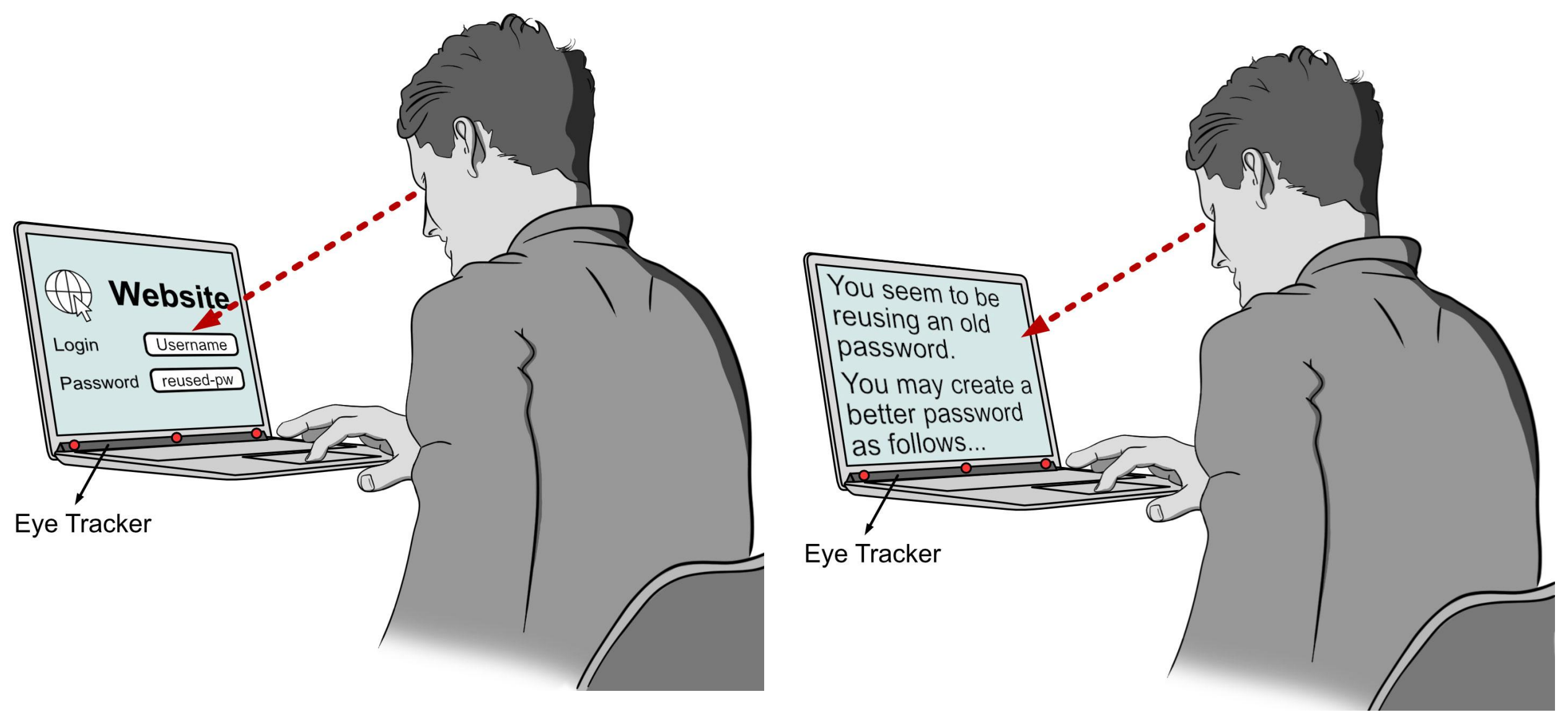
# “Your Eyes Tell You Have Used This Password Before”: Identifying Password Reuse from Gaze and Keystroke Dynamics

***Yasmeen Abdrabou***, Johannes Schütte, Ahmed Shams, Ken Pfeuffer, Daniel Buschek, Mohamed Khamis, Florian Alt


Website
Login
Username
Password
reused-pw
Eye Tracker
You seem to be reusing an old password.
You may create a better password as follows...
Eye Tracker

## Motivation

Passwords remain a ubiquitous approach to authentication. While their end has been repeatedly predicted they present a Pareto equilibrium between usability, security, and administrability, i.e. there is no other mechanisms providing an equally good trade-off between the effort required for implementation, ease of administration (e.g., reset / changing credentials), ease of use, and security. However, they have different security issues such as password reuse.

