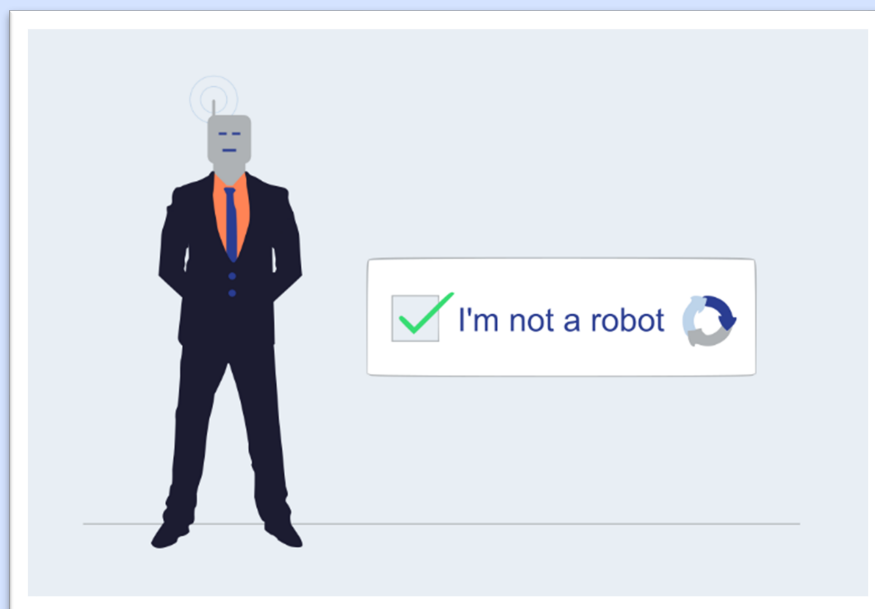




I'm not a robot: CAPTCHAs und digitale Barrierefreiheit



Was ist ein CAPTCHA?

Ein CAPTCHA ist eine kleine Aufgabe auf einer Webseite, mit der überprüft werden soll, ob ein Mensch oder ein Bot die Seite nutzt. Die Abkürzung steht für „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part“.

Der Name beschreibt damit bereits das Ziel: automatisierte Angriffe durch Bots abwehren, ohne echten Nutzenden den Zugang zu Webseiten zu erschweren. Denn Bots können erheblichen Schaden anrichten: Sie erstellen massenhaft Fake-Profile, testen gestohlene Passwörter auf Login-Seiten oder durchsuchen Webseiten nach Daten wie E-Mail-Adressen, um diese für automatisierte Angriffe weiterzuverwenden oder zu verkaufen.

Gleichzeitig sollen echte menschliche Nutzende barrierefrei auf Inhalte und Funktionen im Internet zugreifen können, unabhängig von individuellen Fähigkeiten oder genutzten Hilfsmitteln. Doch genau das gelingt in der Praxis oft nicht. Viele CAPTCHA-Lösungen sind für Menschen mit Beeinträchtigungen schwer oder gar nicht zugänglich.

In diesem Guide zeigen wir euch daher, welche CAPTCHA-Arten es gibt und welche Barrieren sie erzeugen können. Ziel ist es, ein besseres Verständnis für bestehende Möglichkeiten zu schaffen und praktische Hinweise für die Gestaltung digitaler Angebote zu geben.

Sicherheit und Barrierefreiheit: Ein Widerspruch?

Um Webseiten vor automatisierten Angriffen zu schützen, wurde Ende der 1990er Jahre eine erste CAPTCHA-Lösung entwickelt: verzerrte Buchstaben- und Zahlenkombinationen. Diese später als reCAPTCHA v1 bekannte Methode galt zunächst als elegante Lösung: Man nahm an, dass Menschen die Zeichen trotz Verformung lesen und fehlerfrei abtippen können, während Maschinen an der Aufgabe scheitern. In der Praxis jedoch zeigte sich schnell, dass viele Menschen große Schwierigkeiten mit dieser Art von Test hatten. Für Personen mit Sehbehinderungen oder Dyslexie sind Text-CAPTCHAs nicht zugänglich. Auch assistive Technologien wie Screenreader können die verzerrten Zeichen nicht erfassen.

