CAPTCHA and OTP

CAPTCHA

CAPTCHA

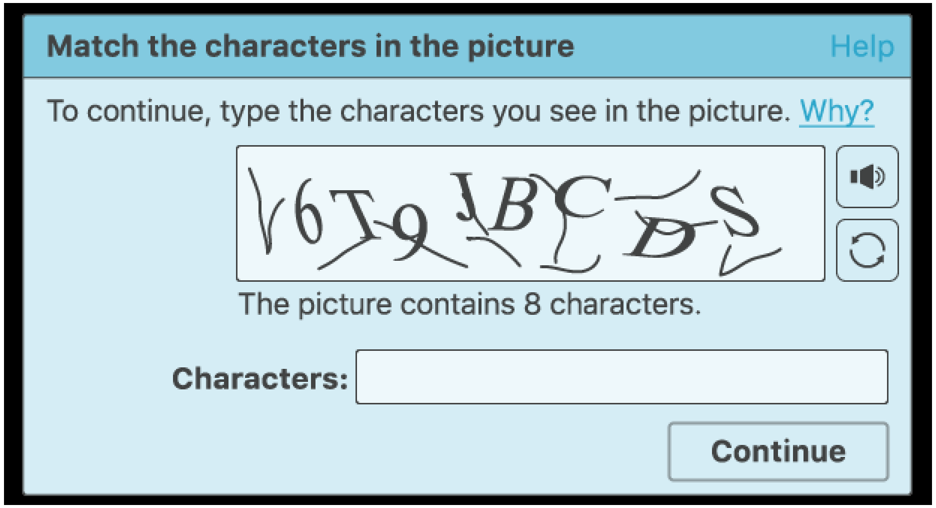
- What is a CAPTCHA?
  - A test is designed to determine if an online user is really a human and not a bot.
  - CAPTCHA is an acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart."
  - Users often encounter CAPTCHA and reCAPTCHA tests on the Internet.
  - Such tests are one way of managing bot activity , although the approach has its drawbacks.

CAPTCHA

- What is a CAPTCHA?
  - Although CAPTCHAs are designed to block automated bots
  - CAPTCHAs are themselves automated
  - They're programmed to pop up in certain places on a website, and they automatically pass or fail users

How does a CAPTCHA work?

- Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters.
- The letters are distorted so that bots are not likely to be able to identify them.
- Topass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form.
- If the letters don't match, users are prompted to try again. Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages.



Match the characters in the picture

To continue, type the characters you see in the picture. Why?

The picture contains 8 characters.

Characters:

How does a CAPTCHA work?

- – The idea is that a computer program such as a bot will be unable to interpret the distorted letters,

- – while a human being, who is used to seeing and interpreting letters in all kinds of contexts –different fonts, different handwritings, etc. – will usually be able to identify them.

- – The best that many bots will be able to do is input some random letters, making it statistically unlikely that they will pass the test.

- – Thus, bots fail the test and are blocked from interacting with the website or application, while humans are able to continue using it like normal.

How does a CAPTCHA work?

- Advanced bots are able to use machine learning to identify these distorted letters, so these kinds of CAPTCHA tests are being replaced with more complex tests.

- Google reCAPTCHA has developed a number of other tests to sort out human users from bots.

What is reCAPTCHA?

- reCAPTCHA is a free service Google offers as a replacement for traditional CAPTCHAs

- reCAPTCHAtechnology was developed by researchers at Carnegie Mellon University, then acquired by Googlein 2009.

- reCAPTCHA is more advanced than the typical CAPTCHA tests.

