THE CAPTCHA CONFLICT – A CONSUMER'S CHOICE BETWEEN SECURITY AND CONVENIENCE

Steffen Zorn, Curtin University, Australia
Pedram Hayati, BAE System stratsec, Australia

INTRODUCTION

The web has become a mainstream shopping channel in developed countries. Whereas 79 percent of Americans use the Internet, 72 percent of these Internet users shop online and 78 percent seek information online about a product or service prior to an intended offline purchase (Pew Internet n. D.). Similarly, online shopping in Australia is booming. Internet shoppers spent an average 2,500 A$ in 2007 with online sales expected to grow to around $10 billion over the next five years (Sydney Morning Herald, 2011; The Daily Telegraph, 2007). For shoppers the web offers vast information and 24/7 access to online stores worldwide. Consequently for 78 percent of Internet users convenience is the main reason to shop online, followed by saving time and the chance to get bargains (Horrigan 2008). Furthermore online experience, using the web for work and other activities such as reading news, predicts online buying behavior (Bellman, Lohse and Johnson 1999).

Yet some consumers are hesitant shopping online, mainly because of security concerns (Bellman, Lohse and Johnson 1999; Hoffman, Novak and Peralta 1999; Horrigan 2008). 75 percent of Internet users avoid sending credit card or other personal information over the Internet. Solving security issues would account for an estimated 7 percent increase of online shoppers (Horrigan 2008).

Security mechanisms protect resources from malicious users in limiting access to authorized users (Josang, Ismail and Boyd 2007). Captcha filters are an example of online security measures (Shirali-Shahreza and Shirali-Shareza 2008; Yan and Ahmad 2008). A captcha - Completely Automated Public Turing test to tell Computers and Humans Apart - is the most common technique to prevent automated attacks on online platforms. Captchas can prevent fake registrations through computer programs or automated spam distribution (Bowman, Debray and Peterson 1993; Shirali-Shahreza and Shirali-Shareza 2008). For example, e-mail services on the web provide free accounts to interested users and generate revenue in showing advertisements on the log-in page. Captcha filters prevent automated account registration to acquire large numbers of free accounts which could then be used to distribute spam (Motoyama et al. 2010). Another example are websites selling tickets such as *ticketmaster.com* using captcha filters for access control to prevent automated purchases of large numbers of tickets which could then be resold (Determann and Gutierrez 2008). Using captcha filters helps website owners save resources for legitimate users and keep the performance of the system on an appropriate level (Shirali-Shahreza and Shirali-Shareza 2008).

Different forms of visual and non-visual captcha challenges exist (Shirali-Shahreza and Shirali-Shareza 2008). Most websites use visual challenge captchas consisting of distorted alphanumeric characters, too difficult for text recognizing software to solve and therefore preventing automated solving. Yet humans can decipher the text and respond to the challenge correctly (Motoyama et al. 2010; Shirali-Shahreza and Shirali-Shareza 2008).

Captchas intend to be easy for human users but difficult for computer programs to solve (Burzstein, Bethard, Fabry, Mitchell and Jurafsky 2010; Shirali-Shahreza and Shirali-Shareza 2008). However a study revealed the design intention to be easy for humans to solve has limitations in practice. Whereas solving image captchas resulted in an agreement among three users of 70 percent, audio captchas showed a poor agreement of 31.2 percent. Users' captcha solving time exceeded the optimal solving time by up 285 percent. This indicates captchas are harder to solve in reality than planned (Burzstein, Bethard, Fabry, Mitchell and Jurafsky 2010).

Whereas captchas increase website security, captchas require effort in solving them and thus might reduce the convenience of the web experience. Research has investigated how captchas relate to user behavior on a functional level – how design relates to accuracy and response time. However little research has investigated how the effort of solving a captcha relates to consumer behavior (Motoyama et al. 2010). For example, firms might acquire potential customers with advertising campaigns but lose them before an initial transaction because of an inconvenient captcha security measure. This paper investigates how consumers perceive the trade-off between convenience and security. For academia this study should help broadening the understanding of online consumer preferences driving the purchasing process. Practitioners could be interested to understand if some security measures are inconvenient for potential customers and drive them away.

