No ano de 2022, diversas empresas sofreram tentativas de ataques cibernéticos que poderiam impactar diretamente a segurança dos dados. Portanto, é recomendado que funcionários e clientes de lojas virtuais sempre mantenham suas senhas de acesso atualizadas, alterando-as a cada três meses. Pensando nisso, cite pelo menos três métodos para melhorar essas senhas, com foco em fortalecê-las.

A segurança das senhas é crucial para proteger informações sensíveis contra ameaças cibernéticas. Aqui estão três métodos recomendados para fortalecer senhas:

1. **Complexidade e Comprimento:**
   * Crie senhas complexas que combinem letras maiúsculas e minúsculas, números e caracteres especiais.
   * Evite usar palavras comuns ou sequências óbvias.
   * Aumente o comprimento da senha. Senhas mais longas geralmente são mais seguras.

Exemplo: **#C&yP1tR@5**

1. **Evite Informações Pessoais Óbvias:**
   * Evite usar informações pessoais facilmente disponíveis, como nome, aniversário ou nome de familiares.
   * Não utilize sequências óbvias, como "12345" ou "abcdef".

Exemplo: Evite senhas como **Joao1985** ou **Senha123**.

1. **Utilização de Gerenciadores de Senhas:**
   * Considere o uso de gerenciadores de senhas confiáveis. Eles geram senhas complexas e armazenam de forma segura, eliminando a necessidade de lembrar várias senhas.
   * Configure senhas únicas para cada serviço ou conta online.

Exemplo de gerenciador de senha: **1Password**, **LastPass**, **Bitwarden**.

Lembrando que é essencial educar os funcionários e clientes sobre a importância de manter senhas seguras, bem como instruí-los sobre práticas de segurança cibernética, como a autenticação de dois fatores (2FA). Além disso, a atualização regular das senhas é uma boa prática para reduzir o risco de comprometimento da conta.