Como criar senhas fortes para evitar golpes? Especialista dá dicas

Saiba como criar um 'cofre' para armazenar informações

A **criação de senhas fortes** continua sendo uma das medidas mais eficazes para proteger informações pessoais em computadores e smartphones. O alerta

A **criação de senhas fortes** continua sendo uma das medidas mais eficazes para proteger informações pessoais em computadores e smartphones. O alerta é do professor **Wendel Rodrigues**, doutor em computação e docente do Instituto Federal do Ceará (IFCE), que leciona disciplinas nas áreas de redes e **segurança da informação**.

“A gente vai ter que trabalhar com senhas que não são associadas a palavras e dicionários, que usem letras maiúsculas e minúsculas. Muitas vezes você pode, para não esquecer, tentar associar a uma música, uma canção que você gosta... Aí você pega só as iniciais e usa isso como senha, agrega um número, agrega um caractere especial, tipo uma arroba, um cifrão”, sugere.

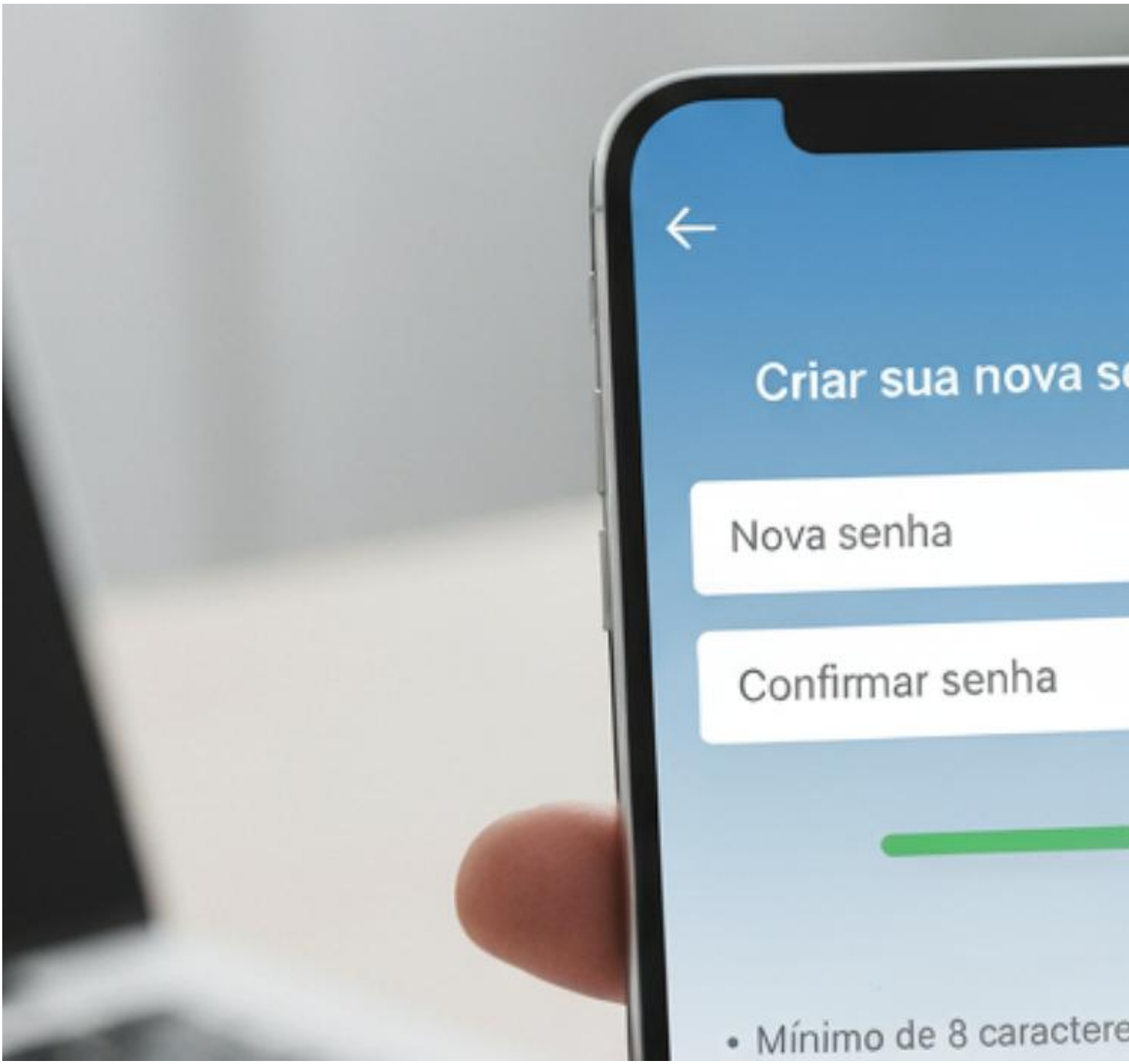
O que não usar ao criar uma senha forte:

1. Não usar palavras comuns ou de dicionário
2. Não usar sequências óbvias: jamais utilize sequências numéricas
3. Não usar informações pessoais facilmente identificáveis
4. Não usar a mesma senha em vários sistemas. Se uma vazar, todas as suas contas ficarão vulneráveis.
5. Não manter a mesma senha por tempo indeterminado. A recomendação é alterá-las periodicamente.