As mentioned perceived security and convenience relate to online consumer behavior. Security is important as it is an antecedent of consumers' trust in a website which has a positive impact on purchase intention (Chen and Barnes 2007; Yousafzai, Pallister and Foxall 2003). Trust is a set of beliefs one partner of a relationship holds about another and important for success in the online marketplace as it eliminates uncertainty and perceived risk (Pavlou 2003). Risk is the defining characteristic of trust as a transaction without risk lacks the necessity of trust (Yousafzai, Pallister and Foxall 2003). Consumer trust includes two main dimensions – perceived honesty and benevolence (Flavian and Guinaliu 2006).

On the web, consumers have limited opportunities to see and try a product and therefore have to rely on, and trust a website's information (Chen and Barnes 2007; Josang, Ismail and Boyd 2007). Risk is high and thus trust crucial where consumers have limited information about merchants, for example, when exchange partners have never transacted with each other before and lack experience. Risk is highest where consumers have to take the risk of prior performance and for example have to pay for a product before receiving it or have to submit credit card details and bear the risk of credit card fraud (Josang, Ismail and Boyd 2007).
A lack of trust results in a low likelihood of consumers engaging with a website (Hoffman, Novak and Peralta 1999). Consumers discount or reject messages from an untrustworthy source (Hovland and Weiss 1951). Consequently, a website lacking security features might convert few website visitors to customers as the perceived risk is too high.

In addition to reducing perceived risk and motivating consumers to engage in a relationship, security and trust can drive a relationship (Palmatier 2008). For example products that meet customers' security expectations enhance customer satisfaction (Chitturi, Raghunathan and Mahajan 2007). After trust has developed in the merchant/customer relationship, a partner in such a relationship will accept risks such as making an investment or trying a new product without an immediate concession or formal guarantee (Palmatier 2008). Summarizing, security helps to increase trust in a website and is of high importance in an early customer lifecycle stage to drive a relationship.

Convenience relates to when and where consumers can shop (Bhatnagar, Misra and Rao 2000). As mentioned web shops are always open and the web's search capabilities enable consumers to compare numerous website alternatives at a fraction of the cost and time comparing different physical retail stores. The web can serve as a one-stop shop, increases search efficiency and reduces travel time, costs, and related frustrations such as fighting for parking space and queuing in check-out lines (Bhatnagar, Misra and Rao 2000; Childers, Carr, Peck and Carson 2001; Szymanski and Hise 2000). The Internet reduces cost and adds convenience (Bhatnagar, Misra and Rao 2000). However, convenience may come at a price. For example online shoppers' perceived risk on the web might outweigh convenience for some categories such as apparel and clothing, for example when a shirt might not fit (Bhatnagar, Misra and Rao 2000). Similarly, security measures such as captcha filters might be inconvenient for some customers as solving them requires some effort.

For academia it is interesting to investigate how this trade-off between security and convenience relates to consumer behavior. Practitioners might be interested to see which security measures are acceptable for customers.

METHODOLOGY

To investigate how consumer behavior relates to online security measures, the study used sponsored search advertisements to attract visitors to the website of a company specializing in rugged IT hardware solutions (www.roamingtech.com.au). Sponsored search provides measurability and enables advertisers to control the quality of website visitors (Jansen et al. 2009). The study aimed for a high number of clicks but more importantly for a high quality of visitors. Therefore the campaign used a limited number of product specific keywords such as 'rugged laptop' or 'toughbook' which activated one of the two ads (Figure 1).

Looking for a ToughBook? We specialize in Rugged Hardware and have 20+ years experience www.roamingtech.com.au	Best Priced Ruggedized IT Get your Ruggedized Laptop from us! Competitive prices + free delivery www.roamingtech.com.au

Figure 1: Sponsored Search Advertisements

The landing page of the advertising campaign redirected website visitors to a website with a routing component, a captcha component and an exit component (Figure 2).

