How brain type influences online safety

WORKING PAPER

Tyler Moore and Ross Anderson
Computer Laboratory, University of Cambridge
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
firstname.lastname@cl.cam.ac.uk

Abstract

Many information security mechanisms fail in practice through poor usability. For example, phishing is a rapidly-growing form of online crime; both real-world experience and academic research demonstrate that many users do not heed the available security indicators. Various explanations have been given, from a lack of training to poor indicator design. In this paper, we offer a more fundamental explanation, namely that people's brain type significantly influences their success or failure at recognizing online scams. We describe a survey which tested ability to recognize phishing scams, as well as brain type. Our results emphasise that security mechanisms should be designed to be usable by the widest possible range of people.

1 Introduction

Information security products have long been designed by geeks and for geeks. Designers focused on the technical features of protection mechanisms, leaving the interface as an afterthought. This often led to unusable software. Whitten and Tygar's seminal paper found that users made critical errors when configuring PGP because of to its unwieldy interface [12]. More recently, there has been an explosion of interest in designing usable security mechanisms. Unfortunately, this does not mean that today's mechanisms are much better. Schechter et al. found that a substantial proportion of users ignored browser warnings [10], while Egelman et al. conducted an experiment simulating a phishing attack, finding that 97% of participants ignored passive warnings and 21% ignored active warnings [5].

The response to such work has been mixed. Some have emphasized the need to design better security mechanisms [4], while others have argued that more user education is needed. Financial institutions and governments have developed initiatives to improve user education, such as Get Safe Online in the UK [6] and the National Cyber Security Alliance in the US [9], while researchers have developed various techniques, from educational games [11] to embedding training messages in email [8]. The prevailing view seems to be that, with a bit more user training or improved mechanisms, people will stop falling for online scams. Blaming the users may certainly appear to be in the short-term economic interests of many other stakeholders.

But we believe there are deeper forces at play. We argue that some people are better wired to accurately process the warnings presented to them. To test our hypothesis, we surveyed 132 participants to gauge their ability to recognize phishing scams, followed by a personality test developed by the psychologist Simon Baron-Cohen [1]. We find that personality does indeed significantly impact peoples' success in recognizing phishing scams. In particular, people with high 'systemizing' quotients fare better than those with lower quotients, and people with high 'empathizing' quotients fare worse than those with lower scores. The difference between the two quotients turns out to be a particularly good predictor of scam detection ability.

