User Perception of CAPTCHAs: A Comparative Study between University and Internet Users

Arun Reddy 1 and Yuan Cheng $^2 [0000-0001-7176-3951]$

¹ Intel Corporation, Santa Clara CA 95054, USA r3ddy.arun@gmail.com
² Grand Valley State University, Allendale MI 49401, USA chengy@gvsu.edu

Abstract. CAPTCHAs are commonly used to distinguish between human and bot users on the web. However, despite having various types of CAPTCHAs, there are still concerns about their security and usability. To address these concerns, we surveyed over 250 participants from a university campus and Amazon Mechanical Turk. Our goal was to gather user perceptions regarding the security and usability of current CAPTCHA implementations. After analyzing the data using statistical and thematic methods, we found that users struggle to navigate current CAPTCHA challenges due to increasing difficulty levels. As a result, they experience frustration, which negatively impacts their user experience. Additionally, participants expressed concerns about the reliability and security of these systems. Our findings can offer valuable insights for creating more secure and user-friendly CAPTCHA technologies.

Keywords: CAPTCHA · Authentication · Usability.

1 Introduction

The "Completely Automated Public Turing Test to tell Computers and Humans Apart" (CAPTCHA) [1] is a popular challenge-response-based test that distinguishes real human users from bots on websites. CAPTCHAs prevent abuse such as false form submissions, fraudulent purchases, spam emails, and fake registrations. Since its inception in the late 1990s, CAPTCHAs have taken on various forms, including text, image, audio, and video. However, security concerns have arisen as CAPTCHAs have become more commonplace on major websites. Text-based CAPTCHAs are vulnerable to optical character recognition (OCR) technology [17,16,23], while image-based CAPTCHAs are susceptible to machine learning attacks [7]. Meanwhile, the security of audio and visual CAPTCHAs can be compromised by Hidden Markov Model-based attacks [19]. Even other types of CAPTCHAs have been found to be vulnerable under the influence of cookie tracking, tag frequency-based attacks, side-channel attacks, and simple JavaScript code [21,14,11,22].

An ideal CAPTCHA should ace both security and usability. However, to defend against attacks, CAPTCHA systems often introduce distortion and noise

to their challenges, making them more difficult for users to solve. Text-based CAPTCHAs, in particular, often contain scattered lines, dots, and distorted characters that require extra user effort. Furthermore, these distortions can be especially unfriendly to users whose native language does not use the Latin alphabet [24]. Image-based CAPTCHAs can also present accessibility challenges for users with visual impairments or color blindness [24]. On the other hand, audio and video-based CAPTCHAs may have issues with large file sizes and limited time for users to comprehend the content [2,20].

Creating a secure yet user-friendly CAPTCHA system poses complex challenges. To gain insight into what this type of system should entail, we set out to answer three research questions:

- What do users prefer in CAPTCHAs?
- How usable are current CAPTCHAs?
- How can we effectively balance security and usability when implementing CAPTCHAs?

We surveyed over 250 participants from two groups, including computer science students at a public university and individuals from Amazon Mechanical Turk. The survey evaluated the user experience of CAPTCHAs through quantitative and qualitative methods. We found that illegible texts/images and unclear instructions were the main reasons for failing a CAPTCHA challenge in one attempt. Additionally, human errors like lack of time and inattention also contributed to failures. We discovered that when users could not solve a CAPTCHA in one attempt, they often abandoned webpages, causing a decrease in traffic. The study revealed that users do not enjoy solving CAPTCHAs but see it as a necessary burden. We also analyzed the differences in responses between the two user groups and explored factors contributing to these variances.

In the following sections, we review relevant literature in Section 2. We then detail the user study design in Section 3. In Section 4, we present the quantitative and qualitative findings. We discuss the findings and suggest future work in Section 5 before the concluding remarks in Section 6.

2 Related Work

In this section, we will discuss the literature relevant to our study.

2.1 CAPTCHA Security

Chellapilla et al. argued that the difficulty of a CAPTCHA is ideal if humans solve the challenge with a success rate of at least 90% while automatic scripts achieve a success rate of less than 0.01% [3]. Below, we outline some existing techniques for breaking common CAPTCHA types, including text-based, image-based, and audio/video-based.

Text-based CAPTCHAs, typically using alphanumeric characters, are vulnerable to optical character recognition (OCR) algorithms. This technique breaks

down the image into smaller segments containing a single character. It then matches against standard letter templates using a pattern recognition algorithm. Yan et al. presented a low-cost attack on text-based CAPTCHAs developed by tech giants such as Microsoft, Google, and Yahoo [23]. The authors developed an attack that could segment the challenges generated. It also identified the exact location of all the characters in the order they appeared. Nguyen et al. discovered a method to break 3D CAPTCHAs without using OCR techniques by extracting pixel blocks from the characters of CAPTCHA challenges and using them for automated recognition [17]. Mori et al. utilized a shape context matching algorithm to crack Gimpy CAPTCHA with 33% accuracy [16].

