ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Tell Me Where You Live and I Will Tell Your P@Ssw0rd: Understanding the Macrosocial Variables Influencing Password's Strength

Andreanne Bergeron | GoSecure; University of Montreal, Canada,
ORCID: 0000-0001-9013-6662

Abstract

Users' habits in relation to cybersecurity are frequently examined from the micro perspective, using survey results to obtain impactful variables from individuals, focusing on usability and security factors of passwords. In this paper, the influence of macrosocial factors on password strength is studied in order to offer a global comprehension of the influence of the environment on users. Using the list of the 200 most common passwords by countries released by NordPass in 2021, logistic regression has been used to predict macrosocial variable influencing password strength. Results show that (1) Literacy level of a population; (2) Voice and accountability; (3) Level of global cybersecurity; and (4) Level of data breaches exposure significantly predict users' password strength performance. The author discusses the impact of government on password hygiene of users hoping to influence the development of policies around cyber security configurations and investment set by nations and institutions.

Keywords
password, macrosocial influence, authentication, users' behaviour, users protection

Received: 28.07.2023

Accepted: 06.11.2023

Published: 27.11.2023

Cite this article as:
A. Bergeron "Tell Me Where You Live and I Will Tell Your P@Ssw0rd: Understanding the Macrosocial Variables Influencing Password's Strength," ACIG, vol. 2, no. 1, 2023, DOI: 10.60097/ACIG/162863

Corresponding author:
Andreanne Bergeron, GoSecure; University of Montreal, Canada; ORCID: 0000-0001-9013-6662; E-MAIL: andreanne.bergeron.5@umontreal.ca

1. Introduction

Passwords are words, strings of characters, or some form of interactive message used to prove identity and gain access to a resource or a place. They constitute the first line of defence for computer-based technologies and were used for millennia as the Roman military were reportedly using passwords to distinguish allies from enemies [1]. Today, even if attack-resistant validation schemes exist, passwords constitute the most popular strategy of authentication.

People usually have a multitude of different passwords and when they create them, they often use a strategy to make it easy to remember [2, 3]. Past studies have shown that users intend to choose weak passwords, which are usually easy to be remembered but vulnerable to be guessed [4, 5]. Also, study reveals that textual passwords are often reused, which have been shown to be an important security threat of passwords [6].

Researchers demonstrated the influence of a person's environment and exposure to the Internet on their online security behaviour [7, 8]. Password creation strategy, defined as the active approaches that can be used by a password creator to create memorable passwords [9, 3], also seems to be influenced by a person's environment. For example, it was identified that students from the United States have a higher risk perception toward surveillance than students from the United Kingdom [8]. Also, Yang et al. [10] discuss the cultural influence in password choice. They explain the weak passwords strength level of Chinese by the rapid growth of Internet users and e-commerce markets in China. They hypothesize that providers may not have paid enough attention to security issues because of the focus on market expansion. The results of the aforementioned studies suggest that there is a structural difference in cybersecurity habits between countries [11].

The present study aims to explore the various macrosocial elements contributing to the structural difference between countries in users' choice of password. The contribution of governments to the problem or to the solutions can be evaluated through this assessment. In order to observe countries' differences, the password strength performance of users will be compared to macrosocial variables that could influence password creation strategy.

1.1. Macrosocial Variables Influencings Users

Few studies show evidence that there is a structural difference between countries in password habits (e.g., [11]) but

the macrosocial variables influencing it have rarely been directly tested. To explore the different variables that could play a role in password habits, the literature on macrosocial variables influencing the different aspect of technology, like the use of Internet in general, is considered. Several macrosocial elements might be taken into consideration when evaluating the reasons why users have different levels of performance according to their environment. First, if there is a difference in cybersecurity habits between countries, the characteristics of the government might be an element influencing users. Second, the characteristics of the population, which is directly related to users, would also be an element explaining the impact of the environment. Finally, external variables like cyber-attacks and the level of cyberattack victimization of a country might also be a part of the explanation.

Characteristics of the government. The economic aspect of a government might influence Internet habits. Prior studies have found that a country's economic development level helps predict the use of internet in a society [12]. Gross domestic product (GDP) is the most closely watched and important economic indicator and considers different variables about a country's economy, including its consumption and investment [13, 14]. It could be hypothesized that economic indicator would influence not only the use of internet, but other habits related to them.