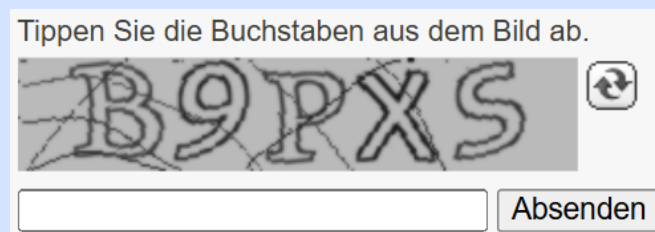


Abbildung 1: Text-CAPTCHA

Um diese Barrieren zu adressieren, wurden Audio-CAPTCHAs eingeführt. Nutzende hören dabei eine Reihe von Zahlen oder Wörtern mit Störgeräuschen und sollen diese korrekt wiedergeben. Doch auch diese Variante bringt neue Hürden mit sich: Für Menschen mit Hörbeeinträchtigungen, auditiven Verarbeitungsstörungen oder kognitiven Einschränkungen sind die Aufnahmen schwer oder gar nicht verständlich.

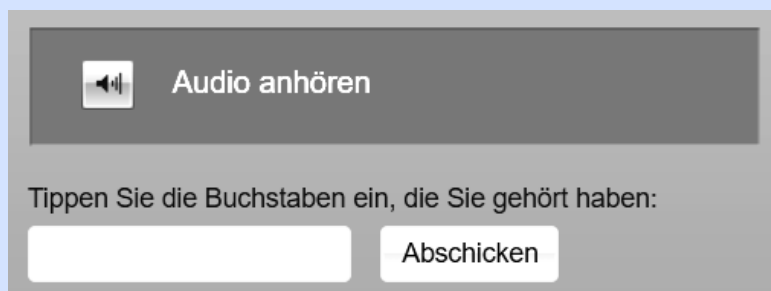


Abbildung 2: Audio-CAPTCHA

Als nächste Evolutionsstufe folgten bildbasierte CAPTCHAs, bei denen Objekte in Fotos erkannt und ausgewählt werden müssen, z. B. alle Felder mit Ampeln oder Fahrrädern. Diese Methode setzt gutes Sehen und räumliches Erkennen voraus. Seheingeschränkte oder blinde Menschen können diese Tests kaum eigenständig lösen und empfinden diese häufig als frustrierend.

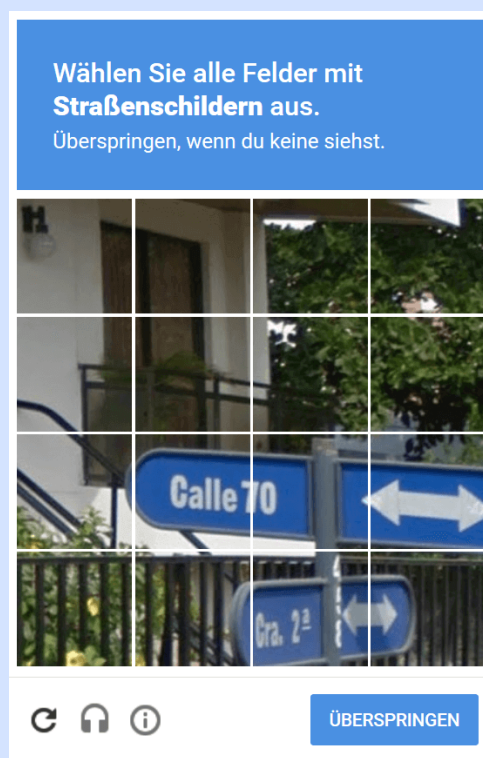


Abbildung 3: Bild-CAPTCHA

Auch mathematische Aufgaben wurden getestet, um Menschen und Bots zu unterscheiden. Fragen wie „Was ist 74 minus 36?“ setzen jedoch Zahlenverständnis, Konzentration und sprachliches Erfassen voraus. Für Menschen mit Dyskalkulie, Aufmerksamkeitsstörungen oder kognitiven Einschränkungen kann das zur unüberwindbaren Hürde werden.



