SECURITY-MINDED

Recomendações práticas de segurança para o dia a dia.

TRANCADO A CHAVE

A criação de senhas fortes proporciona uma segurança melhor com o mínimo de trabalho

Você pode comprar um pequeno cadeado por menos de um dólar — mas não pode contar com ele para proteger itens valiosos. Um ladrão provavelmente conseguiria abrir um cadeado barato sem muito esforço ou simplesmente quebrá-lo. Ainda assim, muitas pessoas utilizam senhas analogamente fracas para "trancar" seus bens mais valiosos, inclusive dinheiro e informações confidenciais.

Felizmente, todo mundo pode aprender a criar e a gerenciar senhas mais fortes. É uma maneira fácil de reforçar a segurança, tanto no trabalho quanto em casa.

O que torna uma senha "forte"?

Digamos que você precise criar uma senha nova com pelo menos 12 caracteres e que inclua algarismos, símbolos e letras maiúsculas e minúsculas. Você pensa em uma palavra da qual pode se lembrar, muda a primeira letra para maiúscula, acrescenta um algarismo e finaliza com um ponto de exclamação. O resultado: ***Testamento1!***

Infelizmente, os hackers dispõem de ferramentas sofisticadas que podem quebrar facilmente senhas baseadas em palavras encontráveis em dicionários (como "testamento") e padrões comuns, como tornar maiúscula a primeira letra.

Aumentar a complexidade, a aleatoriedade e o comprimento de uma senha pode torná-la mais resistente às ferramentas dos hackers. Por exemplo, uma senha de oito caracteres pode ser adivinhada por um atacante em menos de um dia, mas uma senha de 12 caracteres levaria duas semanas. Uma senha de 20 caracteres levaria ***21 séculos***.

Você pode aprender mais sobre criação de senhas fortes no treinamento de conscientização quanto à segurança da sua organização. A sua organização talvez tenha também diretrizes ou uma política de senhas em vigor.

A importância da exclusividade

Muitas pessoas reutilizam senhas em diversas contas e os atacantes aproveitam-se desse comportamento arriscado. Se um atacante obtém uma senha — mesmo que seja uma senha forte — ele pode tentar utilizá-la para acessar outras contas valiosas.

Veja a seguir um exemplo da vida real: há dez anos, Alice entrou em um fórum on-line de jardinagem. Ela também criou uma conta de pagamentos on-line e *utilizou a mesma senha*. Ela logo esqueceu-se do fórum de jardinagem, mas anos depois alguém acessou sua conta de pagamentos e roubou uma grande soma de dinheiro.

Os hackers possuem ferramentas sofisticadas que podem quebrar facilmente senhas baseadas em palavras de dicionário e padrões comuns.

DICAS PARA FAMILIARES E AMIGOS

Considere compartilhar o que você aprendeu sobre senhas e pergunte a seus familiares e amigos o que eles sabem sobre cybersecurity e quais foram suas experiências.

1. **Nunca reutilize senhas** – Crie uma senha forte e exclusiva para cada conta ou dispositivo. Dessa forma, se uma única conta for hackeada, as outras contas não correrão risco.
2. **Crie senhas longas e complexas** – Senhas baseadas em palavras de dicionário, nomes de animais de estimação ou outras informações pessoais podem ser adivinhadas pelos atacantes.
3. **Use um gerenciador de senhas** – Essas ferramentas podem armazenar e gerenciar com segurança as suas senhas, além de gerar senhas novas fortes. Alguns podem até avisar caso uma senha tenha sido comprometida.

Alice não sabia que o fórum de jardinagem tinha sido hackeado e que as credenciais dos usuários tinham sido vazadas on-line. Um atacante provavelmente tentou reutilizar a senha vazada de Alice em sites populares — e eventualmente teve sorte.

Como proteger suas senhas

1. **Não anote suas senhas** – Muitos cometem o erro de anotar senhas em bilhetes adesivos e deixá-los à mostra. Mesmo que você esconda a sua senha, alguém ainda poderá encontrá-la. Da mesma forma, não guarde suas informações de login em um arquivo no seu computador, mesmo que você criptografe esse arquivo.
2. **Não compartilhe senhas** – Não há como você se certificar de que os outros manterão suas credenciais protegidas. No trabalho, você pode ser responsabilizado caso alguma coisa aconteça quando alguém estiver conectado como se fosse você.
3. **Não salve informações de login no seu navegador** – Alguns navegadores armazenam essas informações de maneiras inseguras e uma outra pessoa pode acessar as suas contas caso se apodere do seu dispositivo.