Phishing Resiliency Across Socio-Cultural Spheres: Cyrillic Orthographic Zone vs. The Five Eyes

William Smeal, Yash Kumar, Vaibhav Vishwanath, L. Jean Camp, Alexander Alexeev

School of Informatics and Computing, Indiana University Bloomington

Introduction

Phishing attacks are a global phenomenon and have therefore necessitated the implementation of organizational cyber security training designed specifically to aide individuals in identifying potential phishing attempts. Despite these preventative measures, a large proportion of internet users across the world are still susceptible to phishing attacks [7]. Our study evaluates phishing resiliency across several countries within the Cyrillic Orthographic Zone (COZ): Belarus, Bulgaria, Russia, and Ukraine, and compares these results with a similar study conducted with participants from the Five Eyes, the Anglophone intelligence alliance consisting of Australia, Canada, New Zealand, the United Kingdom, and the United States. The countries we have chosen share a common linguistic and literary history, representing nations in which the use of Cyrillic script is not only most prominent in cyberspace, but also culturally significant.

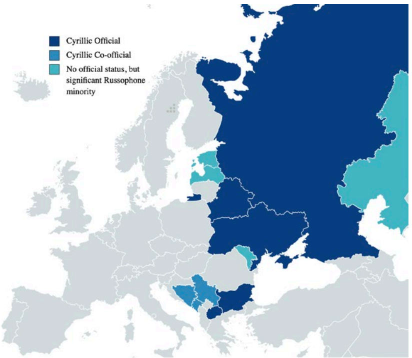


Figure 1 The Cyrillic Orthographic Zone

For the purposes of this study, we define phishing resilience as the ability to both correctly identify an illegitimate site as illegitimate and to identify a legitimate site as legitimate. The first requires recognizing when a domain name resembles the imitations cyber criminals typically employ when designing their attacks. The second timate site, where no such deceptive changes have been made. The goal is contribute to the existing body of literature regarding the interaction of cultural and individual dimensions of phishing resilience. Our aim is to expand upon research trends that enable global or region-specific approaches in reducing the risk of insecurity brought about by successful phishing attacks.

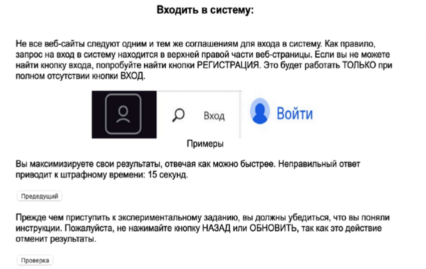
Phishing is an attack that inherently leverages human interaction. This style of attack leverages human interaction [6]. Research on phishing resilience has targeted internet users in the English-speaking world [12]. One factor pertaining to ongoing phishing susceptibility is the increasingly elaborate nature of attacks even as more preventative measures are regularly introduced [8]. Despite investments in anti-phishing mechanisms and training, phishing attacks continue to prove profitable. Ultimately, human beings are the last line of defense in tackling phishing attacks and a better understanding of human factors is therefore key to advancing studies of phishing susceptibility and resilience [17].

To expand the understanding of cultural and linguistic factors in phishing resilience we reproduced an on-line experiment implemented by Camp et al, reproducing an examination of resilience in the Five Eyes in the Cyrillic Orthographic Zone. In a cross-national study, Camp et. al. test phishing resilience with the goal of identifying commonalities between comparable nationalities, more specifically English-speaking, western, industrialized democracies [2]. Significant research has indicated that Western, educated, industrialized, rich and democratic (WEIRD) populations cannot be assumed in other populations with high confidence. Research on human factors in phishing is concentrated in the wealthiest Anglophone nations, where phishing emails were first researched in response to attempts to obtain America Online accounts. This may be a result of the comparatively high population of internet users, the hegemonic status of the English language on the internet, or the relative wealth of in the Anglosphere [4], [16].

