



# SANTANDER BOOTCAMP CIBERSEGURANÇA

## Explicação Código - Detecção de Phishing

### 1. Função verificar\_phishing

Essa função é o núcleo do script. Ela recebe como parâmetro o corpo de uma mensagem [texto do e-mail que você deseja verificar].

Como funciona?

- **Lista de palavras suspeitas:** Você criou uma lista chamada **palavras\_suspeitas** com termos comuns em golpes de phishing, como "ganhe", "prêmio", "urgente", etc.
- **Converte para minúsculas:** Para evitar problemas com letras maiúsculas/minúsculas, a mensagem do e-mail é convertida para letras minúsculas usando **mensagem.lower()**. Assim, por exemplo, "GANHE" ou "ganhe" serão tratados da mesma forma.
- **Laço de verificação:** Usando um **for**, você percorre cada palavra na lista de palavras suspeitas e verifica se ela está na mensagem com a expressão **if palavra in mensagem**. Se encontrar uma palavra, você classifica o e-mail como "Phishing" e para a verificação retornando essa classificação.
- **Retorno seguro:** Caso nenhuma palavra suspeita seja encontrada, a função retorna "Seguro", indicando que o e-mail parece confiável.

### 2. Entrada do usuário

- Você usa **input()** para permitir que o usuário insira o texto do e-mail que deseja analisar.
- O método **strip()** remove quaisquer espaços extras no início ou no final do texto para garantir que a análise seja precisa.

### 3. Classificação e saída

- O texto inserido pelo usuário é passado como argumento para a função **verificar\_phishing**.
- O resultado da classificação [Phishing ou Seguro] é armazenado na variável **resultado**.
- Por fim, você usa **print()** para exibir o resultado de forma amigável, com a mensagem **Classificação: {resultado}**.

### Exemplo de uso

Imagine que o usuário insira o seguinte e-mail:

```
"GANHE um DESCONTO exclusivo agora mesmo!"
```

1. A função converte tudo para minúsculas: **"ganhe um desconto exclusivo agora mesmo!"**.
2. A verificação detecta as palavras "ganhe" e "desconto" na mensagem.
3. Retorna **"Phishing"**.

Por outro lado, se o usuário insere algo como:

```
"Olá, gostaria de confirmar nossa reunião amanhã."
```

1. Nada corresponde à lista de palavras suspeitas.
2. A função retorna **"Seguro"**.

### Benefícios

1. **Facilidade de Uso:** A entrada e análise são diretas, permitindo que qualquer pessoa use o código sem necessidade de conhecimento técnico avançado.
2. **Aumenta a Segurança:** Reduz os riscos de cair em golpes de phishing ao alertar o usuário sobre mensagens potencialmente perigosas.
3. **Personalizável:** A lista de palavras suspeitas pode ser facilmente expandida ou ajustada para atender a diferentes necessidades.
4. **Conscientização:** Ensina aos usuários sobre os termos comuns usados em golpes, incentivando práticas mais seguras de uso de e-mail.
5. **Base para Melhoria:** Pode servir como um ponto de partida para o desenvolvimento de sistemas mais robustos, como integração com inteligência artificial ou análise de padrões mais complexos.