Evite senhas com referências pessoais e clichês

Em primeiro lugar é necessário abolir as senhas óbvias, que envolvam pistas pessoais: Datas de Aniversário, casamento, nome dos filhos, ou qualquer coisa que esteja relacionada a vida do usuário, se utilizada de uma forma simplificada, serão sempre as primeiras alternativas dos *hackers*.

Senhas com sequências numéricas ou alfabéticas também costumam ser comuns. Outras como “*password*”, “senha” ou combinações óbvias como “123456” também são modelos recorrentes. Lembre-se: Uma senha fácil de se recordar, é também fácil de se descobrir.

Preste atenção nas combinações de sua senha

Reutilizar senhas em diferentes sites e aplicações não é aconselhado. Usar a mesma senha ou ainda investir em pequenas variações de uma senha padrão, como “123abc” e “abc123”, pode simplificar o trabalho para os hackers.

Use a criatividade! Pense em sequências diferentes, alterne números e letras e considere investir em símbolos. Uma alternativa que também pode ser eficaz é utilizar frases pouco convencionais.

Se preferir usar informações pessoais e datas marcantes de sua trajetória, pense em siglas que possam traduzi-las e transforme em uma senha forte mesclando com diferentes tipos de caracteres. Essa pode ser uma saída para auxiliar a sua memória e, ainda assim, garantir uma senha segura.

Mantendo suas senhas fortalecidas

Segundo conteúdo disponibilizado no site da Microsoft, abaixo listamos as principais características que tornam uma senha forte:

– Pelo menos oito caracteres;

– Não contém seu nome de usuário, seu nome real ou o nome da empresa;

– Não contém uma palavra completa;

– É bastante diferente das senhas anteriores;

– Contém caracteres de cada uma destas quatro categorias:

1. Letras maiúsculas: A, B, C;
2. Letras minúsculas: a, b, c;
3. Números: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9;
4. Símbolos do teclado (todos os caracteres do teclado não definidos como letras ou números) e espaços: ` ~ ! @ # $ % ^ & \* ( ) \_ – + = { } [ ] | : ; ” ‘ , . ? /

Todas essas variáveis poderão ajudá-lo a criar uma próxima ou nova senha potente e de total confiança. Além disso, outros fatores também podem auxiliar a manter todas as suas contas seguras, entre eles:

**Usar um gerenciador de senhas:** Estas aplicações criam senhas aleatórias, além de armazená-las todas em sua conta, garantindo segurança e facilidade na hora dos logins. Um bom exemplo deste tipo de recurso é o [1Password](http://1password.com/);

**Mudar as senhas frequentemente:** Normalmente criamos uma senha para um site e nunca mais mudamos. Segundo as boas práticas dos profissionais da área de TI, é recomendado que uma senha seja alterada a cada três meses e nunca seja usada novamente;

**Usar plug-ins de senha:**Diversos sites trazem a opção de utilizar os logins do Google e do Facebook para se cadastrar, evitando assim que você precise pensar em mais senhas. Essa opção é de grande apoio, pois permite que se invista esforços para manter uma quantidade menor de senhas fortalecidas e também facilitando sua alteração periódica;

**Autenticação Dupla:**Esse método serve como uma proteção extra, que adiciona mais um passo antes de acessar a conta em questão. Geralmente são ativados através de códigos de segurança enviados para o celular, e-mails de confirmação ou perguntas secretas.