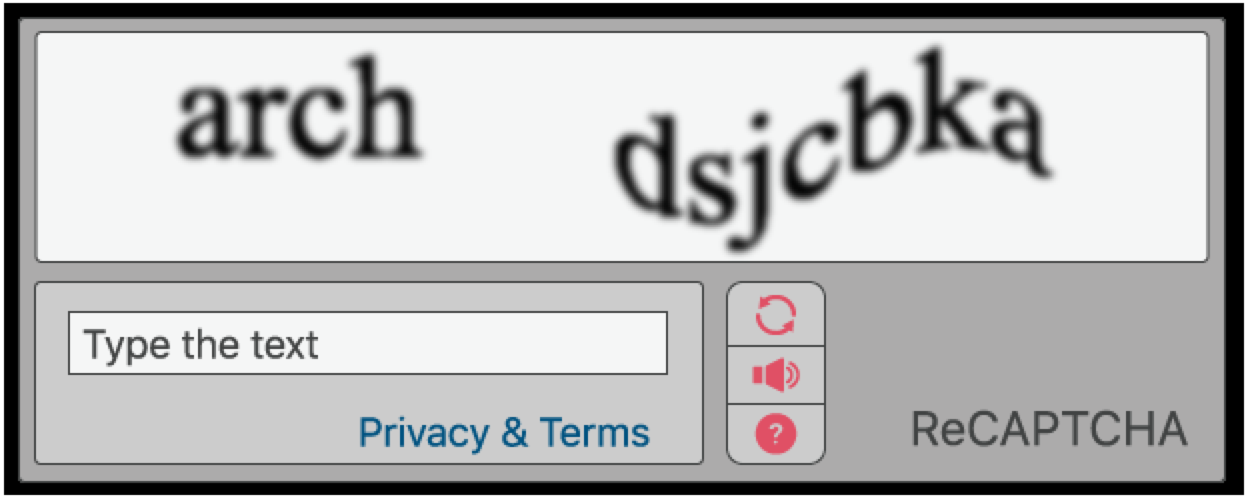
- Like CAPTCHA, some reCAPTCHAs require users to enter images of text that computers have trouble deciphering.

- Unlike regular CAPTCHAs, reCAPTCHA sources the text from real-world images: pictures of street addresses, text from printed books, text from old newspapers, and so on.

What is reCAPTCHA?

- Over time, Google has expanded the functionality of reCAPTCHA tests so that they no longer have to rely on the old style of identifying blurry or distorted text.

- Other types of reCAPTCHA tests include:
  - Image recognition
  - Checkbox
  - General user behavior assessment (no user interaction at all)



What is reCAPTCHA?

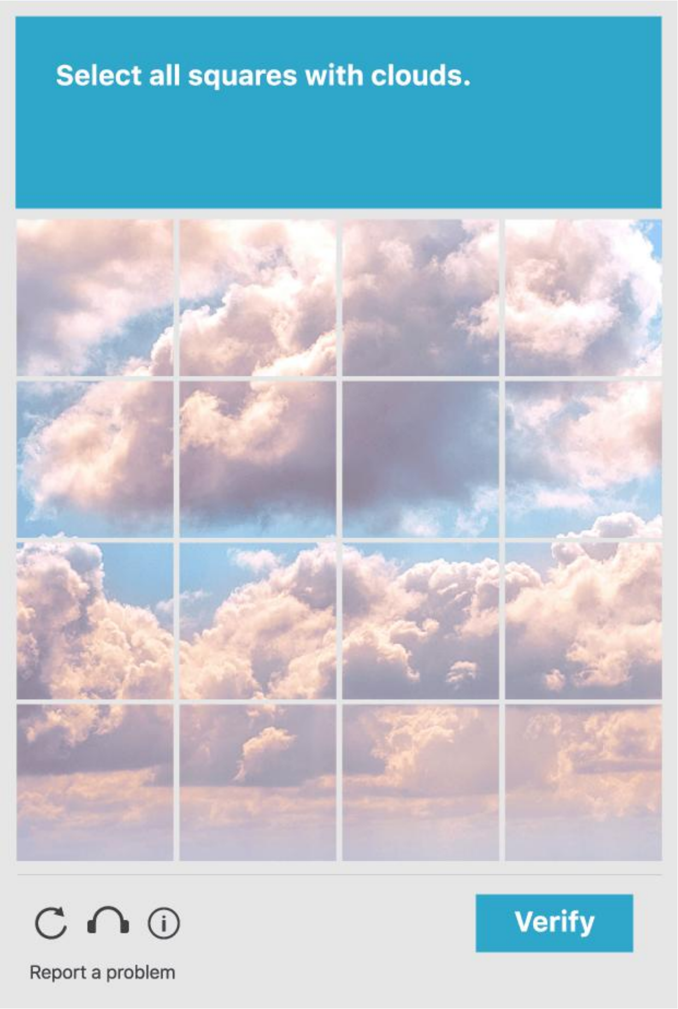
- **How does an image recognition reCAPTCHA test work?**

- For an image recognition reCAPTCHA test, typically users are presented with 9 or 16 square images.