Along with the economy, the investment and the commitment of countries to cybersecurity is an important variable to consider as the relation is more direct. Researchers have found that when a country invests and commit into the cybersecurity sector, the annual losses due to cybercrime over the country's Gross National Income decreases [15]. The investments in cybersecurity can include education and tools to help users to more efficiently manage their Internet use.

Characteristics of the population. Digital skills and the overall ability to use the internet are two elements that are directly linked to literacy. Internet users are reading expository text in a hypertext format where ideas are connected by links, headings, icons, and graphics; those elements necessitate similar reading strategies as those used with print text reading [16]. In other words, to seek, evaluate, and use information found on the Internet, readers must navigate through Internet text and apply their knowledge of the reading process. To understand correctly what a password is and to write one, people need to read. Research has shown that password security practices typically conflict with general usability principles [17]. The challenges faced by low-literacy users when creating and managing passwords

are likely to extend beyond those experienced by the public. Literacy level affects password habits [18].

External events: Data breaches. According to the Identity Theft Resource Centre's Annual Data, there were 1862 data breaches in 2021. Researchers have shown that the United States was highly represented in data breaches, and they explain this by their high level of economic activity as well as by their relatively high notification rates they have compared to other countries [19]. Luxemburg, Canada and Great Britain follow the United States in the list of countries most affected by data breaches [19]. When calculating the country-based probability variable, another study shown that France and Brazil have relatively higher probability of data breaches than the other countries [20]. Researchers state that the probability of a data breach is influenced by the country in which it happens [20].

There seems to be a relationship between the influence that data breaches might have on users and their habits. Campbell et.al. [21], examined the stock market reaction to newspaper reports of information security breaches at 38 publicly traded U.S. corporations during the period January 1, 1995 to December 31, 2000. Among the 43 different events, the authors found a highly significant negative market reaction to information security breaches involving unauthorized access to confidential data. Moreover, in their study on 6,000 users from the United States, after a data breach notification, victims changed their password or PIN (51%) or switched to a new account (24%) [22]. The literature suggests that users actively assess the consequences of breaches and react accordingly.

1.2. Aim of the study

Users' habits in relation to cybersecurity is frequently examined from the micro perspective, using survey results to obtain impactful variable from individuals, focusing on usability and security factors of passwords [23, 24]. In this paper, the influence of macrosocial elements on password strength[1] is studied in order to offer a global comprehension of the influence of the environment on users. Exploring the different concept of technology and their flaws at the country level encourages future development of new technologies and improve related capital investments (e.g., [28, 29]).

A descriptive analysis of leaked lists of passwords in 2021 is conducted to determine which macrosocial variables would be included in the model and therefore play a formative role in how users formulate their passwords across countries. Then, a prediction model help

1 — Strong passwords are usually characterized by larger number of characters, containing upper and lowercase letters, numbers and special characters [25]. Also, a strong password should avoid using dictionary words [26, 27].

identify the extent to which variables influence password strength. This study is innovative as it allows to investigate trends in password formulation with regard to social context. The impact of our study is a move toward a better understanding of human behaviour in the context of password formulation specifically, to enable the future crafting of more targeted cybersecurity interventions that would lead to positive online behavioural change.

2. Method

2.1 Sample

Each year, the company NordPass release a list of the 200 most common passwords by country. The list of passwords is compiled using the many cybersecurity incidents (data breaches containing users' password) that occur in 2021. In total, the list rose from 4 terabytes of information and contain 49 countries. The complete list of countries can be found in Appendix A.

The list comprises between 169,656 and 146,837,497 users' account per country. The average time to crack passwords is 2082684.368 seconds (range from 0 to 3,214,080,000 seconds). The majority of passwords included in the list can be cracked in less than a minute (61%). The fact that the mean time to crack a password is high in a country means that high quality passwords were included in the 200 most commonly used: the password can be common, but the overall strength is high.