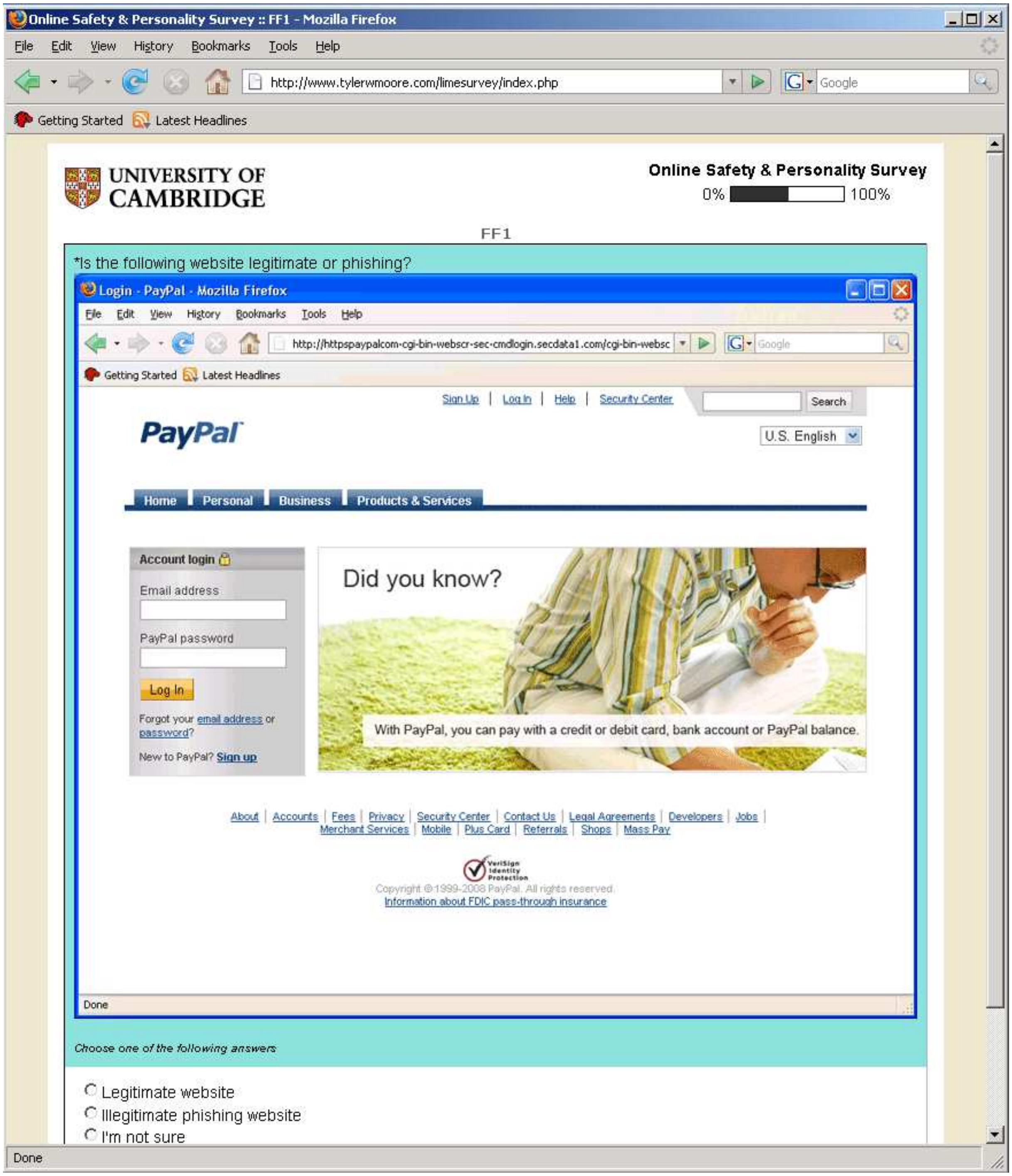
2 Survey structure

We set out to test our hypothesis that personality affects responsiveness to security mechanisms quickly and simply. Consequently, we devised an online survey where respondents are presented with screenshots of various websites and asked to judge whether they are phishing or not. Such a survey is a lightweight and imperfect test of people's susceptibility to phishing; more thorough methods have been discussed in the literature, such as experiment-based approaches that simulate phishing attacks [5]. However we decided to conduct a rapid test of our hypothesis first, and we anticipate continuing the work using more detailed experiments in future.

Participants are first asked several demographic questions, followed by a page explaining what phishing is. The instructions read:

> Phishing is the term used for criminals enticing people into visiting websites that impersonate the real thing. Phishing websites dupe people into revealing passwords and other credentials, which will later be used for fraud. The most common targets of phishing attacks are financial institutions, but any website asking for login credentials such as passwords may be impersonated.
>
> You may receive emails claiming to be sent from your bank. Sometimes, indeed, the emails can be from your bank. Other times, the emails are sent by fraudsters. These emails include links to websites that appear to be from your bank, but are in fact from elsewhere. The following questions include pictures of a number of websites. Sometimes the website matches the bank. Other times, the website is a fake phishing website. It is up to you to decide which websites are legitimate and which are fake.

Participants are then presented with a sequence of 12 screenshots from various websites (see Figure 1 for an example), and they are asked to answer whether the website is legitimate, or a phish, or that they are unsure. In fact, the only relevant information we supplied to participants comes from the URL present in the address bar. As we included a screenshot for the entire


Online Safety & Personality Survey :: FF1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.tylerwmoore.com/limesurvey/index.php
Google
Getting Started Latest Headlines
UNIVERSITY OF CAMBRIDGE
Online Safety & Personality Survey
0% 100%
FF1

*Is the following website legitimate or phishing?

Login - PayPal - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://httpspaypalcom-cgi-bin-webscr-sec-cmdlogin.secdata1.com/cgi-bin-websc
Google
Getting Started Latest Headlines
Sign Up | Log In | Help | Security Center
Search
PayPal
U.S. English
Home Personal Business Products & Services
Account login
Email address
PayPal password
Log In

Forgot your email address or password?

