Two-Step Verification

Software Support - 2023-08-08 - Security / Privacy

Two-step verification (also known as Two-Factor Authentication) helps protect you and your data by making it more difficult for someone else to log in to your Kahootz account. It uses two different forms of identity: your password (something you know) and a security code from your phone (something you have).

2FA (also known as 2SV) helps keep your account secure because even if someone else finds your password, they'll be blocked if they don't have access to your phone. You can also generate single-use recovery codes to use when you don't have your phone or it gets lost or damaged.

Site Owners can enable two-step verification that uses phone-based Authenticator Apps for all the users on their site.
(Click *Account, which is your username > Site Admin > Settings > Security Settings to enable*).
This option is available for both Professional and Enterprise accounts.

Kahootz can also support two-step verification via SMS code or automated voice call to mobile or landline numbers. There is an additional cost for this feature (£1/user/month); please contact support for details.

Kahootz Enterprise site owners can also control who needs to use two-step verification (all users, just workspace managers, just site owners) and other security and login settings.

What's an Authenticator App?

Authenticator apps generate secure codes that you can use to sign in. They're not unique to Kahootz - you can use them with many sites and internet services (including Microsoft, Google and Amazon). They do not have access to your Kahootz password or account information.

Apps are available for phones, tablets and desktops. If you don't have one, go to your device's App Store, search for "Authenticator App", and install it.

Popular apps include Google Authenticator, Microsoft Authenticator and Twilio's Authy; for full details, please refer to our KB article for guidance.

What if I get a message that my security code is invalid?

For your protection, the codes only work briefly - your app will automatically generate a new security code every 30 seconds. Enter the six digits immediately after you see them on your phone. Most apps will show how long the code is valid as a moving bar or spinning wheel.

If you still see an error message after trying again, please ensure the time is set accurately on your mobile device. Since security codes are time-sensitive, the time on your mobile device must be accurate; otherwise, your security codes will get rejected by Kahootz. We recommend you set your phone to update the time automatically; however, if you do have any issues, then please refer to the "What if my codes generated next don't work?" section within this KB article.

What if I don't always have access to my phone?

You can configure the app on several devices, a phone, tablet or even Windows 10 desktop, giving each device a different name, and then choose which to use when logging in.

If you do not have access to any of these, you can use a recovery code to log in. Recovery codes allow you to access your account whenever you are unable to provide a verification code, which can happen if you are travelling or if you lose your phone, for full details about recovery codes, please refer to our KB article.

If you are unable to provide a verification code and you do not have a recovery code, you can contact your Site Owner or raise a ticket with Kahootz Support via email. They will attempt to verify your identity with the answers to the security questions you provided at setup. They will provide you with a one-off recovery code to use.

Please note that Kahootz Support is not allowed to provide codes over the telephone under any circumstances.

I've lost/changed my phone with the authenticator app on it.

You'll need to use a recovery code or other pre-linked device to get into your account or the security questions as above.

Once you have accessed your account, you can revoke access to the authenticator app on your old phone from "*Account which is your username > Password and Security > Devices*". You can delete the old device and add a new one; please refer to this KB article.

How does this work?

We use a standard open algorithm called Time Based One Time Passwords – or TOTP. It's an openly published algorithm for generating codes based on the current time, and a secret token shared between the site and the app. Any programmer can write an Authenticator

app that uses the algorithm.

Kahootz sends your device a special unique token (one for each device) via the barcode or typed code you use to set up the authenticator. Your app stores that, combined with the current time (accurate to 30 seconds) through the algorithm and shows a six "6" digit code. That code changes every 30 seconds. Kahootz also knows your token(s) and can calculate the same number and see if it matches the current digits or the ones on either side, giving a 90-second validity for each code (which caters for typing time and small clock differences)

The recovery codes use roughly the same principle but have an incrementing number instead of the time, which only allows you to use each generated number once.

For more detailed information, research Time Based One Time Passwords, HMAC Based One Time Passwords or RFC6238!

If you wish to proceed, this KB article will assist you in enabling & configuring Two-Step verification.

Related Content

- How-To Install an Authenticator App on your Device for Two-Step Verification
- How-To Add/Delete Authenticator Device for Two-Step Verification
- How-To Enable & Configure Two-Step Verification for Users