PORQUE UTILIZAR UM GERENCIADOR DE SENHAS E QUAIS SÃO OS MELHORES?

ostec
Segurança digital de resultados

Para aumentar sua segurança online, é recomendável fazer o uso de um gerenciador de senhas que garanta senhas fortes e exclusivas para cada uma das contas existentes.

ÍNDICE

INTRODUÇÃO

A maioria das pessoas costuma usar senhas muito fracas e até mesmo repetidas em diferentes aplicações e sites.

Porém, nem de longe isso é o mais indicado quando se trata de segurança, pois, na maioria das vezes, as informações guardadas por essas senhas são importantes e valiosas, então é preciso protegê-las com senhas fortes.

Para aumentar sua segurança online, é recomendável fazer o uso de um gerenciador de senhas que garanta senhas fortes e exclusivas para cada uma das contas existentes.

Os gerenciadores de senhas armazenam suas informações de login de todas as suas contas e evitam que você digite-as sempre que precisar acessar um site protegido por senha.

As senhas são criptografadas e guardadas pelo gerenciador, que por sua vez, é protegido por uma senha mestra e essa sim é uma senha forte que você precisa decorar.

Continue a leitura para tirar as dúvidas sobre gerenciadores de senha e descobrir quais são os mais seguros e indicados.

PORQUE NÃO SE DEVE REPETIR SENHAS?

Criar uma senha e utilizá-la para diversas contas, como Facebook, e-mail e Instagram, por exemplo, é um hábito que muitas pessoas têm.

Mesmo que essa senha seja consideravelmente forte, isso pode gerar problemas graves para os usuários.

Frequentemente nos deparamos com notícias de que um grande número de senhas de usuários de determinados serviços vazou na web e, caso isso venha a acontecer com você, ter a mesma senha repetida em outro site pode ser um grande problema.

Isso se deve ao fato de que pessoas mal-intencionadas que tenham acesso a dados como seu endereço de e-mail, nome de usuário e senha, podem tentar acessar outras contas além daquela que sofreu o vazamento.

Se você faz uso das mesmas informações de login em todos os lugares, um vazamento em um site poderia dar as pessoas acesso a todas as suas contas.

Para evitar que vazamentos de senhas sejam altamente prejudiciais, o ideal é utilizar uma senha exclusiva e forte para cada site/aplicação.
As senhas devem ser imprevisíveis, longas, contendo números, letras e símbolos.

Mas criar tantos códigos mirabolantes e ainda ter que decorá-los para usar no dia a dia é estressante.
É aí que entra o gerenciador de senhas.

COMO FUNCIONA UM GERENCIADOR DE SENHAS?

Quando você utiliza um gerenciador de senhas e precisa logar em algum site, convencionalmente o processo é bem simples, bastando você acessá-lo e permitir que as credenciais de acesso sejam preenchidas automaticamente pelo gerenciador de senhas.

Contudo, para que o processo transcorra desta maneira, você deverá ter previamente cadastrado a aplicação e suas credenciais de acesso no

gerenciador de senhas, ou então ter feito acesso ao site e permitido que o gerenciador de senhas salve os dados de acesso, durante a fase de login.

Depois de cumprida a etapa de registro das credenciais de acesso no gerenciador de senhas, sempre que necessitar acessar uma aplicação, basta você utilizar a senha mestra que os dados de acesso serão preenchidos automaticamente, liberando acesso ao aplicativo/site.

Em resumo, você não precisa digitar seu endereço de e-mail, nome de usuário e outros dados, o aplicativo fará todo trabalho por você, além de manter suas senhas fortes e protegidas.

No momento em que for criar uma nova conta em algum serviço, o gerenciador também poderá ser utilizado na geração de uma senha segura, já fazendo o armazenamento da mesma para futuros acessos a esta aplicação.

Ele também pode ser configurado para preencher automaticamente informações em formulários da web.

GERENCIADORES DE SENHA SÃO REALMENTE SEGUROS?

Uma das maiores preocupações de todos: quem garante que suas informações salvas no gerenciador de senhas não serão roubadas?

