Escolhendo e protegendo suas senhas

Por que você precisa de senhas fortes

Você provavelmente usa senhas, códigos PIN ou frases de acesso todos os dias: desde sacar dinheiro no caixa eletrônico ou usar seu cartão de débito em uma loja, até fazer login em seu e-mail ou em uma loja virtual. Acompanhar todas as combinações de números, letras e palavras pode ser frustrante, mas essas proteções são importantes porque os hackers representam uma ameaça real às suas informações. Muitas vezes, um ataque não é especificamente direcionado à sua conta, mas visa usar o acesso às suas informações para lançar um ataque maior.

Uma das melhores maneiras de proteger informações ou propriedades físicas é garantir que apenas pessoas autorizadas tenham acesso a elas. Verificar se quem solicita o acesso é realmente a pessoa que diz ser é o próximo passo. Esse processo de autenticação é ainda mais importante e difícil no mundo cibernético. As senhas são o meio mais comum de autenticação, mas só funcionam se forem complexas e confidenciais. Muitos sistemas e serviços foram invadidos com sucesso devido a senhas não seguras e inadequadas. Uma vez que um sistema é comprometido, ele fica aberto a exploração por outras fontes indesejadas.

Como escolher boas senhas

Evite erros comuns

A maioria das pessoas usa senhas que são baseadas em informações pessoais e fáceis de lembrar. No entanto, isso também facilita para um atacante descobri-las. Considere um PIN de quatro dígitos. O seu é uma combinação do mês, dia ou ano do seu aniversário? Contém o seu endereço ou número de telefone? Pense em como é fácil encontrar a data de aniversário ou informações semelhantes de alguém. E a sua senha de e-mail, é uma palavra que pode ser encontrada no dicionário? Se sim, ela pode estar sujeita a ataques de dicionário, que tentam adivinhar senhas com base em palavras ou frases comuns.

Embora intencionalmente soletrar uma palavra errado ("ceulullar" em vez de "celular") possa oferecer alguma proteção contra ataques de dicionário, um método ainda melhor é confiar em uma série de palavras e usar técnicas de memória, ou mnemônicos, para ajudá-lo a lembrar como decodificá-la. Por exemplo, em vez da senha "hoops", use "?EgDjbb" para "[Eu] [g]osto [D]e [j]ogar [b]asquete[b]ol". Usar letras minúsculas e maiúsculas adiciona outra camada de obscuridade. Mudando o mesmo exemplo usado acima para "Eg!Dj8b." cria uma senha muito diferente de qualquer palavra do dicionário.

Tamanho e complexidade

O *National Institute of Standards and Technology* (NIST) desenvolveu diretrizes específicas para senhas fortes. De acordo com as orientações do NIST, você deve considerar o uso da senha ou frase secreta mais longa permitida (8 a 64 caracteres) sempre que possível. Por exemplo, "Padrão2beisebol#4mYmiemale!" seria uma senha forte porque possui 28 caracteres e inclui letras maiúsculas e minúsculas, números e caracteres especiais. Você pode experimentar diferentes variações de uma frase secreta, por exemplo, algumas aplicações limitam o comprimento das senhas e outras não aceitam espaços ou certos caracteres especiais. Evite frases comuns, citações famosas e letras de músicas.

O que fazer e o que não fazer

Depois de criar uma senha forte e memorável, é tentador reutilizá-la, mas não o faça! Reutilizar uma senha, mesmo que seja forte, coloca suas contas em risco tanto quanto o uso de uma senha fraca. Se os invasores adivinharem sua senha, terão acesso às suas outras contas com a mesma senha. Use as seguintes técnicas para desenvolver senhas exclusivas para cada uma de suas contas:

- Use senhas diferentes em sistemas e contas diferentes.
- Use a senha ou frase mais longa permitida por cada sistema de senha.
- Desenvolva mnemônicos para lembrar senhas complexas.

- Considere usar um programa gerenciador de senhas para acompanhar suas senhas. (Veja mais informações abaixo.)
- Não use senhas baseadas em informações pessoais que possam ser facilmente acessadas ou adivinhadas.
- Não use palavras que possam ser encontradas em qualquer dicionário de qualquer idioma.

Como proteger suas senhas

Depois de escolher uma senha fácil de lembrar, mas difícil de adivinhar por outros, não a escreva e não a deixe em algum lugar onde outros possam encontrá-la. Escrevê-la e deixá-la em sua mesa, ao lado do seu computador, ou, pior ainda, colá-la no seu computador, torna-a facilmente acessível para alguém com acesso físico ao seu escritório. Não compartilhe suas senhas com ninguém e esteja atento a atacantes que tentem enganá-lo por meio de ligações telefônicas ou mensagens de e-mail solicitando que você revele suas senhas.

Programas chamados gerenciadores de senhas oferecem a opção de criar senhas aleatórias para todas as suas contas. Em seguida, você acessa essas senhas fortes com uma senha principal. Se você usa um gerenciador de senhas, lembre-se de usar uma senha principal forte.

Problemas de senha podem surgir da capacidade dos seus navegadores da web de salvar senhas e suas sessões on-line na memória. Dependendo das configurações do seu navegador da web, qualquer pessoa com acesso ao seu computador pode descobrir todas as suas senhas e acessar suas informações. Lembre-se sempre de fazer logout quando estiver usando um computador público (na biblioteca, em uma lan house ou até mesmo em um computador compartilhado em seu escritório). Evite usar computadores públicos e Wi-Fi públicos para acessar contas sensíveis, como bancárias e de e-mail.

Não há garantia de que essas técnicas impedirão um invasor de descobrir sua senha, mas tornarão mais difícil.

Não esqueça do básico sobre segurança

- Mantenha seu sistema operacional, navegador e outros softwares atualizados.
- Use e mantenha um software antivírus e um firewall.
- Escaneie regularmente seu computador em busca de spyware.
- Tenha cautela com anexos de e-mail e links não confiáveis.
- Fique atento a atividades suspeitas em suas contas.

Fonte: CISA

Revisão #1
Criado 2023-05-12 17:57:06 UTC por suporte
Atualizado: 2023-05-12 17:57:21 UTC por suporte