Lösen Sie die Rechenaufgabe!

$21+42=?$

Senden

Abbildung 4: Mathematisches CAPTCHA

Weniger verbreitet, aber ebenfalls genutzt, sind Logikrätsel oder Trivia-Fragen wie „Welche Zahl gehört nicht in die Reihe?“ oder „Wer war der erste Mensch auf dem Mond?“. Solche Aufgaben setzen abstraktes Denken, kulturelles Wissen und gute Lesefähigkeit voraus. Diese Anforderungen schließen beispielsweise Personen mit Lernschwierigkeiten, niedrigem Bildungsgrad oder geringen Deutschkenntnissen aus.



Drehen Sie den Gegenstand in die korrekte Position.

Prüfen Zurücksetzen

Abbildung 5: Logikrätsel als CAPTCHA

Neuere Systeme wie reCAPTCHA v2 („Ich bin kein Roboter“-Checkbox) oder invisible reCAPTCHA versuchen, Bots durch eine Verhaltensanalyse zu erkennen. Analysiert werden etwa Mausbewegungen oder Tippverhalten. Diese Methoden sind weniger aufdringlich als klassische Rätsel. Doch wer mit der Tastatur statt der Maus navigiert, Hilfsmittel wie Screenreader verwendet oder motorische Einschränkungen hat, verhält sich oft anders als der Durchschnitt. Diese Abweichung können dazu führen, dass Betroffene fälschlicherweise als Bots eingestuft werden und dann doch ein zusätzliches, oft schwer zugängliches CAPTCHA lösen müssen.

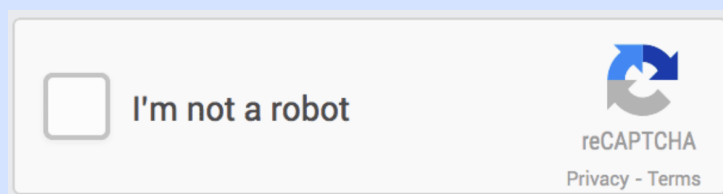


Abbildung 6: Signalbasiertes CAPTCHA (Verhaltensanalyse)

Neben den Problemen mit der Barrierefreiheit zeigen sich bei den bereits vorgestellten CAPTCHAs auch deutliche Schwächen bei der Nutzerfreundlichkeit. Unabhängig vom Thema Behinderung benötigen Nutzende meist mehrere Anläufe, um CAPTCHAs zu lösen oder scheitern regelmäßig daran. Besonders ältere Personen oder Menschen mit wenig Erfahrung im Umgang mit digitalen Anwendungen empfinden die Tests oft als verwirrend oder frustrierend.

Hinzu kommt ein weiterer entscheidender Faktor: Bots werden immer besser und somit verlieren CAPTCHAs kontinuierlich an Wirkungen. OCR-Technik knackt verzerrte Texte, Spracherkennung überwindet Audio-CAPTCHAs, moderne KIs erkennen Objekte auf Bildern und verhaltensbasierte CAPTCHAs lassen sich durch simulierte Bewegungen täuschen. Diese Entwicklungen sorgen für einen stetigen Innovationsdruck: CAPTCHA-Systeme müssen sowohl zugänglich für Menschen als auch robust gegen immer ausgefeiltere Bots sein.

Barrierefreie Alternativen zu klassischen CAPTCHAS

Um die Barrieren klassischer CAPTCHAs zu vermeiden, wurden in den letzten Jahren alternative Ansätze entwickelt.

Proof-of-Work-Verfahren (z. B. Friendly CAPTCHA)

Diese Methode verlagert die Sicherheitsprüfung auf den Computer: Im Hintergrund muss der Rechner eine komplizierte Rechenaufgabe lösen. Der Mensch selbst bekommt davon nichts mit. Da Bots mehrere Anfragen gleichzeitig an Webseiten stellen, stoßen sie bei vielen Rechenaufgaben schnell an ihre Grenzen. Diese CAPTCHAs helfen allen, die bei klassischen CAPTCHAs durch unverständliche, visuelle oder akustische Aufgaben benachteiligt sind.