New to PayPal? Sign up

Did you know?

With PayPal, you can pay with a credit or debit card, bank account or PayPal balance.

About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs |
Merchant Services | Mobile | Plus Card | Referrals | Shops | Mass Pay
VeriSign Identity Protection

Copyright © 1999-2008 PayPal. All rights reserved.

Information about FDIC pass-through insurance

Choose one of the following answers

○ Legitimate website
○ Illegitimate phishing website
○ I'm not sure

Figure 1: Screenshot of phishing test.

browser, participants were free to make their judgement using other irrelevant information, from the presence of an `https` padlock to the overall look and feel of the website.

Again, it would have been nice to provide some users with instructions on what to look for. In this way, we could test the educational efficacy of different training methods. However, for simplicity we left this to future work.

After answering the phishing questions, participants are presented with two sets of 40 questions. The first tests a person's systemizing quotient (SQ), while the second tests an empathizing quotient (EQ). These tests were devised by Baron-Cohen, appearing in [1, pp. 201–216], and were used with his permission. Each question is a statement (e.g., "I really enjoy caring for other people"), and participants are asked whether they strongly or slightly agree or disagree with each statement.

Baron-Cohen's theory holds that people naturally have different brain types. In essence, those with 'type S' brains (high SQ scores) excel at building and understanding systems, while those with 'type E' brains (high EQ scores) are good at understanding the perspectives of others. From this theory, we would expect that people with type S personalities are more likely to excel at tasks such as understanding how to parse URLs correctly, while people with type E personalities are more likely to assess a website's validity by assessing its overall look and feel and by aggregating different signals to take a holistic judgement. This latter strategy works well when judging whether a physical environment is suspect, but it fails miserably when judging whether a website is dodgy.

3 Survey results

3.1 Demographics of respondents

We advertised via email newsletters to students across the University of Cambridge, enticing prospective participants to take our 'Online Safety and Personality Quiz' with the following blurb:

> Would you like to learn your brain type, test your online safety skills, and help out Cambridge researchers? Please fill out the Online Safety and Personality Survey. In around 15 minutes, you can learn how to spot online banking scams and find out if you are an 'empathizer' or 'systemizer'.

Therefore, we made it somewhat apparent to the respondents what they were getting involved in by agreeing to the survey. This might possibly afford some selection bias, though it might also have attracted people curious to test their personalities.

In all, we received 132 completed responses (77 female, 55 male). Nearly all were students (unsurprising given the advertising medium) between the ages of 18 to 30. The background of

	value	σ	p	Significance
Intercept (β_0)	8.306	1.134	2.47×10^{-11}	0.001
SQ (β_1)	0.04334	0.02128	0.0438	0.05
EQ (β_2)	-0.01402	0.01822	0.4430	
isFemale (β_3)	-1.989	0.4875	7.92×10^{-5}	0.001
StudiesITScienceEngr (β_4)	-0.02781	0.5106	0.9566	

Table 1: Statistical data for linear regression matching survey data.

students was also varied across all university disciplines. 67 people reported Mozilla Firefox as their primary browser (51%), 51 used Microsoft Internet Explorer (39%), and the remaining 14 (10%) used other browsers (e.g., Safari, Opera). We presented screenshots matching their reported browser where IE or Firefox was reported, and presented screenshots in IE for the remaining 10% of respondents.

3.2 Impact of brain type on results

We have devised a simple linear regression to test for correlation between recognition of phishing websites and SQ and EQ scores:

$$\mathsf{PhishScore} = \beta_0 + \beta_1\mathsf{SQ} + \beta_2\mathsf{EQ} + \beta_3\mathsf{isFemale} + \beta_4\mathsf{StudiesITScienceEngr}$$

The independent variable PhishScore gives the number of questions (out of 12 total) answered correctly for the phishing assessment. We included four dependent variables in the regression. SQ and EQ indicate the scores on the systemizing and empathizing tests, respectively.[1] We also include gender using the dummy variable isFemale, which is set to 1 if the respondent is female and 0 if male. Finally, we include the dummy variable StudiesITScienceEngr, which is set to 1 if the respondent studies IT, the natural sciences or engineering, and 0 otherwise.

