispositivo ou sistema. Eles são essenciais para proteger o acesso a sistemas e dados sensíveis. Existem três principais métodos de autenticação:

Algo que apenas você conhece

Este método de autenticação inclui senha, uma pergunta de segurança, um número PIN ou alguma informação pessoal. O objetivo é que apenas o usuário conheça essa informação.

Algo que apenas você possui

Este tipo de método de autenticação envolve algo que que o usuário tem em sua posse. Exemplos comuns incluem cartões de identificação, chaves físicas, um dispositivo como um *smartphone* que recebe um código de verificação por SMS ou através de um aplicativo de autenticação.

Algo que você é

Este é um método de autenticação biométrica que utiliza características físicas do usuário para verificação. Exemplos dessa categoria incluem impressões digitais, padrões de retina, varreduras faciais, etc.

O QUE É AUTENTICAÇÃO DE DOIS FATORES OU 2FA

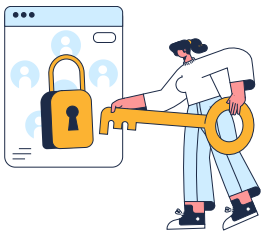
Originária do termo em inglês "*two-factor authentication*", a 2FA, ou autenticação de dois fatores, é um recurso de segurança oferecido pelos prestadores de serviços *on-line* em que é exigido que o usuário forneça duas formas de autenticação no processo de *login* de sua conta.

COMO FUNCIONA A 2FA

Ao acessar uma conta, será solicitado o primeiro fator de autenticação: nome de usuário e senha.

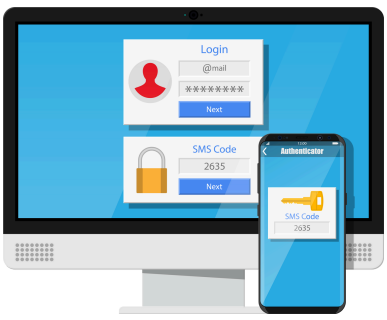
Em seguida, você deverá informar o segundo fator disponibilizado pelo prestador do serviço online. Normalmente, trata-se de algo que você possui, como um código de acesso único enviado por e-mail ou uma mensagem de texto com o código de verificação enviada ao seu número de telefone ou ao seu dispositivo móvel pessoal cadastrado. Em alguns casos, pode ser solicitada uma autenticação biométrica (algo que você é).

Somente após a entrega desses dois itens, seu acesso ao serviço será liberado.



QUEM DISPONIBILIZA A AUTENTICAÇÃO DE DOIS FATORES

Atualmente, a maioria dos serviços comerciais *on-line*, redes sociais e aplicações bancárias e de governo, como o sou.gov, tem a possibilidade de implementação da autenticação de dois fatores.



UTILIZE SENHAS FORTES

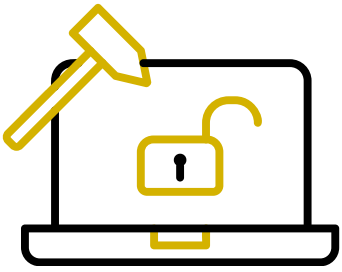
Sempre utilize senhas fortes, compostas por letras maiúscula e minúscula, número e caractere especial (como @, &, *, $)!

COMO A 2FA MELHORA A SUA SEGURANÇA

Camada extra de proteção: a 2FA possibilita uma camada extra de proteção além da senha. Mesmo que um invasor consiga obter sua senha, ainda precisará passar por uma segunda camada de autenticação.

Alerta de atividade suspeita: caso alguém tente fazer *login* em sua conta, você vai receber uma solicitação de 2FA que não foi iniciada por você, isso pode ser um sinal de que alguém está tentando acessar sua conta (nessa situação é aconselhável alterar a senha e verificar se existe atividade suspeita em sua conta).

Proteção contra golpes financeiros: muitos serviços bancários e financeiros usam a 2FA para proteger transações, diminuindo significativamente a ocorrência de fraudes financeiras.



Proteção contra *phishing* e ataques de força bruta: a 2FA é eficiente contra ataques de *phishing* e força bruta. Mesmo que o invasor consiga obter sua senha, ele ainda precisaria acessar sua segunda forma de autenticação.

Proteção contra *keyloggers*: *keyloggers* são programas maliciosos que registram as teclas pressionadas em um dispositivo. Mesmo que um *keylogger* obtenha sua senha, a 2FA pode impedir o acesso à sua conta, pois o código de autenticação é único para cada sessão de *login*.