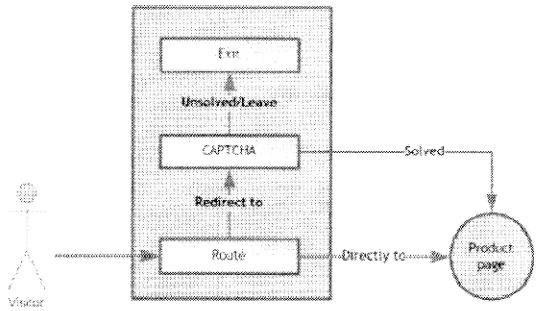

Figure 2: Routing and Captcha Component

The routing component randomly routed to the product page or to a captcha webpage to create two groups – visitors that had to go through the captcha filter to visit the website (captcha users) and visitors without the captcha stimuli (non-captcha users). Furthermore the routing component recorded the number of visitors who intended to visit the product page, visitors who were routed to the product page, and visitors who were redirected to the captcha.

Using common best practices, the captcha component generated captcha challenges (von Ahn, Maurer, McMillen, Abraham and Blum 2008). After solving the captcha challenge, this component redirected the visitor to the product page. The captcha component recorded the duration users needed to solve the assigned challenge, the number of challenges assigned to a single visitor, and the number of solved challenges.

The exit component recorded the number of visitors who left the website because of the captcha challenge, because they could not solve the challenge or "closed" the webpage without any attempt to solve the challenge.

Web analytics software provided behavioral data of the landing page such as how many pages a user visited and how long visitors stayed on site.

RESULTS AND DISCUSSION

The experiment ran from June, 1st and stopped June, 10th when Google disapproved the ads because redirecting from the company homepage to the server which hosted the captcha violated Google's advertising policy. After following Google's policy, the experiment continued on June, 17th and ended July, 1st.

Within the 25 days duration, the campaign created 124 clicks with a high click-through rate (CTR) of 2.64 percent compared to global CTRs of below .1 percent (eMarketer 2010). 30 visitors were directed to the product page without having to solve the captcha, visited on average 2.4 pages and spent 263 seconds on the website. Of the remaining 94 visitors, 57 bounced off and left the captcha immediately without trying to solve it. Visitors solving the captcha successfully visited on average 2 pages and spent 351 seconds on the website.

Given the non-normality of the data, a Kruskal-Wallis test investigated behavioral differences, pages viewed and time on site, of the company's captcha and non-captcha users. Yet the Kruskal-Wallis test showed insignificant differences for both behavioral measures time on site ($p=.560$) and page views ($p=.602$).

CONCLUSIONS AND IMPLICATIONS FOR THEORY AND PRACTICE

This study investigated the trade-off between convenience and security of using captchas as a security measure, and the implications for consumer behavior. Given that 61 percent of website visitors who had to solve the captcha bounced off shows that consumers seem to prefer convenience over security measures, at least when these security measures require user effort and therefore are inconvenient.

Interestingly, visitors solving the captcha and landing on the webpage as intended showed insignificant behavioral differences from non-captcha users. The effort of solving a captcha has no impact on users' motivation on a website.

For academia this study shows that web users prefer convenience over security which requires user effort. However a high user effort in solving a captcha filter had little impact on consumer behavior on the website. For practitioners the study shows

that security measures might help increase consumer trust in a website but might come at a cost. Many potential customers perceived solving a captcha as inconvenient and bounced off before reaching the website. Consequently security measures should avoid increasing visitor effort and reduce convenience.

The study has a number of limitations. The website was a very specific niche market B2B website selling high-priced products. This limits the generalizability of the findings. Future studies could investigate the trade-off between convenience and security on other websites such as B2C retail websites or B2B websites in a different market. Furthermore this very specific niche market only attracted a limited number of visitors. Future research should attract more visitors allowing for normal distributed data.

Future research could also investigate if the design of captcha filters and related webpages impact consumer behavior. As the study showed the captcha on a blank page with little information, visitors might have misunderstood the purpose of the captcha filter and left because of uncertainty. Future research could investigate how different forms of captcha explanation might impact on the captcha bounce rate.

Furthermore captchas are not the only security measure on websites. For example payment systems such as Paypal add an additional security layer in offering systems which create unique security codes. Paypal customers use these unique codes along with their username and password. Whereas such a system improves security, it requires additional user effort to access a Paypal account. It would be interesting to investigate if customers value such a system.

REFERENCES

Available Upon Request