A resposta mais correta para essa questão é: ninguém.

Porém, os gerenciadores de senhas mais conhecidos são muito confiáveis.

Obviamente já houve casos negativos, como quando o LastPass sofreu um ataque e os hashes de autenticação foram acessados indevidamente.

Porém, os cofres dos usuários continuaram protegidos, pois eles não são armazenados no mesmo local, e as informações são salvas com proteção por hardware para dificultar ou impedir que a criptografia seja quebrada.

Caso você prefira e se sinta mais seguro, pode utilizar um gerenciador de senhas que possua a opção de armazenar dados apenas localmente, sem enviá-los para nenhum servidor.

O 1Password, por exemplo, permite salvar o banco de dados no HD e sincronizar com o smartphone pela rede local.

O KeePassX, que é open source, nem possui integração nativa com a nuvem, você precisa configurar tudo manualmente se quiser ter acesso as senhas em qualquer lugar, armazenando seu cofre em serviços como Dropbox e Google Drive. Porém, não é o recomendável.

Sendo online ou não, os gerenciadores de senhas são melhores do que confiar apenas na sua memória, utilizar o recurso nativo do navegador ou guardar tudo num desprotegido senhas.txt.

ALGUNS GERENCIADORES DE SENHAS

Separamos dez excelentes gerenciadores de senhas, que estão repletos de recursos poderosos e intuitivos, para garantir que seus dados mais confidenciais permaneçam permanentemente protegidos. Confira.

Dashlane

Esse gerenciador de senhas conta com uma interface intuitiva e atraente, que facilita na hora de gerar senhas fortes e armazená-las em segurança.

Após salvar uma senha, o Dashlane a preenche automaticamente sempre que necessário.

O Dashlane também permite armazenar outras informações pessoais e dados de pagamento, para que você não precise

sempre preencher formulários online.
É possível também salvar notas, anexos e outras informações importantes através do recurso Secure Notes.

Além disso, ele oferece acesso a um amplo painel de identidade que classifica seu status de segurança online e permite que você saiba o que pode ser aprimorado, para aumentar sua segurança ao longo do tempo.

Este gerenciador de senhas disponibiliza uma versão gratuita que limita você a apenas um dispositivo e permite salvar até 50 senhas.

Já a versão premium conta com armazenamento e dispositivos ilimitados, além de acesso a um recurso de monitoramento da dark web.

O plano premium pode ser testado por 30 dias com garantia de reembolso.

INTUITIVE PASSWORD™
MILITARY-GRADE PASSWORD MANAGER

O Intuitive Passwaord armazena todos os dados de rede por trás de camadas de firewalls, e o acesso a seus bancos de dados é rigorosamente controlado por certificados de aplicativos.

Ele também oferece um robusto antivírus, que é atualizado regularmente.

Esse gerenciador de senhas protege sua própria rede contra ataques de DDoS e faz uso de um serviço de escaneamento de malware em tempo real para manter seus servidores permanentemente protegidos.

Ele não armazena suas senhas em texto simples, fazendo uso PBKDF2, exclusivo para cada credencial, com o objetivo de ocultar suas senhas de crackers.

Além disso, ele oferece autenticação de dois fatores através do algoritmo de senha de uso único baseado em tempo TOTP.

Disponível nas opções gratuita e premium.

Uma outra opção de gerenciador de senha que oferece autenticação de dois fatores aprimorada e suporta autenticação biométrica em dispositivos compatíveis.

Suas senhas serão convenientemente preenchidas automaticamente, enquanto a senha mestra somente

poderá ser salva por você, sem permanecer visível nos servidores ou dispositivos da empresa.

De forma muito segura, irá armazenar suas informações de cartões de crédito e sincronizar com todos os seus dispositivos.

O Sticky Password oferece um plano gratuito e um plano premium. No plano sem custo você pode usufruir de uma avaliação de 30 dias da versão premium.

LogmeOnce

Um gerenciador de senhas confiável que oferece várias opções de login com autenticação de dois fatores automática.