Conti et al. summarized the main breaking strategies against image-based CAPTCHAs [4]. Some image-based CAPTCHAs just hide the solutions on the client-side, making them vulnerable to reverse engineering attacks. Others store pre-computed challenge answers in databases, thus prone to exhaustive searches or even random guesses if the number of responses is small. If such databases are compromised, these CAPTCHAs become easy prey. Golle employed a support vector machine classifier to automatically solve the Asirra CAPTCHA with a high success rate [7]. Instead of solving shape or image recognition, Hernandez-Castro et al. introduced a side-channel attack that leverages the JPEG file size to measure image continuity [10].

Sano et al. presented an attacking method against both audio and visual CAPTCHAs using Hidden Markov Models (HMMs) [19]. The method could decode the audio and visual variants of Google's reCAPTCHA with success rates of 58.75% and 31.75%, respectively. Kluever et al. proposed a video CAPTCHA mechanism and discussed a frequency-based attack that is effective against the proposed mechanism [13]. The video CAPTCHA challenge requires users to submit three relevant tags as a solution. However, an automated program can exploit publicly available tag frequency estimation to break the mechanism.

2.2 CAPTCHA Usability

Yan et al. proposed a 3D framework to examine CAPTCHA usability that used distortion, content, and presentation to study various CAPTCHA types [24]. Sauer et al. studied the accessibility and usability of audio CAPTCHAs and found that their proposed scheme was accessible but had a low success rate of less than 90% due to solvability challenges [20]. Fidas et al. conducted a user survey to evaluate CAPTCHA usability [6]. The authors found that every other user needed at least two attempts to pass a CAPTCHA challenge, and that background patterns in CAPTCHAs had little impact on security and affected usability. Krol et al. compared and contrasted three CAPTCHA mechanisms: a traditional text-based reCAPTCHA, PlayThru, and NoBot [15]. They focused on holistic user experience in solving CAPTCHAs. Time and workload were the two parameters used to compare the CAPTCHA mechanisms. They observed that using tablets resulted in significantly more hassles. Bursztein et al. led a study in which more than 300,000 CAPTCHAs were solved by workers on Amazon Mechanical Turk [2]. The authors demonstrated that CAPTCHAs are hard

4 A. Reddy et al.

for humans to solve, and audio-based CAPTCHAs are more tedious than their counterparts. Reynaga et al. presented users with nine CAPTCHA mechanisms with unconventional input schemes to enhance usability [18]. The study, however, found that users preferred conventional methods due to familiarity. Gossweiler et al.'s study found dissatisfaction with text-based CAPTCHAs [8], while Ho et al. experimented with CAPTCHA usability where participants had to solve CAPTCHAs several times [12].

2.3 Comparison with This Work

Our work explores user perspectives on CAPTCHA security and usability, with a focus on the latter. We integrate usability issues identified in Yan et al.'s work [24] into our survey questions. Unlike prior studies focusing on specific CAPTCHA types (e.g., text-based [24,8], audio-based [20], or multiple types [15,18]), we aim for a comprehensive overview encompassing all types. The closest work to ours is Fidas et al.'s user survey [6]. Both studies address the user perceptions on security-usability trade-offs, attempts required to solve CAPTCHAs, language influences, etc. However, we want to investigate how user views have evolved since a decade ago as CAPTCHAs become more prevalent. Furthermore, we recruit participants from two distinct sources to see if their opinions vary significantly. Conversely, Fidas et al.'s study did not reveal where they recruited the 210 participants.

3 Methodology

This study aimed to understand how users perceive and adopt CAPTCHA mechanisms. To this end, we conducted an online survey to collect participants' views on the security and usability of CAPTCHAs. It was reviewed and approved by our institution's Institutional Review Board.

3.1 Recruitment

We recruited participants from two sources: Amazon Mechanical Turk and university students majoring in Computer Science. We refer to these two groups as MTurk users and university users hereafter.

Amazon Mechanical Turk, also known as MTurk, is a marketplace where we can hire a diverse workforce to complete virtual tasks requiring human intelligence. Compared to traditional participants in social science studies, MTurk users typically vary widely in age, income, education, and location [9]. We selected candidates with a Human Intelligence Task (HIT) rate of over 90% and more than 50 approved HITs for the study. Each participant was paid a \$1 incentive for completing the 5-minute survey. Within 30 minutes, we received 150 responses, primarily from the United States.

University users were recruited from a public university in the United States. All participants in this group were enrolled in upper-division computer science courses and had a technical background.

3.2 Study Design

We used Qualtrics, a web-based survey tool, to conduct the anonymous survey. To avoid malpractice, participants would get a unique code at the end so they could only take the survey once.

Our questionnaire comprised 23 questions. The first seven questions gathered demographic information and determined survey eligibility. The next 16 questions focused on participants' perceptions of various CAPTCHA schemes regarding security and usability.