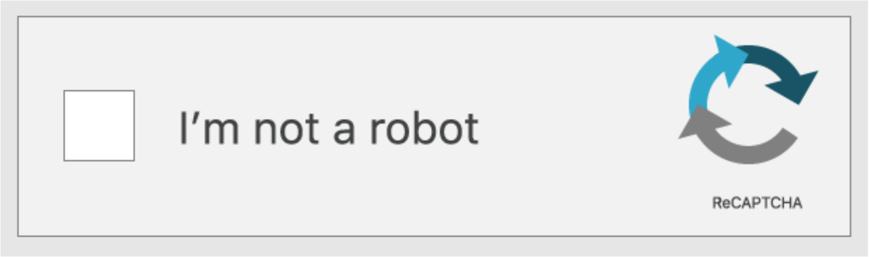
- The images may all be from the same large image, or they may each be different.

- A user has to identify the images that contain certain objects, such as animals, trees, or street signs.

- If their response matches the responses from most other users who have submitted the same test, the answer is considered "correct" and the user passes the test.



Select all squares with clouds.



□ I’m not a robot

reCAPTCHA tests with a single checkbox

What is reCAPTCHA?

- **How does an image recognition reCAPTCHA test work?**

- For an image recognition reCAPTCHA test, typically users are presented with 9 or 16 square images.

- The images may all be from the same large image, or they may each be different.

- A user has to identify the images that contain certain objects, such as animals, trees, or street signs.

- If their response matches the responses from most other users who have submitted the same test, the answer is considered "correct" and the user passes the test.

one-time password (OTP)

OTP

- A one-time password (OTP) is a string of numbers and/or characters that is generated and sent to a user to be used for a single login attempt or transaction.

What are the benefits of OTPs?

- OTPs reduce the risk around passwords.

- **Forgotten passwords**
  - One of the most common uses of OTPs is the case where a user has forgotten their password, or had their account breached.

  - An OTP may be issued to the user to access their account before they are prompted to reset their password.

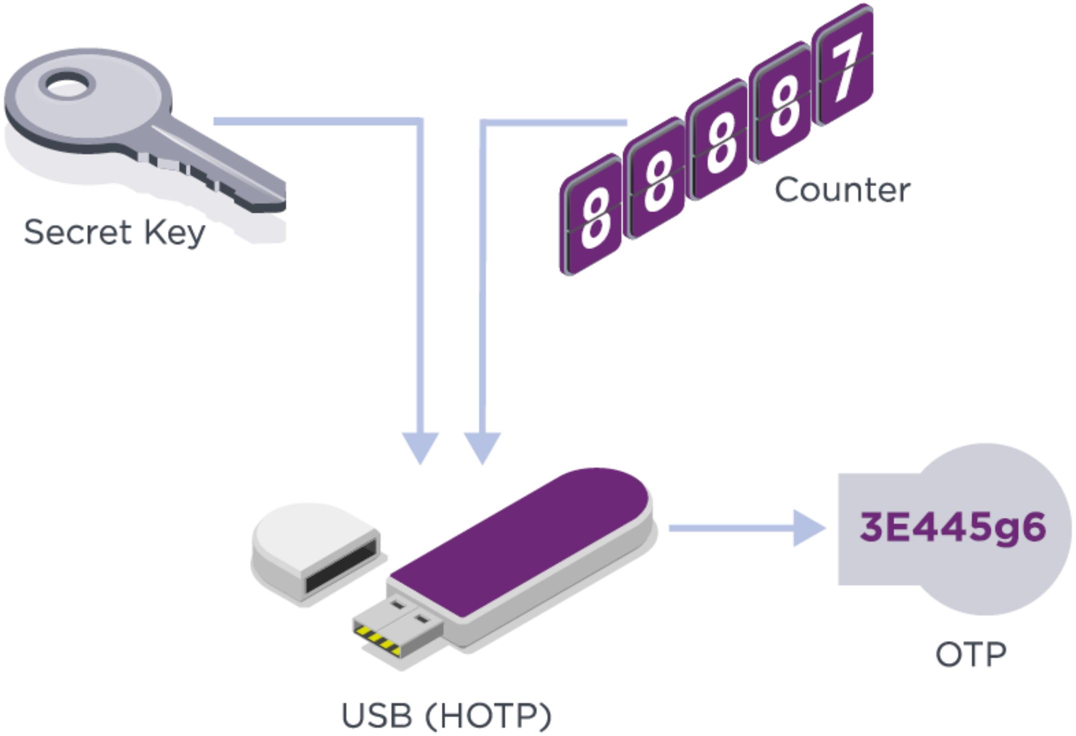
What are the benefits of OTPs?