## Concept

We explore the concept of identifying the reuse of text-based passwords from gaze and typing behavior. We investigate:

1) **Prediction accuracy** across different phases of the password creation process

2) Influence of the **protected data sensitivity on the classification**.

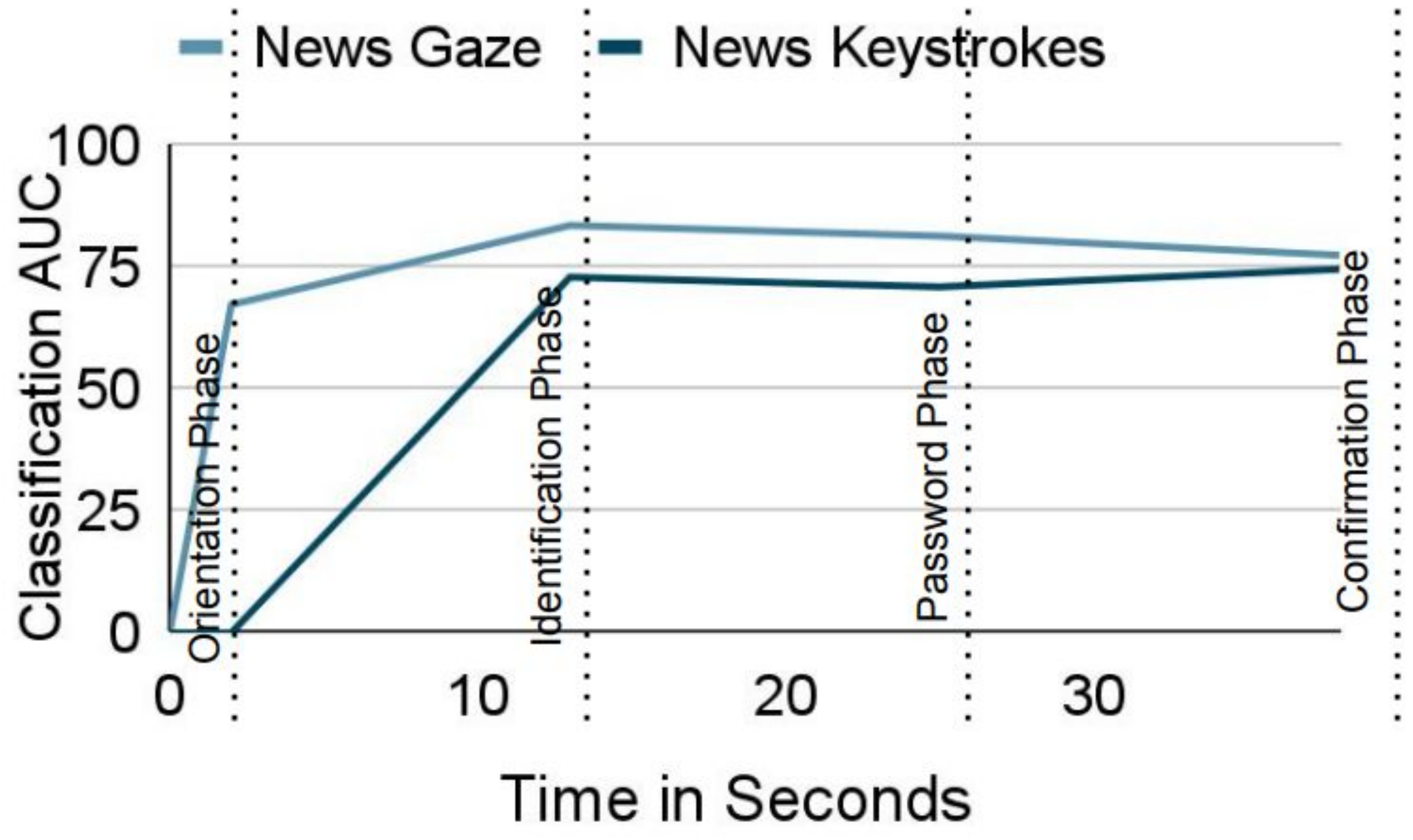
## Study Design

- **Study Setting**: university cafeteria
- **Sample**: 52 participants
- **Task**: register for two service (university email, news webpage), different in the perceived sensitivity of the protected data

