Ten Security Rules for Using the George Key App

Minimise the risk of your George Key app being compromised by following these simple rules

1. **Download apps from official stores only**
   Install apps only from App Store, Google Play and HUAWEI AppGallery.
   Never install apps from unverified sources. **Only use the original operating system** and do not make any modifications to it that would allow full admin control to someone else (root or jailbreak). **Do not buy or use devices which have been modified in this way.**

2. **Choose a secure PIN**
   A PIN must be **six digits** long**.** Choose a PIN that you can easily remember but is difficult for someone else to guess. **Never disclose your PIN to anyone, and change it regularly.**
   You can also use the fingerprint recognition feature "Touch ID" or the face recognition feature "Face ID" to secure access to the app. If your device has these features, we recommend using them.

3. **Check the "Touch ID" settings**
   There are two biometric options to secure access to the George Key app: Touch ID and Face ID

   Touch ID

   You can use your fingerprint to secure access to your device as well as to the app. If you decide to use the Touch ID feature to access George Key, **make sure the device does not contain anyone else's fingerprint. If it does, delete it from the device.**

   Face ID

   You can also use your face to secure access to your device as well as to the app. If you have a twin or a sibling with a strong resemblance to you, **the bank and the app developers recommend you do not use this security feature.**

4. **Be wary of free Wi-Fi networks**
   When working with bank apps, we recommend primarily using mobile data. Free Wi-Fi networks allow a stranger to eavesdrop on your connection and steal your sensitive data (e.g., login details). You can use the **George Key app even if your device is offline** which will help you avoid having to use free Wi-Fi networks

5. **Think carefully about the devices you want to install the app on**
   You can install the app on more than one device. However, if you share the device with other members of your household or friends, you are also giving them access to your apps, including George Key. **Install the app on devices that only you use.**

6. **Properly secure access to the devices the app is installed on**

We recommend using modern technologies, such as fingerprint recognition. If your device does not have a fingerprint recognition feature, **the PIN for unlocking your device should be different from the one you use to access the George Key app.**

7. **Only confirm transactions you have performed yourself**

   If the George Key app asks you to authorise a transaction or a sign-in to George and you are not attempting to do either at that moment, **do not authorise the request under any circumstances and call the toll-free number 800 207 207.**

8. **Protect your mobile device**

   Install an antivirus programme on your mobile device. Update this program as well as the whole operating system regularly.

9. **Set up the features to find and delete your device**

   If you lose your device or it gets into the wrong hands, **you can search for the device, lock it or delete the information on it remotely**. These features can be found on Android devices in Settings under “Find my device” and on IOS devices in Settings under “Find My iPhone.” You can find detailed instructions on how to activate these security features in the user manual to your device.

10. **If something doesn’t feel right, contact us**

    If you suspect that the security of your internet banking or mobile apps has been compromised, contact us immediately. You can call our toll-free number **800 207 207** (+420 956 777 956 if you are calling from abroad) or send an email to **csas@csas.cz**