2.2. Measures

In order to account for the strength of passwords, the mean time to crack the password, which was already included in NordPass passwords list, was observed. Then, several macrosocial variables have been considered to create a model explaining the level of password strength. A total of 29 different measures have been scrutinized in the exploration of possible model explaining performance of countries in password strength. In order to maintain a low risk of overfitting in the model, a limited number of variables can be inserted in relation to the number of cases (49 countries). The literature reports that one predictive variable can be studied for every ten events (i.e., number of countries) [30, 31]. The complete list of measures that have been considered can be found in Appendix B. In order to determine the five variables to be entered in the model, the first step was to do a correlation matrix. This allowed to avoid highly correlated variables to be entered the model together. Then,

different models were tested using an amalgam of variables from the list with a special attention to the important aspect identified in the literature review. The contribution of the variable to the model were very stable and most of them have been chosen because they were predicting password strength. The five variables chosen to enter the final model are named and defined below.

Voice & Accountability (2020)

It is one of six components of governance indicator as stipulated by the World Bank. It reflects perceptions of the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media.

Global Cybersecurity Index (2020)

The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level and is composed of 25 indicators that monitor and compare the level of the cybersecurity commitment of countries with regard to the five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score. It represents the most comprehensive measures of cybersecurity commitment of countries compared to many other measures that are published by corporations [15].

Cybersecurity Exposure Index (2020)

The Cyber Exposure Index is based on data collected from publicly available sources in the dark web and deep web and from data breaches. From this data, signs of sensitive disclosures, exposed credentials and hacker-group activity against companies are identified.

Literacy (2022)

This measures the percentage of adults in a country who are able to read and write their common language. A higher literacy rate is an indication of higher standards of education and the good ability of the population to find formal employment.

GDP per Capita (2020)

Gross domestic product (GDP) is the standard measure of the value added created through the production of goods and services in a country during a certain period. As such, it also measures the income earned from that production, or the total amount spent on final goods and services (fewer imports).

2.3. Analysis

Multiple linear regression (MLR), also known simply as multiple regression, is a statistical technique that uses several explanatory variables to predict the outcome of a response variable. Multiple regression is an extension of linear regression that uses just one explanatory variable. MLR assumes that there is a linear relationship between the dependent variable and the independent variables. It also assumes that the data should not show multicollinearity, which occurs when the independent variables (explanatory variables) are highly correlated. The amount of error in the residuals is similar at each point of the linear model, the observations should be independent of one another and occurs when residuals are normally distributed [32]. All those assumptions have been tested through data observation. The software IBM SPSS 28 was used to do the analysis.

3. Results

Multiple linear regression was used to test if the five macrosocial variables under study significantly predicted password strength. The overall regression was statistically significant ($R^2 = 0.36$, $F = 23.46$, $p = < 0.004$). The model is presented in Table 1.

Table 1. Multiple Linear Regression Results (standard deviation from the mean).

(Constant)	-84076485.358*** (23719091.430)
Voice and accountability	141343.544** (50531.714)
Global Cybersecurity Index	384493.225** (114063.016)
Cybersecurity Exposure Index	49756239.387*** (12339781.870)
Literacy	288067.744* (156148.862)
GDP per Capita	27.981 (71.114)
R-squared	0.36
Number of observations	49
***p<0.001; **p<0.05; *p<0.1	

It was found that Voice and accountability (β=141343.544, p=0.008), Global Cybersecurity Index (β=384493.225, p=0.002), Cybersecurity Exposure Index (β=49756239.387, p=0.000), and level of literacy (β=288067.744, p=0.072) significantly predicted password strength. It was also found that the GDP per capita (β=27.981, p=0.696) did not significantly predict password strength.

4. Discussion

The analysis of the present study help identifies a variety of different macrosocial measures significantly predicting password strength of users: literacy, voice and accountability, level of global cybersecurity, and the level of cybersecurity exposure. Considering past literature on the subject, one variable was surprisingly not associated with an increase password strength, that is, the GDP per capita. Each of those measures are presented in this section in the light of previous work through broader categories: Characteristics of the government, characteristics of users and external variables.

4.1. Characteristics of the Government

Freedom in a country has shown to have an impact on Internet use. Voice and accountability indicator reflects perceptions of the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media. Researchers suggest that greater levels of Internet diffusion are associated with greater levels of voice and accountability [33, 34]. Musa et al. [35] argue that developing countries are more resistant than developed countries to the introduction of technologies that can be used to fight corruption, such as Internet-based technologies. Beyond the use of internet, the impact of freedom is seen on cybersecurity. A strong positive association has been shown between Cybersecurity Capacity Scale and cross-national indicators of citizen perceptions of having voice and accountability [36]. The result of the present study confirms the impact of voice and accountability on password performance as this variable is a good predictor of password strength.

The adoption of technology in a country has been proven to be impacted by many factors including its economic development and growth [37]. Compared to more developed countries, countries that are less developed possess inferior infrastructure, less effective manpower (partly because of low education levels), and business models that have not shifted from the industrial age to the information age [38]. The wealth disparity has also been noted to impact technology adoption, although previous studies have examined the wealth disparity from a micro level [39 – 42]. The result of the present study indicates that wealth disparity does not influence the strong password hygiene as GDP was not significantly predicting password strength. This result might be explained by the sector in which developed countries invest but also other influencing variable like experience in the IT sector. Past studies have shown that countries need to acquire experience with IT before investments begin to

reward the country economically [43]. Benefiting from resources is not enough to explain effective use of technology.

Even if the GDP is not a significant element in citizen password strength, the level of investment of a government in cybersecurity has an impact on security of users. The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level. Researchers have found that as the score for the Global cybersecurity increases, the annual losses due to cybercrime for each country over their Gross National Income decreases [15]. The literature shows that commitment of countries to fight against cybersecurity is profitable economically. The present study goes further by showing the impact on users by demonstrating that this type of investment predicts better password strength performance.

4.2. Characteristics of Users at a Macro-Level

Literacy is an important aspect to consider in this study as it is directly connected to the use of technologies. To seek, evaluate, and use information found on the Internet, readers must navigate through Internet text and apply their knowledge of the reading process [16]. Today's definition of literacy is being broadened to include "literacy skills necessary for individuals, groups, and societies to access the best information in the shortest time to identify and solve the most important problems and then communicate this information" [44]. Most knowledge of late trends on technology is acquired by information found on the Internet. Because bei;00ng knowledgeable is closely related to the capacity to acquire this knowledge (e.g., being able to read), people with low level of literacy can hardly adapt. The challenges faced by low-literacy users when creating and managing passwords are documented and research indicates that they are higher than the general population [18]. Research shows that when users' level of cyber security knowledge increases, so does their cybersecurity behaviour contributing to good hygiene [45]. However, if users are not able to get this information about cybersecurity because of their inability to read, their security will be impacted. The results of the present study are therefore not surprising: when the level of literacy of a population increases, the strength of passwords also increases.

4.3. External Variables Influencing Countries

The results show that the number of cybersecurity incidents exposure of a country is positively associated with password

change. The more a country is under attack, the more people use strong passwords. This suggests that people might be sensible to the importance of protecting data with strong passwords when they are exposed to more cybersecurity incidents. Users are well aware of the meaning of a data breach [46], and it influences their behaviour. For example, there is a highly significant negative market reaction to information security breaches involving unauthorized access to confidential data [21]. In their study on 6,000 users from the United States, after a data breach notification, victims changed their password or PIN (51%) or switched to a new account (24%) [22]. Users are also recognized to be comfortable with proactive password resetting in the event of reuse and sharing information with other identity providers [46]. Therefore, users are aware of what will protect them and are more likely to do it when they are increasingly exposed to incidents. This demonstrates the resilience of users when they live in hostile environment but also the importance of making this information public as this knowledge is a protective factor for users. Mandatory reporting of data breaches introduced in Canada in 2018 [47] might be contributing solution to protect users.

4.4. Limitations

The set of data taken from Nordpass present important limitations as the method used to estimate the time to crack is unspecified. The list was investigated because the mean time to crack appears to be high. Some passwords from the list were weak (e.g., kallynlavallee) but were associated with a cracking time of more than 100 years. This is considered an important limitation of the dataset. However, the unspecified method is used consistently across the countries. Therefore, the metric could be used for the comparative analysis as it is consistent and can be relied upon.

Also, this study takes into consideration a macro perspective of the password strength, but a myriad of element can influence users' choices. The objective of the present study was to explore the influence of different large-scale policies and not individuals' decisional process.

5. Conclusion

The present study helps understand the importance of macrosocial variables on predicting password strength of users. It points toward the fact that some characteristics of the government influences password strength performance of users. For example,

democratic countries and countries in which the government invests in cybersecurity increase the password performance of users. The economic commitment of countries to fight against cybersecurity has been proven to be profitable economically and this study show that it is also associated with password strength of their citizens. Government has an important role to play on the cyber-protection of users whether it is direct (by investing in cyber security) or indirect (by prioritizing democracy and education).

Another important element raised by the present study is that exposure to data breaches increases the strength of user's password. This can be explained by the fact that the population adapt to the threat and this behaviour point toward the importance of mandatory reporting of data breaches by organizations. If they are confronted to mandatory reporting, users are more likely to know about the breaches and continue to adapt their behaviour and it becomes a protection factor.

Through a better understanding of human behaviour in the context of password formulation, our research focuses on identifying common denominators in behaviour that can lead to increased user vulnerabilities in online password formulation. The novelty of our exploratory research lies in our attempt to understand macrosocial variable associated with cybersecurity. The implication of this study concerns the development of policies around cyber security configurations and investment set by nations and institutions.

Funding

This work did not benefit from any funding.

Disclosure statement

The author has no conflict of interest.

References

[1] E. E. Best, "The literate Roman soldier," *The Classical Journal*, vol. 62, no 3, pp. 122–127, 1966.

[2] E. Stobert and R. Biddle, "The password life cycle: user behaviour in managing passwords," presented at the 10th Symposium on Usable Privacy and Security (SOUPS 2014), 2014. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/stobert. [Accessed: July 28, 2023].

[3] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, R. Shay, "Measuring Real-World Accuracies and Biases in Modeling Password Guessability," presented at the 24th USENIX Security Symposium, 2015. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/ur. [Accessed: July 28, 2023].

[4] A. Das, J. Bonneau, M. Caesar, N. Borisov, X. Wang, "The tangled web of password Reuse," in Proc. NDSS, 2014. [Online]. Available: https://www.cs.umd.edu/class/spring2017/cmsc818O/papers/tangled-web.pdf. [Accessed: July 28, 2023].

[5] J. Yan, A.F. Blackwell, R.J. Anderson, A. Grant, "Password memorability and security: empirical results," IEEE Security & Privacy, vol. 2, no. 5, pp. 25–31, 2004. [Online]. Available: doi: 10.1109/MSP.2004.81.

[6] W. Han, Z. Li, M. Ni, G. Gu, W. Xu, "Shadow attacks based on password reuses: A quantitative empirical view," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 2, pp. 309–320, 2018. [Online]. Available: doi: 10.1109/TDSC.2016.2568187.

[7] L. Bosnjak, B. Brumen, "What do students do with their assigned default passwords?," in 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, 2016, pp. 1430–1435.

[8] P. Van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computer and Human Behavior*, vol. 75, pp. 547–559, 2017, doi: 10.1016/j.chb.2017.05.038.

[9] M. Zviran, W.J. Haga, "Cognitive passwords: The key to easy access control," *Computers & Security*, vol. 9, no. 8, pp. 723–736, 1990, doi: 10.1109/JCIT.1990.128279.

[10] C. Yang, J. L. Hung, Z. Lin, "An analysis view on password patterns of Chinese internet users," *Nankai Business Review International*, 2013, doi: 10.1108/20408741311303887.

[11] V. Nedvěd, "Careless society: Drivers of (un) secure passwords," M.A. thesis, Charles University, Prague, 2021. [Online]. Available: https://dspace.cuni.cz/handle/20.500.11956/126879. [Accessed: July 28, 2023].

[12] J. Corrales, F. Westhoff, "Information technology adoption and political regimes," *International Studies Quarterly*, vol. 50, no. 4, pp. 911–933, 2006, doi: 10.1111/j.1468-2478.2006.00431.x.

[13] M. Kummu, M. Taka, J.H. Guillaume, "Gridded global datasets for gross domestic product and Human Development Index over 1990–2015," *Scientific data*, vol. 5, no.1, pp. 1–15, 2018, doi: 10.1038/sdata.2018.4.

[14] L. Fioramonti, L. Coscieme, L.F. Mortensen, "From gross domestic product to wellbeing: How alternative indicators can help connect the new economy with the Sustainable Development Goals," *The Anthropocene Review*, vol. 6, no. 3, pp. 207–222, 2019, doi: 10.1177/2053019619869947.

[15] K. Farahbod, C. Shayo, J. Varzandeh, "Cybersecurity indices and cybercrime annual loss and economic impacts," *Journal of Business and Behavioral Sciences*, vol. 32, no. 1, pp. 63–71, 2020.

[16] E. Schmar-Dobler, "Reading on the Internet: The link between literacy and technology," *Journal of adolescent & adult literacy*, vol. 47, no. 1, pp. 80–85, 2003.

[17] D. Weirich, M.A. Sasse, "Pretty good persuasion: a first step towards effective password security in the real world," *Proceedings of the 2001 workshop on New security paradigms*, 2001. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/508171.508195. [Accessed : July 28, 2023].

[18] C. Rinn, K. Summers, E. Rhodes, J. Virothaisakun, D. Chisnell, "Password creation strategies across high – and low-literacy web users," *Proceedings of the Association for Information Science and Technology*, vol. 52, no. 1, pp.1–9, 2016, doi: 10.1002/pra2.2015.145052010052.

[19] K.M. Hogan, G.T. Olson, M. Angelina. (2020*). A comprehensive analysis of cyber data breaches and their resulting effects on shareholder wealth.* [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589701. [Accessed : July 28, 2023].

[20] A. M. Algarni, V. Thayananthan, Y. K. Malaiya, "Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems," *Applied Sciences*, vol. 11, no. 8, pp. 3678, 2021, doi: 10.3390/app11083678.

[21] K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer security*, vol. 11, no. 3, pp. 431–448, 2003, doi: 10.3233/JCS-2003-11308.

[22] L. Ablon, P. Heaton, D.C. Lavery, S. Romanosky, *Consumer attitudes toward data breach notifications and loss of personal information*. Santa Monica: Rand Corporation, 2016.

[23] C. Braz, A. Seffah, D. M'Raihi, "Designing a trade-off between usability and security: a metrics based-model," IFIP Conference on human-computer interaction, Rio de Janeiro, 2007, pp.114–126. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-74800-7_9. [Accessed : July 28, 2023].

[24] N. Gunson, D. Marshall, H. Morton, M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computer Security*, vol. 30, no. 4, pp. 208–220, 2011, doi: 10.1016/j.cose.2010.12.001.

[25] D. Florencio, C. Herley, "A large-scale study of web password habits," *Proceedings of the 16th international conference on World Wide Web,* 2007. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1242572.1242661. [Accessed: July 28, 2023].

[26] A. K. Kyaw, F. Sioquim, J. Joseph, "Dictionary attack on Wordpress: Security and forensic analysis," Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, 2015, pp. 158–164. [Online]. Available: https://ieeexplore.ieee.org/document/7435522 [Accessed: July 28, 2023].

[27] A. Narayanan, V. Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," Proceedings of the 12th ACM conference on Computer and communications security, Alexandria, 2005, pp. 364–372. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1102120.1102168. [Accessed: July 28, 2023].

[28] A. P. H. de Gusmão, M. M. Silva, T. Poleto, L. C., e Silva, A. P. C. S. Costa, "Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory," *International Journal of Information Management*, vol. 43, pp. 248–260, 2018, doi: 10.1016/j.ijinfomgt.2018.08.008.

[29] H. Taherdoost, "A review of technology acceptance and adoption models and Theories," *Procedia manufacturing*, vol. 22, pp. 960–967, 2018, doi: 10.1016/j.promfg.2018.03.137.

[30] F. E. Harrell, K.L. Lee, D.B. Mark, "Multivariable prognostic models: issues in developing models, evaluating assumptions and adequacy, and measuring and reducing errors," *Statistic in Medecine*, vol. 15, no. 4, pp. 361–387, 1996, doi:10.1002/(sici)1097-0258(19960229)15:4<361::aid-sim168>3.0.co;2-4.

[31] P. Peduzzi, J. Concato, E. Kemper, T.R. Holford, A.R. Feinstein, "A simulation study of the number of events per variable in logistic regression analysis," *Journal of Clinical Epidemiology*, vol. 49, no. 12, pp. 1373–1379, 1996, doi:10.1016/s0895-4356(96)00236-3.

[32] L.E. Eberly, "Multiple linear regression," in *Topics in Biostatistics*, W. T. Ambrosius, Totowa: Humana Press, 2007, pp. 165–187, doi: 10.1007/978-1-59745-530-5_9.

[33] N. M. Jakopin, A. Klein, "Determinants of broadband internet access take-up: Country level drivers," *Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*, vol. 13, no. 5, pp. 29–47, 2011, doi: 10.1108/14636691111160626.

[34] N. Kock, L. Gaskins, "The mediating role of voice and accountability in the relationship between Internet diffusion and government corruption in Latin America and Sub-Saharan Africa," *Information Technology for Development*, vol. 20, no. 1, pp. 23–43, 2014, doi: 10.1080/02681102.2013.832129.

[35] P.F. Musa, P. Meso, V.W. Mbarika, "Toward sustainable adoption of technologies for human development in sub-Saharan Africa: Precursors, diagnostics, and prescriptions," *Communications of the Association for Information Systems,* vol. 15, no. 33, pp. 592–608, 2005, doi:10.17705/1CAIS.01533.

[36] *S.* Creese, W.H. Dutton, P. Esteve-González, R. Shillair, "Cybersecurity capacity-building: cross-national benefits and international divides," *Journal of Cyber Policy*, vol. 6, no. 2, pp. 214–235, 2021, doi: 10.1080/23738871.2021.1979617.

[37] L. Kano, E. W. Tsang, H. W. C. Yeung, "Global value chains: A review of the multi-disciplinary literature," *Journal of international business studies*, vol. 51, no.4, pp. 577–622, 2020, doi: 10.1057/s41267-020-00304-2.

[38] K. Vu, K. Hartley, A. Kankanhalli, "Predictors of cloud computing adoption: A cross-country study," *Telematics and Informatics*, vol. 52, no. 101426, 2020, doi: 10.1016/j.tele.2020.101426.

[39] M. M. Alam, M. W. Murad, "The impacts of economic growth, trade openness and technological progress on renewable energy use in organization for economic co-operation and development countries," *Renewable Energy*, vol. 145, pp. 382–390, 2020, doi: 10.1016/j.renene.2019.06.054.

[40] N. Ameen, R. Willis, M.H. Shah, "An examination of the gender gap in smartphone adoption and use in Arab countries: A cross-national study," *Computers in Human Behavior*, vol. 89, pp. 148–162, 2018, doi: 10.1016/j.chb.2018.07.045.

[41] V. Dutot, V. Bhatiasevi, N. Bellallahom, "Applying the technology acceptance model in a three-countries study of smartwatch adoption," *The Journal of High Technology Management Research*, vol. 30, no.1, pp. 1–14, 2019, doi: 10.1016/j.hitech.2019.02.001.

[42] H. Edquist, P. Goodridge, J. Haskel, "The Internet of Things and economic growth in a panel of countries," *Economics of Innovation and New Technology*, vol. 30, no. 3, pp. 262–283, 2021, doi: 10.1080/10438599.2019.1695941.

[43] N. Terzi, "The impact of e-commerce on international trade and employment," *Encyclopedia of e-commerce development, implementation, and management,* (IGI Global), pp. 2271–2287, 2016.

[44] D. J. Leu, "Our children's future: Changing the focus of literacy and literacy instruction," *The Reading Teacher*, vol. 53, no. 5, pp. 424, 2000.

[45] N. A. G. Arachchilage, S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp.304–312, 2014, doi: 10.1016/j.chb.2014.05.046.

[46] S. Karunakaran, K. Thomas, E. Bursztein, O. Comanescu, "Data breaches: User comprehension, expectations, and concerns with handling exposed data," Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, 2018, pp. 217–234, 2018.

[47] Government of Canada. "Breach of Security Safeguards Regulations," 2018. [Online]. Available: https://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html. [Accessed: July 28, 2023].

Appendix A

Description of password performance by country (N=200).

Country	Mean time to crack in seconds	Minimum	Maximum	Number of users in the list	% of passwords cracked in less than a minute
Australia	59767.98	0	10713600	3083341	79
Austria	1026148.21	0	96422400	695307	68.5
Belgium	22398.15	0	1036800	729661	59.5
Brazil	16137346.42	0	3214080000	4943358	55.5
Canada	4998296.04	0	996364800	5277926	81
Chile	7088718.69	0	1221350400	846354	49.5
China	105039.75	0	2332800	14739683	62.5
Colombia	571740.54	0	96422400	1379631	68.5
Czech R.	81197.92	0	10713600	2288530	65.5
Denmark	489720.11	0	96422400	862571	63.5
Estonia	72966.45	0	10713600	169656	40.5
Finland	24447.04	0	1036800	268236	44
France	67423.91	0	10713600	16160255	54.5
Germany	542675.26	0	96422400	28364318	75.5
Greece	811402.15	0	160704000	861187	80
Hungary	3819.54	0	259200	1159682	48.5
India	1105793.28	0	96422400	8186249	41
Indonesia	43517736.92	0	3214080000	3223828	49
Ireland	2662.44	0	86400	590381	69.5
Israel	10124.02	0	1036800	793908	92
Italy	94203.67	0	10713600	14030845	46.5
Japan	8406.08	0	1036800	1906700	67.5
Korea	949.88	0	86400	910432	84.5
Latvia	23643.52	0	1036800	181072	55

Country	Mean time to crack in seconds	Minimum	Maximum	Number of users in the list	% of passwords cracked in less than a minute
Lithuania	125648.91	0	10713600	406310	40.5
Malaysia	8881.79	0	1036800	1359725	69
Mexico	497790.64	0	96422400	2162221	65.5
Netherlands	767603.60	0	128563200	1636625	56
New Zealand	191147.84	0	32140800	1367054	64
Nigeria	52514.64	0	5356800	757126	40.5
Norway	7633.67	0	1036800	528173	64.5
Philippines	27538.36	0	1036800	2750631	62.5
Poland	10237.31	0	1036800	4412538	46
Portugal	6186350.94	0	996364800	2282038	41.5
Romania	34072.51	0	1036800	1509270	46
Russia	140715.11	0	26784000	146837497	84.5
Saudi Arabia	561965.62	0	96422400	547759	58.5
Slovak Republic	7275.04	0	1036800	702289	51
South Africa	2749.12	0	86400	609061	61.5
Spain	5676283.41	0	996364800	5493452	58.5
Sweden	5091.35	0	172800	1194218	62
Switzerland	82651.48	0	10713600	657863	77
Thailand	560172.86	0	96422400	2055344	65
Total	2082684.37	0	3214080000	3944162	40.5
Turkey	3809402.54	0	514252800	1829898	77
Ukraine	75958.79	0	10713600	529433	78
United Arab Emirates	1515.82	0	86400	7440559	80.5
United Kingdom	6120.43	0	1036800	31229262	84.5
United States	759.68	0	86400	6026634	12
Vietnam	6344824.74	0	996364800	3083341	79

Appendix B

List of the variables that have been tested before determining the final model.

Female participation in workforce (2019)
Freedom of press (2019)
Legal framework's adaptability to digital business models (2019)
Digital skills (2019)
Digital Adoption Index (2016)
DAI Business Sub-index (2016)
DAI People Sub-index (2016)
DAI Government Sub-index (2016)
Number of secured servers (2020)
Mobile cellular subscription (2019)
Voice and accountability (2020)
Political stability (2020)
Government effectiveness (2020)
Regulatory quality (2020)
Rule of law (2020)
Control of corruption (2020)
National Cybersecurity Index (2020)
Global Cybersecurity Index (2020)
Basel AML Index (2020)
Cybersecurity Exposure Index (2020)
Cyber Legislation Rating (2020)
Cyber-Safety Score (2020)
GDP per Capita (2020)
Data breaches (2021)
Internet Users (2020)
IQ (2022)
Literacy (2022)
Education (2022)