

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.

- **Complexidade da Senha:**
  - Inclua uma combinação de letras maiúsculas e minúsculas.
  - Adicione números e caracteres especiais, como "! @ # \$ %".
  - Evite informações pessoais óbvias, como nomes, datas de nascimento ou palavras comuns.
- **Comprimento da Senha:**
  - Utilize senhas longas, pois senhas mais longas são geralmente mais seguras.
  - Considere frases ou combinações de palavras que sejam fáceis para você lembrar, mas difíceis para os outros adivinharem.
- **Não Reutilize Senhas:**
  - Evite usar a mesma senha para diferentes contas online.
  - Utilize gerenciadores de senhas para criar e armazenar senhas únicas para cada serviço.
  - Se uma senha for comprometida, isso limitará o impacto em outras contas.

Lembre-se de que a educação sobre práticas seguras na internet é crucial. Além disso, a autenticação de dois fatores (2FA) é uma camada adicional de segurança que adiciona um passo extra para verificar a identidade do usuário, o que pode ser extremamente eficaz na proteção de contas contra acessos não autorizados.