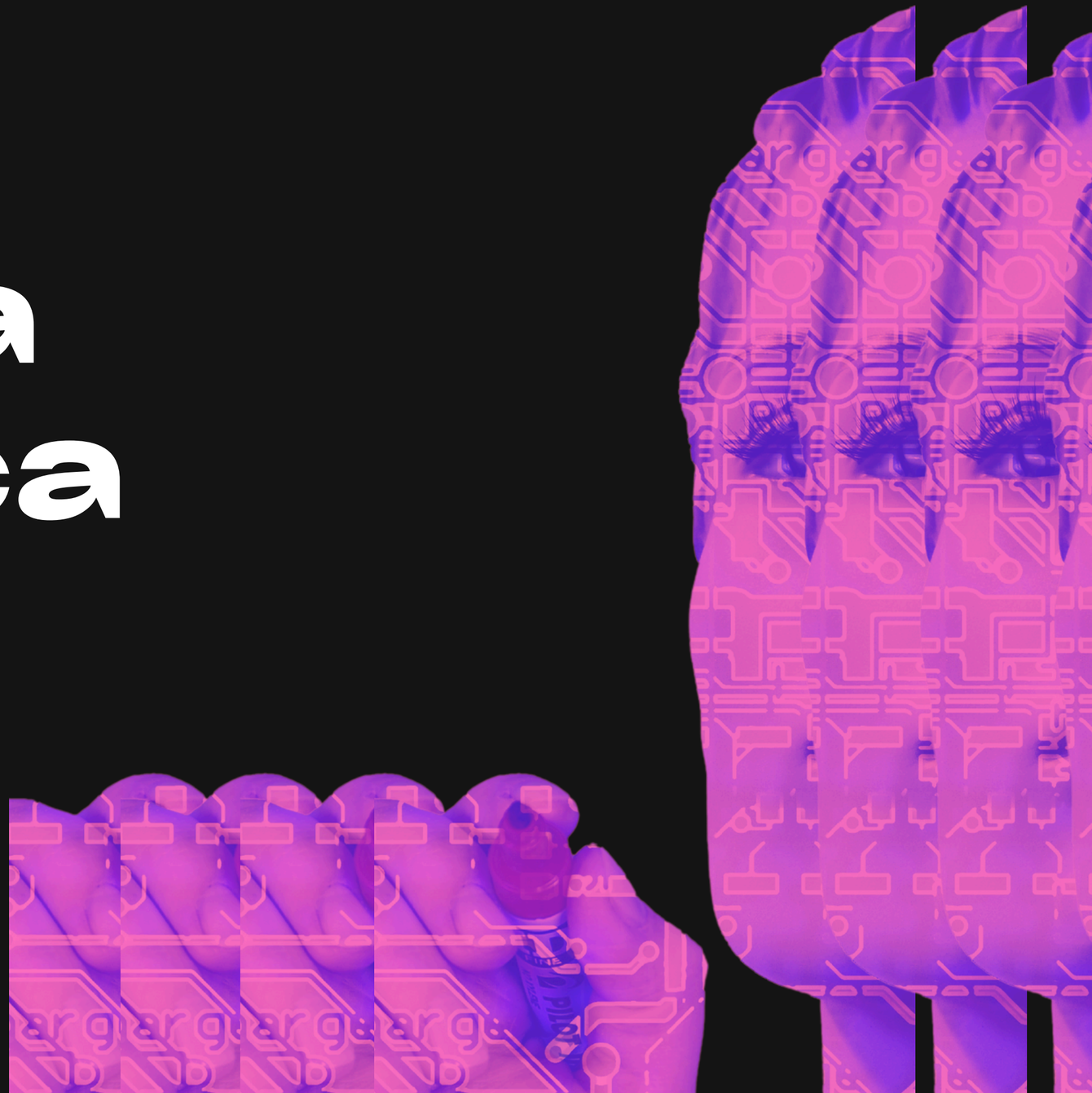
Segurança Cibernética



O que é segurança cibernética?

