An Evaluation of the Password Practices on Leading e-Commerce Websites in South Africa

Silas Formunyuy Verkijika(✉)

Department of Computer Science and Informatics,
University of the Free State, Bloemfontein, South Africa
vekasif@gmail.com

Abstract. Despite the emergence of numerous authentication methods, passwords have remained the dominant authentication mechanism for e-commerce websites. However, password authentications if often widely criticized, especially due to the ease with which it can be compromised by end-users as they often have poor password security behaviors. Nevertheless, a plethora of evidence suggests that the blame should not only be placed on the users as many engage in poor password security practices because they lack sufficient guidance and support on how to maintain good password security behaviors. Indeed, many researchers over the years have shown that user password security behaviors can be significantly enhanced by provided guidance and support on how they can create and maintain strong passwords. Yet, it remains uncertain how well e-commerce website providers have learned these essential lessons. As such, this study is aimed at evaluating the password practices of e-commerce websites in South Africa (SA). After evaluating 37 leading e-commerce websites in the country, it was observed that the majority (92%) of the websites had poor password practices with over 81% offering no guidance for users to enhance their password behaviors. This problem is certainly worse than it should be in this day and age. Consequently, there is an urgent need for e-commerce service providers in SA to improve their password security practices as this is vital for enhancing the password behaviors of their website's users.

Keywords: Password restrictions · Password guidance · e-Commerce website South Africa

1 Introduction

The proliferation of technology has provided numerous opportunities for people to change several aspects of their lives. One such change relates to the way people now conduct their shopping activities using the Internet. This phenomenon, generally termed as electronic commerce (e-commerce) has seen rapid development over the past decade [1, 2]. Many Global e-commerce giants like Amazon and eBay record billions of US dollars in revenue every year. In recent years, there have also been noticeable success stories among e-commerce businesses in South Africa (SA) such as Takealot and Spree [3, 4]. For example, Takealot recorded over 2.9 million transactions from a

H. Venter et al. (Eds.): ISSA 2018, CCIS 973, pp. 104–114, 2019.
https://doi.org/10.1007/978-3-030-11407-7_8

million customers in 2016, generating revenue of R2.3 million [3]. Similarly, Spree reported a 500% growth in 2014 [4]. Additionally, recent estimates suggest that e-commerce transactions in SA amounted to about R10 billion in 2017 [5]. Many factors account for the growth in e-commerce adoption around the world. However, a key factor that still continues to deter user adoption of e-commerce websites around the globe is the perceived security risk associated with e-commerce transactions [1, 6].

One of the most commonly used security measure in e-commerce websites is user authentication using passwords [7]. This is not surprising as passwords have remained the most dominant method of authentication amidst the growing alternatives [7, 8]. In fact, password mechanisms are widely preferred in online websites because of their ease of use, conceptual simplicity, and administrative inexpensiveness [9]. Password authentication as a concept is not a significant security problem in itself, but the greatest weakness of password authentication is the poor practices of the people who create and use these passwords [10]. As a result, passwords are more and more being subjected to a plethora of attacks by malicious individuals as they find it easy to exploit the human weaknesses associated with the creation and management of poor passwords [8]. Many studies over the years have shown that user online passwords are quite predictable and can easily be guessed [8]. This is a significant concern, especially for e-commerce users who store valuable information assets (e.g. credit card information, email addresses, bank account details) in their online e-commerce accounts. Moreover, users have been known to continuously misuse passwords and as such require support and guidance in creating and managing passwords [11, 12].

There is evidence suggesting that the password practices of online websites can be instrumental in improving the password security behaviors of its users [11]. In particular, websites that provide guidance on the creation of strong passwords are likely to help their users to have better password behaviors [11]. Yet, despite the existing evidence, many websites still allow their users to figure things out for themselves, with even leading websites around the world still having poor password practices [12]. Since password use has remained widespread among e-commerce websites amidst the existing alternatives, it is imperative to ensure that best password practices are adopted by the website owners [10, 11]. In SA, little is known about the password practices on the country's leading e-commerce websites. Thus, the question this study seeks to answer is "what password security practices are implemented by SA e-commerce websites".

