9. A complexidade da senha é uma droga (use senhas em vez disso)
8 caracteres com complexidade não é mais uma senha segura. Em vez disso, use um mínimo de 12 caracteres e treine os usuários nas frases secretas.

Quanto mais longa a senha, melhor.
As frases secretas são simplesmente duas ou mais palavras aleatórias colocadas juntas. Você pode adicionar números e caracteres se quiser, mas eu não faria disso um requisito.

Estudos mostraram que quando você exige complexidade, ela é usada em um padrão semelhante e depois repetida. Os hackers perceberam isso e agora existem enormes listas de senhas (disponíveis gratuitamente) que contêm milhões de senhas fáceis de adivinhar.

Conhece alguém que usa senhas como essa?

- S @ mmer2018 ou Winter2018! Junho de 2018 $
- P@ssw0rd
- 123Mudar$
- Mudar123$

Estas são senhas horríveis e são facilmente adivinhadas.

Senhas longas e o uso da técnica de frase secreta tornam mais difícil para o software de cracking de senha e para os hackers adivinharem.

- Melhor política de senha
- Definir senhas de 12 caracteres
- Lembre-se de 10 histórico de senha
- use senhas

Política de bloqueio 3 tentativas

A chave para usar frases secretas é ser totalmente aleatório com cada palavra, você não quer digitar uma frase onde a próxima palavra possa ser adivinhada.

- Boas senhas com senhas
- Bucketguitartire22
- Screenjugglered
- RoadbluesaltCloud

Os exemplos acima são totalmente aleatórios. Levariam muito tempo para quebrar e provavelmente ninguém iria adivinhá-los.

O NIST atualizou recentemente suas diretrizes de política de senha na **Publicação Especial 800-63** para atender aos novos requisitos para políticas de senha.
Se sua organização deve atender a determinados padrões, certifique-se de que esses padrões suportem essas recomendações de senha.

Além disso, certifique-se de atualizar a política escrita de sua empresa.