Privacy and the Duo Mobile Application

Summary: There have been questions regarding the use of the DUO Mobile application (app) by UHS users related to privacy. This document is designed to provide additional information regarding the security and privacy of the Duo Mobile App.

➢ The sole purpose of installing the DUO Mobile app is to provide users with a convenient second method of authentication option for UHS systems.
➢ Users have the ability to choose the second method of authentication from a variety of options including: SMS text messages, passcodes, security tokens, hardware fobs and through the Duo mobile app. Users are not required to install or use the Duo mobile application for access to UHS systems.

Information Collected by the Duo Mobile App

The Duo Mobile app DOES collect information for the purpose of providing assurance that the mobile device is also secure, as well as providing the information necessary to investigate a potential cybersecurity incident should it arise.

Installing the Duo app on your phone/device allows UHS administrators (not Duo employees) to see the following information:

- Type of device enrolled

- Operating System and Version used on device

- IP addresses from which the user connects

- Geolocation information from which the user connects (primarily city and state)

- Phone number of the user device*

The information noted above is stored on Duo's servers. Most of this information is also captured separately by the university when the user's account is accessing campus Active Directory resources. *NOTE: This number is only used as a unique identifier for the device which individual clients choose to use for 2FA and is not used for other purposes.

The Duo Mobile app also requests permission to use the camera. This is how the app is able to take a photo of the QR code used for enrollment. The app will function without camera permission, but users that choose not to grant this permission will need to use an SMS text message to enroll.

Functions Not Granted to the Duo Mobile App

Installing the DUO Mobile app DOES NOT allow UHS administrators to manage your mobile device in any way. Specifically, the Duo Mobile App CANNOT:

- Access your user data like your contacts
- Read your text messages
- Access or read your browsing history
- Access your photos (but it can use your camera to scan a QR code if you explicitly allow that permission)
- Access your files
- Erase your device
- See information about other applications installed on your device

The DUO Mobile application will also ask you whether you wish to share Application usage information with Duo. Users can choose to allow or deny.

For most UHS users, the DUO Mobile Application provides the most convenient and best user experience for 2-Factor authentication.

Users with any questions or concerns about 2FA or Duo should contact UHS Information Security.

Mary E. Dickerson, MBA, CISSP, CISM, PMP
Assistant Vice-Chancellor, IT Security
Chief Information Security Officer
University of Houston System
Department Phone: 832-842-4695
Department Email: security@uh.edu

July 2023