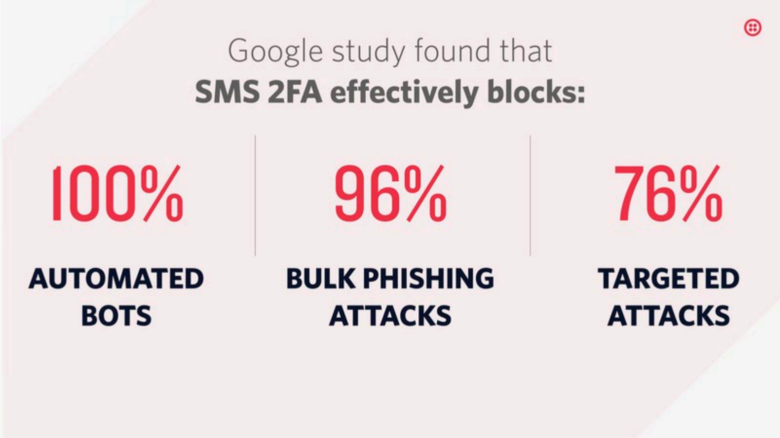
# Two Factor Authentication

Two-factor authentication (commonly abbreviated **2FA** and also known as multi-factor authentication MFA) adds an extra layer of security to your user's account login by requiring two types of authentication. This is usually something your user knows and something they have. Two-factor authentication is a common authentication best practice to increase account security normally provided by passwords.



Things like password reuse, poorly encrypted passwords, social engineering, and leaked databases make even a secure password vulnerable. By requiring users to add a second factor to their authentication flow, an account with a compromised password will still be protected. Even targeted attacks are more difficult because the attacker would be required to access to different forms of authentication. A Google study showed that SMS based authentication "can block up to 100% of automated bots, 99% of bulk phishing attacks, and 66% of targeted attacks".

Bryt uses SMS two-factor authentication. This means that the user will be required to know their password when a user signs up or logs in to the application a numeric code is sent to their mobile device via SMS. The numeric code will be required to access the application. Once the user accesses the application on a specific device, the user can choose to "trust" the device in the future. By default. The Bryt application does not automatically turn on two factor authentication. Unless the client has a global requirement for 2FA, the option to use 2FA is left to each individual user.