Security of your accounts

When it comes to logging in to important Internet accounts, security should always be a priority. The mailbox and all the accounts on which you have money can undoubtedly be considered important accounts. Undoubtedly, this is also the case for GLOCIN accounts. If possible, be sure to enable Two Factor Authentication each time you log in.

In practice, logging in is done in such a way that, in addition to the password, you must enter another code that is automatically generated by Google Authenticator. You then enter this code during login. Next, you enter this code in Glocin to confirm transactions and changes. The new code is generated every 30 seconds. However, you do not need to worry that you would not manage to do this in time. Each generated code is valid for another 30 seconds after it expires.

The process of logging in itself takes a few seconds longer, but your account is much more secure and even if hypothetically someone gets to your password, it will not be enough to log in.

How Google Authenticator works

Google Authenticator automatically generates six-digit codes which are needed to log in to different accounts.
These codes change regularly and are firmly linked to your phone.

So, to access your account, they would need both your password and physical access to your phone. This adds another layer of security, and any attempt to gain control over your account is much more complicated for potential attackers.

Two Factor Authentication with Google Authenticator

Where to download Google Authenticator?

Google Authenticator is available for Android and iOS mobile devices and is available on both Google Play and the App Store:

Download Google Authenticator from Google Play

Download the Google Authenticator app from App Store

How to enable Two Factor Authentication (2FA)

Enabling Two Factor Authentication is very easy. Follow these steps:

1. After logging in to the Glocin portal, go to your profile and select the option of enabling Two Factor Authentication on the security tab. This option is usually offered to you during registration, otherwise you will usually find it under the “Security” tab.

2. You will see a QR code to link your account with your phone.

3. Download and start Google Authenticator on your phone and click on the red circle with the + symbol at the bottom right.

4. Select barcode scan option to turn on the camera and point it at the QR code.

5. The QR code is loaded into Google Authenticator and the account is linked directly to your phone.

6. When logging in to the Glocin Portal or another service, you need to turn on the Google Authenticator app and enter the generated code.

What if I lose my phone or delete Google Authenticator?

Google Authenticator is not directly linked to your Google Account and is not synced with any device. This ensures security, because you really need to have a cell phone on you to obtain and write down the code. On the other hand, if the phone is lost or the app is deleted, it is not possible to retrieve the linked accounts by reinstalling the app.

When you enable the Two Factor Authentication with Google Authenticator, a private code that can be entered directly into Google Authenticator will be generated for you. If you go back to the tutorial, in point 4 you would select the Enter provided key option instead of the QR code.

Write the generated 2fa private code in a safe place, ideally write it on a piece of paper and keep it safe. If you delete the app and do not have access to this code, it is usually very complicated to access the Glocin portal or other service and you will need to prove that you are the owner of the account.

What if I buy a new mobile phone or need to transfer Google Authenticator to another phone?

In these two cases, if you have your phone on which Google Authenticator was originally installed, you can do the following.

- The first and easiest way is to log into the Glocin portal, go to your profile and on the security tab you will see the option to display your current key at the bottom. Write down the code from the Google Authenticator app which belongs to that account in the portal and click on view private key. On the portal, you will see your private code and QR code so you can transfer your login to another phone.

- The second more complicated way is to manually type your private code into the new device, which you have carefully written down and kept in a safe place.

E-mail, photos, desktop, wallet, diary, and the like are not a safe place. Think safely or lose your money.