Criptografia

DANILLO ARAÚJO DE PAIVA

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.

Fortalecer senhas é uma prática fundamental para melhorar a segurança das contas online. Aqui estão três métodos para criar senhas mais robustas:

1. Complexidade e Comprimento:
- **Complexidade:** Use uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Isso aumenta significativamente a complexidade da senha.
- **Comprimento:** Senhas mais longas são geralmente mais seguras. Tente criar senhas com pelo menos 12 caracteres ou mais.

Exemplo:
- Frase ou sequência fácil de lembrar, mas com caracteres especiais e números adicionados. Por exemplo, transformar "GatoAmarelo" em "G@t0_4m@r3l0".

2. Evitar Informações Pessoais Óbvias:
- Evite informações pessoais facilmente acessíveis ou associadas a você, como nomes próprios, datas de nascimento, ou palavras encontradas em dicionários.
- Não use sequências óbvias, como "123456" ou "qwerty".

Exemplo:
- Não use combinações fáceis, como "Senha123" ou "NomeAnoNascimento".

3. Uso de Gerenciadores de Senhas:
- Utilize um gerenciador de senhas confiável para criar e armazenar senhas complexas de forma segura.
- Isso permite que você use senhas exclusivas para cada conta sem precisar memorizar todas elas.

Exemplo:
- Ferramentas como LastPass, 1Password ou Bitwarden podem ajudar a gerar senhas fortes e armazená-las com segurança.

Além dessas práticas, é essencial atualizar suas senhas regularmente e habilitar a autenticação de dois fatores (2FA) sempre que possível. A combinação dessas técnicas pode significativamente reforçar a segurança das suas contas online.