- **Replay attacks**
  - In a replay attack, a user’s login credentials, including their password, are intercepted.
  - If the password is static, the attacker would now have access to that user’s account.
  - But when an OTP is used, the password intercepted by the hacker is no longer valid as it was already used once when the user logged into their account and can thus no longer be reused.

- **Multi-factor authentication**
  - OTPs can add an additional layer of authentication.
  - Using security tokens, OTPs can be generated for users to provide as an additional form of authentication, which increases security and reduces the risk of a breach.

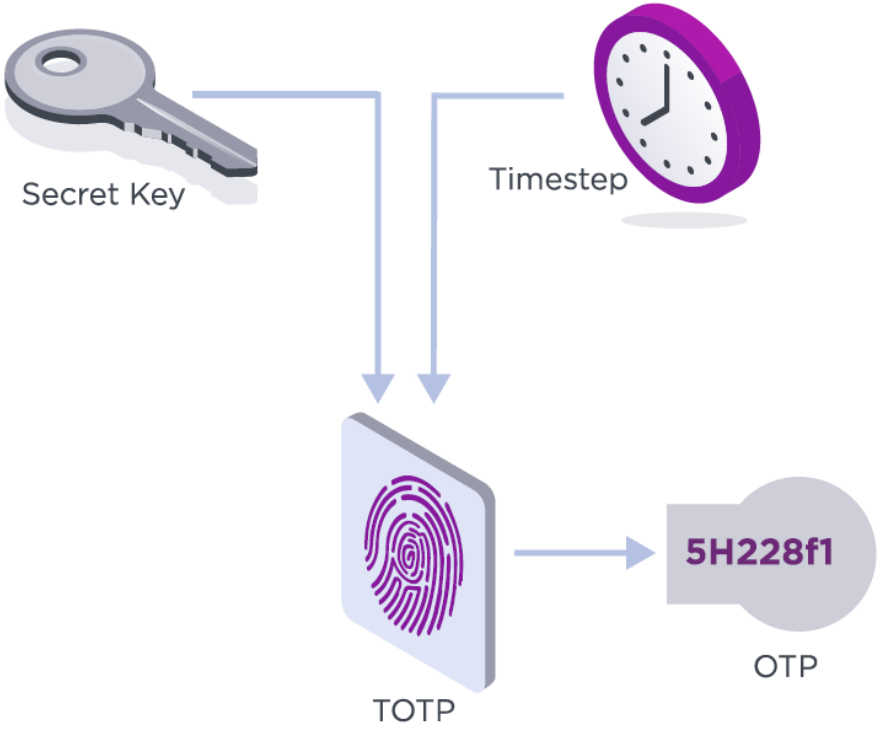
What are the types of OTPs?

- **Hash-based OTP (HOTP)**
  - This type of OTP is generated and sent to a user based on a hash algorithm that syncs the OTP code with counter that changes incrementally.



What are the types of OTPs?

- **Time-based OTP (TOTP)**
  - This type of OTP is time-based, in that it provides a window of time within which the OTP code will be valid.
  - In general, time steps are 30-60 seconds in length. If the user does not enter the OTP code within the specified time step, they must request a new one.



How are OTPs provided to users securely?

- OTPs are generated and sent to users securely using security tokens.
- **Hard tokens**
  - Smart cards, USB keys, keyless entry systems, mobile phones, and Bluetooth tokens are all capable of generating OTPs.
  - A hard token may be connected, disconnected, or completely contactless.
- **Soft tokens**
  - A push notification to email, via SMS, or an app is the common form of OTP soft tokens.

How are OTPs provided to users securely?

- Autonomous security mechanism where a user is provided an OTP for every login.

- Thus, these terms should not be used synonymously as OTP is just one of many forms of 2FA/MFA and can also stand alone as its own security solution.

Is an OTP more secure than a static password?

- Yes.

- OTPs add an additional layer of security to static passwords. Passwords alone are a vulnerable form of identity verification, responsible for 81% of security breaches.

- Adding another layer of authentication to passwords ensures better security.

- Of course, you could get rid of passwords altogether by going passwordless.