Rodrigues ressalta que o usuário deve evitar termos comuns e senhas óbvias. “Você não deve colocar palavras comuns, palavra 'lápis', palavra 'caderno', palavra 'computador'. Muitas vezes o pessoal usa '1234', usa a palavra 'senha'. Evite usar esse tipo de senha, porque é a primeira coisa que o pessoal que tenta invadir seu sistema vai tentar também”, disse.

Segundo o professor, informações pessoais também não devem ser usadas como senha. “O nome do esposo, da esposa, do namorado, do filho também se evita, porque quem conhece sua família vai tentar também usar essas palavras".

Com que frequência preciso mudar uma senha?



Legenda: A mistura de letras, números e caracteres especiais aumenta a segurança das senhas

Foto: Reprodução/Gemini

A recomendação é trocar as senhas periodicamente. “A cada três meses, se você puder alterar suas senhas, teria um bom resultado na segurança. Muitas vezes senhas vazam. E, se você é aquela pessoa que usa mesmo assim em vários sistemas, na hora que tem um vazamento sai em cadeia, sai em sequência, vai ali pegando todos os teus sistemas e você fica vulnerável”, alertou.

O professor também comentou sobre o uso da biometria. “Quando você usa aplicativo do celular que ele usa tanto a digital como o seu rosto, informações que são biométricas, que pertencem a você e só você tem, isso garante um maior nível de segurança, sim. Entretanto, ela pode também criar outros entraves. Se você estiver dormindo, por exemplo, alguém ali sorrateiramente pega seu celular e usa seu dedo ou usa sua face para

tentar abrir uma aplicação que não deveria abrir".

Para quem tem dificuldade em memorizar diferentes combinações, Rodrigues sugere os chamados cofres de senhas. Tecnicamente, são gerenciadores de dados que categorizam senhas e demais informações confidenciais, e habilitam logins de "um clique" para mais eficiência.

O cofre de senhas refere-se à parte criptografada do software gerenciador de senhas que armazena as senhas e dados digitalmente.

Veja cinco aplicativos para criar um cofre de senhas:

1. **LastPass:** É um dos mais conhecidos e oferece uma vasta gama de recursos, incluindo preenchimento automático, geração de senhas fortes, armazenamento seguro de notas e informações bancárias, e sincronização entre múltiplos dispositivos. Tem uma versão gratuita robusta e planos pagos com funcionalidades adicionais.

2. **1Password:** Muito elogiado pela interface intuitiva e design elegante, o 1Password oferece recursos completos para gerenciamento de senhas, além de proteção para documentos e informações confidenciais. É conhecido pela forte segurança e compatibilidade com diversos sistemas operacionais. Geralmente requer uma assinatura paga.

3. **Bitwarden:** Uma excelente opção de código aberto, o Bitwarden se destaca por oferecer muitos recursos de nível premium na versão gratuita. Ele permite sincronização ilimitada entre dispositivos, armazenamento de senhas, notas seguras, informações de cartão de crédito e identidades. É uma ótima escolha para quem busca segurança e funcionalidades sem custo.

4. **Dashlane:** Além de gerenciar senhas, o Dashlane oferece recursos como monitoramento da dark web para alertar sobre vazamentos de dados, VPN integrada em planos premium e preenchimento automático inteligente. A interface é amigável e foca na facilidade de uso combinada com segurança

5. **Keeper Security:** Conhecido por sua segurança de nível empresarial e certificações, o Keeper oferece um cofre de senhas robusto com criptografia de ponta a ponta, auditoria de senhas, e a capacidade de compartilhar registros de forma segura. Possui planos pessoais, familiares e empresariais.

De forma prática, os cofres também incluem uma função de "autopreenchimento" que lembra senhas, dados de contas e endereços ao acessar diferentes páginas e aplicativos.

“Você teria uma senha única e abre um aplicativo que tem todas as tuas senhas, de tudo que é sistema. Eles são muito úteis e têm boas aplicações que fazem isso de forma gratuita. E são confiáveis. Podem ficar tranquilos que são confiáveis", concluiu o professor.

**Wendel Rodrigues é doutor pela Universidade de Lille 1 - França com tema de tese relacionado à Computação de Alto Desempenho usando GPUs com abordagens MDE. Possui estágio pós-doutoral em Gestão da Inovação pelo Lambton College, Canadá. Trabalhou como pesquisador em tempo integral no INRIA (Institut National de Recherche en Informatique et Automatique) e parcialmente na Universidade de Hertfordshire, UK. Mestre em Computação com dissertação na área de ensino de redes de computadores. Possui graduação em Engenharia Elétrica com ênfase em Informática pela Universidade Federal do Ceará (1998). É professor titular do Instituto Federal de Tecnologia do Ceará nos cursos de telemática, engenharias da computação e de telecomunicações. Tem experiência na área de Ciências da Computação, com ênfase em Hardware, atuando principalmente nos seguintes temas: engenharia de software, computação de alto desempenho e segurança de redes.*