COMO CRIAR SENHAS FORTES E PROTEGER SEUS DADOS NA UFV

O acesso a ambientes virtuais é essencial no mundo digital, e com a UFV não poderia ser diferente. Por meio dos sistemas de informação, você, seja estudante, técnico ou professor, pode executar várias tarefas importantes no seu dia a dia. E é fundamental que você garanta sua autenticidade e confidencialidade ao acessar esses sistemas.

A senha é um dos principais mecanismos de proteção. No entanto, por medo de esquecer ou por simples comodidade, muita gente tem o hábito de criar senhas fracas para acesso a e-mail, programas e plataformas. Se a senha é muito simples para você, também será para uma pessoa mal intencionada que queira roubar seus dados ou se passar por você.

O que é uma senha forte?

Uma senha forte é aquela difícil de adivinhar. Trata-se de uma combinação de caracteres construída para dificultar a descoberta por pessoas ou por programas de computador, impedindo invasões às contas digitais e garantindo mais segurança.

A força de uma senha pode ser medida pelo tempo e quantidade de tentativas que seriam necessárias para um invasor descobri-la. Para isso, ela deve ter algumas características:

- Ser longa, com pelo menos 8 caracteres, mas de preferência ainda mais.
- Ser complexa, com um conjunto imprevisível de caracteres.
- Ser exclusiva, evitando-se usar a mesma senha para acesso a contas ou sistemas diferentes.

Os sistemas de senhas atuais usam os caracteres padrão ASCII. Isso significa que você pode criar uma combinação mesclando números, letras e símbolos (!, @, #, $). Em geral, caracteres acentuados ou com cedilha (os chamados diacríticos) devem ser evitados, pois nem sempre são compatíveis com os sistemas que armazenam essas senhas.

Para ter uma senha forte, você pode seguir algumas orientações:

- Use frases ou expressões, que fazem a senha ser longa.
- Combine maiúsculas, minúsculas e caracteres especiais.
- Evite usar dados pessoais que possam ser facilmente descobertos por outras pessoas, como nomes de pessoas ou empresas, datas, números de telefone ou de algum documento, como CPF e RG. Também não utilize informações facilmente acessíveis, como as dos seus perfis em redes sociais.
- Evite padrões comuns como “123456” ou “admin” na senha. Não use sequências numéricas nem alfabéticas. Usar padrões de teclado, como “qwerty” ou “asdfgh”, também é uma má ideia.
- Evite a substituição óbvia de caracteres. É sempre bom mesclar letras e números na hora de criar uma senha, mas cuidado ao usar números e símbolos que substituem letras de forma óbvia, como o zero no lugar da letra “O”, o cinco em vez do “S” ou o símbolo @ substituindo a letra “a”, por

exemplo. Muitos hackers hoje têm softwares sofisticados que codificam facilmente essas substituições e elas acabam não cumprindo seu papel.

Dicas para criar uma boa senha

Todavia, se uma senha deve ser complexa e imprevisível, como fazer para memorizá-la? Na verdade, ter uma senha que seja relativamente fácil de lembrar é importante. Não é nada útil ter uma senha formada por 20 caracteres aleatórios que tenha que ser anotada em um papel porque a pessoa que a utiliza não se lembra dela. Uma senha como “SucoDeCenouraComLimaoR$1.99” é tão segura como “jHsTFOyEMrFmARzGyMtaT”, mas é bem mais fácil de lembrar.

Crie senhas fáceis de lembrar, que estejam relacionadas a algum vínculo afetivo marcante ou a uma experiência pessoal. Porém, fique atento a informações que possam ser acessíveis por quem o conhece ou visita suas redes sociais.

Você poderia usar como senha:

- Um trecho da letra de uma música, de um filme ou de um livro, mas cuidado para não usar frases já muito famosas.
- Palavras aleatórias combinadas: escreva uma frase sem sentido com palavras não relacionadas, separando-as com algum símbolo, o que dificulta a associação com dados pessoais.
- Uma abreviação ou acrônimo: crie uma senha usando as primeiras letras de cada palavra de uma frase que seja fácil de lembrar.

Em vez de criar uma senha “na unha”, você pode usar um gerador de senhas para criar combinações complexas e aleatórias. Essa é uma opção mais segura que dificulta qualquer tentativa de adivinhação, e há várias opções de geradores que você acessa apenas pesquisando em algum motor de busca, como o Google.

Se você já escolheu uma senha, você pode medir a força dela usando ferramentas confiáveis disponibilizadas por organizações de segurança da informação. Um exemplo é o verificador de senhas da Kaspersky (uma conhecida empresa de antivírus), disponível aqui.

Exemplos de boas senhas

Para ilustrar o que conversamos até aqui, veja alguns exemplos de boas senhas aplicando algumas das recomendações que vimos:

Exemplo 1:

`gato$montanha2azul%futebol`

É uma boa senha porque concatena 4 palavras aparentemente não relacionadas, usando números e símbolos no meio delas. Com isso, ela ficou longa e usa vários tipos de caracteres.

Exemplo 2:

`EUqUsO!vAcOaG?`

É uma boa senha porque foi construída a partir de uma frase fácil de lembrar: “Eu quero sorvete! Vamos comer agora?”. A senha seguiu a regra de usar as duas primeiras letras de cada palavra, sendo a segunda letra sempre maiúscula, e manter os símbolos de exclamação e interrogação. É uma senha razoavelmente longa, com 14 caracteres, misturando caracteres especiais (“!” e “?”), letras maiúsculas e minúsculas.

Exemplo 3:

`!HMnrsQ4VaGnJ-tT`

Essa senha é forte porque foi gerada usando um gerador de senhas aleatórias. Não é fácil de lembrar, mas é guardada com segurança em um gerenciador de senhas.

Outros bons hábitos

Além de ter uma senha forte, outros hábitos são muito bem-vindos para garantir a segurança no acesso a sistemas de informação.

- Não use a mesma senha para tudo. Se alguém descobrir sua senha de alguma conta, pelo menos não poderá acessar outro sistema com essa mesma senha.
- Procure alterar as senhas de forma periódica. Em alguns casos, a troca regular da senha é obrigatória, e senhas anteriores não podem ser reutilizadas. Além disso, ao trocar de senha, não use uma que seja parecida com a anterior.
- Use um gerenciador de senhas: utilize ferramentas confiáveis para gerar senhas complexas e armazenar as combinações de forma segura, eliminando a necessidade de decorar.
- Evite anotar senhas em aplicativos desprotegidos, como bloco de notas e similares. Se precisar anotar a senha, não a deixe disponível na sua mesa ou computador. Guarde as senhas escritas em algum lugar secreto ou trancado. Em vez de escrever sua senha, considere a possibilidade de escrever uma dica que o faça se lembrar da senha. Por exemplo, se a sua senha for "Ipanema$Aniversario#38!anos", pode anotar "A minha viagem favorita".
- Considere a possibilidade de adicionar um segundo fator de autenticação, que reforça a segurança do seu acesso a um sistema.

Saiba mais

Para mais informações sobre como criar uma boa senha, acesse os links a seguir, que foram utilizados para elaborar este material.

Dicas do Serasa para criar senha forte e proteger informações online
Dicas do Google para criar uma senha forte
Dicas da Microsoft para criar uma senha forte
Dicas da Kaspersky para gerar senhas fortes e exclusivas