There is evidence suggesting that online consumers in the SA have poor password practices [13]. Moreover, a key concern observed among SA online consumers is that many tend to perceive themselves as proficient password users, yet their actual password behaviors fall short of expectations [13]. This might suggest the lack of password support practices from the side of the country's online systems, as has been the case in some parts of the world [11, 12]. As such, if e-commerce websites in the country do not provide the needed guidance on good password practices, the users will continue to be at risk of potential exploitations due to their poor password practices. This is important because even if the website itself provides adequate security, but allows poor password practices, then its user's accounts can still be easily compromised as was the case with Apple iCloud [14]. Consequently, it is imperative to assess the current password practices on SA's e-commerce websites as this can provide valuable insights for the industry at large to refine their practices in a manner that will better support their users

and improve their general password security behaviors. As such, the main objective of this is to evaluate the password practices of selected e-commerce websites in SA.

The rest of the paper is structured as follows. The next section presents the literature review which encompasses password restriction and guidance practices. Afterward, the methodology used for the selection and evaluation of the e-commerce websites is presented. Thereafter, the analyses and discussion of the findings are presented. Lastly, the conclusion of the study is presented.

2 Literature Review

There are two common categories of password practices that can be implemented on websites to enhance user password behaviors [10–12]. The first category deals with enforcing numerous restrictions that force the website users to create strong passwords, while the second category deals with the guidance provided by the website on how users can create strong passwords. Each of these categories is discussed below.

2.1 Password Restriction Practices

One of the most common approaches for enhancing the password security behaviors of website users is to enforce restrictions, as this ensures that all users of the website meet some minimum acceptable standards for creating passwords. Good password restriction practices are often common among enterprise information systems; however, these practices are often overlooked by public facing systems like e-commerce and e-government websites [12, 15]. Researchers over the years have emphasized the need for password restriction practices as effective implementation of these practices ultimately leads to the creation of better quality passwords by users [11]. Some of the common restrictions needed on e-commerce websites include enforcing minimum length of the password, preventing the user of the surname as password, preventing the use of the user ID as password, preventing the use of the word "password" or "123456" as a valid password, preventing the use of common dictionary words, and enforcing composition to create complex passwords.

General norms uphold that good passwords should have a minimum of 8 characters and also have a combination of different characters such as upper-case and lowercase letters, symbols and numerals [12, 16, 17]. These aspects help to enforce minimum length and composition thus making the passwords difficult to crack. Additionally, weak passwords are easily cracked with dictionary attacks and as such, it is increasingly advisable to restrict the use of common dictionary words as passwords [8, 16]. Some other essential restrictions include restricting the use of user ID and surnames as this information is often easily available to hackers and can serve as a starting point for cracking the user's password. Preventing the use of a user's surname as the password is particularly important when the website collects such information from the user [12]. Other password choices like "123456" and the word "password" have been widely revealed to be the most commonly used passwords for many years [18]. As such, malicious individuals are likely to use these passwords as a starting point when trying to crack a user's password.

Consequently, it is imperative for e-commerce websites to restrict the use of these common passwords to minimize their user's vulnerability to attacks.

2.2 Password Guidance Practices

In addition to providing restrictions, it is important for a website to provide guidance to users on the creation of quality passwords. This follows from the growing evidence suggesting that user password behavior can be significantly improved when guidance is provided [11, 19, 20]. Furnell [12] emphasised the need for password guidance on websites to be tangible enough to not only tell the user what needs to be done as is the case with restrictions but to further elucidate to the user why it is necessary to create a password in a certain manner. The provision of guidance does not necessarily mean that users will follow it; however, there is empirical evidence to suggest that guidance significantly improves user password behavior [11]. Some of the common guidance approaches used on websites include providing password meters and general tips on the creation of quality passwords [12]. Password meters enable the users to enhance their password behaviors by providing visual feedback on the strength of their passwords. Ur et al. [20] showed that pass-word meters helped users to create quality passwords. However, a key concern has been differences in the quality of password meters as some are poorly developed while others have good and stringent rules [11]. Password meters with stringent rules enable users to create better passwords [11, 20]. As such, it is imperative to ensure that available password meters on websites are well developed. In addition to password meters, websites can include advice to users on the creation of quality passwords. An example of password tips used by Amazon is presented below (Fig. 1).