We first asked participants about different CAPTCHA types they had encountered daily, including math, text identification, image selection, image dragging or dropping, audio/video, and game CAPTCHAs. We also allowed participants to specify any other CAPTCHA types they experienced. We then asked participants to rate these different CAPTCHA types on a five-point Likert scale, from "Least preferable" (1) to "Most preferable" (5). Next, we asked participants if they had solved a CAPTCHA in a language other than English. If so, we asked them what type of non-English CAPTCHAs they preferred (e.g., text vs. audio/video). We allowed them to choose neither or both in this question.

The next few questions were about usability. We first focused on small devices, such as a phone or a tablet. We asked participants if factors such as screen size, orientation, network bandwidth, and processor speed played a role in their perception. We then asked participants if, generally, they could solve a CAPTCHA in a single attempt. For those who generally took more than one attempt to solve a CAPTCHA, we followed up with an open-ended question to gather information about the reasons behind their difficulties. We asked them if factors such as size, shape, color, distortion features, or background patterns made it harder for them to solve the challenge. We also designed some questions on users' frustration concerning solving CAPTCHA tests. We asked participants if they had ever abandoned a website because of a CAPTCHA challenge.

As a security mechanism itself, the security of CAPTCHAs is also a significant concern. The last three questions attempted to understand users' perspectives on CAPTCHA security and overall effectiveness.

We screened potential participants based on their previous experience with CAPTCHAs and advanced only those who had solved a CAPTCHA at least once to the rest of the survey. We also recorded the time taken to complete the survey and discarded any results that were completed in less than 15 seconds. However, no participant was disqualified for this reason. We received 154 responses from MTurk users, discarding four incomplete ones. Meanwhile, all 109 responses from university users were valid.

3.3 Demographics

Before presenting our findings, we provide a summary of our respondents' demographics, outlined in Table 1.

Our survey included 259 valid respondents, with a higher proportion of males (62%) compared to females (32%). Among university users, only 14% were fe-

Table 1: Demographics

	МТ	urk	Un	iv.	Tot	al
	No.	%	No.	%	No.	%
Gender						
Male	82	55	90	83	172	66
Female	68	45	15	14	83	32
Non-binary	0	0	2	2	2	1
Decline to say	0	0	2	2	2	1
Age						
18-24	6	4	65	60	71	27
25-34	69	46	38	35	107	41
35-44	38	25	5	5	43	17
45-54	19	13	1	1	20	8
55-64	12	8	0	0	12	5
64 or older	6	4	0	0	6	2

	МТ	urk	Un	iv.	Tot	al
	No.	%	No.	%	No.	%
Education						
Less than high school	2	1	0	0	2	1
degree						
High school degree	9	6	5	5	14	5
Some college experience	17	11	55	50	72	28
Associate degree	15	10	36	33	51	20
Bachelor's degree	85	57	13	12	98	38
Postgraduate degree	22	15	0	0	22	8
Language						
Native English speaker	136	91	87	80	223	86
Non-native speaker	14	9	22	20	36	14

male. Although we would have preferred a more balanced gender ratio in university users, these proportions align with the U.S. national average (18%). The ages of our respondents ranged from 19 to 70 years old, with an average age of 32 and a standard deviation of 11.39. The largest age group was 25-34, constituting 41% (107 out of 259) of respondents. Of these 107 respondents, 69 were MTurk users, and 38 were university users. Meanwhile, 60% of university users (65 out of 109) were aged 18-24. MTurk users had diverse educational backgrounds, with over 70% holding a bachelor's degree or higher. In contrast, most university users (88%) were pursuing their first bachelor's degree. Among respondents, 86% (223) were native English speakers. On the other hand, there are relatively more nonnative English speakers in university users (20%), reflecting the diversity of the university's student body.

3.4 Hypotheses

The following null hypotheses were formulated in this study:

- (H1) There is no significant difference in the user perception of preferred CAPTCHA types between the two user groups.
- (H2) There is no significant difference in the user perception of solving CAPTCHAs on smaller devices between the two user groups.
- (H3) Both user groups abandon CAPTCHA challenges for similar reasons.
- (H4) There is no significant difference in the user perception of CAPTCHA difficulty between the two user groups.
- (H5) There is no significant difference in the user perception of CAPTCHA security between the two user groups.
- (H6) There is no significant difference in overall opinion of CAPTCHAs between the two user groups.

4 Findings

After gathering the responses, we analyzed the data from the Likert and closed-ended questions. We wanted to determine if there is any difference between the two distinct user groups, MTurk and university users, regarding their perspectives on CAPTCHAs.

Use and preferences on CAPTCHA types We surveyed respondents on their use of different CAPTCHA types, including math, text identification, image recognition, image drag and drop, audio/video, and game/puzzle. Figure 1 shows that image recognition is the most prevalent type (224 votes, 89%) for both user groups, followed by text identification CAPTCHAs (189 votes, 75%). The least used were audio/video CAPTCHAs (57 votes, 23%). These results align with current market trends, with many websites still using Google reCAPTCHA v2 or earlier versions, featuring image recognition challenges. Text identification CAPTCHAs remain competitive, as websites like Amazon and Facebook continue to utilize them. However, audio/video CAPTCHAs, initially designed for users with disabilities, face practical challenges due to accessibility and availability issues.

