Additional security measures for Kahootz Enterprise

Graham Smith - 2017-03-27 - Security / Privacy

Kahootz Enterprise customers can enable additional security measures on their sites to provide a greater level of security for themselves and their users.

Custom password policies provide rules for valid passwords (e.g. more than 8 characters, must contain numeric values and punctuation etc.) and also control password-reuse policy, lockouts after failed login attempts and inactivity timeouts.

Two-Step Verification adds another level of security by also sending a secure code to a user's Security Device (e.g. a mobile phone) after they have entered their login ID and password. They must enter this secure code to complete their login. This ensures that the system uses something they know (password) and something they have (mobile phone) as the two factors of authentication.

Two-Step Verification via an Authenticator App can be enabled on all Kahootz Professional sites. Kahootz Enterprise sites can also enable the Authenticator App for all users, and can also enable two-step verification delivered via SMS code or Voice Call, either for site owners (no additional cost) or for all users (additional cost).

Each user who requires Two-Step Verification will need to register a verified Security Device. This can either be a mobile phone or a land-line number that they have access to. When they first log in, they will be taken through this process if they don't already have a Security Device setup. In addition, they will be required to answer 3 Security Questions that can be used to assist in verifying them if they are unable to complete their login with Two-Step Verification at any time.

All additional security settings can be accessed and changed at any time via **My Profile > Passwords and Security**, once users are logged in and authenticated. Users can add further Security Devices, modify existing ones or change their Security Questions. Any changes made to the Security Profile will require the user to enter their login password. New Security Devices must be verified using a secure code before they can be used as part of the login process. Unverified devices are clearly marked and can be verified at any time.

> To enable Two-Step Verification on your Kahootz site, please contact support.

Related Content

- Optional password security rules