Table 1 gives the details for the regressions. SQ has a statistically significant (to 0.05) positive impact on the phishing score, when controlling for the other factors. Female respondents tended to perform worse on the test, while studying science, engineering or IT had no appreciable impact on test performance.

In addition to the regression, we use a simple plot to get a visual feel for the effects of EQ and SQ on scores. Figure 2 plots the SQ (left) and EQ (right) scores for each of the respondents against the number of websites correctly identified as phishing or legitimate. Higher y values indicate users are more proficient at detecting phishing websites. Low EQ and SQ scores appear on the left, while higher scores appear on the right.

[1] An SQ score below 20 is considered low, 20–39 average, 40–50 above average, over 50 very high (80 is the maximum score). An EQ score below 32 is considered low, 33–52 average, 53–63 above average, over 64 very high (80 is the maximum score).

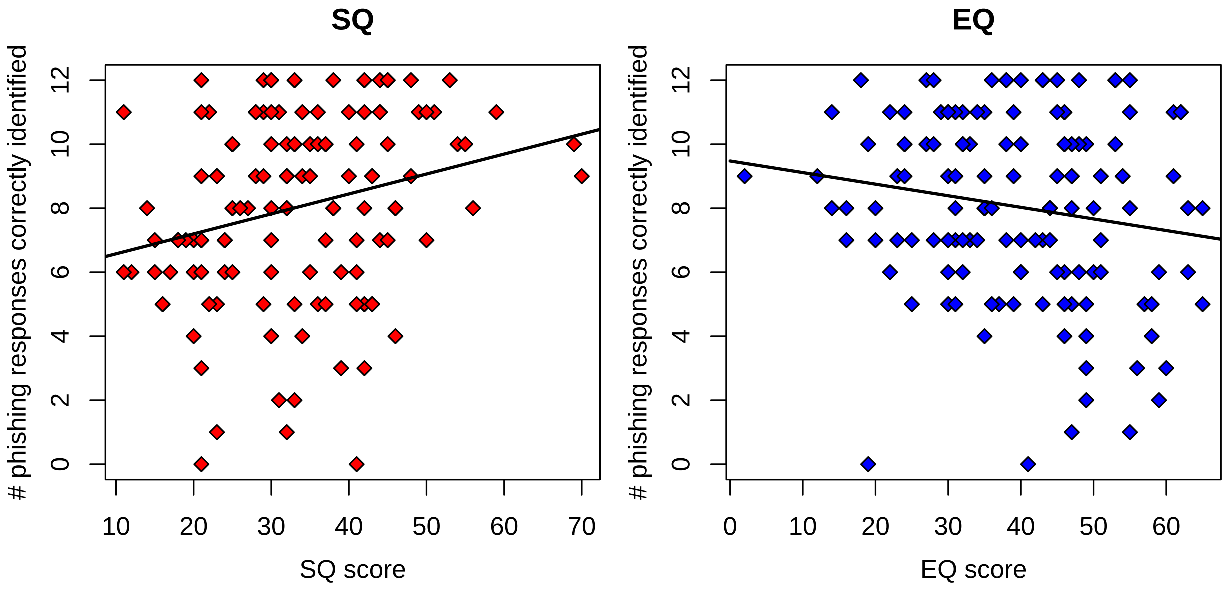


Figure 2: SQ score (left) and EQ score (right) compared to the number of phishing responses correct.

Respondents who scored well on the phishing test appear throughout the range of EQ and SQ scores. However, many people who fared poorly on the phishing test also scored low on the SQ test. Furthermore, many people who fared poorly on the phishing test also scored high on the EQ test. This result reinforces our hypothesis that type E people are more likely to be duped by phishing attacks, and that type S people are more likely to recognize impersonating phishing attacks as such.

Figure 2 also plots a fitted linear regression line. The slope of the line in Figure 2 (left) is positive, which implies that higher SQ scores match a better recognition of phishing websites. The slope of the line in Figure 2 (right) is negative, which implies that higher EQ scores match a worse recognition of phishing websites.