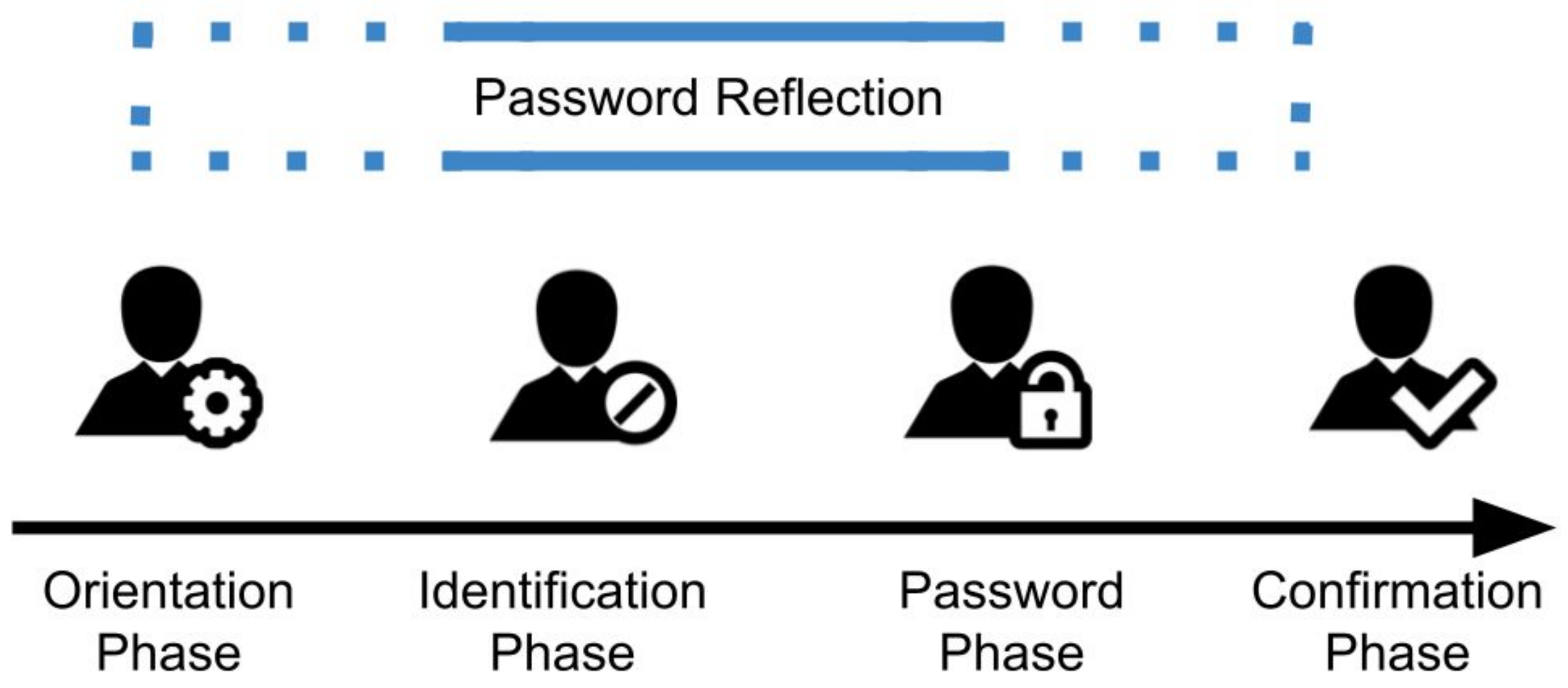
We analysed the passwords’ characteristics and trained service dependent and independent classifiers.

## Results

- Password characteristics and length were similar for the new and reused passwords.
- Keystroke dynamics were different for the new and reused passwords. For example, **flight time** and **thinking time** were longer for the new passwords.
- Gaze behaviour was different for the new and reused passwords. For example, **participants had more and longer fixations when creating new passwords.**
- We trained the ML classifier for **single phases** as well as for the **cumulative phases.** Password reuse can already be detected while users think about their password and enter their ID.

