Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Autenticação de dois fatores

Edição nº18
Dezembro/2021

A autenticação de dois fatores, também conhecido pela sigla 2FA originária do inglês "two-factor authentication" é um recurso oferecido por vários prestadores de serviços online que acrescentam uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação. A primeira forma – em geral – é a sua senha. O segundo fator pode ser qualquer coisa, dependendo do serviço. O mais comum dos casos, é um SMS ou um código que é enviado para um e-mail. A teoria geral por trás de dois fatores de autenticação é que para efetuar login, deve-se juntar algo que você sabe, como a sua senha e algo que você possui, como o seu token. Esta funcionalidade está presente nos principais sites e aplicativos atuais, como Google, Facebook, Instagram, Amazon, Dropbox, PayPal e Mercado Livre.

A autenticação de dois fatores não é um método infalível, mas é uma excelente barreira para prevenir a intromissão indesejada nas suas contas online. É de conhecimento público que as senhas são fatores de segurança problemáticos: as senhas de complexidade fracas são fáceis de lembrar, mas são fáceis de serem adivinhadas. As senhas de complexidades fortes podem ser difíceis de adivinhar, mas também são difíceis de lembrar. Devido a isso, a maioria dos usuários que tem dificuldades na criação de senhas, utilizam a mesma senha para todas as suas contas. Nesse sentido, a autenticação de dois fatores, pelo menos, faz com que um cibercriminoso não só tenha que descobrir sua senha, como também acessar o segundo fator, muito mais difícil de conseguir.

Os principais tipos de autenticação em duas etapas são:

- **Através de código enviado por SMS: quando alguém tenta entrar em sua conta de um novo dispositivo, ou mesmo de um novo navegador com sua senha, ao clicar em "entrar" ou "enviar", ele será direcionado para uma nova tela solicitando um código. Este código foi enviado para o número de celular cadastrado como um SMS;**
- **Através de PIN previamente cadastrado: quando você faz login em um novo smartphone ou de vez em quando, o aplicativo pede um número PIN de seis dígitos já cadastrado para poder iniciar/continuar seu funcionamento. Por exemplo o WhatsApp;**
- **Através do uso da biometria: o sistema pode usar dados biométricos tais como impressão digital, timbre de voz ou scanner da íris do olho para ser uma segunda fonte de autenticação;**
- **Através de chave de segurança física tal como token USB ou um chaveiro: esses dispositivos podem ser inseridos no PC ou celular, ou gerar um código único aleatório para ser usado ao fazer login em determinado serviço;**
- **Através de notificação via PUSH: há aplicativos que enviam uma notificação push para o celular, em vez de um código numérico. Neste caso, o usuário precisa tocar na tela para conceder ou negar o acesso à conta. O funcionamento é o mesmo das solicitações do Google, que funcionam em smartphones Android ou iPhone (iOS) com Smart Lock, Gmail ou o app do Google conectado à conta.**

É importante lembrar que a autenticação de dois fatores não está disponível para todos os sites ou serviços; é necessário que a plataforma ofereça esse recurso. Para as aplicações que contam com esta funcionalidade, o primeiro passo é acessar as configurações da conta e ativar a função. Geralmente a funcionalidade está na seção "Segurança".

O método de autenticação de dois fatores é seguro e, até o momento, é a melhor proteção que você pode ter. Existe um segundo benefício para sistemas de autenticação de dois fatores, que permite que você saiba quando alguém adivinhou sua senha. Se você receber um código de autenticação de dois fatores no seu dispositivo móvel ou em sua conta de e-mail e você não estava tentando entrar na conta associada a ele, isso é um bom sinal de que alguém adivinhou sua senha e está tentando roubar sua conta. Se isso acontecer, você deve mudar sua senha imediatamente. Nunca clique em nenhum link contido no e-mail de alerta. Por segurança, vá diretamente no site/app do serviço em questão e altere sua senha.

Fique ligado! No próximo mês falaremos sobre Google Hacking

Tribunal Regional Eleitoral - RN