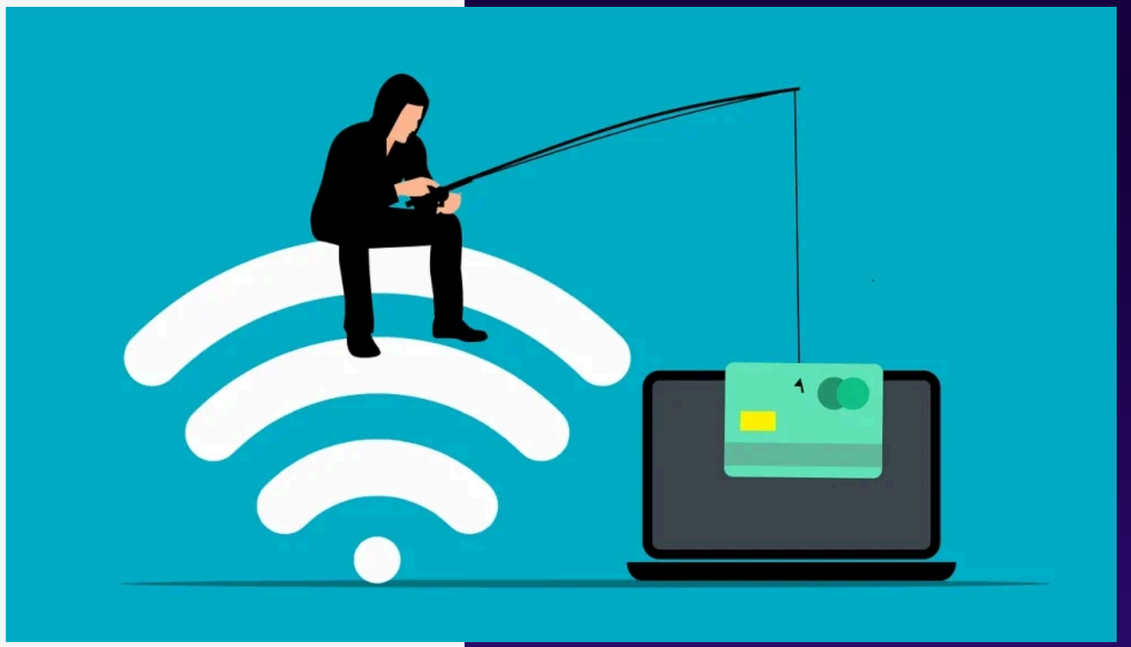

Principais
Ameaças
Cibernéticas

Malware:

UM TIPO DE PROGRAMA DE COMPUTADOR DESENVOLVIDO PARA INFECTAR O COMPUTADOR DE UM USUÁRIO LEGÍTIMO E PREJUDICÁ-LO DE DIVERSAS FORMAS.

Phishing

É um tipo de crime cibernético popular no qual os criminosos tentam obter informações confidenciais, como senhas, números de cartão de crédito, informações bancárias ou outros dados pessoais, fingindo ser uma entidade confiável

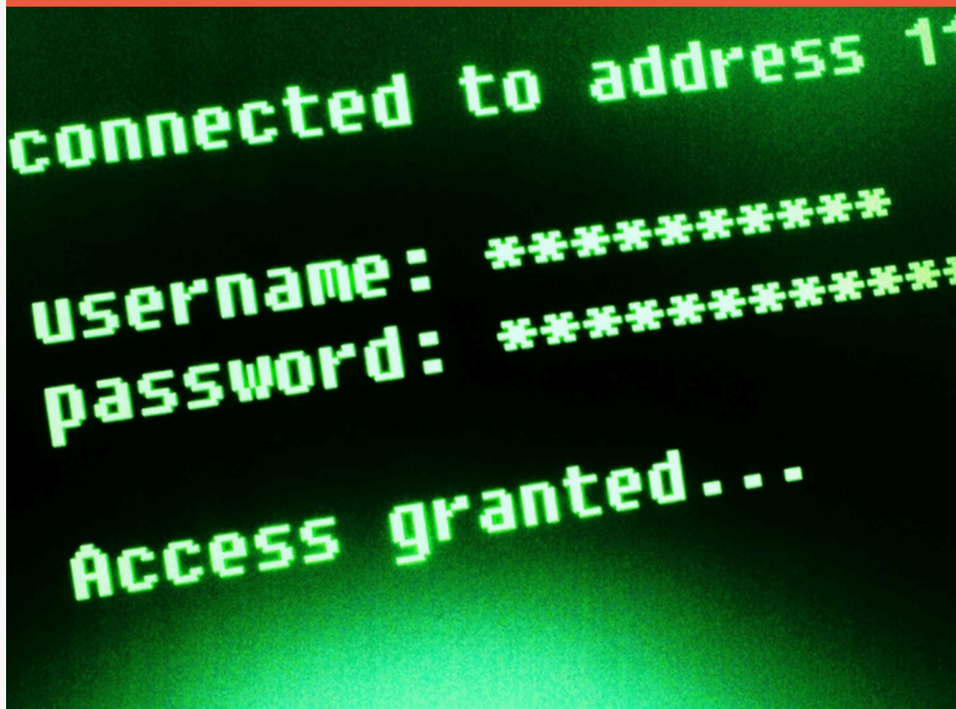


Ransomware

É UM SOFTWARE DE EXTORSÃO QUE PODE BLOQUEAR O SEU COMPUTADOR E DEPOIS EXIGIR UM RESGATE PARA DESBLOQUEÁ-LO

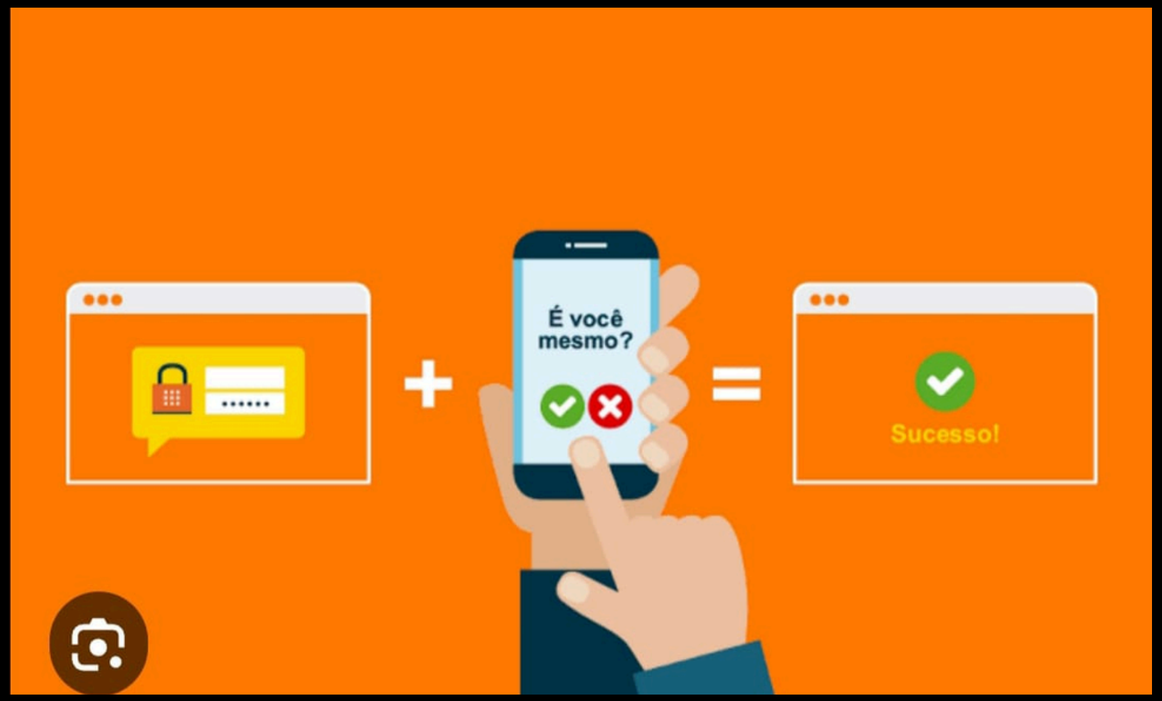
Ataques de Força Bruta

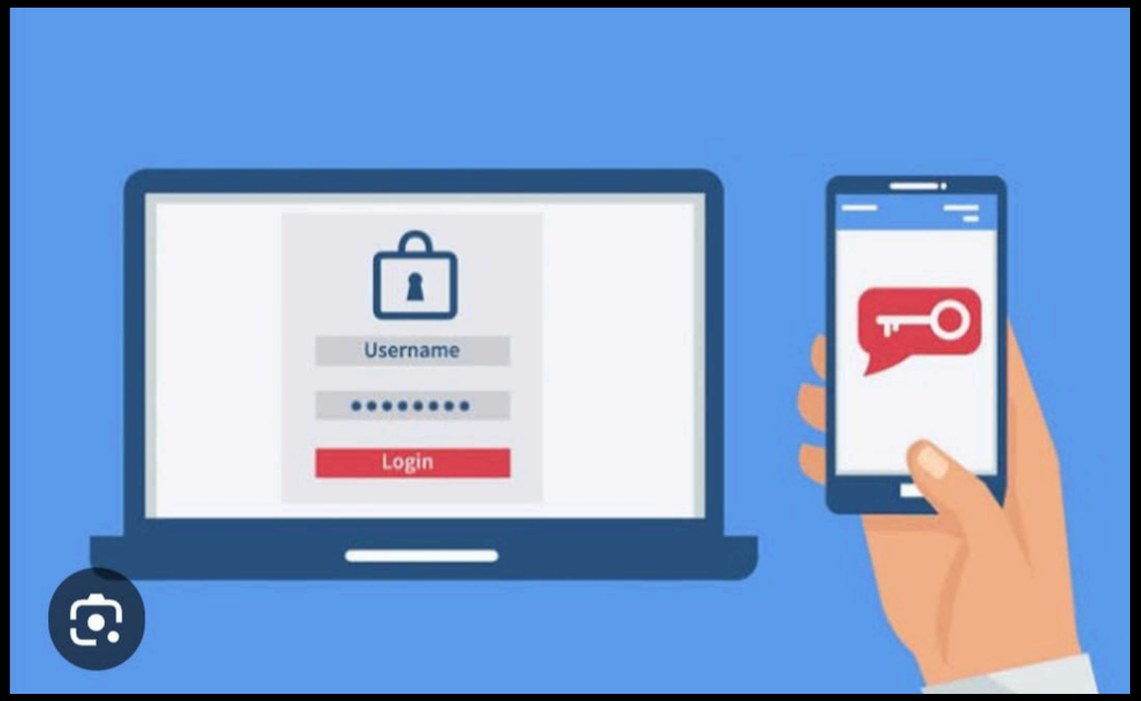
Consiste em todo e qualquer método usado por um invasor para descobrir uma senha, uma chave criptográfica ou outro tipo de informação sigilosa, por meio de tentativa e erro.



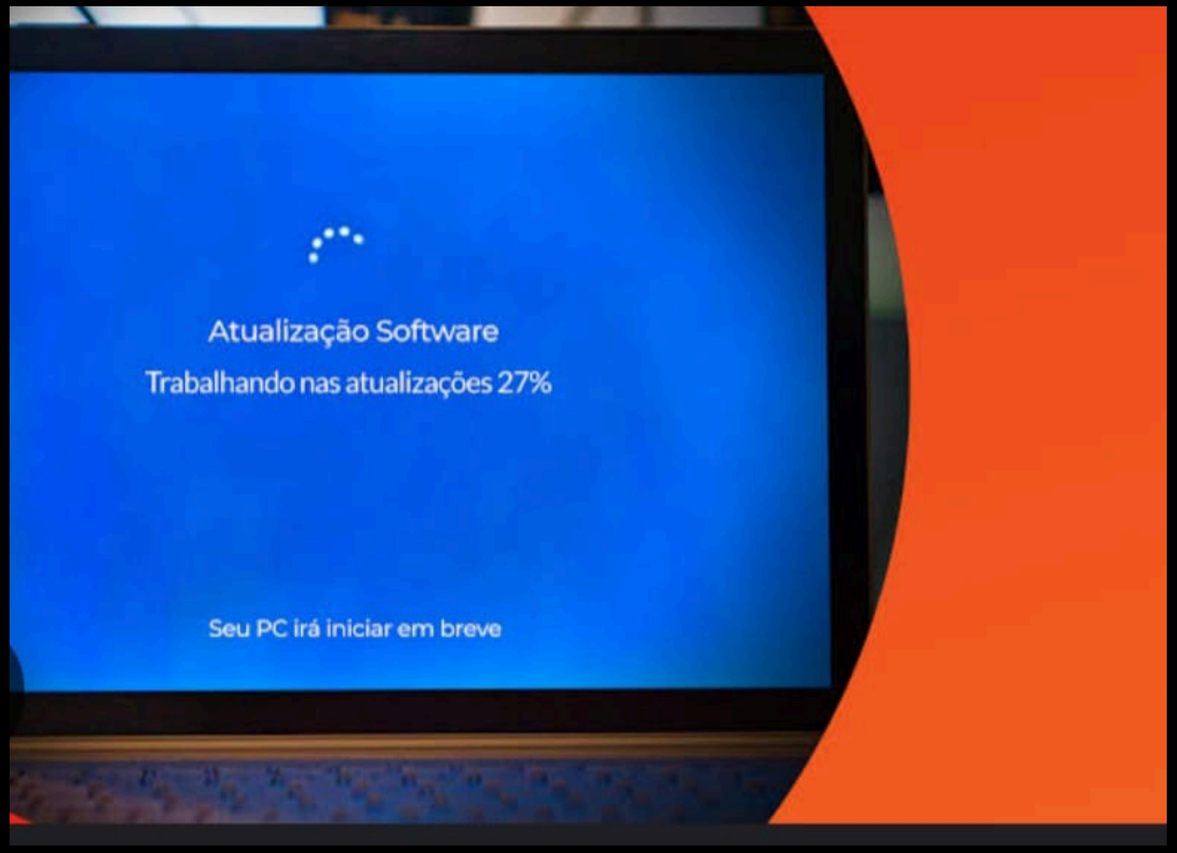
QUESTÕES

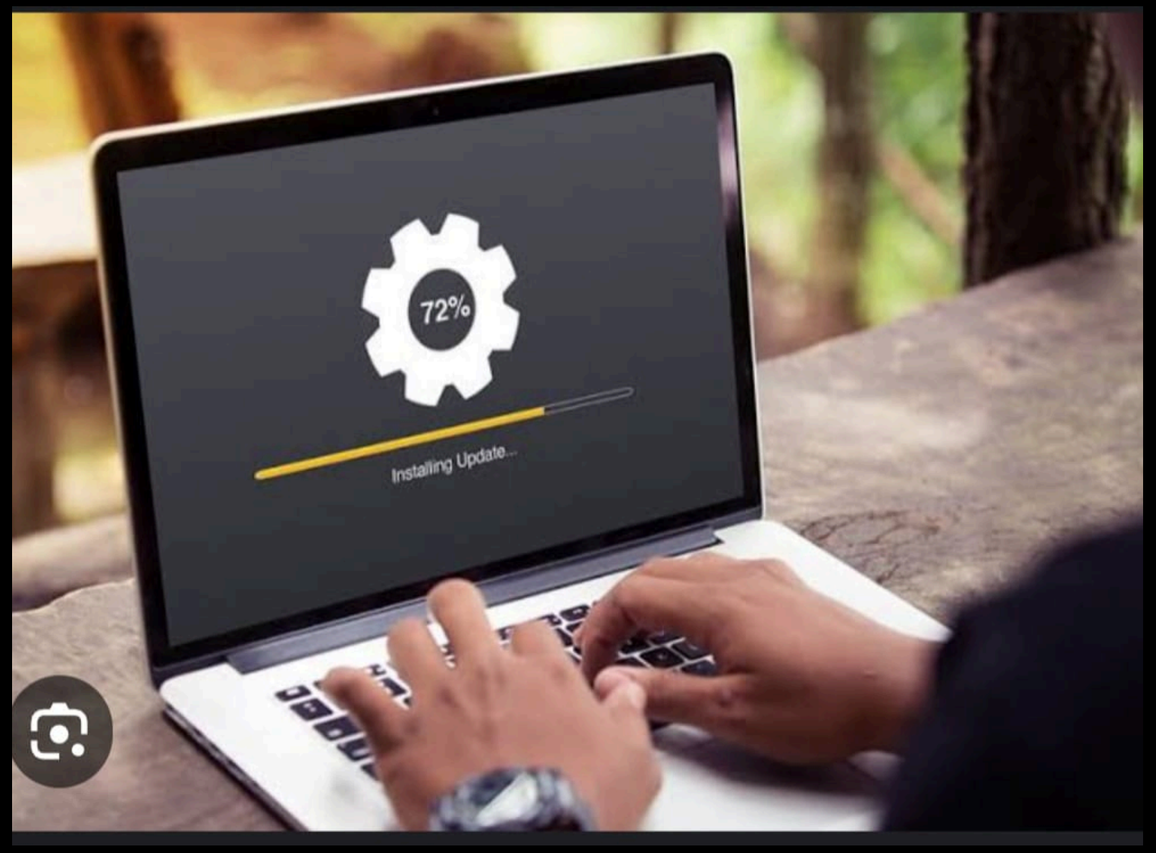
- O que é autenticação de dois fatores e como ela melhorar a segurança online?





2. Qual é a importância de manter seu software e sistemas operacionais atualizados na segurança cibernética?



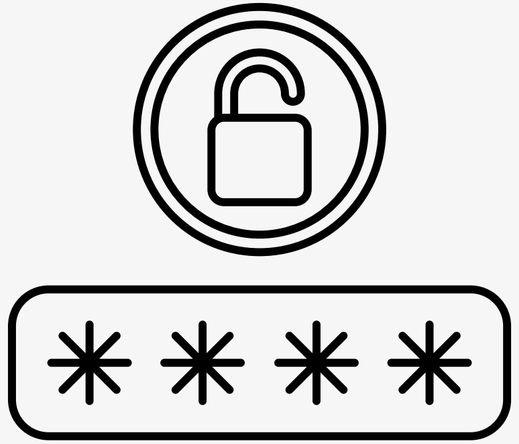


Como se proteger ?

- Senhas fortes
- Verificação em duas etapas (Google Authenticator)
- Antivírus
- Pirataria

Senhas fortes

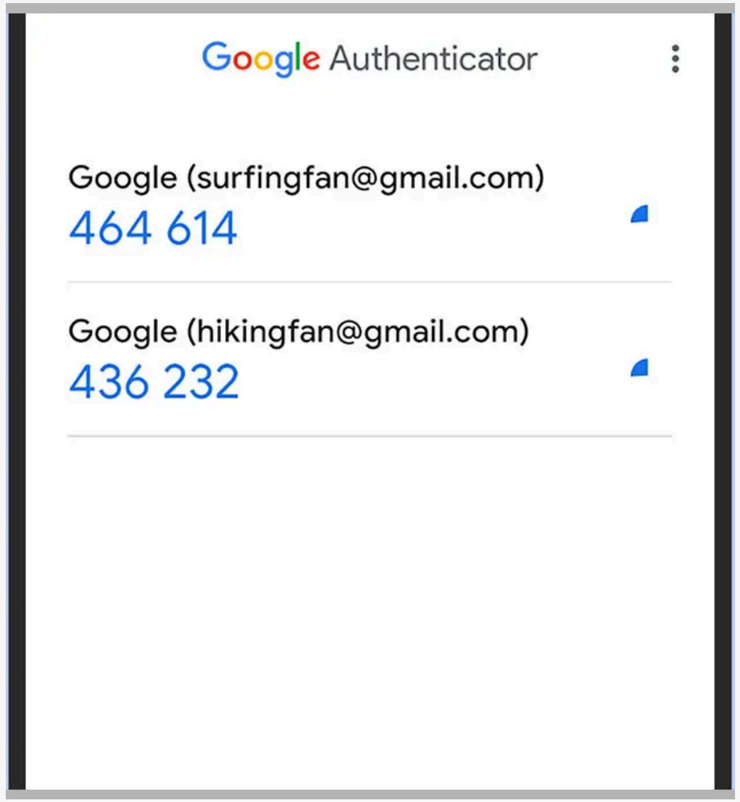
- De 8 a 12 caracteres
- Mistura de letras, números e símbolos
- Maiúsculas e minúsculas



Autenticação de dois fatores

- Algo que você sabe (Sua senha)
- Algo que você tem (Código temporario)

Google authenticator



Antivírus

- Proteção contra malwares
- Segurança de dados pessoais
- Verificação de arquivos e downloads

Pirataria

- Riscos de segurança
- Sem suporte, sem atualizações