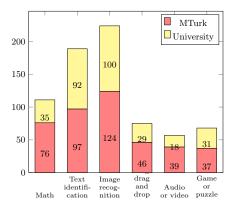


Fig. 1: Use of different CAPTCHAs (n=253)

We then asked respondents to rank their preferences for different CAPTCHAs on a scale of 1 to 5, with 1 being least preferable and 5 being the most preferable. Figure 2 shows the preferences of MTurk users, and Figure 3 presents those of university users. Text identification is the most preferred CAPTCHA among MTurk users (55 votes, 37%), followed by image recognition (45 votes, 31%). Conversely, university users favored image recognition the most (33 votes, 31%), with text identification as their second choice (23 votes, 22%).

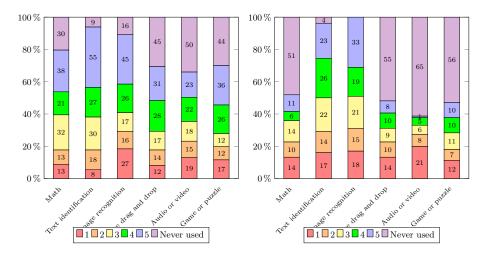


Fig. 2: Preferences of MTurk users

Fig. 3: Preferences of university users

We also observed that over half of university users never solved any of the other four CAPTCHA types, whereas MTurk users showed a more diverse usage pattern. Additionally, a significant difference was observed between the two groups in their CAPTCHA preferences (p-value < 0.05), as determined by an Analysis of Variance (ANOVA) test. This disparity could be due to several factors, including age, as most university users were under 25 years old.

CAPTCHAs in non-English languages In our survey, only 3% of respondents reported encountering a non-English CAPTCHA, with Portuguese being the most common language at 37.5%, followed by other languages like Hindi, Tamil, Turkish, French, Japanese, and Korean. Among these respondents, 50% preferred text-based CAPTCHAs, while 13% favored audio/video CAPTCHAs, and 25% preferred both. However, due to the limited sample size, further research is needed to understand user preferences in this area.

Solving CAPTCHAs on a smaller device To investigate the impact of device size on CAPTCHA-solving, we asked respondents about their preferences. Our results show that 68% of respondents found it easier on a computer than on a phone or a tablet, while 32% perceived no difference. Notably, our analysis revealed a significant difference in opinions between MTurk and university users, with a chi-squared p-value of 0.0004. This finding indicates the need for additional research to explore and address usability issues on small devices.

We received feedback from 172 respondents on why they found using one device easier than the other. The majority (74%) cited size and orientation as the main reasons, with 73% from MTurk users and 78% from university users. Additionally, over half (58%) considered input method (Touch vs. Keyboard/Mouse) as an essential factor. This information is depicted in Figure 4.

Table 2: Solving CAPTCHAs on a small device

	MTurk	Univ.	Total
Easier on a	a 114 (78%)	58 (55%)	172
computer			
Easier on a	a 0 (0%)	1 (1%)	1
phone/table	et		
Same	33 (22%)	47 (44%)	253

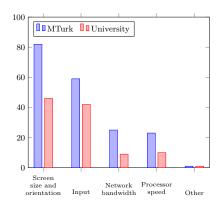


Fig. 4: Reasons for choosing computers over small devices (n=172)

Failing a CAPTCHA challenge on a single attempt Solving CAPTCHAs can be a frustrating experience for users. In our survey, we asked respondents about their success rate in solving CAPTCHAs on the first attempt. We found that a staggering 28% of respondents could always solve a CAPTCHA challenge on the first try, as shown in Table 3. However, 3% of respondents consistently struggled with CAPTCHAs. We also asked them to share their experiences of failure in an open-ended question.

Table 3: Solving CAPTCHAs in one attempt

		MTurk	Univ.	Total
Always	n	52	19	71
Aiways	%	35%	18%	28%
Frequently	n	90	85	175
rrequently	%	61%	80%	69%
Rarely	n	5	2	7
Italely	%	3%	2%	3%
		147	106	253

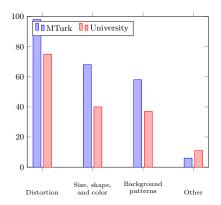


Fig. 5: Why CAPTCHAs are hard to use?

Respondents commonly cited image blurriness or unclear visuals as a primary issue. For instance, respondent P2 complained: "I can't always see the images clearly." P122 stated: "The picture was too dark fuzzy or unclear." P17 commented: "Pictures too blurred or small to see properly."

In addition, text clarity was also cited as a problem, with respondents stating that the font, font size, and text formatting could have been easier to read. For example, P25 said: "Cannot recognize font." P197 shared: "CAPTCHA text or image can be distorted beyond recognition." P101 echoed this opinion: "A lot of times the text or number identification for Amazon logins is really unclear." P14 also wrote: "The text ones are sometimes really difficult to read." Some respondents reported having to refresh the CAPTCHA test for a clearer one.

Furthermore, the perceived similarity of letters and numbers in CAPTCHAs was another highly cited reason for failure. For example, respondents had trouble distinguishing letters like '9' vs. 'g,' "vv" vs. 'w,' 'I' vs. '1.' P73 explained: "Some letter number combos like nine g and one I l and s f and o zero and similar letter number combo are very difficult to solve." P53 shared the same concern: "With text identification, it is sometimes difficult to ascertain the letter correctly like a letter l and number one can be similar." These similarities often led to typing errors and failures in solving CAPTCHAs on the first attempt.

Human errors are inevitable and have caused many user failures when interacting with CAPTCHAs. Some users did not spend sufficient time on solving CAPTCHAs, while others gave inadequate attention to CAPTCHA tests. These errors are particularly prevalent in image recognition and text identification CAPTCHAs, which prevail in the market. P259 shared their experience, stating: "Mistaken letter or misheard a letter." Similarly, P32 mentioned difficulties encountered in text CAPTCHAS, noting: "Sometimes miss a picture or put a letter in the wrong place in a text CAPTCHA." These challenges are not unique to them. P89 struggled with image CAPTCHAs, expressing frustration: "Usually, it's on the image ones and I just miss one of the items or squares it wants me to click." Users often face difficulty deciding whether to select a particular image segment when only a small portion of the target object is visible. P163 highlighted a common error: "Normally incorrect image selected or character." P33 also expressed their frustrations, stating: "I did not select all the pictures." Responses such as "carelessness," "typo," "accidental click," and "rushed" were also common.

Some text CAPTCHAs are case-sensitive, which posed a challenge for participants who struggled to determine the required accuracy. As a result, they often had to attempt the test multiple times before passing. P64 talked about such experience, stating: "Typing a lowercase while CAPTCHA needs an uppercase." This issue commonly leads to another problem: unclear instructions. Many respondents observed vague or incomplete instructions in the CAPTCHAs they tried to solve. P181 recounted their experience, saying: "The image says to click all the stoplights, and I don't know if it wants me to click the little bit on a square that is part of it but not really the stoplights." Additionally, P129 expressed frustration with the system rejecting seemingly correct answers, stating: "I don't know. I type the exact text from the image, and then it says it's wrong. The first one is probably always expired or something." Our findings suggest that intentionally obscuring instructions may be a deliberate choice to enhance CAPTCHA's difficulty for bots.

Why did you give up? We investigated if respondents ever left a webpage due to CAPTCHA failures. Figure 6 illustrates their tendency to abandon after multiple failed attempts or just a single attempt. Surprisingly, 75% of university users would persist until success. In contrast, nearly 65% of MTurk users opted to abandon, with 19% leaving immediately after a single failure compared to 7% of university users.

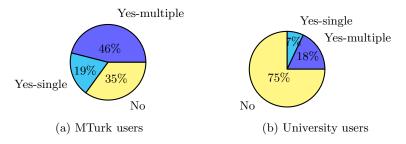


Fig. 6: Leaving a webpage after failed attempts

To gain further insights, we posed a related question, aiming to ascertain if users left a webpage because they simply did not want to solve a CAPTCHA. Among university users, 62% reported that they would remain on the webpage despite the presence of a CAPTCHA. In contrast, nearly 65% of MTurk users admitted to leaving a webpage due to finding CAPTCHAs challenging or annoying, or discovering alternative bypass methods.

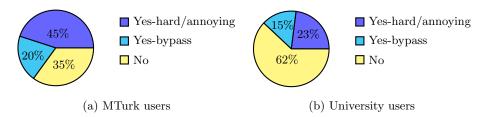


Fig. 7: Leaving a webpage when a CAPTCHA is present

The two user groups exhibited significantly different behaviors in response to these questions (p < 0.0001, chi-squared test). We believe that active MTurk users tend to complete tasks or jobs as much as possible within a given time frame. They probably extend this mindset to their browsing experiences and have little patience towards CAPTCHAs. Conversely, university students, being techsavvy and goal-oriented, show more patience during the authentication process.

Perceived CAPTCHA difficulty The next two questions address the perceived difficulty of CAPTCHAs. We asked respondents to select the feature that contributes most to CAPTCHA difficulty. Figure 5 presents the distribution of votes from our participants. Distortion emerged as the primary factor that makes CAPTCHAs challenging to use, aligning with the insights gathered from user responses in Section 4. Notably, 98 MTurk users (65%) and 75 university users (69%) endorsed this option. Size, shape, and color were also identified as troublesome factors, with 68 votes from MTurk users (45%) and 40 votes from university users (37%). Background patterns ranked third, albeit with a narrow margin (58 votes from MTurk users and 37 votes from university users).

Next, we inquired about respondents' perceptions of the trend in CAPTCHA difficulty over time. As illustrated in Figure 8, 43% of MTurk users felt that CAPTCHAs are becoming increasingly hard to solve, while 49% of university users believed that CAPTCHA difficulty has remained consistent. A chi-squared test of independence revealed significant differences between the responses of the two user groups (p = 0.008).

