

FAQs – OKTA Verify App

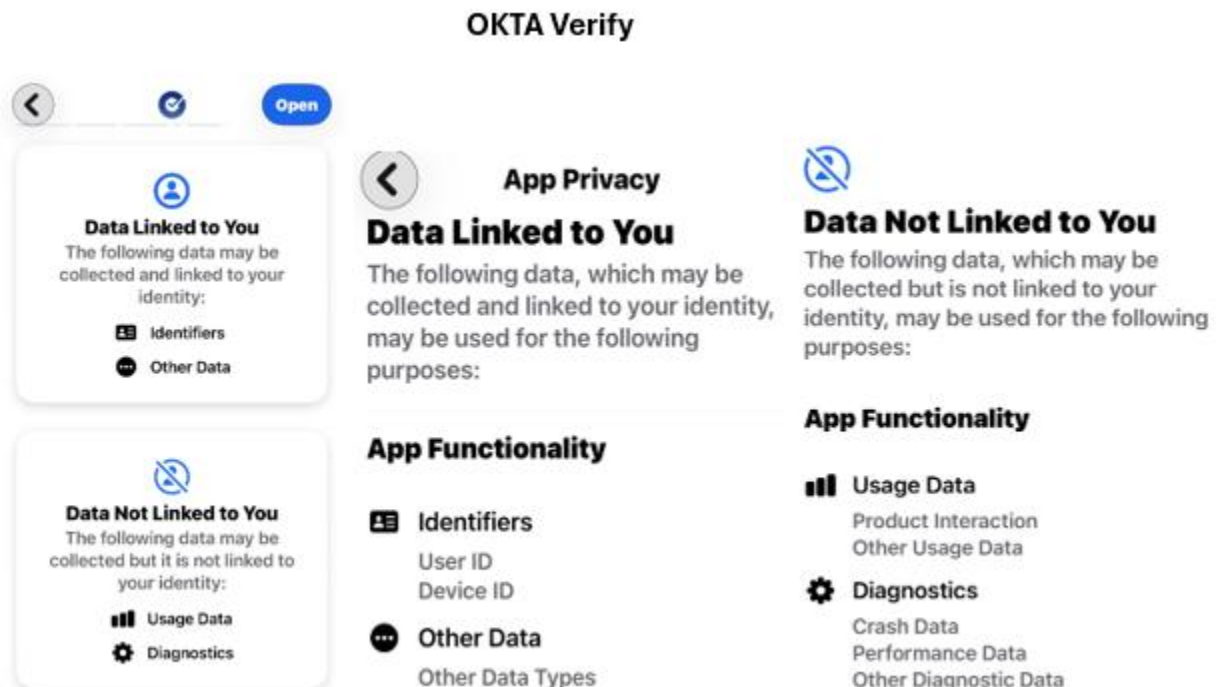


- **Is my personal data safe if I install OKTA Verify on my phone?**
 - The OKTA Verify app, like other authentication apps such as the Microsoft Authenticator, is strictly for authentication purposes only and does not access personal data on your device. Your IT department cannot use this app to access or track your phone activity. The State of Indiana does not own the OKTA Verify App and therefore cannot use it to access, view, or remove any personal data, information, or other apps from your device, regardless of whether the mobile device is personal or state-owned.
- **Am I required to install Ivanti Neurons (Mobile Device Management) on my device if I want to install the OKTA Verify app?**
 - **No.** Ivanti is only required in situations where a user would like to access State of Indiana resources, including Secure Wi-Fi. If the only goal is to install OKTA Verify for authentication purposes, there is no additional requirement for any other apps to be installed.
- **If I want to install the OKTA Verify app on my personal device, how can I download it from State's Apps@Work app store without having to install Ivanti Neurons?**
 - For personal devices, you do not need to access Apps@Work or install Ivanti Neurons to obtain the app. Under these circumstances, you can install the OKTA Verify App directly from the **Apple App store** or **Google Play store**.
- **What happens if I get a new phone?**
 - For security reasons, Okta Verify is tied to one device at a time. You will need to sign in using another method or contact your company's IT support to enroll your new device.
- **What if I don't have cell signal or Wi-Fi?**
 - The app still works for push notifications or codes as long as you have a connection.

- **What are the storage requirements for the app?**
 - The OKTA Verify app is small (under 40 MB) and does not require significant phone storage.
- **Why should I trust this app?**
 - The OKTA verify app only requires permission for things like your camera (to scan codes) and notifications (to send you notifications). It is designed to be a **security tool only** and **cannot access your personal photos, texts messages, emails**, etc.
 - By contrast, apps that users commonly install on their device, such as Tik Tok, Facebook, WhatsApp, etc. require more extensive permissions to your device as shown below (information pulled directly from the app store):

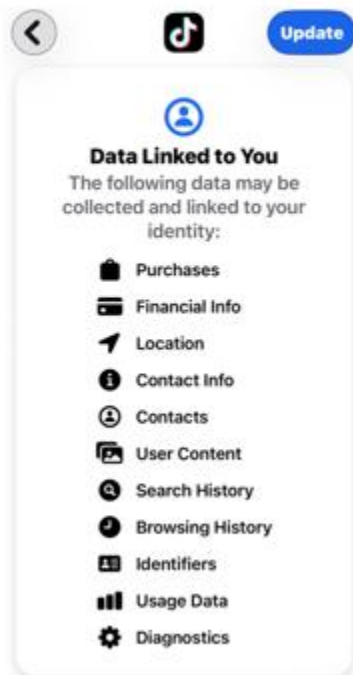
OKTA Verify vs. Other Popular Apps

OKTA Verify only has access to limited details on the mobile device, and those details allow the authentication process to take place. This is only triggered when an authentication is initiated by the user (logging into a work application that requires MFA)

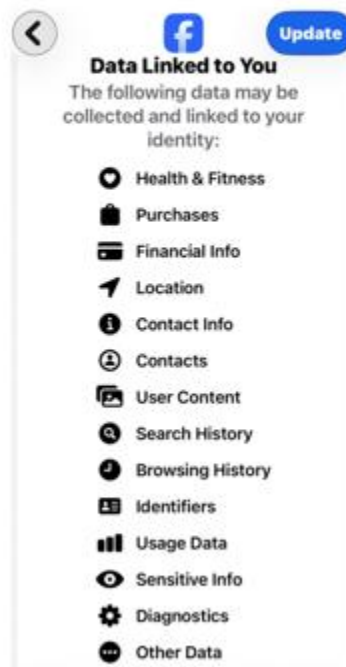


Comparatively, other popular apps including **Tik Tok**, **Facebook**, and **WhatsApp** have access to many personal details on a mobile device including financial info, location, contact info, user data, etc.

Tik Tok



Facebook



WhatsApp