Experiment Design

This study aims to evaluate the relationship between demographic factors, computer knowledge and skills, website familiarity, and risk assessment behaviors and phishing resilience. The participants in this study are native speakers of Russian or Bulgarian languages from Belarus, Bulgaria, Russia, and Ukraine.

Participants were presented with both legitimate and illegitimate versions of websites written in their native tongues. Our dataset was created with screenshots of legitimate sites and modified screenshots to represent simulated phishing sites. We bitmapped the login variants and back button to make these parts of the site clickable and instructed participants to click the login feature in any of its possible forms if the site presented appeared to be legitimate. When participants were presented with a site they deemed to be illegitimate, we asked them to click the back button, which is universally represented.



Входить в систему:

Не все веб-сайты следуют одним и тем же соглашениям для входа в систему. Как правило, запрос на вход в систему находится в верхней правой части веб-страницы. Если вы не можете найти кнопку входа, попробуйте найти кнопки РЕГИСТРАЦИЯ. Это будет работать ТОЛЬКО при полном отсутствии кнопки ВХОД.

Вы максимизируете свои результаты, отвечая как можно быстрее. Неправильный ответ приводит к штрафному времени: 15 секунд.

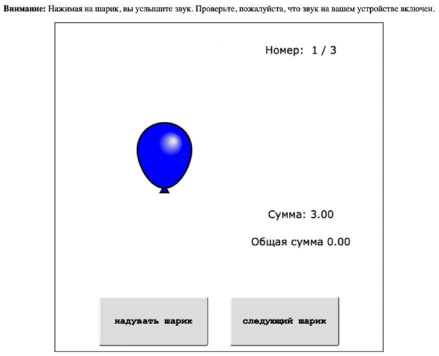
Прежде чем приступить к экспериментальному заданию, вы должны убедиться, что вы поняли инструкции. Пожалуйста, не нажимайте кнопку НАЗАД или ОБНОВИТЬ, так как это действие отменит результаты.

Figure 2 Experimental Instructions for Indication of Trustworthy or Untrustworthy Sites

Experiment Procedure

A total of 200 participants were recruited to participate in this experiment, which was conducted over a period of 5 days across all four countries. For participation in the study, participants needed to be at least 18 years of age and nationals of one of Belarus, Bulgaria, the Russian Federation, or Ukraine, and a native speaker of Russian or Bulgarian language. Initially, participants were presented with a study information sheet (SIS) and, after agreeing to participate in the study, we requested basic demographic information including an email address so as to track their responses throughout the experiment, as well as to ensure participants could participate in the study only once.

Upon the collection of demographic information, participants proceeded to a BART (Balloon Analog Risk Task) experiment. The BART was used to measure participants' risk-taking behavior prior to recording any results from the simulated environment, instructions to which were provided upon completion of the BART test. In order to test participants' comprehension and ensure they understood the procedures of the experimental task, we included a series of confirmation questions addressing the experiment controls, bonus pay, single attempt policy, and time penalty. Upon completing these comprehension questions the experimental task began and participants were presented with a series of ten websites in their native languages. Upon completion of the experimental phishing task, participants proceeded to a final survey, which collected information pertaining to website familiarity, security knowledge, computer expertise, and website risk assessment behavior. These questions are available in the appendix along with an English translation.



Внимание: Нажимая на шарик, вы услышите звук. Проверьте, пожалуйста, что звук на вашем устройстве включен.

Номер: 1 / 3

Сумма: 3.00

Общая сумма 0.00

Figure 3 The Balloon Analog Risk Task

Analytical Approach

The goal of this work is to provide statistical data regarding potential links between socio-cultural traits and online risk perception. The two socio-cultural groups analyzed in this study are Slavic Cyrillic countries, which we will refer to as group COZ, and the Anglophone group of countries known as the Five Eyes, which we will refer to as AFE. In order to reach a conclusion regarding the influence of socio-cultural factors, we will conduct two stages of statistical testing. Firstly, we will produce statistics comparing the members of the COZ group in order to identify differences in the following areas: A) demographic factors, B) Technical Expertise, C) Website Familiarity, and D) Risk Assessment Behavior, and E) Phishing Resilience. We will then apply statistical tests, primarily the Analysis of Variance (ANOVA), to identify any statistically significant differences between countries.

