Criando Senhas Seguras para suas transações de Cash Management e Trade

As senhas se tornaram parte integral em nossas vidas, para acessarmos nossas estações de trabalho, internet banking, e-mail pessoal e, inclusive, nossos telefones. Uma senha forte é um componente importante para nos protegermos contra a fraude, mas um número significativo de usuários on-line continuam utilizando senhas frágeis.

Senhas Comuns

As violações de dados foram notícias frequentes em 2016 e 2017. Embora, teoricamente, existam muitas possibilidades para uma senha, os estudos mostram que as 25 senhas mais usadas representam 50% em uma amostra de 10 milhões de senhas.[1] Essas senhas comuns são as primeiras que um fraudador vai tentar atacar, e caso você as utilize, sua segurança estará em risco.

Como os fraudadores Atacam

É muito mais fácil criar uma senha segura quando entendemos como um cibercriminoso trabalha para hackear nossa conta. O "hackeamento" se industrializou e atualmente, a maioria das violações é feita por softwares automáticos.

Os programas utilizados pelos hackers começam testando as senhas mais utilizadas antes de avançar para as palavras e frases comuns, como nomes de pessoas, lugares ou equipes de esportes. O programa depois continua buscando todas as palavras do dicionário antes de tentar milhões de combinações de caracteres aleatórios, até que senha é decifrada ou o hacker busca uma solução mais fácil.

[1] http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/

Os exemplos abaixo mostram em quanto tempo um hacker levaria, com um computador doméstico, para decifrar cada senha:

senha	1 segundo	My S5nhA	19 minutos
Senha	1 segundo	Senh@Forte	13 dias
senha1	2 segundos	Est5éminha5enha	8 anos
senha17	3 minutos	Uma_SEnh@ FOrte	33 anos
Senha2017	3 minutos	Cr3arUmasenh@FOrte	400 anos

Dicas para criar uma Senha Segura

- As senhas devem ter pelo menos oito caracteres e devem incluir uma combinação de letras, números e símbolos. Como regra geral, quanto mais longa for a senha, mais forte será.
- Alternar entre maiúsculas e minúsculas ajuda a reforçar a senha. Por exemplo, a palavra 'transferência' poderia ser escrita 'tRAnsFeRênCIa'.
- Utilize "linguagem hacker" substituindo algumas letras por números de aspecto similar ou caracteres especiais. Por exemplo, a palavra "banking" poderia ser escrita como "b@ Nk1nG".
- Basear sua senha em uma frase pode te ajudar a lembrar combinações mais complexas. Por exemplo 'HumPty dUmpty S@T'.
- Outra boa maneira de lembrar uma senha mais complexa é pensar em uma oração e depois utilizar a primeira letra de cada palavra. Por exemplo, 'Boston está a 4 horas de Nova York de carro' poderia ser digitado 'Bea4hdNYdc'.

Erros comuns que devem ser evitados

- Não use informações, palavras comuns, nomes, equipes desportivas ou lugares em suas senhas.
- Acrescentar um número, no final de uma palavra conhecida (por exemplo 'computador1') não torna uma senha mais segura.
- Não reutilize a mesma senha para diferentes contas on-line, já que uma única violação poderia resultar em múltiplas fraudes.
- Nunca anote suas senhas; elas podem ser facilmente roubadas de seu computador ou escritório.
- Não compartilhe suas senhas com amigos, colegas ou qualquer pessoa que solicitar essa informação por telefone.

1581915 07/17