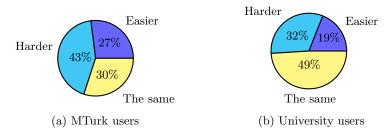


Fig. 8: Trend of CAPTCHA difficulty

Accessibility concerns Accessibility is crucial for user experience, yet several respondents shared frustrations with CAPTCHA accessibility. P12 noted that "audio files sometimes did not properly load when solving an audio CAPTCHA." This issue may be attributed to poor Internet connectivity. P262 reported an unpleasant experience with audio CAPTCHAs: "Helping a customer in which they had a hard time in hearing." However, without further information, we were not sure about the reason behind this incident. Additionally, P181 encountered issues when using small mobile devices, particularly in touchscreen mode. They stated, "I was on a mobile phone and tried to solve a CAPTCHA and when I couldn't click on the screen, I chose to make it an audio CAPTCHA and it failed to let me solve it." This complaint echoes the general sentiment among our respondents regarding CAPTCHAs on small screens.

How secure are current CAPTCHAs? We also assessed users' perceptions of CAPTCHA security. The results, shown in Figure 9, indicate that 49% of

MTurk users praised the effectiveness of CAPTCHAs, while 45% agreed that CAPTCHAs do a decent job. Conversely, only 15% of university users expressed high confidence in CAPTCHA effectiveness, with 70% thinking CAPTCHAs do an okay job.

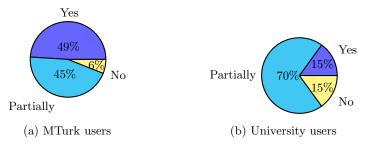


Fig. 9: Can CAPTCHAs detect bots?

Next, we inquired about respondents' views on whether current CAPTCHA schemes can keep up with the advancing attack techniques. Figure 10 reveals that 69% of university users were uncertain. Similarly, 41% of MTurk users shared this uncertainty, while 44% expressed confidence in CAPTCHA security. These findings suggest that university users are more aware of security threats around us since many of them have taken security courses and are tech-savvy. However, they also highlight the need for greater public awareness and education on cybersecurity and digital threats.

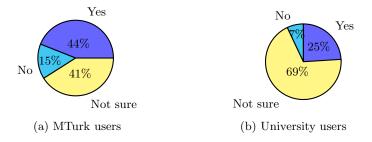


Fig. 10: Are CAPTCHAs resistant to attacks?

Final stance The final question aimed to gather respondents' overall opinions regarding the security and usability of current CAPTCHAs. We found that 44% of university users deemed CAPTCHAs secure, while 66% found them usable. In contrast, MTurk users exhibited higher levels of confidence in CAPTCHA security, with 64% considering them secure and approximately 55% perceiving them

Table 4: Final stance on CAPTCHAs

	MTurk	University
Secure and usable	35 (24%)	20 (19%)
Secure but usability is a concern	57 (40%)	27 (25%)
Usable but security is a concern	43 (30%)	50 (47%)
Neither secure nor usable	9 (6%)	9 (8%)

as usable. Only a small proportion of MTurk users (6%) and university users (8%) viewed CAPTCHAs as neither secure nor usable. Once again, a significant disparity emerged between the overall opinions of the two user groups regarding CAPTCHAs (p = 0.021, chi-squared test).

5 Discussions

All six null hypotheses in our study were rejected, indicating significant variations in user perceptions of CAPTCHA issues between MTurk users and university users.

We observed distinct preferences for CAPTCHA types and differing perspectives on CAPTCHA difficulty trends among the two user groups. While more MTurk users claimed to always solve CAPTCHAs on the first attempt (35% vs. 18%), they also tended to give up on CAPTCHA challenges compared to university users, who demonstrated greater persistence and patience. User age played a role in these differences. Unlike Fidas et al.'s study [6], we did not categorize respondents by specific age groups. However, our findings indicated that MTurk users, who were generally older (96% aged 25 or older), differed from university users, of whom the majority (60%) were under 25 years old. Our results also aligned with previous research [18] that highlighted preferences for different CAPTCHA schemes on smartphones among younger individuals. Moreover, our study corroborated the finding that older participants are more likely to solve CAPTCHAs on the first attempt [6].

Contrary to common belief, MTurk users in our study, despite having a higher level of education (72% holding a bachelor's or postgraduate degree), exhibited less concern for CAPTCHA security (64% considered it secure). We attribute this discrepancy to the influence of technical background rather than education level. Our university users, mainly from a computer security class, displayed greater awareness of increasing security threats on the Internet.

Both MTurk users and university users found solving CAPTCHAs on smaller devices equally challenging (100% for MTurk users and 99% for university users). Screen size, orientation, and input methods were identified as the top obstacles in this context. Many general CAPTCHA issues persisted and may even be exacerbated on smaller devices, including distortion, font size, and background patterns. To address these concerns, we support the recommendations by Reynaga

et al. [18] that CAPTCHAs on smaller devices should adopt input mechanisms with cross-platform support, maintain a consistent orientation, and employ a minimalist design to reduce screen occupancy.

