Verifying the identity of a user logged into a secure system is an important task in the field of information security. In addition to a password, it may be appropriate to include behavioral biometrics in the authentication process. The biometrics-based system monitors the user's behavior, compares it with his usual actions, and can thus point out suspicious inconsistencies. The goal of this thesis is to explore the possibility of creating a user identity verification model based on his behavior (usage of mouse and keyboard) in a web application. The work includes creation of a new keystroke and mouse dynamics dataset. The main part of the thesis provides the analysis of features (user characteristics) which can be extracted from the obtained data. Subsequently, we report the authentication accuracy rates achieved by basic machine learning models using the selected set of features.