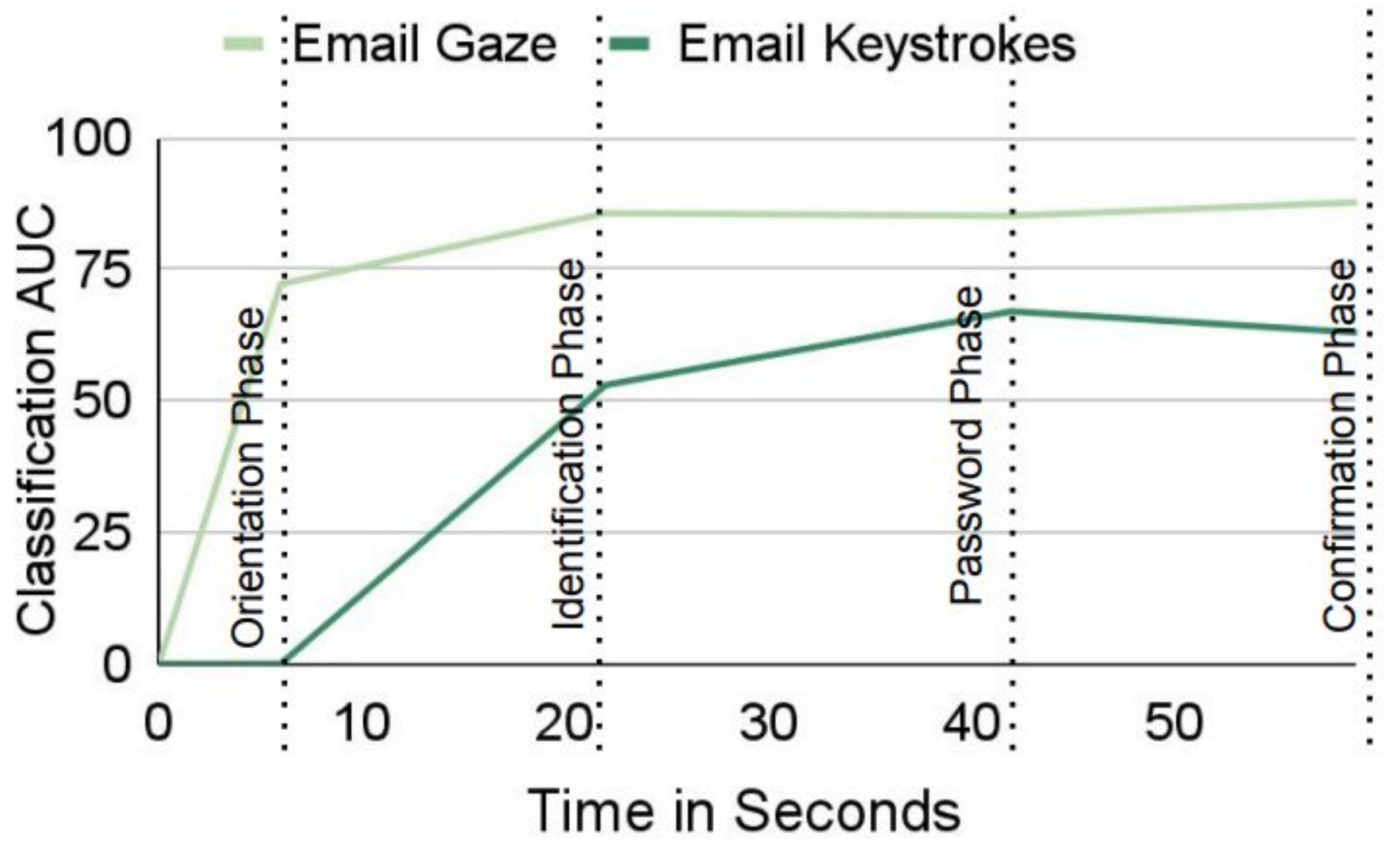


## Password Registration Process



## Classification Results

- Gaze features yield a higher accuracy, (**87.7%**) compared to keystroke dynamics (**75%**) across the different phases.
- The classification accuracy was slightly **higher** for the **email** client.
- Gaze data is available from the beginning of the registration, whereas keystroke dynamics are only available as the user starts typing.



Published Paper

## Takeaway Messages

- We present a novel approach of using gaze movements and keystroke dynamics for password reuse detection.
- Gaze is more informative than typing.
- Data sensitivity influences the accuracy of password reuse prediction.
- Dissecting the password registration process enriches prediction.

Lets Connect

RI CODE Research Institute Cyber Defence Bundeswehr University Munich
University of Glasgow
AARHUS UNIVERSITY
UNIVERSITÄT BAYREUTH