O login no gerenciador pode ser feito usando seu exclusivo reconhecimento de fotos via autenticação de dois fatores com reconhecimento biométrico, código PIN ou uma tradicional senha mestra.

Ele oferece recursos antirroubo para garantir que suas informações confidenciais de login permaneçam seguras caso seu dispositivo seja perdido ou roubado.

É possível fazer logout, bloquear o dispositivo, excluir todos os seus dados ou localizar seu dispositivo através de um localizador GPS, tudo de forma remota.

O LogMeOnce oferece opções gratuitas e premium para clientes e empresas, além de disponibilizar intuitivas extensões de navegador e apps nativos.

Um eficaz gerenciador de senhas voltado para empresas, mas que funciona bem como gerenciador de senhas pessoal.

O software passou em várias auditorias independentes que confirmaram que o Keeper é seguro e confiável.

Ele faz uso de uma exclusiva arquitetura de segurança de conhecimento zero para garantir que ninguém, inclusive o próprio Keeper, obtenha acesso as suas informações privadas armazenadas no gerenciador de senhas.

O Keeper sempre criptografa seus dados no dispositivo antes de enviá-los para o Cloud Security Vault.

A única maneira de decriptografar e acessar os dados armazenados no Keeper, é através do uso de sua senha mestra, a qual apenas você possui acesso.

O Keeper disponibiliza autenticação de dois fatores, além de login biométrico e do Keeper DNA, que permite confirmar sua identidade usando seu Apple Watch ou Android Wear.

Através do seu iPhone ou iPad, você pode utilizar sua impressão digital para acessar seu cofre do Keeper, via touch ID.

O plano gratuito é limitado, permitindo usar o gerenciador de senha em um único dispositivo móvel, com um limite de armazenamento de dados de 100 MB.

O plano premium para uso pessoal pode ser experimentado de forma gratuita por 30 dias. A versão de avaliação para planos corporativos é de 14 dias.

Uma excelente opção, caso sua principal preocupação seja a segurança.

O 1Password protege seus dados confidenciais de login por meio de criptografia de ponta a ponta.

Ele gera uma chave secreta com base em sua senha mestra privada para criptografar e autenticar seus dados.

Isso significa que suas informações não poderão ser comprometidas, mesmo que alguém obtenha acesso ao seu notebook ou celular.

Para que seus dados fiquem protegidos contra os cibercriminosos, o 1Password também emprega uma senha

remota segura para autenticar suas credenciais de login em seu dispositivo, para que você jamais precise enviar sua senha mestra pela internet.

Para proteger você contra o malware e tentativas de phishing, o software analisa seus sites acessados e seu navegador antes de preencher automaticamente as informações da sua conta.

O 1Password não conta com uma versão gratuita, mas você pode usar a versão de avaliação por 30 dias sem custo para descobrir se o serviço atende sua necessidade.

São vários planos disponíveis para uso pessoal e corporativo e você pode escolher o melhor para você.

O NordPass é um novo e poderoso gerenciador de senhas do excelente provedor de VPN NordVPN.

O processo de registro das credenciais de acesso é bastante simples, tornando o uso o aplicativo muito intuitivo.

Além disso, ele oferece armazenamento seguro para suas anotações privadas e informações de cartões de crédito.

Nenhum dado decriptografado é transmitido a partir do seu dispositivo, é impossível para qualquer pessoa (além de você) acessar seus dados privados de login.

A autenticação de dois fatores é opcional, mas é recomendado ativar esse recurso para garantir que nenhum hacker seja capaz de acessar seu cofre de senhas, mesmo que de alguma forma consiga obter uma cópia de sua senha mestra do NordPass.

Oferece um plano gratuito, que pode ser usado pelo tempo que você quiser. O plano premium permite sincronizar seus dados em até seis dispositivos. Você pode testá-lo por 7 dias gratuitamente.

RememBear

Faz uso dos melhores recursos de segurança para manter suas senhas protegidas sem comprometer sua conveniência.

