Two Factor Authentication

Two Factor Authentication or 2FA is a security system whereby you are given a randomly generated code when you try to log in to a site or system. There are lots of different ways of using 2FA, some of which are explained here.

The safe pictured has two different locks. A key and a then a numeric key code pad. Two Factor Authentication is a similar system - an additional layer of security for your Hopt Admin Panel account.

The 'key' - your login and password for example, is the first security step. A strong password using a mixture of letters, numbers and symbols is important.

The 'keypad' - just like your 2FA method, offers enhanced security that is really difficult to hack.

Mobile Phone - a text with a code is sent to your phone number when you try to log in. Anyone with your mobile phone would be able to see the code flash up on your screen when you receive the message.

Token on an App - Authenticator apps can be placed on multiple devices and store multiple 2FA sites so they are quite good for centralising the process. The app generates a code when you log in to it that is on a visual timer and changes when the time has elapsed.
The app method is even more secure as you usually have to use a code or fingerprint to open your phone and access the app.

Google Authenticator

Microsoft Authenticator

AUTHY
One App for All your Accounts

Examples of authenticator apps. Others are available.