5 cuidados que você deve ter com as suas senhas

Talvez você nunca tenha parado para pensar, mas as senhas são mais antigas do que a própria computação. É praticamente impossível descobrir quando surgiu a ideia de usar uma palavra ou frase convencionada entre duas partes para fins de reconhecimento. Porém, basta nos lembrarmos de que, no conto “Ali Babá e os Quarenta Ladrões”, escrito há centenas de anos, a expressão “abre-te sésamo” já era usada para abrir a caverna que guardava os tesouros dos larápios.

Quando falamos do mundo digital, podemos atribuir o sistema de autenticação por senhas a Fernando Corbató, cientista da computação norte-americano que faleceu em julho de 2019 aos 93 anos de idade. Corbató contribuiu notoriamente para a evolução da informática em diversos aspectos; no entanto, sua mais famosa colaboração foi, sem dúvidas, a de permitir que diferentes indivíduos usassem o mesmo computador (quando essas máquinas ainda eram gigantescas e caríssimas) sem que um acessasse os documentos do outro.

HACK3R_
RANGER5

O engenheiro resolveu que seria uma boa ideia particionar a máquina e proteger cada repartição com uma única palavra individual, que apenas o usuário escolhido conheceria. De lá para cá, esse sistema evoluiu muito. Usar uma simples palavra como senha deixou de ser seguro, já que adivinhá-la se tornou uma tarefa relativamente fácil. Com o passar do tempo, uma combinação simples de letras e números também passou a ser ineficaz.

Hoje em dia, o mercado de segurança da informação trava uma luta ferrenha para garantir a segurança da identidade digital dos internautas. Afinal, muitos usuários ainda cometem erros crassos quando o assunto é higiene de senhas. Neste relatório, vamos listar alguns bons hábitos e contar algumas curiosidades a respeito das famosas *passwords* — além, é claro, de dar algumas dicas importantes para garantir a proteção das suas informações online.

1) NÃO USE UMA SENHA FRACA

Vamos começar pelo mais óbvio: infelizmente, ainda é gigantesco o número de internautas que usam senhas incrivelmente fracas e de fácil adivinhação. De acordo com uma recente pesquisa, as dez senhas mais usadas ao redor do mundo são, na seguinte ordem: 123456, 123456789, qwerty, password, 12345, qwerty123, 1q2w3e, 12345678, 111111 e 1234567890. Aqui no Brasil, é bastante comum o uso de nomes (sejam próprios, de celebridades, de marcas ou times esportivos), datas de aniversário e assim por diante.

Além de serem de extremamente fáceis de adivinhar, essas senhas podem ser quebradas de forma praticamente instantânea com o uso de um software de força bruta. Uma senha com nove dígitos, formada por letras maiúsculas, minúsculas e números, pode até parecer forte, mas um atacante consegue quebrá-la em aproximadamente três dias — um tempo razoável de se esperar caso o ator malicioso esteja realmente decidido a invadir a sua conta.

Hoje em dia, uma senha minimamente segura é composta por pelo menos 10 dígitos, incluindo números, letras maiúsculas e minúsculas e caracteres especiais. Dessa forma, seriam necessários cinco anos para decifrá-la — o suficiente para desanimar qualquer possível invasor.

2) USE UM GERENCIADOR DE SENHAS

A melhor senha é aquela da qual você não se lembra. Se ela é tão longa e complexa que nem o próprio usuário consegue memorizar, obviamente será impossível adivinhá-la e muito difícil quebrá-la com força bruta. Alguns internautas, apesar de terem conhecimento desse fato, acabam cometendo o erro de anotar as senhas em post-its, cadernos ou até mesmo no bloco de notas do computador ou celular. Ora, não adianta de nada ter uma senha complexa se elas estão facilmente acessíveis para qualquer pessoa!

Gerenciadores de senhas são softwares projetados especialmente para armazenar suas credenciais de forma segura e criptografada — e, ainda melhor, mantendo-as sincronizadas entre seus diferentes dispositivos. Você só precisa se lembrar da senha-mestra para abrir seu cofre. Uma vez aberto, o programa se encarrega de preencher formulários de login de maneira automática. Em smartphones que possuem tal funcionalidade, você pode contar com a identificação biométrica para abrir o cofre, o que confere ainda mais segurança ao processo.

É importante frisar que existem diversos gerenciadores de senhas disponíveis no mercado. Alguns são completamente gratuitos, enquanto outros oferecem de graça um plano simples com certas limitações. Vale a pena investir na assinatura de um plano premium para usufruir de tudo o que o software oferece. Em geral, elas são relativamente baratas, custando bem menos do que a dor de cabeça de ter uma conta importante invadida por criminosos cibernéticos. É só colocar na ponta do lápis.

3) MONITORE VAZAMENTOS DE DADOS

O Brasil continua figurando nas mais altas posições na lista de países que mais sofrem com vazamentos de dados. Só em 2021, foram 2,8 bilhões de dados sensíveis expostos na rede. Agora, pare e pense em quantas contas você possui em serviços online, redes sociais, aplicativos web e afins. Qualquer uma delas pode ser atacada a qualquer momento, fazendo com que suas credenciais sejam comprometidas. Todo esse material geralmente vai parar em fóruns obscuros da dark web, onde cibercriminosos negociam logins a preço de banana.

Felizmente, já existem diversos serviços de monitoramento pessoal que você pode aderir para ser alertado caso uma das suas senhas faça parte de um vazamento. Eles usam robôs que vasculham os quatro cantos da web em busca de novos bancos de dados comprometidos, analisando-os e tentando encontrar alguma menção à sua pessoa. Hoje em dia, alguns navegadores, inclusive, contam com essa funcionalidade parcialmente embutida.

Você pode não acreditar, mas ser notificado assim que uma das suas credenciais for comprometida pode fazer toda a diferença. Essa informação privilegiada lhe dá o poder de trocar seu login e senha em questão de segundos, antes que sejam comprados por algum meliante virtual.

4) JAMAIS REPITA SUAS SENHAS

Agora, imaginemos que uma das suas credenciais tenha sido vazada em um ataque e você não saiba disso, pois não contratou um serviço de monitoramento. Uma das primeiras coisas que os cibercriminosos fazem com senhas vazadas é iniciar uma campanha de *password spraying*. Basicamente, eles usam seus próprios robôs para tentar fazer login em outros serviços online com aquela combinação. Visto que muitas pessoas usam as mesmas senhas para diversas contas, eles geralmente têm sucesso nessa empreitada.

Nunca, jamais, em hipótese alguma, use a mesma senha para mais de um aplicativo, site, serviço ou rede social. Caso sua credencial seja comprometida, você corre o risco de ter não apenas uma, mas duas, três ou mais contas invadidas.

5) USE UM SEGUNDO FATOR DE AUTENTICAÇÃO

Por fim, nunca é demais frisar a importância da autenticação de dois fatores. Com essa camada adicional de segurança, mesmo que todas as medidas que citamos até aqui deem errado, um ator malicioso ainda não conseguirá invadir a sua conta, já que precisará de outra combinação aleatória, a qual apenas você terá acesso. Porém, tome cuidado ao usar a autenticação dupla via SMS, já que mensagens de texto podem ser facilmente interceptadas.

O mais seguro é utilizar um aplicativo dedicado que gera códigos de autenticação baseadas em assinatura temporal — uma tecnologia que conhecemos como *time-based one-time password* (senha descartável baseada em tempo ou TOTP). Em geral, esses aplicativos são gratuitos e fáceis de usar.

O FUTURO É PASSWORDLESS?

Vale a pena lembrar que diversas empresas de tecnologia estão se esforçando para criar aquilo que chamamos de “futuro passwordless” — ou seja, um mundo no qual não precisaremos mais nos preocupar com senhas, pois usaremos outras formas de autenticação. Esses métodos prometem não apenas ser mais seguros do que as passwords tradicionais, mas também mais simples e amigáveis, facilitando o nosso cotidiano no universo digital. Porém, enquanto esse sonho não se tornar uma realidade, é crucial tomar todo o cuidado possível com as suas senhas.

TESTE A NOSSA PLATAFORMA
GRATUITAMENTE DURANTE 15 DIAS!

HACKERRANGERS.COM.BR

HACK3R_
RANGERS

Bibliografia
Use this chart to see how long it’ll take to crack your passwords (Komando, março de 2021)
Most common passwords: latest 2022 statistics (CyberNews, maio de 2022)
Brasil teve 2,8 bilhões de dados expostos em 2021 (TecMundo, fevereiro de 2022)