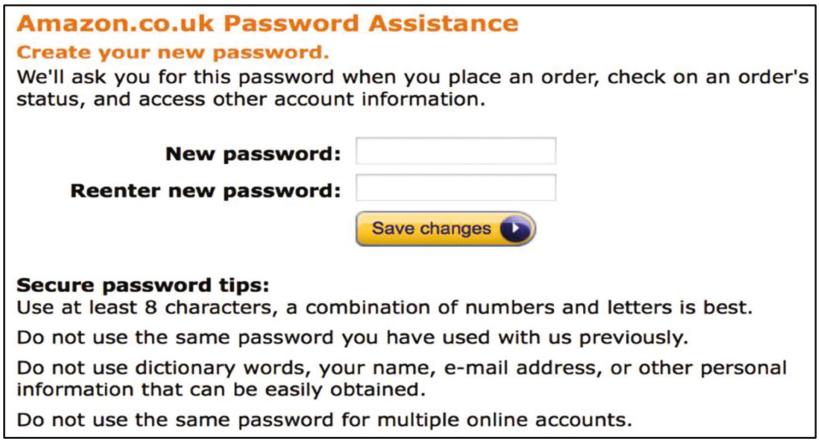

Fig. 1. Password assistance by Amazon [12]

3 Methodology

3.1 Selection of e-Commerce Websites

The present study aimed at evaluating the password practices of SA e-commerce websites. Although there are many e-commerce websites in SA, there is no comprehensive database for these websites. However, there have been significant efforts by companies like uAfrica and Pricecheck to evaluate and recognize leading SA e-commerce websites through their e-commerce awards. In 2015, uAfrica (www.uafrica.com) released a list of 50 leading e-commerce websites in SA [21]. This study used this list as the primary database for recognized e-commerce websites in the country. Even though the 50 leading e-commerce websites do not represent all e-commerce websites in the country, focusing on leading websites have two major advantages. Firstly, the password practices of leading websites are likely to influence a wide pool of e-commerce end users as these websites attract the majority of e-commerce traffic in the country. Secondly, other providers often mimic the practices of leading websites and use them as standards for their own websites [12]. Thus, the password practices in leading websites could reflect that of the majority of SA e-commerce websites. Among the 50 leading e-commerce websites by uAfrica, 5 were eliminated from the present study because they were offline, while another 8 were eliminated because they did not have signup functionality. As such, a total of 37 e-commerce websites were evaluated in the present study (See Appendix).

3.2 Evaluation Approach

The password practices of the leading websites were evaluated by creating user accounts on the websites and using the process to review the different practices adopted by the website. This approach is similar to the guideline review approach commonly used in usability studies where an interface is evaluated against a set of guidelines to determine if it performs as expected. In the present study, the guidelines used were those that have been validated in the password security literature. These guidelines focused on two domains namely (1) does the website provide relevant restrictions to ensure users create good passwords and (2) does the website provide guidance and support that aims to enhance user password selection practices. The outcome of the assessment is presented in the next section.

4 Analyses and Discussion

4.1 Restrictions Implemented by SA e-Commerce Websites

One of the most common password restrictions implemented on most websites is the minimum length of the password. Table 1 presents the information on password restrictions among SA e-commerce websites.