Zeitbasierte Filter

Diese Technik prüft, wie schnell ein Formular ausgefüllt wird. Bots agieren oft in Millisekunden. Menschen brauchen länger. Ist das Formular verdächtig schnell ausgefüllt, wird der Absender blockiert – ganz ohne zusätzliche Interaktion.

Honeypot-Technik

Im Formular wird ein zusätzliches Feld eingebaut, das nur Bots sehen, Menschen jedoch nicht. Wird das Feld befüllt, ist die Anfrage verdächtig.

Wichtig: Das Feld darf nicht zu sehen sein und muss für Screenreader un erreichbar sein. Dazu blendet man es mit `style="display:none"` und `aria-hidden="true"` aus.

Proof-of-Personhood-Systeme

Diese Systeme prüfen nicht nur, ob eine Anfrage von einem Menschen kommt, sondern ob es sich um eine individuelle reale Person handelt. Möglich wird das durch kryptografische Verfahren, Gerätediagnosen oder verifizierte Identitäten. Dieser Ansatz steckt noch in der Entwicklung. Langfristig könnten Proof-of-Personhood-Systeme eine benutzerfreundliche Sicherheitslösung für alle sein.

Checkliste

Damit Sicherheitsmechanismen auf eurer Webseite niemanden ausschließen, solltet ihr folgende Hinweise bei der Umsetzung beachten:

- ✓ Verzichtet auf klassische Bild- oder Audio-CAPTCHAs. Wählt stattdessen Verfahren, die ohne Nutzerinteraktion auskommen und passiv im Hintergrund ablaufen.
- ✓ Beachtet das Zwei-Sinne-Prinzip. Gebt also niemals visuelle Anweisungen wie „Wählen Sie alle Bilder mit Ampeln“, ohne Alternativen anzubieten.
- ✓ Stellt sicher, dass alle Sicherheitslösungen mit assistiven Technologien kompatibel sind. Testet dafür eure Software mit Screenreadern und verschiedenen Eingabemethoden (Tastatur, Sprache etc.).
- ✓ Informiert Nutzende über die verwendete Schutzmaßnahme, z. B. mit einem Hinweis wie „Zum Schutz gegen Spam verwenden wir eine barrierefreie Sicherheitsprüfung im Hintergrund.“
- ✓ Führt regelmäßige Prüfungen durch, um sicherzustellen, dass neue Sicherheitsmechanismen keine unbeabsichtigten Barrieren einführen.

Glossar

- » **Assistive Technologien:** Hilfsmittel wie Screenreader, Braillezeilen oder Sprachausgabe, die Menschen mit Beeinträchtigungen die Nutzung digitaler Inhalte ermöglichen.
- » **Bot:** Ein Bot ist ein Computerprogramm, das automatisch Aufgaben ausführt, für die sonst Menschen nötig wären. Zum Beispiel Webseiten durchsuchen oder Nachrichten beantworten.
- » **CAPTCHA:** Kleine Aufgabe auf einer Webseite, mit der überprüft werden soll, ob ein Mensch oder ein Bot die Seite nutzt. Kurz für: Completely Automated Public Turing test to tell Computers and Humans Apart.
- » **Dyslexie:** Auch „Lese-Rechtschreib-Störung“ genannt. Eine Lernstörung, bei der das Lesen und Schreiben schwerfällt.
- » **Dyskalkulie:** Auch „Rechenstörung“ genannt. Eine Lernstörung, bei der das Verstehen und Anwenden von Zahlen und Rechenregeln erschwert ist.
- » **Screenreader:** Ein Programm, das Texte auf dem Bildschirm vorliest oder in Braille ausgibt. Es hilft blinden oder sehbehinderten Menschen, Computer und Webseiten zu nutzen.
- » **OCR:** Kurz für „Optical Character Recognition“ (optische Zeichenerkennung). Eine Technik, mit der Texte aus Bildern oder gescannten Dokumenten automatisch erkannt und digital lesbar gemacht werden.
- » **Zwei-Sinne-Prinzip:** Wichtige Informationen sollen immer über mindestens zwei Sinne wahrnehmbar sein, zum Beispiel visuell (sehen) und auditiv (hören).