We also compared the difference SQ−EQ to the phishing scores, because it is often the case that those who have comparatively high SQ scores have comparatively low EQ scores, and vice versa. Figure 3 plots the results, and Table 1 lists the details for the regression. Unsurprisingly, the effect is positive and statistically significant. In other words, people with high SQ and low EQ do better than those with low SQ and high EQ.

4 Conclusion

There are many reasons why some people do not heed security indicators, from unusable design to poor training. In this note, we have described an experiment that has confirmed another reason: personality. This is a significant result, because it means that we cannot place all of the blame on the actions of poorly-informed users. We anticipate conducting more sophisticated

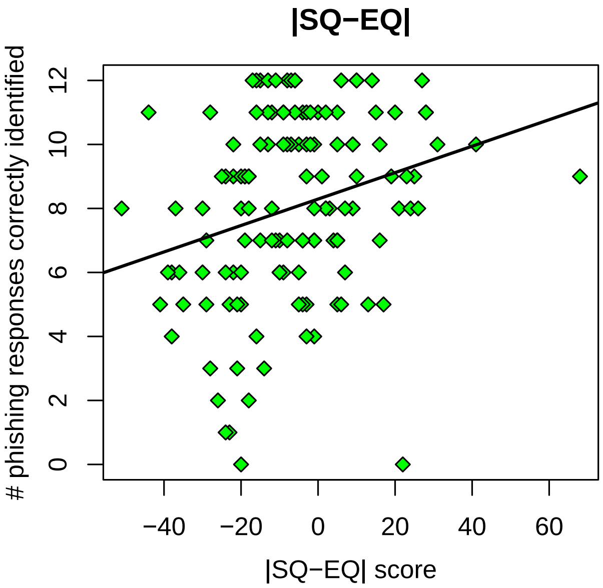


Figure 3: SQ score minus EQ score versus the number of phishing responses correct.

experiments to confirm our present findings. In addition, as most men have SQ $\geq$ EQ and most women have EQ $\geq$ SQ, our results suggest gender discrimination; gender HCI researchers have argued that some system designs discriminate against women [2, 3], and our work appears to add security to the list. We therefore suggest that security designers should begin trying to devise indicators that work for people of different brain types.

Acknowledgements

Tyler Moore is supported by the UK Marshall Aid Commemoration Commission and by US National Science Foundation grant DGE-0636782.

References

[1] S. Baron-Cohen: The Essential Difference: The Truth About the Male and Female Brain. Basic Books, 2003.

[2] L. Beckwith, C. Kissinger, M. Burnett, S. Wiedenbeck, J., Lawrance, A. Blackwell, C. Cook: Tinkering and gender in end-user programmers' debugging. In *ACM Conference on Human Factors in Computing Systems*, pp. 231-240, 2006.

[3] J. Cassell: Genderizing HCI. MIT Media Lab, 1998.

[4] L. Cranor and S. Garfinkel (Eds.): Security and Usability: Designing Secure Systems that People Can Use. O'Reilly, 2005.

[5] S. Egelman, L. Cranor and J. Hong: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (ACM CHI)*, pp. 1065–1074, 2008.

[6] Get Safe Online: `http://www.getsafeonline.org/`.

[7] M. Jakobsson and S. Myers (Eds.): Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley, 2006, ISBN: 978-0-471-78245-2.

[8] P. Kumaraguru, Y. Rhee, A. Acquisti, L. Cranor, J. Hong and E. Nunge: Protecting people from phishing: the design and evaluation of an embedded training email system. In *ACM CHI*, pp. 9005–914, 2007.

[9] National Cyber Security Alliance: `http://www.staysafeonline.org/`.

[10] S. Schechter, R. Dhamija, A. Ozment and I. Fischer: The emperor's new security indicators: an evaluation of website authentication and the effect of role playing on usability studies. In *IEEE Symposium on Security and Privacy (S&P)*, pp. 51–65, 2007.

[11] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge: Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Symposium On Usable Privacy and Security (SOUPS)*, 2007.

[12] A. Whitten and J. D. Tygar: Why Johnny can't encrypt. In *8th USENIX Security Symposium*, pp. 169–184, 1999.