Our study reveals that CAPTCHAs remain difficult to use. Moreover, current CAPTCHA designs heavily rely on visual processing, rendering them inaccessible to millions of people with visual impairments [5]. There is a growing demand for simpler and less burdensome solutions. Google's reCAPTCHA v2 introduced Invisible CAPTCHAs in 2014, but privacy concerns persist. We believe an invisible and passive CAPTCHA scheme with a frictionless user experience is the right direction. Such a design frees users from the need to solve CAPTCHA challenges directly. It leverages the nature of a user's device and behavioral activities (e.g., CPU usage, memory usage, keystrokes, mouse movement, browser tabs, etc.). It should be accessible to everyone and less annoying. More importantly, it needs to be transparent about the use of user information. Our future agenda involves developing and testing such a new mechanism to address identified concerns.

6 Conclusion

In this study, we surveyed 259 respondents from a university and Amazon Mechanical Turk to examine user perceptions of CAPTCHAs, focusing on usability and security. Our findings revealed significant disparities between the two groups. We explored possible explanations for these differences, including age and technical background. Both groups struggled with current CAPTCHA schemes, leading to failure and frustration. Our insights offer recommendations for designing more user-friendly CAPTCHAs. Future research can use our findings to develop more effective and efficient solutions.

Appendix A Survey Questions

1.	What is your age?
2.	What is your gender?
	□ Male
	□ Female
	□ Non-binary
	□ Prefer not to say
3.	What is the highest level of education that you have completed?
	☐ Less than high school degree
	☐ High school degree or equivalent (e.g., GED)
	□ Some college but no degree
	☐ Associate degree
	□ Bachelor's degree
	☐ Graduate degree
4.	Which of the following best describes your current occupation?
	□ Unemployed

16	A. Reddy et al.
	□ Self-employed □ Student □ Education □ Healthcare □ Information technology □ Real estate and development □ Retail □ Law □ Agriculture □ Government □ Other
5.	Which of the following best describes you?
	□ Native English speaker □ Non-Native English speaker
6.	When was the last time you solved a CAPTCHA? [Skip to end survey if "I have never solved a CAPTCHA" is selected] Today In the last week In the last two weeks In the last month In the last six months In the last year It has been over a year since I solved a CAPTCHA I have never solved a CAPTCHA
7.	Have you solved the below CAPTCHA types? Select all that
	applies. □ Math CAPTCHA □ Text Identiciation CAPTCHA □ Select Images CAPTCHA □ Drag or Drop Images CAPTCHA □ Audio/Video CAPTCHA □ Game/Puzzle CAPTCHA □ Other (Please Specify)
8.	Rate these CAPTCHA types on a scale of 1 - 5 where 1 is least preferable to you and 5 being the most preferable to you. □ Math CAPTCHA (1, 2, 3, 4, 5, Never solved) □ Text Identiciation CAPTCHA (1, 2, 3, 4, 5, Never solved) □ Select Images CAPTCHA (1, 2, 3, 4, 5, Never solved) □ Drag or Drop Images CAPTCHA (1, 2, 3, 4, 5, Never solved) □ Audio/Video CAPTCHA (1, 2, 3, 4, 5, Never solved) □ Game/Puzzle CAPTCHA (1, 2, 3, 4, 5, Never solved)
9.	Have you solved a CAPTCHA in a language other than English? If yes, please specify all the languages. $\hfill\Box$ Languages $\hfill \Box$

	□ No
10.	If you ever solved a non-English CAPTCHA, what type do you prefer? □ Audio/Video □ Text □ Neither □ Both
11.	Do you think solving a CAPTCHA is easier on a computer than on a phone/tablet? □ Easier on a computer. □ Easier on a phone/tablet. □ Same in both cases.
12.	In the last question, what is the reason for selecting one over the other? Select all that applies. □ Screen size and orientation □ Input (touch vs. keyboard/mouse) □ Network bandwidth □ Processor speed □ Other (Please explain)
13.	Generally, are you able to solve a CAPTCHA in a single attempt? Always Rarely Never
14.	Please explain the reason for failing in the first attempt.
15.	What according to you makes a CAPTCHA hard to use? □ Distortion feature □ Size, shape, and color □ Background patterns □ Other (Please explain)
16.	What are your thoughts about the CAPTCHA trend over the years? □ They are getting harder to solve. □ They are getting easier to solve. □ They are the same.
17.	Did you ever leave a webpage because you could not solve a CAPTCHA? Select all that applies. ☐ Yes, I had to leave because I could not solve after multiple attempts. ☐ Yes, I left because I could not solve in a single attempt. ☐ No
18.	Did you ever leave a webpage because you did not want to solve

a CAPTCHA? Select all that applies.

References

18

A. Reddy et al.

- von Ahn, L., Blum, M., Langford, J.: Telling humans and computers apart automatically. Commun. ACM 47(2), 56–60 (Feb 2004)
- 2. Bursztein, E., Bethard, S., Fabry, C., Mitchell, J.C., Jurafsky, D.: How good are humans at solving CAPTCHAs? a large scale evaluation. In: 2010 IEEE Symposium on Security and Privacy. pp. 399–413 (2010)
- 3. Chellapilla, K., Larson, K., Simard, P., Czerwinski, M.: Designing human friendly human interaction proofs (HIPs). In: the SIGCHI Conference on Human Factors in Computing Systems. p. 711–720. CHI '05, ACM, New York, NY, USA (2005)
- Conti, M., Guarisco, C., Spolaor, R.: CAPTCHaStar! a novel CAPTCHA based on interactive shape discovery. In: Manulis, M., Sadeghi, A.R., Schneider, S. (eds.) Applied Cryptography and Network Security. pp. 611–628. Springer International Publishing, Cham (2016)

- Fanelle, V., Karimi, S., Shah, A., Subramanian, B., Das, S.: Blind and human: Exploring more usable audio CAPTCHA designs. In: the 16th Symposium on Usable Privacy and Security (SOUPS 2020). pp. 111–125. USENIX Association (2020)
- Fidas, C.A., Voyiatzis, A.G., Avouris, N.M.: On the necessity of user-friendly CAPTCHA. In: the SIGCHI Conference on Human Factors in Computing Systems. p. 2623–2626. CHI '11, ACM, New York, NY, USA (2011)
- Golle, P.: Machine learning attacks against the Asirra CAPTCHA. In: the 15th ACM Conference on Computer and Communications Security. p. 535–542. CCS '08, ACM, New York, NY, USA (2008)
- 8. Gossweiler, R., Kamvar, M., Baluja, S.: What's up CAPTCHA? a CAPTCHA based on image orientation. In: the 18th International Conference on World Wide Web. p. 841–850. WWW '09, ACM, New York, NY, USA (2009)
- Henrich, J., Heine, S.J., Norenzayan, A.: The weirdest people in the world? Behavioral and Brain Sciences 33(2-3), 61–83 (2010)
- 10. Hernández-Castro, C.J., R-Moreno, M.D., Barrero, D.F.: Using JPEG to measure image continuity and break Capy and other puzzle CAPTCHAs. IEEE Internet Computing 19(6), 46–53 (2015)
- Hernandez-Castro, C.J., Ribagorda, A.: Pitfalls in CAPTCHA design and implementation: The math CAPTCHA, a case study. Computers & Security 29(1), 141–157 (2010)
- 12. Ho, C.J., Wu, C.C., Chen, K.T., Lei, C.L.: DevilTyper: a game for CAPTCHA usability evaluation. Computers in Entertainment (CIE) 9(1), 1–14 (2011)
- 13. Kluever, K.A., Zanibbi, R.: Video CAPTCHAs: Usability vs. security. In: the IEEE Western New York Image Processing Workshop (2008)
- Kluever, K.A., Zanibbi, R.: Balancing usability and security in a video CAPTCHA.
 In: the 5th Symposium on Usable Privacy and Security. SOUPS '09, ACM, New York, NY, USA (2009)
- Krol, K., Parkin, S., Sasse, M.A.: Better the devil you know: A user study of two CAPTCHAs and a possible replacement technology. In: NDSS Workshop on Usable Security (USEC). vol. 10 (2016)
- Mori, G., Malik, J.: Recognizing objects in adversarial clutter: breaking a visual CAPTCHA. In: 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. vol. 1, pp. I–I (2003)
- 17. Nguyen, V.D., Chow, Y.W., Susilo, W.: On the security of text-based 3D CAPTCHAs. Computers & Security 45, 84–99 (2014)
- 18. Reynaga, G., Chiasson, S., van Oorschot, P.C.: Exploring the usability of CAPTCHAS on smartphones: Comparisons and recommendations. In: NDSS Workshop on Usable Security (USEC). vol. 112 (2015)
- Sano, S., Otsuka, T., Itoyama, K., Okuno, H.G.: HMM-based attacks on Google's reCAPTCHA with continuous visual and audio symbols. Journal of Information Processing 23(6), 814–826 (2015)
- Sauer, G., Hochheiser, H., Feng, J., Lazar, J.: Towards a universally usable CAPTCHA. In: the 4th Symposium on Usable Privacy and Security. vol. 6, p. 1 (2008)
- 21. Sivakorn, S., Polakis, J., Keromytis, A.D.: I'm not a human: Breaking the Google reCAPTCHA. Black Hat **14** (2016)
- 22. Vitas, F.: How to bypass "slider CAPTCHA" with JS and Puppeteer. https://filipvitas.medium.com/how-to-bypass-slider-captcha-with-js-and-puppeteer-cd5e28105e3c (2019), accessed: 2023-06-02

- A. Reddy et al.
- 23. Yan, J., El Ahmad, A.S.: A low-cost attack on a Microsoft CAPTCHA. In: the 15th ACM Conference on Computer and Communications Security. p. 543–554. CCS '08, ACM, New York, NY, USA (2008)
- 24. Yan, J., El Ahmad, A.S.: Usability of CAPTCHAs or usability issues in CAPTCHA design. In: the 4th Symposium on Usable Privacy and Security. p. 44–52. SOUPS '08, ACM, New York, NY, USA (2008)