# Dokumentacja Użytkowa – PhishGuardian

PhishGuardian to rozszerzenie przeglądarki stworzone w celu wykrywania i zarządzania podejrzanymi wiadomościami e-mail. Używa uczenia maszynowego do identyfikacji podejrzanych wiadomości e-mail i oferuje opcje oznaczania ich jako bezpieczne lub przenoszenia do kosza. Rozszerzenie jest zbudowane przy użyciu Flask dla backendu i JavaScript dla frontendu.

## 1. Funkcje:

- Wykrywanie podejrzanych wiadomości e-mail za pomocą uczenia maszynowego.
- Możliwość oznaczania podejrzanych wiadomości e-mail jako bezpieczne.
- Możliwość przenoszenia podejrzanych wiadomości e-mail do kosza.

## 2. Instalacja:

### Wymagania wstępne:

- Python 3.6+
- Flask
- scikit-learn
- Przeglądarka Chrome

### Konfiguracja backendu:

1. Sklonuj repozytorium:
    - git clone https://git.wmi.amu.edu.pl/s452649/PhishGuardian.git
    - cd PhishGuardian/backend
2. Zainstaluj wymagane pakiety Pythona:
    - pip install -r requirements.txt
3. Uruchom backend Flask:
    - python app.py

### Konfiguracja Rozszerzenia

1. Otwórz Chrome i przejdź do chrome://extensions/.
2. Włącz "Tryb deweloperski" przełącznikiem w prawym górnym rogu.
3. Kliknij "Wczytaj rozszerzenie bez pakietu" i wybierz katalog extension w katalogu PhishGuardian.

# 3. Użycie:

1. Kliknij ikonę rozszerzenia PhishGuardian na pasku narzędzi Chrome.
2. Zaloguj się adresem e-mail oraz hasłem do poczty serwisu Outlook (na razie obsługiwane są tylko konta Outlook).
3. Użyj przycisku "Fetch Emails", aby pobrać wiadomości e-mail.
4. Wybierz wiadomość z listy i kliknij przycisk "Classify Email", aby przeskanować wiadomość.
5. Jeśli wiadomość zostanie sklasyfikowana jako podejrzana, pojawi się tekst "This email is: Suspicious".
6. Jeśli wiadomość nie jest podejrzana, pojawi się tekst "This email is: Not suspicious".
7. Jeśli wiadomość zostanie oznaczona jako podejrzana, możesz użyć przycisku "Mark as Safe", aby oznaczyć wiadomość jako bezpieczną, lub przycisku "Delete Email", aby usunąć wiadomość.

# 4. Interfejs użytkownika:

### Popup HTML

- **Sekcja logowania**: Umożliwia użytkownikowi wprowadzenie danych logowania e-mail serwisu Outlook w celu zalogowania się.
- **Sekcja kontrolna**: Pojawia się po zalogowaniu użytkownika i oferuje przyciski do pobierania wiadomości e-mail, klasyfikacji oraz wylogowania się.

# 5. Powiadomienia:

- **This email is: Suspicious**: Pojawia się, gdy wykryta zostanie podejrzana wiadomość e-mail, oferując opcje "Mark as safe" i "Delete email".
- **This email is: Not suspicious**: Informuje użytkownika, że wiadomość e-mail jest bezpieczna.

# 6. Pliki i katalogi:

### Katalog backend:

- app.py: Główny plik aplikacji Flask.
- spam_classifier_model.pkl: Wstępnie wytrenowany model uczenia maszynowego do klasyfikacji wiadomości e-mail.
- vectorizer.pkl: Wstępnie wytrenowany wektoryzator do przekształcania treści wiadomości e-mail w format odpowiedni dla klasyfikatora.
- source.txt: Zawiera link, z którego pobrano zestawy danych.

- lingSpam.csv, enronSpamSubset.csv, completeSpamAssasin.csv: Zestawy danych używane do trenowania modelu (użyto modelu Random Forest).
- data_join.py: Skrypt, który łączy trzy zestawy danych w jeden plik CSV o nazwie joined_data.csv.
- joined_data.csv: Połączony zestaw danych wynikający z data_join.py.
- ML.ipynb: Notatnik Jupyter zawierający informacje o uczeniu maszynowym oraz szczegóły dotyczące wektoryzatora.
- requirements.txt: Plik zawierający listę wymaganych pakietów Pythona.

**Katalog extension:**

- popup.html: Główny plik HTML interfejsu rozszerzenia.
- popup.js: JavaScript obsługujący interakcje w popupie, takie jak logowanie, pobieranie wiadomości e-mail i obsługę odpowiedzi.
- background.js: JavaScript zarządzający zadaniami w tle rozszerzenia, takimi jak otwieranie popupa.
- styles.css: CSS zawierający style interfejsu rozszerzenia.
- manifest.json: Plik konfiguracyjny dla rozszerzenia Chrome.
- images/icon16.png, images/icon48.png, images/icon128.png: Ikony używane w rozszerzeniu.

# 7. Działanie:

1. **Logowanie**: Użytkownicy logują się za pomocą swoich danych logowania do e-maila używając rozszerzenia.
2. **Pobieranie wiadomości**: Rozszerzenie pobiera wiadomości e-mail z serwera i wyświetla je w popupie.
3. **Klasyfikacja wiadomości**: wiadomości e-mail klasyfikowane sąjako podejrzane lub nie. Wyniki klasyfikacji są przechowywane i przypisane do każdej wiadomości.
4. **Oznaczanie jako bezpieczne/usuwanie**: Użytkownicy mogą oznaczać podejrzane wiadomości jako bezpieczne lub je usuwać. Działania te są odzwierciedlane w backendzie, a interfejs użytkownika jest odpowiednio aktualizowany.