Conclusion

We will describe our current cross-national study on phishing resilience within the primary members of the Cyrillic Orthographic Zone. The participants in this study are all native speakers of a Slavic language written in Cyrillic script and nationals of the countries included in this study. We will then compare the results of this study with those found by Camp et al., researching the levels of phishing resilience in the Anglophone Five Eye countries. Our contribution will highlight the factors that correlate with high phishing resilience, as participants will inevitably display varying levels of phishing knowledge, computing expertise, or familiarity with indicators of internet security. The results of our experiment will also present a valuable contribution to the debate over the efficacy of individualized international anti-phishing mechanisms accounting for regional and cultural differences versus universal anti-phishing mechanisms.

References

[1] Alkhozae, Mona Ghotaish, et. al. "Phishing websites detection based on phishing characteristics in the webpage source code." IJICTR 1.6 (2011).

[2] Camp, J., S. Das, J. Dev, M. Grobler, and D. Kim, "Cross-national study on phishing resilience," Workshop on Usable Security and Privacy, 2021.

[3] Camp, L. Jean, et al. "Measuring human resilience in the face of the global epidemiology of cyber attacks." Proceedings of the 52nd HICCS. 2019.

[4] Chaudhry, Junaid Ahsenali, Shafique Ahmad Chaudhry, and Robert G. Rittenhouse. "Phishing attacks and defenses." International Journal of Security and Its Applications 10.1 (2016): 247-256.

[5] C. W. Choo, "Information culture and organizational effectiveness," International Journal of Information Management, vol. 33, no. 5, pp. 775–779, 2013.

[6] L. Cranor, J. Downs, and M. Holbrook, "Decision Strategies and Susceptibility to Phishing", Proceedings of the second symposium on Usable privacy and security, 2006.

[7] Das, Sanchari, et al. "All about phishing: Exploring user research through a systematic literature review." arXiv preprint arXiv:1908.05897 (2019).

[8] R. Dhamija, M. Hearst, J.D. Tygar, "Why phishing works", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006.

[9] Egelman, Serge, Lorrie Faith Cranor, and Jason Hong. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings." SIGCHI Conference on Human Factors in Computing Systems. 2008.

[10] Ermakova, L. "Spam and phishing detection in various languages," International Journal "Information Technologies and Knowledge", Vol. 4, No 3, 2010.

[11] Flores, Waldo Rocha, et al. "Investigating personal determinants of phishing and the effect of national culture." Information & Computer Security (2015).

[12] S. Purkait, "Phishing counter measures and their effectiveness – literature review", Information Management & Computer Security, Vol 20 Issue 5, 2012.

[13] Rajivan, Prashanth, et al. "Factors in an end user security expertise instrument", Information & Computer Security, 2017.

[14] Sample, C. "Culture and cyber behaviors: DNS defending," Journal of Information Warfare Vol. 14, No. 4, 2015.

[15] Sheng, Steve, et al. "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions." Proceedings of the SIGCHI conference on human factors in computing systems. 2010.

[16] Wolk, R. The effects of English language dominance of the internet and the digital divide. 2004 International Symposium on Technology and Society (IEEE Cat. No. 04CH37548). IEEE, 2004.

[17] Zhuo, Sijie, et al. "SoK: Human-Centered Phishing Susceptibility." arXiv preprint arXiv:2202.07905 (2022).

[18] Дерюгин, Роман Александрович. "Киберпреступность в России: современное состояние и актуальные проблемы." Вестник МВД России 2 (2019): 46-49.

[19] Кузнецов, Максим Валерьевич. Социальная инженерия и социальные хакеры. БХВ-Петербург, 2007

[20] Старостенко, Олег Александрович. "Природа и способы совершения мошенничества с использованием информационно-телекоммуникационных технологий." Вестник Удмуртского университета. Серия «Экономика и право» 30.4 (2020): 576-582.