A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...



# Gerenciamento de Senhas

## Visão geral

O passo mais importante que você pode dar para se proteger online é utilizar uma senha forte e única em suas contas e aplicativos. Infelizmente, é quase impossível lembrar de todas as diferentes senhas de todas as suas contas. Por isso a maioria das pessoas utiliza a mesma senha. Infelizmente, reutilizar a mesma senha para diferentes contas é perigoso, porque uma vez que alguém a descobre poderá acessar todas as suas contas. Uma solução simples é utilizar um gerenciador de senhas, às vezes denominado cofre de senha. São programas que armazenam de forma segura todas suas senhas, facilitando o processo de ter diferentes senhas para cada conta. Gerenciadores de senhas simplificam porque ao invés de ter de lembrar de todas as senhas, você terá de lembrar apenas da senha mestre do seu gerenciador de senhas.

### Editor Convidado

Chris Christianson é consultor de segurança de informação sediado na California, com 20 anos de experiência e inúmeras certificações técnicas. Ele já deu várias conferências e contribuiu para muitos artigos industriais. Você pode acessar o Chris em **@cchristianson** e **https://ismellpackets.com**.

## Como funciona o gerenciador de senhas

Gerenciadores de senhas funcionam armazenando todas as suas senhas num banco de dados, às vezes chamado de cofre. O gerenciador de senhas criptografa o conteúdo do cofre e protege sua senha mestre. Quando você precisar recuperar suas senhas, como para entrar em sua conta do banco ou email, basta você digitar a senha mestre de seu gerenciador de senhas para desbloquear o cofre. Em vários casos o gerenciador de senhas vai automaticamente recuperar sua senha e fazer o login para você. Isso torna simples o processo de ter centenas de senhas fortes e únicas, pois você não terá que se lembrar de todas elas.

Alguns gerenciadores de senha armazenam seu cofre no seu computador ou celular, e outros armazenam na nuvem. Além disso, a maioria dos gerenciadores de senha tem a habilidade de sincronizar automaticamente sua senha do cofre em vários dispositivos que você autorizar. Dessa forma quando você atualizar uma senha no seu notebook, essa alteração vai ser sincronizada em todos os seus dispositivos. Independentemente de onde você tem seu banco de dados armazenado, você precisa instalar o gerenciador de senhas em seu sistema ou dispositivo para poder utilizá-lo. Na primeira vez que você configurar seu gerenciador de senhas, você precisa inserir ou importar seus logins e senhas.

© SANS Institute 2017

# Gerenciamento de Senhas

Depois disso, o gerenciador de senhas pode detectar quando você tentar se registrar em uma nova conta online ou atualizar uma senha de uma conta existente e ele atualiza automaticamente o cofre. Isto é possível porque a maioria dos gerenciadores de senhas trabalha lado a lado com seu navegador. Essa integração também permite fazer login automaticamente em seus sites.

É essencial que a sua senha mestra que você utiliza para proteger seu gerenciador de senhas seja forte e muito difícil de alguém adivinhar. Nós recomendamos que você faça uma frase secreta como sua senha mestre, que é um dos tipos mais fortes de senha possível. Se o seu gerenciador de senhas tiver verificação em duas etapas, utilize para sua senha mestre. Finalmente, certifique-se de lembrar de sua senha mestre. Caso você se esqueça, não vai poder acessar nenhuma das suas senhas.

*Os gerenciadores de senhas são um modo simples de armazenar e utilizar com segurança todas as suas diferentes senhas.*

## Como escolher um gerenciador de senhas

Existem vários gerenciadores de senha para escolher. Na seção de recursos nós fornecemos um link para análises de gerenciadores de senha. Enquanto isso, quando for procurar o melhor gerenciador de senhas, tenha em mente que:

- Ele tem de ser simples de utilizar.  Se você achar que é muito complexo para entender, ache um que se adapte melhor à sua experiência e estilo;
- O gerenciador de senhas tem de rodar em todos os seus dispositivos em que você precisa de senha para utilizar. E também deve ser fácil de manter sincronizadas suas senhas em todos seus dispositivos;
- Utilize apenas gerenciadores de senha confiáveis e bem conhecidos. Cuidado com produtos sem versões recentes ou que tenham pouco ou nenhum feedback da sua comunidade;
- Criminosos cibernéticos podem criar falsos gerenciadores de senha para furtar suas informações. Desconfie de vendedores que promovem sua própria solução de encriptação;
- Evite gerenciadores de senha que dizem ser capaz de recuperar sua senha mestre. Isso significa que eles conhecem sua senha mestra, o que te deixa exposto a muitos riscos;
- Certifique-se de que o Gerenciador de Senhas que você escolheu, continua sendo atualizando e corrigido e certifique-se de estar utilizando a versão mais nova sempre;

© SANS Institute 2017

# Gerenciamento de Senhas

- O gerenciador de senhas deve ter a capacidade de gerar automaticamente senhas fortes para você e mostrar o nível de segurança das que você escolher;
- O gerenciador de senhas também deve te dar opção de armazenar outros dados confidenciais, como respostas das suas perguntas secretas de segurança, cartões de crédito ou número de fidelidade em companhias aéreas.

Gerenciadores de senha são uma forma segura de armazenar suas senhas e outros dados confidenciais. No entanto, uma vez que salvaguardam informações muito importantes, tenha certeza de utilizar uma senha mestre única e forte, que seja não só difícil para um invasor adivinhar, mas fácil de você se lembrar.

## Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em securingthehuman.sans.org/ouch/archives.

## Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop

Marta Visser – Tradutora autônoma

Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

## Recursos

| | |
|---|---|
| Principais gerenciadores de senha de 2017 (em inglês): | https://www.pcmag.com/article2/0,2817,2407168,00.asp |
| Frases de Acesso: | https://securingthehuman.sans.org/ouch/2017#april2017 |
| Verificação em duas etapas: | https://www.securingthehuman.org/ouch/2015#september2015 |
| Bloqueie seu Login: | https://www.lockdownyourlogin.org/ |
| Dica de segurança do dia do SANS: | https://www.sans.org/tip-of-the-day |

OUCH! é publicado pelo “SANS Securing the Human” e distribuído sob o licenciamento Creative Commons BY-NC-ND 4.0 license. A distribuição ou utilização desta publicação em programas de treinamento é permitida desde que seu conteúdo não seja modificado. Para traduções ou mais informações entre em contato pelo ouch@securingthehuman.org

Board Editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser