OUCH!

SANS SECURITY AWARENESS

Sua edição mensal de conscientização de segurança

Simplificando as senhas

Visão geral

Você sempre escuta que suas senhas são fundamentais para proteger suas contas (o que é verdade!), mas raramente te contam sobre um jeito simples de criar e gerenciar com segurança todas suas senhas. Veja abaixo três passos simples para simplificar suas senhas, bloquear suas contas e proteger seu futuro.

Frase secreta

Os dias de senhas complicadas e malucas acabaram. Essas senhas são difíceis de lembrar, difíceis de digitar e, com os computadores super-rápidos de hoje em dia, pode ser fácil para um atacante cibernético decifrá-las. O segredo para as senhas é torná-las longas, quanto mais caracteres você tiver, melhor. Estas são conhecidas como frases secretas, um tipo de senha forte que usa uma frase curta ou palavras aleatórias. Veja estes dois exemplos

É hora de um café forte!

caracol-perdido-rastejar-praia

Ambas são fortes, têm mais de vinte caracteres, fáceis de lembrar e de digitar, mas são difíceis de decifrar. Você vai se deparar com sites ou situações solicitando que você adicione símbolos, números ou letras maiúsculas à sua senha, o que é bom. Lembre-se de que o tamanho é o mais importante.

Gerenciadores de senhas

Você precisa de uma senha exclusiva para cada conta. Se você reutilizar a mesma senha para diversas contas, estará correndo um grande risco. Tudo o que um atacante cibernético precisa fazer é invadir um site que você usa, roubar todas as senhas, inclusive a sua, e usá-la para fazer login em todas as suas outras contas. Acontece com muito mais frequência do que você imagina. Não acredita? Dê uma olhada no site www.haveibeenpwned.com para ver quais dos sites que você usa foram invadidos e suas senhas potencialmente comprometidas. Então, o que você deveria fazer? Usar um gerenciador de senhas.

São programas de computador especiais que armazenam com segurança todas suas senhas em um cofre criptografado. Basta se lembrar de uma senha, aquela do seu gerenciador de senhas. O gerenciador de senhas recupera automaticamente suas senhas sempre que precisar delas e faz login em sites por você. Também possuem outras funcionalidades, como guardar suas respostas a perguntas secretas, avisando quando você reutiliza senhas, um gerador de senhas que garante o uso de senhas fortes e muitas outras funcionalidades. A maioria dos gerenciadores de senhas também sincroniza de modo seguro em praticamente qualquer computador ou dispositivo, assim, independentemente do sistema que estiver usando, terá acesso fácil e seguro a todas suas senhas.

Por fim, certifique-se de anotar a senha no seu gerenciador de senhas e guardá-la em um lugar seguro em sua casa. Alguns gerenciadores de senhas permitem até mesmo imprimir um kit de recuperação do gerenciador de senhas. Dessa maneira, se você esquecer a senha do seu gerenciador de senhas, terá um backup. Ou, se você ficar doente ou estiver em uma emergência, seu cônjuge ou um parente confiável poderá recuperar as informações em seu nome.

Verificação em duas etapas

A Verificação em duas etapas (normalmente denominada Autenticação de dois fatores ou Autenticação de múltiplos fatores) oferece uma camada adicional de segurança. Isso exige que você tenha duas coisas ao fazer login em suas contas, sua senha e um código numérico gerado por seu smartphone ou enviado ao seu telefone. Esse processo garante que, mesmo que um atacante cibernético tenha sua senha, ela não poderá acessar suas contas. A verificação em duas etapas é fácil de configurar e você normalmente só precisa usá-la uma vez ao fazer login em um novo computador ou dispositivo. Ative isso sempre que puder, principalmente para suas contas mais importantes, como contas bancárias ou de aposentadoria, ou acesso ao seu e-mail. Se você estiver usando um gerenciador de senhas, é extremamente recomendável protegê-lo com uma senha forte e a verificação em duas etapas.

Pode parecer bobagem, mas esses três passos simples contribuirão bastante para proteger seu trabalho, sua reputação e seu futuro financeiro.

Editor convidado

Justin Henderson *(@SecurityMapper) é co-fundador da H & A Security Solutions, um Instrutor Certificado do SANS Institute e autor dos cursos SANS Cyber Defense e SIEM. Ele adora tudo sobre defesa cibernética e trabalha como consultor há quinze anos.*

Recursos

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi