Loyalty cards and the problem of CAPTCHA: 2nd tier security and usability issues for senior citizens

David M. Cook
Security Research Institute, Edith Cowan University

Apoorv Kumar
Edith Cowan University

Charwina Unmar-Satiah
Edith Cowan University

DOI: 10.4225/75/57b6a03bd9392
13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (pp. 101-111), Edith Cowan University Joondalup Campus, Perth, Western Australia.

LOYALTY CARDS AND THE PROBLEM OF CAPTCHA: 2ND TIER SECURITY AND USABILITY ISSUES FOR SENIOR CITIZENS

David M. Cook[1,2], Apoorv Kumar[1], Charwina Unmar-Satiah[1]
[1]School of Computer and Security Science, [2]Security Research Institute
Edith Cowan University, Perth Australia
d.cook@ecu.edu.au, apoorv@our.ecu.edu.au, csatiah@our.ecu.edu.au

Abstract

Information Security often works in antipathy to access and useability in communities of older citizens. Whilst security features are required to prevent the disclosure of information, some security tools have a deleterious effect upon users, resulting in insecure practices. Security becomes unfit for purpose where users prefer to abandon applications and online benefits in favour of non-digital authentication and verification requirements. For some, the ability to read letters and symbols from a distorted image is a decidedly more difficult task than for others, and the resulting level of security from CAPTCHA tests is not consistent from person to person. This paper discusses the changing paradigm regarding second tier applications where non-essential benefits are forgone in order to avoid the frustration, uncertainty and humiliation of repeated failed attempts to access online software by means of CAPTCHA.

Keywords
CAPTCHA, Information Security, Senior Citizens, Technology Acceptance, Perceived Usefulness, Turing

INTRODUCTION

The visual and audible tests known commercially as 'Completely Automated Public Turing tests to tell Computers and Humans Apart' (CAPTCHA) are ubiquitous across online activities where there is a need to filter out automated scripts and bots. The general public associate them as tests for the presence of human interplay (Pope and Kaur, 2005). Within the broad range of such tests there are some CAPTCHA tests that seem decidedly harder to successfully complete than others. Senior citizens make decisions about their own online interactions based upon needs and wants (Gatto, and Tak, 2008; Cook, Szewcyzk, and Sansurooah, 2011). This paper highlights an important difference between difficult CAPTCHA tests, user-friendly tests, and their associated acceptance or rejection based more upon user needs, than the needs of information security standards (Fidas, Voyiatzis, and Avouris, 2011; Datta, Li, and Wang, 2005)

Inconsistent ease of CAPTCHA use

The use of CAPTCHA as a Turing test designed to confirm human interaction has been described as patchy and intermittent (Yan and El Ahmad, 2008; Hernandez-Castro and Ribagorda, 2010). The advent of bots and scripts that replicate human user activities has brought about an increasing need for vigilance in establishing user access by humans rather than automated (Schlaikjer, 2007). However some CAPTCHA images seem easy, whilst others are vastly more difficult to ascertain with certainty. Despite these irregular and sporadic results, information security protocols such as CAPTCHA have been seen as a widely used method of testing for the presence of human interaction (Pope and Kaur, 2005; Shirali-Shahreza and Shirali-Shahreza, 2008; Conway, 2014).

CAPTCHA tests are generally difficult for bots to deceive, and reasonably straightforward for most people to use (Biljani and Robertson, 2014). However, the need for visual (and in some cases audible) interaction places many older people at a disadvantage (Nazir, Javed, Khan, Khayam, and Li, 2011). In the first instance senior citizens are more likely to suffer from some form of visual impairment than younger people, since eyesight and hearing degenerate over time (Klein, Peto, Bird, and Vannewkirk, 2004; Gordon-Salant, 2005). On the basis of a cohort of seniors that is growing in size and longevity of age (Keating and Wetle, 2008), the need to satisfy older people's user experiences means that some non-essential online services can suffer from user rejection (Holzinger, Searle, and Nischelwitzer, 2007; Jonsson, Nass and Lee, 2004). CAPTCHA is an exemplar of an authentication tool that disadvantages the elderly, and may lead to dissatisfaction, uncertainty, and ultimately the rejection of non-essential online services.

Hypothesis

In researching the security and usability aspects of CAPTCHA it was understood that elderly people held perceptions about their own acceptance (and rejection) of online technologies where usage-choices were influenced by necessity (Friemel, 2014). The research proposition was based on the possibility that commercial organisations engaged in mimicking the need for security. The following null hypotheses were formulated for this research.

a. There is no discernible difference between the individual CAPTCHA tests used in critical online services and the CAPTCHA tests used in non-essential online services such as loyalty cards.

b. People with age-related impairments such as vision and hearing impairments do not accept or reject the security of their access to technology on the basis of user-friendliness.

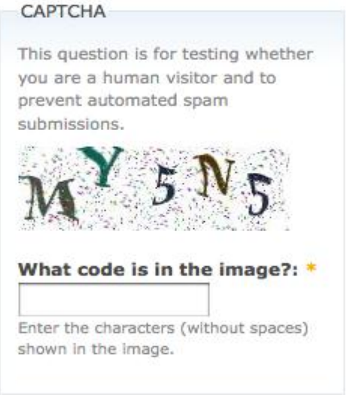
Method

To test for CAPTCHA usability we analysed the security and user-friendliness of 32 loyalty cards and loyalty-based online services. Our research focused on access for private and personal information. Not all of the test sample used CAPTCHA. Eighteen percent (18%) of loyalty cards used CAPTCHA in addition to other elements as part of a multi factor authentication approach. Twelve percent (12%) had no CAPTCHA but required users to physically present the loyalty card or its number as proof of identity and authenticity.

The use of loyalty cards and loyalty services tests for the combined need for security and user-friendliness within a continuous, dynamic commercial setting. It requires the repeat usage of CAPTCHA tests rather than once-only scenarios that are not as representative of the commercial imperatives that affect security choices.

The Development and acceptance of CAPTCHA

CAPTCHA is a Turing test (Shirali-Shahreza and Shirali-Shahreza, 2008), that protects against the development of Artificial Intelligence (AI) and assists in distinguishing humans from automated scripts (Goswami, Powell, Vatsa, Singh, and Moore, 2014; Tangmanee and Sujarit-Apirak, 2013). Alan Turing developed the original model to distinguish between man and machine (Guerra-Pujol, 2012). Initial tests attempted to convince human judges of the humanness of a computational interaction (Fig. 1). Thus if a computer's interaction could not be distinguished from human interaction, then that computer was judged to have a high level of human-like intelligence (Epstein, Roberts, and Beber, 2008).



CAPTCHA

This question is for testing whether you are a human visitor and to prevent automated spam submissions.

What code is in the image?: *

Enter the characters (without spaces) shown in the image.

Figure 1. Standard CAPTCHA text-based test set against a noisy background.

A CAPTCHA trial is premised upon a test which most humans can pass but that current computer programs cannot pass. The normative versions of this test is a trial that exhibits textual images in the form of distorted text or audible samples which are superimposed against a noisy background. Such background noise increases the difficulty for the automated attempts but is not designed to overly limit the attempts by humans (Yan, 2009). In this way each test incorporates a Turing test embedded in the trial to verify the existence of human interaction (Ibid). The test therefore requires both a challenge to the user and a response (Moradi and Keyvanpour, 2015) (Fig. 2). CAPTCHA is accepted as a near-ubiquitous, accepted standard in security technology (Yan and El Ahmad, 2008).

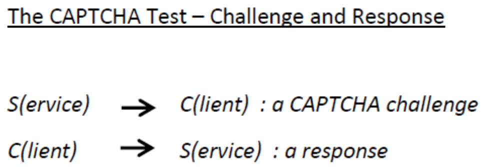

The CAPTCHA Test – Challenge and Response
S(ervice) → C(lient) : a CAPTCHA challenge
C(lient) → S(ervice) : a response

Figure 2. The Challenge and Response test of CAPTCHA

The Gap between Security and User Friendliness

Security and useability jostle for superiority in online programs and applications. Whilst compromises are made, there is an expectation that security will not budge from the need to maintain a secure system (Fidas, et al., 2011). The result is that user-friendliness defers to security wherever there is a high level critical need (Fig. 3). Examples of online applications include financial apps, medical information programs, and wherever the privacy of the information is of concern. Other applications that have commercial appeal but are less-essential have a greater emphasis on user-friendliness than security (Karunathilake, Balasuriya, and Ragel, 2009). A useable CAPTCHA must be both human friendly, yet also possess enough robust characteristics to deter would-be attackers from writing and deploying automated scripts (Yan and El Ahmad, 2008; Fidas et al., 2011).

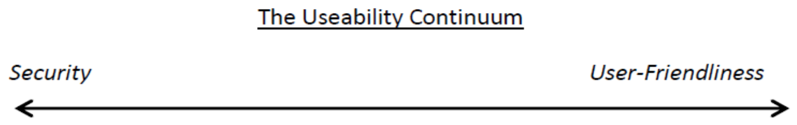


Figure 3. The Usability Continuum for security and user-friendliness

The User-Friendliness of CAPTCHA for certain groups

In their research about the widespread usability of CAPTCHA, Kluever and Zanibbi (2009) identified the critical properties for CAPTCHA. The most challenging is that the CAPTCHA test must be user friendly. However, user-friendliness is a highly subjective term (Charness and Boot, 2009), and there are numerous measurements for user friendliness (Shirali-Shahreza and Shirali-Shahreza, 2008). Ambiguity surrounds studies that compare usage with usability, since in cases where users feel obligated or mandated, their usage does not equate to user-friendliness (Kim, Ferrin and Rao, 2008; Vance, Elie-Dit-Cosaque, and Straub, 2008; King, Ureel, Kumar, and Wallace, 2013). Certain segments have difficulty with normative CAPTCHA tests, including elderly people (King et al., 2013). Elderly people experience greater levels of visual and auditory degeneration (Millward, 2003; de Koning and Gelderblom, 2006). Since CAPTCHA is a test of humanness based upon visual and audio acknowledgements, the degree of user-friendliness for the elderly becomes significant (ANPEA, 2008). Seniors demonstrate indecision in securing essential activities that require a high level of digital security (Ibid).

Accessibility problems and the commercial need for alternative CAPTCHAs for older people

Organisations pursuing the online interest of older persons need to address a range of age-related accessibility issues (Charness and Boot, 2009). Websites selling commodities like travel and event tickets or services like web-based email and blogs use CAPTCHA to protect themselves from bots (Jenjarrussakul and Matsuura, 2014). Although used to prevent bot access, the CAPTCHA test is problematic for users who are blind, visually impaired or dyslexic (Conway, 2014). Given the number of elderly people with vision impairment, CAPTCHA poses a challenge for ICT systems that require human authentication. Emerging security and privacy protection methods have created more accessibility barriers for visually impaired users (Sauer, Holman, Lazar, Hoccheiser & Feng, 2010). Systems that 'time-out' pose a challenge for persons with vision impairment who need time to interpret a CAPTCHA (Ibid).

In contrast to security protection, commercial organisations prefer to attract customers, by focusing on the user experience (Gao, Wang, Fan, Qi, and Liu, 2014). The online loyalty habits of elderly people are instructive in understanding different CAPTCHAs. In visual CAPTCHAs humans can take advantage of context to guess an obscured character within a word. This explains why most visual-based CAPTCHA has moved away from random sequences of characters in favor of complete words (Pope and Khushpreet, 2005). This allows humans to recognize contextual clues in order to solve CAPTCHA tests (Schlaikjer, 2007). Whilst some new CAPTCHA tests place primary focus on issues of robustness (Gao et al., 2014), recent changes make CAPTCHAs appear more usable as evidenced by Google's amended *No-Captcha Re-Captcha* tests (Ndibwile, Govardhan, Okada, and Kadobayashi, 2015). These tests use multiple pictures of up to ten objects requiring a test to check human ability to select images of similar themes (Fig. 4). The No-Captcha Re-Captchas are popular because they are easy to solve and the picture background forms the inherent background noise of the test (Google, 2014)

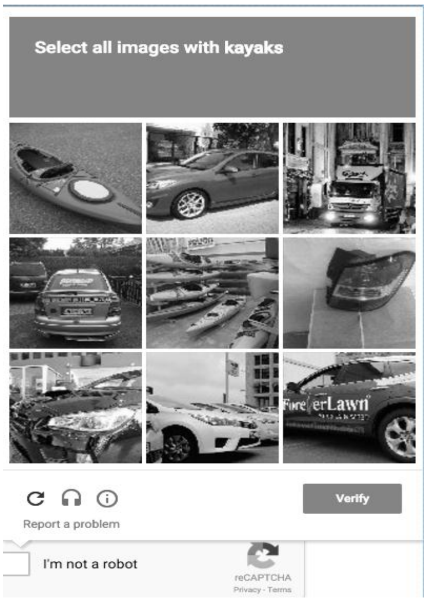


Figure 4. Google's amended No-Captcha Re-Captcha test

CRITICAL AUTHENTICATION VERSUS SECONDARY EXPECTATIONS

CAPTCHA in primary and secondary roles

Whilst CAPTCHA is a common test to filter bots, it is subject to criticism from attacks that have defeated the test (Yan and El Ahmad, 2008; Bilge, Strufe, Balzarotti and Kirda, 2009). As a result CAPTCHA tests are morphing to suit two different levels of expectation. At a higher level they are used in combination with other multi-factor elements to protect critical and essential access to online services (Goswami, Powell, Vatsa, Singh, and Noore, 2014; Moradit and Keyvanpour, 2015: Pope and Khushpreet, 2005). At a secondary level they are simplified to discourage bots whilst maximising the repeated engagement of people in things such as loyalty cards that provide free coffees, free popcorn at movies or shopping rewards (Hassanat, 2014).

Other secondary expectations include preventing anonymous postings on public websites, job listing sites, online voting polls, and the prevention of fake advertisements (Hernandez-Castro and Ribagorda, 2010; Nitin, Arora, Patel, Medury, Naval, Gupta, and Sarin, 2010). They prevent bots from signing up multiple accounts (Abbasi, Kalsoom, and Ziaddin, 2012). CAPTCHA can mitigate against dictionary attacks on online password systems by blocking a password after a certain number of login attempts (Moradi and Keyvanpour, 2015).

Technology Acceptance / Rejection

CAPTCHA can be viewed through two different lenses. Through a high-level security lens, the emphasis is on a no-compromise approach where a CAPTCHA test must sustain the highest probability of passing only humans, with the chance of a bot gaining access being extremely remote. Such a view might prevent access to one or two humans if it meant there was a higher level of security against automated scripts. Through a user-friendly lens, the emphasis might be focused upon maximum user acceptance, with some level of bot prevention, albeit deficient.

At the secondary level, issues of accessibility trump security. Solving distorted characters is problematic for visually-impaired users (Tangmanee and Sujarit-Apriak, 2013). Changing to audio CAPTCHAs is inadequate both in security terms (Bursztein, Bethard, Fabry, Mitchell, and Jurafsky, 2010), and because many visually-impaired come from the ranks of elderly people who become both partially blind and deaf from aging (Dammeyer, 2014; Norberg, Westin, Mozelius, and Wiklund, 2014). Businesses vending non-essential services such as loyalty cards have a difficult choice. If the test is too hard for users then customers are discouraged from availing themselves of the service (US Fed News, 2008). Such businesses choose an easier version of CAPTCHA with correspondingly increased vulnerabilities (Grigoryeva, Shubinskiy, and Mayorova, 2014; Yan and El Ahmad, 2008).

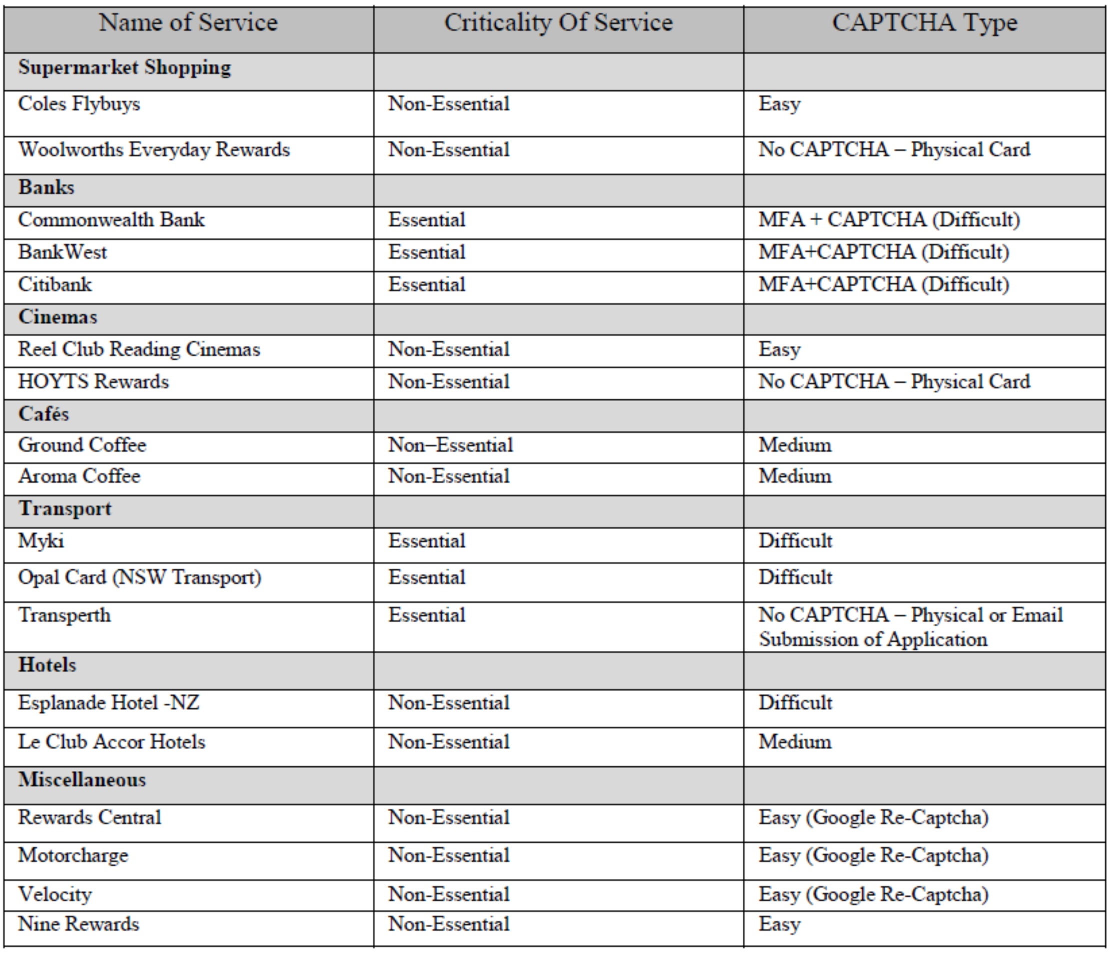
Harder CAPTCHAs will mistakenly castoff some seniors as machines (Baird, Moll, and Wang, 2005: Zhu, Yan, Guanbo, Maowei, and Ning, 2014), whilst some seniors will evaluate criticality and may not be bothered to solve it (Jakobsson, 2012). Widespread use of CAPTCHAs for non-critical programs makes elderly and disabled people perceive the test a preventer instead of enabler (Conway, 2014; Yan and El Ahmad, 2008). User experiences are perceived in negative terms: "*When I get a CAPTCHA that is too bent or twisted, I often have to do it twice. More than that I just leave, and give up on the site*" (Onwudebelu, Fasola, Obi, & Alaba, 2010, p117). Some low resource services ignore accessibility and instead concentrate on maximising profits across younger customer segments (Yamaguchi, Nakata, Watanabe, Okamoto, & Kikuchi, 2014; McAdara-Berkowitz, 2014). Some CAPTCHAs are unreadable, and present a damaging experience to users with impairments (May, 2005; Sauer, Holman, Lazar, Hochheiser, & Feng, 2010)

RESULTS

The results of thirty two essential and non-essential loyalty-based cards and services were analysed to determine the type of CAPTCHAs used in terms of user-friendliness, criticality of service, and the addition of further authentication. From this set eighteen of them were further examined to establish the user experience from the perspective of visual impairment, likely user success, and type of service. The analysis showed that there was a marked difference between the type of authentication offered for access to essential online services than to most non-essential services.

Classifying CAPTCHAs into categories of ease

At first glance the classification of CAPTCHA appears highly subjective. This study categorised CAPTCHA tests into three categories of easy, medium, and difficult based upon four clear conditions. The first condition was to assess the background noise (whether visual or audible) to establish whether the noise was separate to the required object, interacted with the required object, or dominated the CAPTCHA. The second criteria assessed whether the objects were well known, not commonly used, randomly assigned objects. For example, a word such as "free" would be considered well known, a word such as "diurnal" would come under the category of not commonly used, and an assignment of characters such as E#p9z! would fall under the category of random. The third category looked for distortions in the representation of the object. Clear images or crisp sounds would be classed as easy, objects with one form of distortion would be medium, whilst objects with multiple distortions would be categorised as difficult. The final condition examined the physical size of the CAPTCHA (or the standard volume level in the case of audio CAPTCHAs). Those tests that were less than 30mm in width on an A4 template were classed as difficult. Those that were between 30mm and 60mm were classed as medium, whilst those larger than 60mm in width were treated as easy. All the conditions carried the same weighting for the purpose of classification.



Name of Service	Criticality Of Service	CAPTCHA Type
Supermarket Shopping		
Coles Flybuys	Non-Essential	Easy
Woolworths Everyday Rewards	Non-Essential	No CAPTCHA – Physical Card
Banks		
Commonwealth Bank	Essential	MFA + CAPTCHA (Difficult)
BankWest	Essential	MFA+CAPTCHA (Difficult)
Citibank	Essential	MFA+CAPTCHA (Difficult)
Cinemas		
Reel Club Reading Cinemas	Non-Essential	Easy
HOYTS Rewards	Non-Essential	No CAPTCHA – Physical Card
Cafés		
Ground Coffee	Non–Essential	Medium
Aroma Coffee	Non-Essential	Medium
Transport		
Myki	Essential	Difficult
Opal Card (NSW Transport)	Essential	Difficult
Transperth	Essential	No CAPTCHA – Physical or Email Submission of Application
Hotels		
Esplanade Hotel -NZ	Non-Essential	Difficult
Le Club Accor Hotels	Non-Essential	Medium
Miscellaneous		
Rewards Central	Non-Essential	Easy (Google Re-Captcha)
Motorcharge	Non-Essential	Easy (Google Re-Captcha)
Velocity	Non-Essential	Easy (Google Re-Captcha)
Nine Rewards	Non-Essential	Easy

Table 1. Essential versus Non-Essential Authentication using CAPTCHA

Since loyalty cards and services are designed to generate return business on the basis of reward, it was assumed that major acceptance criteria for CAPTCHA deployment would be to retain a user-friendly experience. The results show that CAPTCHA tests fall into five different categories (Table. 1). At the highest level of security 15% of the CAPTCHAs were difficult, and were also deployed in combination with additional Multi Factor Authentication (MFA). A further 17% of CAPTCHAs were difficult, but did not deploy alongside other MFA authentication tests. In the midrange of difficulty only 8% of authentication testing fell into a medium level. At the lower level of security 25% of loyalty cards had CAPTCHAs that were classified as easy. The remaining 35% of loyalty cards and services relied upon Google Re-Captcha as the standard test for human authentication. This last group were assigned a separate classification because although the Google Re-Captchas were all classified as easy, they were substantially lower (easier) than other CAPTCHA tests that registered in the same classification

Where a loyalty card was attached to a financial instrument the overriding trend revealed a difficult CAPTCHA test in combination with a range of other authentication tests and challenges. In such circumstances the results show that banking loyalty services retain security as a no-compromise value to the organisation. If users find the CAPTCHA tests hard, then this is a customer opportunity that is willingly forgone in favour of preserving the higher level of information security.

At the next level of security, the results indicated that essential utility services such as public transport cards had a somewhat difficult CAPTCHA level which often incorporated other multi-factor verifications including secondary email verifications and physical presentation of cards. Whilst not quite as difficult as the CAPTCHA tests used for banking and financial instruments, these essential services jointly fell into a category of critical needs that covered banking and transport.

In the mid-level of security, the analysis showed hotel loyalty programs and high-volume coffee cards where the CAPTCHA tests were of a medium level of difficulty. Below that the results showed supermarket behemoths Coles and Woolworths, both of whom had either low-level CAPTCHA tests in place or the need for a physical presentation of a loyalty card in place of a CAPTCHA test. The results revealed loyalty programs requiring physical presentation of a card because previous use of CAPTCHA had prevented many customers from accessing the loyalty service. Cinema loyalty cards fell into the category below this, with easy CAPTCHA tests and physical loyalty cards in use.

In the category of the least essential loyalty service the CAPTCHA tests were dominated by an easier test using Google No-Captcha Re-Captcha. These miscellaneous non-essential loyalty cards had a lower emphasis upon information security that appeared to be secondary to the preference for a very user-friendly CAPTCHA test.

CAPTCHA for Dummies: reCAPTCHA and perceptions versus reality

The results point to a commercial trend for CAPTCHA tests assigned to non-essential loyalty programs to give users the perception of security whilst also showing a high level of user-friendliness. It suggests that the user-experience of successfully completing a CAPTCHA may be more important than establishing a clear differentiation between a human and bot (Fig. 5). In particular the Google No-Captcha Re-Captcha images regularly allowed test subjects to select some, but not exclusively all of the correct images, whilst still being granted access to an online loyalty-based system or service. The analysis of Google Re-Captcha tests showed nearly one in three attempts would allow a user to select a group of common images, yet allow that user to make mistakes about the selection by including one non-common image, whilst still gaining admittance to the next level of system access. The use of easily solvable tests places into question the commitment to information security by low-level non-essential services that might be tempted to gather larger volumes of personal and private customer information whilst neglecting to allocate the same level of security as a loyalty service that combines the captured privacy information and uses that information alongside a core financial instrument such as a credit card.

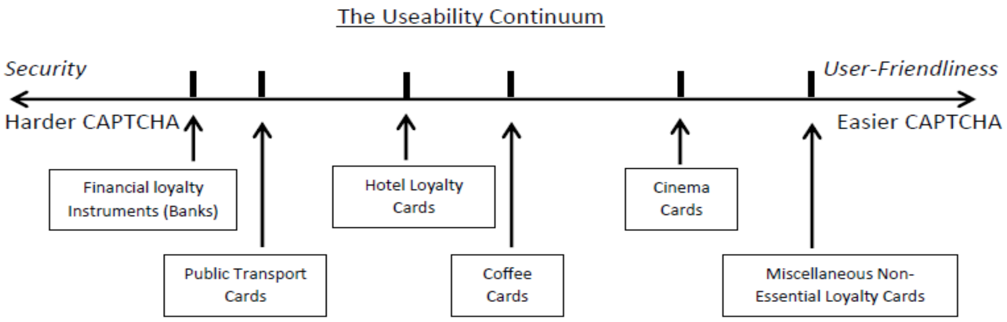


Figure 5. CAPTCHA segmentation across the Useability Continuum

The danger of widespread rejection and other interactions for CAPTCHA

The Seniors cohort includes longer living people who are generationally displaced as novice ICT users, with mixed approaches to the acceptance and usage of technology (Yiwei, Bob, & Robert, 2013). Technologies like CAPTCHA can become an agent of exclusion for the elderly (Gregor, Sloan, & Newell, 2005). Due to the difficulty some seniors face in attempting to solve a CAPTCHA, many prefer to abandon online services that are non-essential (Yiwei et al., 2013). As a result of unsuccessful CAPTCHA experiences, they exhibit negative feelings as frustration and mistrust (Tak & Gatto, 2008; Maddison and Jeske, 2014; Roberts, Indermaur, & Spiranovic, 2013).

CONCLUSION

We conclude that there are different levels of CAPTCHA that are used, and that these differences fall into essential and non-essential categories as perceived by the user. This study analysed CAPTCHA tests belonging to loyalty cards and services. At the critical end of the spectrum, we either identified difficult CAPTCHA tests or financial systems that used multi factor authentication systems instead of CAPTCHA tests. At the non-essential end of the usage spectrum, we identified a much more simplified range of CAPTCHA tests. These non-essential services looked to have employed easier tests in order to retain the commercial imperative of market share, whilst purporting to offer a high level of information security to protect the interests of its users. With reference to our first hypothesis we conclude that there is indeed a discernible difference between the types of CAPTCHA tests used in critical and non-essential online loyalty programs, especially with a financial instrument such as a credit card.

We speculate that some seniors are wary of non-critical online systems where the CAPTCHA tests were so easy that security appeared to be less important than the inclusion of a larger number of customers. Seniors, whilst finding authentication systems for critical systems to be more difficult, are more likely to persist where the system access outweighed the need for user-friendliness. This study used previous acceptance literature to overlay the perceptions of seniors against likely differentiation towards the use or abandonment of online services requiring CAPTCHA authentication. Whilst the analysis is not conclusive, the emerging trend towards easier forms of CAPTCHA tests indicates a market shift towards perceived rather than explicitly robust forms of human authenticity distinctions. Future research will examine a larger sample that will include rejecters of technology who show brand loyalty yet choose physical systems over online loyalty programs. Most loyalty cards fall into a second tier category of ICT services that ask for private information but are far less critical to users than first tier services such as banking, health and government utilities.

REFERENCES

Abbasi, A. R., Kalsoom, S., & Ziauddin, S. (2012). An image-based CAPTCHA scheme exploiting human appearance characteristics. *KSII Transactions on Internet and Information Systems, Volume 6*, pp734 - 739.

ANPEA, (2008) Responding to the financial abuse of older people: Understanding the challenges faced by the banking and financial services sector. Australian Network for the Prevention of Elder Abuse, National Report accessed on the 8th of March 2013 from https://www.google.com.au/?gfe_rd=cr&ei=0gdcVYniK8eN8QfrhoCgAQ&gws_rd=ssl#q=online+banking+compliance+seniors+elderly

Baird, H., Moll, M., & Wang, S.-Y. (2005). A Highly Legible CAPTCHA That Resists Segmentation Attacks. In H. Baird & D. Lopresti (Eds.), *Human Interactive Proofs* (Vol. 3517, pp. 27-41): Springer Berlin Heidelberg.

Bijani, S., & Robertson, D. (2014). A review of attacks and security approaches in open multi-agent systems. *The Artificial Intelligence Review, 42*(4), 607-636. doi: http://dx.doi.org/10.1007/s10462-012-9343-1

Bilge, L., strufe, T., Balzarotti, D., and Kirda, E. (2009) All your contacts belong to us: Automated Identity Theft Attacks on Social Networks, *Proceedings of the18th World Wide Web Conference*, Madrid April 20 – 24. Retrieved from: http://www2009.eprints.org/56/1/p551.pdf

Bursztein, E., Bethard, S., Fabry, C., Mitchell, J. C., & Jurafsky, D. (2010, 16-19 May 2010). *How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation.* Paper presented at the Security and Privacy (SP), 2010 IEEE Symposium on.

Charness, N., & Boot, W. R. (2009). Aging and Information Technology Use: Potential and Barriers. *Current Directions in Psychological Science, 18*(5), 253-258. doi: 10.1111/j.1467-8721.2009.01647.x

Conway, V. (2014). *Website Accessibility in Australia and the National Transition Strategy: Outcomes and Findings*.

Cook, D.M., Szewczyk, P., and Sansurooah, K., (2011) Seniors language paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens. *Proceedings of the 9th Australian Information Security Management Conference*, 63-68, Perth, Western Australia .

Dammeyer, J. (2014). Deafblindness: A review of the literature. *Scandinavian Journal of Public Health*, 1403494814544399.

Datta, R., Li, J., and Wang, J.Z., (2005) Imagination: a robust image-based CAPTCHA generation system. *Proceedings of the 13th Annual ACM International Conference on Multimedia*, pp 331 – 334.

De Koning, J. and Gelderblom, A. (2006) ICT and Older Workers: no unwrinkled relationship. *International Journal of Manpower*, Volume 27, No. 5.

Epstein, R., Roberts, G., and Beber, G. (2008) *Parsing the Turing Test: Philosophical and Methodological issues in the Quest for the Thinking Computer*, Robert Epstein, Gary Roberts, and Grace Beber (Eds). Springer: New York.

Fidas, C.A., Voyiatzis, A.G., and Avouris, N.M. (2011) On the necessity of user-friendly CAPTCHA. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp 2623 – 2626, retrieved 11th September 2014 from http://dl.acm.org/citation.cfm?id=1979325

Friemel, T. N. (2014) The Digital divide has grown old: determinants of a digital divide among seniors, New Media and Society, 2014.pp 1 – 19.

Gao, H., Wang, W., Fan, Y., Qi, J., and Liu, X., (2014) the Robustness of Connecting Characters Together CAPTCHAs. *Journal of Information Science and Engineering*, Volume 30, pp 347 – 369. Retrieved from: http://www.iis.sinica.edu.tw/page/jise/2014/201403_05.pdf

Gitlow, L. (2014). Technology Use by Older Adults and Barriers to Using Technology. *Physical & Occupational Therapy in Geriatrics*, 32(3), 271-280. doi: 10.3109/02703181.2014.946640

Google, (2014) Are you a robot: Introducing No-Captcha, Recaptcha. Accessed 14th September 2015 from: https://googleonlinesecurity.blogspot.com.au/2014/12/are-you-robot-introducing-no-captcha.html

Gordon-Salant, S., (2005) Hearing loss and aging: New research findings and clinical implications. *Journal of Rehabilitation Research and Development*. Vol 42, Issue 4, pp 9 – 23. Retrieved 19th October 2015 from:http://user.medunigraz.at/andreas.holzinger/holzinger/papers%20en/B44_HOLZINGER%20SEARLE%20NISCHELWITZER%20%282007%29%20mobile%20for%20elderly%20LNCS.pdf

Goswami, G., Powell, B.0. M., Vatsa, M., Singh, R., & Noore, A. (2014). FR-CAPTCHA: CAPTCHA based on recognizing human faces. *PLoS ONE, 9*.

Gregor, P., Sloan, D., & Newell, A. F. (2005). Disability and Technology: Building Barriers or Creating Opportunities? *Advances in Computers*, Volume 64, pp. 283-346: Elsevier.http://www.sciencedirect.com/science/article/pii/S0065245804640071

Grigoryeva, I., Shubinskiy, M., & Mayorova, E. (2014). *ICT as a driver for senior citizens' social inclusion*. Paper presented at the Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance, Guimaraes, Portugal.

Guerra-Pujol, F.E. (2012). The Turing test and the legal process. *Information and Communications Technology Law*, 21 (2), pp 113 – 126. DOI: 10.1080/13600834.2012.678648

Hassanat, A. B. A. (2014). Bypassing CAPTCHA by machine--a proof for passing the Turing test. *European Scientific Journal, 10*, pp192- 198.

Hernandez-Castro, C. J., & Ribagorda, A. (2010). Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study. *Computers & Security, 29*(1), 141-157.

Holzinger, A., Searle, G., and Nischelwitzer, A., (2007). On some aspects of improving mobile applications for the elderly, in C. Stephanidid (Ed.): *Universal Access in HCI, Part 1*, HCII 2007, LNCS 4554, pp 923-932 Retrieved 23rd October 2015 from http://user.medunigraz.at/andreas.holzinger/holzinger/papers%20en/B44_HOLZINGER%20SEARLE%20NISCHELWITZER%20%282007%29%20mobile%20for%20elderly%20LNCS.pdf

Jakobsson, M. (2012). *Death of the Internet*. Piscataway, NJ, USA: IEEE Computer Society Press.

Jenjarrussakul, B., and Matsuura, K., (2014) Analysis of Japanese Loyalty Programs Considering liquidity, Security Efforts, and Actual Security Levels. *13th Annual Workshop on the Economics of Information Security*, Pennsylvania State University, June 23 – 24, 2014.

Jonsson, I.M., Nass, C., and Lee, K.M. (2004). Mixing personal computer and handheld interfaces and devices: effects on perceptions and attitudes. *International Journal of Human-Computer Studies*, Volume 61 Issue 1 pp 71 – 83.

Karunathilake, A.K.B., Balasuriya, B.M.D., and Ragel, R.G., (2009) User Friendly Line CAPTCHAs, International Conference on Industrial and Information Systems (ICIIS 2009), pp 210 – 215. Retrieved from: http://arxiv.org/ftp/arxiv/papers/1402/1402.0672.pdf

Keating, N., and Wetle, T.F., (2008). Longevity, health and wel-being: Issues in aging in North America, *Journal of Nutrition, Health and Aging*, Volume 12, Issue 2, pp 99-100.

Kim, D.J., Ferrin, D.L., and Rao, H.R. (2008) A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. *Decision Support Systems,* Volume 44, Issue 2. Pp 544 – 564.

King, H.C., Ureel L. C., Kumar, S., and Wallace, C. (2013). Lessons from Our Elders: Identifying Obstacles to Digital Literacy through Direct Engagement. *6th International Conference on Pervasive Technologies Related to Assistive* Environments (PETRA), Rhodes, Greece, 2013.

Klein, R., Peto, T., Bird, A., and Vannewkirk, M.R., (2004) The epidemiology of age-related macular degeneration, In *American Journal of Ophthamology*, Retrieved on the 24th of October 2015 from https://www.researchgate.net/profile/Tuende_Petoe/publication/6781224_The_epidemiology_of_age-related_macular_degeneration/links/02e7e51d287997bf13000000.pdf

Kluever, K.A., and Zanibbi, R. (2009) Balancing usability and security in a video CAPTCHA, *Symposium on Useable Privacy and Security (SOUPS),* 2009, CA, Retrieved 24th of October 2015 from https://www.acs.org.au/__data/assets/pdf_file/0006/32667/JRPIT44.4.441.pdf

Maddison, J., & Jeske, D. (2014). Fear and Perceived Likelihood of Victimization in Traditional and Cyber Settings. *International Journal of Cyber Behavior, Psychology and Learning* (IJCBPL), Volume 4(4), 23-40. http://www.igi-global.com/article/fear-and-perceived-likelihood-of-victimization-in-traditional-and-cybersettings/120037?camid=4v1a

May, M. (2005). Inaccessibility of CAPTCHA. *Alternatives to Visual Turing Tests on the Web. I: W3C (red.), W3C Working Group Note,* Retrieved on the 3rd of October 2015 from: http://www.circoloruoteclassicherodigino.it/public/en press/contents/Inaccessibility%20of%20CAPTCHA.pdf

McAdara-Berkowitz, J. (2014, 2014/03//). Use CAPTCHA-protected forms to reduce spam originating from your website. *American Medical Writers Association Journal, 29,* 39. http://go.galegroup.com.ezproxy.ecu.edu.au/ps/i.do?p=AONE&u=cowan&id=GALE|A372252871&v=2.1&it=r&sid=summon&userGroup=cowan&authCount=1

Millward, P. (2003) The ‘grey digital divide’: Perception, exclusion and barriers of access to the Internet for older people. *First Monday*, Volume 8, Issue 7

Moradi, M., and Keyvanpour, M., (2015) Captcha and its alternatives: A Review: *Security and Communication Networks,* pp 2035 – 2156.

Nazir, M., Javed, Y., Khan, M.M., Khayam, S.A., and Li, S (2011). Captchecker – Automating Usability – Security Evaluation of Textual CAPTCHAs, *Symposium on Usable Privacy and Security (SOUPS),* 201, July 20, 2011. Pittsburgh, PA. Retrieved 24th October 2015 from http://epubs.surrey.ac.uk/532427/1/SOUPS2011b.pdf

Ndibwile, J, D., Govardhan, A., Okada, K., and Kadobayashi, Y. (2015) Web Server Protection against Application Layer DDoS Attacks using machine Learning and Traffic Authentication, Proceedings of the *2105 IEEE 39th Annual International Vomputers, Software & Applications Conference*. Retrieved October 30th 2015 from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7273365&openedRefinements%3D*%26filter%3DAND(NOT(4283010803))%26pageNumber%3D2%26rowsPerPage%3D100%26queryText%3D(a+pihc+mechanism+against+ddos+attacks)

Nitin, Arora, A. S., Patel, A., Medury, R., Naval, S., Gupta, R., & Sarin, S. (2010). Enhancing E-mail Security by CAPTCHA based Image Grid Master Password. *International Journal of Advancements in Computing Technology, 2*(5), 89-98. URL http://doi.acm.org/10.1145/1526709.1526822

Norberg, L., Westin, T., Mozelius, P., & Wiklund, M. (2014). *Web accessibility by Morse Code modulated haptics for deaf-blind.* Paper presented at the The 10th International Conference on Disability, Virtual Reality and Associated Technologies, Göteborg, Sweden, September 2-4, 2014.

Onwudebelu, U., Fasola, S., Obi, N. C., & Alaba, O. B. (2010). *CAPTCHA Malaise: Users suffer Consequences of the Antispam Technology while the Spammers Adapt.* Paper presented at the Software Engineering and Intelligent Systems, Nigeria

Pope, C., & Kaur, K. (2005). Is It Human or Computer? Defending E-Commerce with Captchas. *IT Professional Magazine, 7*(2), 43. doi: http://dx.doi.org/10.1109/MITP.2005.37

Pope, C., & Khushpreet, K. (2005). Is it human or computer? Defending e-commerce with Captchas. *IT Professional, 7*(2), 43-49. doi: 10.1109/MITP.2005.37

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of Cyber-Identity Theft and Related Fraudulent Activity. Psychiatry, Psychology and Law, 20(3), 315-328. doi: 10.1080/13218719.2012.672275. Retrieved from http://www.researchgate.net/publication/236317807_Fear_of_Cyber-Identity_Theft_and_Related_Fraudulent_Activity

Sauer, G., Holman, J., Lazar, J., Hochheiser, H., & Feng, J. (2010). Accessible privacy and security: a universally usable human-interaction proof tool. *Universal Access in the Information Society, 9*(3), 239-248. doi: 10.1007/s10209-009-0171-2 http://search.proquest.com.ezproxy.ecu.edu.au/docview/743897967?pq-origsite=summon&accountid=10675

Schlaikjer, A. (2007). A Dual-Use Speech CAPTCHA: Aiding Visually Impaired Web Users while Providing Transcriptions of Audio Streams.

Shirali-Shahreza, S., & Shirali-Shahreza, M. (2008). *Bibliography of works done on Captcha*. Paper presented at the Intelligent System and Knowledge Engineering, International Conference.

Tak, S., & Gatto, S. (2008). Computer, Internet, and E-mail Use Among Older Adults: Benefits and Barriers. *Educational Gerontology*, 34(9), 800-811. doi: 10.1080/03601270802243697, Retrieved Oct 6, 2015 from: http://www.tandfonline.com.ezproxy.ecu.edu.au/doi/abs/10.1080/03601270802243697#aHR0cDovL3d3dy50YW5kZm9ubGluZS5jb20uZXpwcm94eS5lY3UuZWR1LmF1L2RvaS9wZGYvMTAuMTA4MC8wMzYwMTI3MDgwMjI0MzY5N0BAQDA

Tangmanee, C., & Sujarit-apirak, P. (2013). Attitudes towards CAPTCHA: A Survey of Thai Internet Users. *Journal of Global Business Management, 9*(2), 29-41. Accessed 20th October 2015 from: URL https://www.acs.org.au/__data/assets/pdf_file/0006/32667/JRPIT44.4.441.pdf

US Federal News, (2008). Usability meets Security. Retrieved on October 23rd from http://ezproxy.ecu.edu.au/login?url=http://search.proquest.com.ezproxy.ecu.edu.au/docview/471101960?accountid=10675

Vance, A, Elie-Dit-Cosaque, C., and Straub, D.W. (2008) Examining trust in information technology artifacts: the effects on system quality and culture. *Journal of Management Information Systems*, Volume 24, Issue 4, pp 73 – 100.

Yamaguchi, M., Nakata, T., Watanabe, H., Okamoto, T., & Kikuchi, H. (2014). *Vulnerability of the conventional accessible CAPTCHA used by the White House and an alternative approach for visually impaired people.* Paper presented at the IEEE International Conference on Systems, Man and Cybernetics (SMC), 2014 Retrieved October 13th from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6974548&tag=1

Yan, J and El Ahmad, A.S., (2008) A low cost attack on a Microsoft CAPTCHA, Proceedings of the 15th ACM conference on Computer and Communications Security, ACM : New York.

Yan, J. (2009). Bot Cyborg and Automated Turing Test. 14th International Workshop, Cambridge, UK. March 2009, Springer Berlin Heidelberg.

Yiwei, C., Bob, L., & Robert, M. K. (2013). Internet Use among Older Adults: Constraints and Opportunities. In Z. Z. Robert, D. H. Robert & K. G. Michael (Eds.), *Engaging Older Adults with Modern Technology: Internet Use and Information Access* Needs (pp. 124-141). Hershey, PA, USA: IGI Global.

Zhu, B.B., Yan. J., Bai, G., Yang,M., and Xu, N., (2014) *Captcha as Graphical Passwords – A New Security Primitive Based on Hard AI Problems*. IEEE Transactions on Information Forensics and Security, Volume 9, issue 6.