O Remembear emprega uma senha remota segura através da troca de chaves de Diffie-Hellman, que verifica sua senha sem expô-la a uma conexão de internet.

Ele protege os dados armazenados em seus servidores através da Amazon Key Management Services.

Ele também adiciona uma camada extra de criptografia

via Transport Layer Security para minimizar sua dependência do HTTPS.

Possui uma versão gratuita que você pode utilizar em um dispositivo e uma versão premium que funciona em todos os seus dispositivos.

O RoboForm facilita para fazer login com apenas um clique, independentemente do site ou aplicativo que você está acessando.

A plataforma captura e armazena suas senhas automaticamente, conforme você navega pela internet, permitindo acessá-las de forma segura em todos os seus dispositivos.

Ele armazena suas senhas em pastas de categorias organizadas, facilitando para localizá-las.
Ele possui um plano gratuito e dois planos premium para uso pessoal, além de um plano premium com versão de avaliação gratuita de 14 dias para uso corporativo.

LastPass •••|

Esse gerenciador de senhas promete simplificar sua vida, e é exatamente isso o que ele faz.

O software com um excelente design funciona no segundo plano do seu dispositivo ou navegador para proteger, armazenar e automaticamente preencher seus dados de login sem complicação.

O LastPass contém um gerador de nome de usuário e senha integrado que ajuda a criar credenciais de login altamente seguras para todas as suas contas.

Ele não pode acessar sua senha mestra ou suas chaves de criptografia. Todos os seus dados são criptografados e decriptografados no próprio dispositivo.

Conta com uma versão gratuita excelente, que permite sincronizar suas informações em dispositivos ilimitados.

Cadastrando-se no plano gratuito, você obtém uma versão de avaliação do LastPass Premium.

DICAS IMPORTANTES PARA USAR UM GERADOR DE SENHAS

Após escolher um gerador de senhas que mais se adequa às suas necessidades, é preciso ficar atento a alguns detalhes.

Como por exemplo a senha mestra, a primeira grande decisão é escolher bem a sua senha mestra, pois ela oferecerá o controle sobre o gerenciador.

Lembre-se que ela será a única senha que você precisará decorar, portanto capriche na escolha.

A senha mestra pode ser alterada sempre que você quiser, mas para isso, é necessário lembrar-se dela. Utilize uma senha forte e segura.

Uma outra dica é mudar as senhas fracas para senhas mais seguras e difíceis de serem quebradas.

Faça proveito dos recursos oferecidos pelos gerenciadores de senhas que identificam senhas fracas e duplicadas para focar sua mudança.

Aproveite o gerenciador de senhas para guardar

informações sensíveis, como números de cartões de crédito.

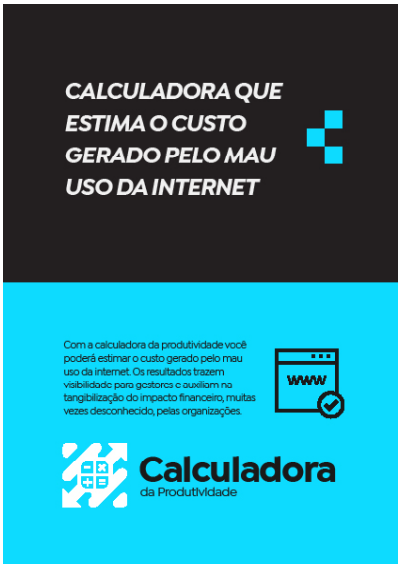
Além de tudo, os gerenciadores possuem uma segurança a mais contra ataques phishing.

Se você receber um e-mail falso dizendo que precisa clicar em um link para alterar alguns dados no site do seu banco, por exemplo, o gerenciador se senhas não preencherá automaticamente as suas informações de login, pois o site falso possui uma URL diferente daquela utilizada oficialmente pela instituição bancária.

Escolher bem um gerenciador de senhas trará inúmeros benefícios a você, além de manter seus dados pessoais e aplicativos mais seguros e poupá-lo de ter que decorar senhas grandes e fortes.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.



VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados