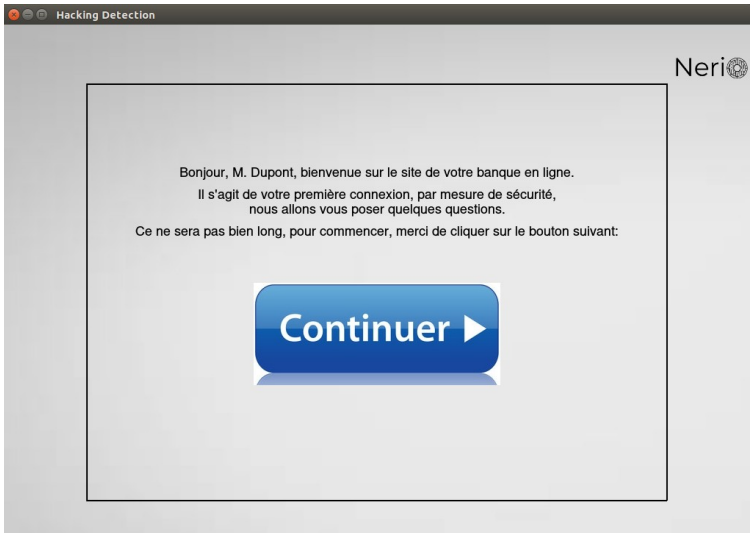
Guide Utilisateur – Projet Nerio

Installation:

Afin de pouvoir faire marcher le code, il est nécessaire d'avoir une distribution Python 3 et d'installer les bibliothèques et API suivantes: PyGame, Scikit-Learn, Panda, Numpy…

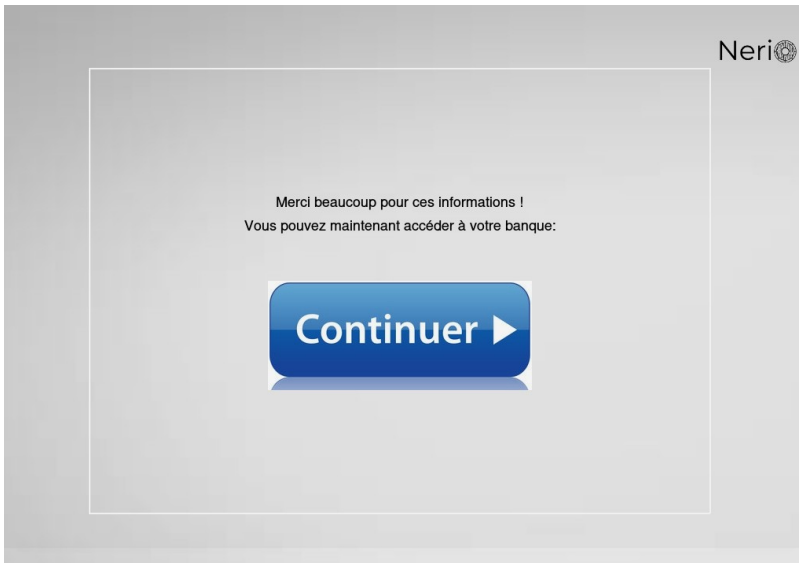
Utilisation:

Il y a deux codes à exécuter. Tout d'abord, lors de sa première connexion (inscription sur le site de la banque), l'utilisateur va lancer le script "hacking_premiere_connexion.py" et va obtenir l'écran suivant:



Il faut alors qu'il clique sur le bouton et réponde aux questions suivantes (toujours avec le clic de la souris):

Une fois cela fait, vous arrivez à l'écran de fin, vos données sont maintenant enregistrées.



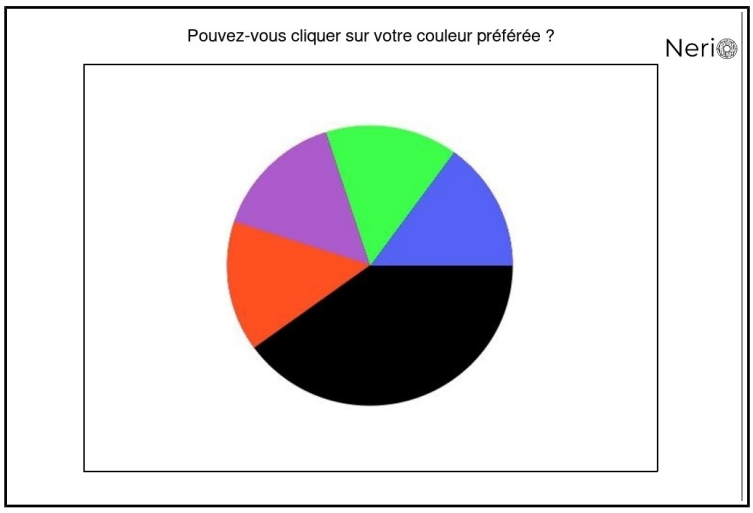
Vous pouvez accéder à vos choix de réponses dans le dossier "profil_user".

Seconde connexion:

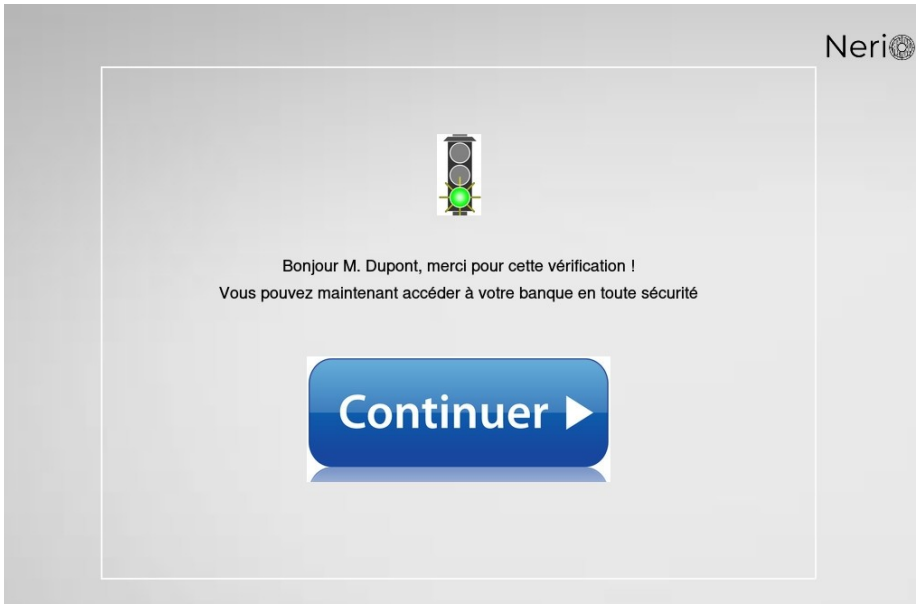
Vous pouvez maintenant exécuter le script "hacking_seconde_connexion.py".

Ce script simule le cas où lors d'une autre connexion, on enregistre une activité suspecte sur votre compte (IP inusuelles, etc…).

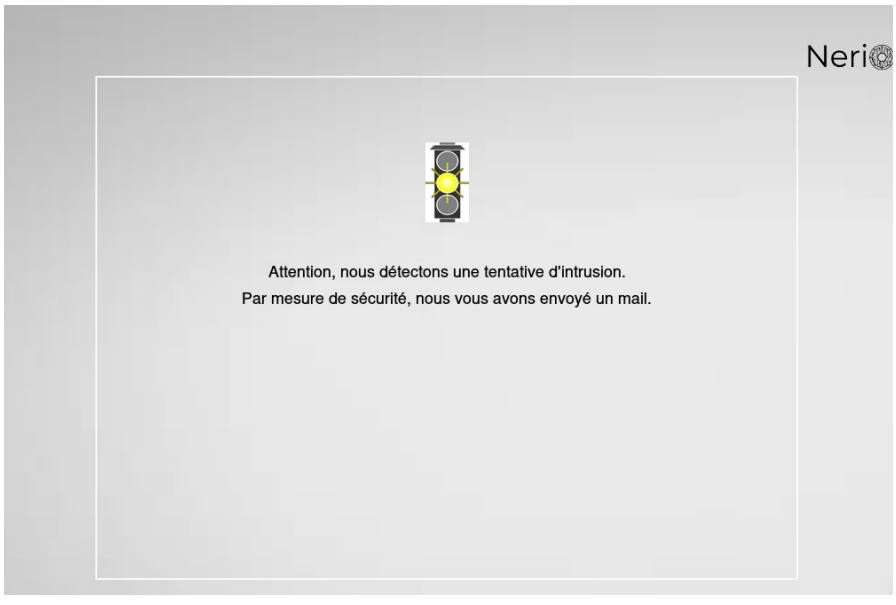
Comme précédemment les questions demeurent les mêmes, toutefois il y a des réponses "intrues" dont la fréquence est plus élevée (de manière à ce qu'un bot qui répond au hasard ne puisse pas réussir):



Dans le cas où l'algorithme de machine learning a détecté que les réponses étaient cohérentes et que la probabilité que ce soit un intrus était élevée (<10%), on a alors:



Dans les autres cas, où il y a une suspicion sur le client, on l'oriente vers une sécurité plus élaborée:
Ici le pourcentage de suspicion est entre 10% et 40%:



Dans le cas où ce pourcentage dépasse les 40%, on demande à une confirmation par SMS (qui coûte plus cher):