It was observed that 14% of the websites had no password length restriction. It is quite uncommon, although not impossible to find leading websites that do not implement minimum password length [10, 12]. Short passwords are quite easy to crack,

Table 1. Minimum length restriction

Length Restriction	Frequency	%
None	5	14
4	2	5
5	9	24
6	17	46
7	1	3
8	2	5
12	1	3

so failing to provide password length restrictions is quite concerning. Also, it was seen that a total of 11 websites had their minimum length restrictions below 6. This is also a very weak practice as it is generally advisable to set minimum password length at 8, even though it is not uncommon to find that a majority of websites use 6 as the minimum password length. The majority of the websites (45%) set their minimum password length at 6 characters. This is not surprising as [12] found that 60% of the 10 world's leading websites he evaluated also set minimum password length at 6 characters. However, some of the websites like Google and Yahoo restrict their minimum passwords to 8 characters, which is in line with security recommendations. Among the SA e-commerce websites evaluated, only 2 (5%) used 8 characters as the minimum password length while one website required user passwords to have a minimum of 12 characters. While it is interesting to see a website that requires a minimum length of 12 characters, it is important to note that this is an acceptable practice used in many websites around the world [22]. In fact, some security experts even suggest that the minimum password length should be increased to 14 characters, especially because of the existence of rainbow tables where it is argued that the likelihood of finding a hash value for any password below 12–14 on an existing rainbow table is very high [23].

Table 2 presents the evaluation of other vital restrictions that websites can implement to improve password behavior.

Table 2. Other restrictions and enforcement of composition

Type of restriction	Websites enforcing the restriction	Websites not enforcing the restriction
Surname	1 (3%)	36 (97%)
"123456"	5 (13%)	32 (87%)
"password"	5 (13%)	32 (87%)
Dictionary words	4 (11%)	33 (89%)
Composition	4 (11%)	33 (89%)

It was observed that only 1 website (3%) restricted the use of the user's surname as a password. Also, five websites each had restrictions for use of common passwords like "123456" and "password". Additionally, four of the websites restricted the use of common dictionary words while four enforced the use of composition in creating

passwords. Similar to [12], websites were considered to enforce composition when they required passwords to have characters in each of the following groups: upper case letter, lower case letter, numeric character, and special/punctuation characters. These findings are concerning as such poor password practices used by the majority of websites could ultimately result in users creating weak passwords that can be easily cracked.

Passwords with composition are usually considered to be highly secure as they are difficult to crack, especially when the composition includes upper and lower case letters, alphanumeric characters, and numbers [8, 20, 24]. As such the fact that up to 89% of the evaluated websites do not have password composition rules is a key concern as users of these websites are likely to have weak passwords that can be easily cracked. Nevertheless, some have argued that passwords with compositions even though more secure are difficult to memorize and use. Thus, website users do not prefer them [25, 26]. This could explain why the majority of the websites do not use password composition. However, as security concerns are vital for the adoption of e-commerce solutions [1, 6], it is imperative to ensure that users create strong passwords. It is quite possible for users to create complex passwords that they can easily remember [24]. One of the evaluated websites was highly security conscious by enforcing strong composition rules with users having to create a strong password with a minimum of 12 characters. The website even helped to auto-generate a complex password for users, which they can change when they log into the system. However, a key drawback to this approach is that system generated passwords are often more difficult to remember as they are random characters that offer little meaning compared to user-generated passwords. Nonetheless, the auto-generated passwords could serve as a guide for the users to understand how to effectively apply password composition rules.

4.2 Password Guidance Practices by SA e-Commerce Websites

In total, it was observed that 5 websites implemented password meters. Likewise, 5 websites also provided password tips for users as guidance for creating strong passwords. However, these websites were not necessarily distinct. In fact, 3 of the websites had both a password meter and provided tips for creating strong passwords, while 2 only implemented password meters and another 2 only provided password tips.

Password meters and tips have been shown to improve user password behavior in several studies [11, 19, 20]. Password meters and tips are important because they address some of the limitations of enforcing restrictions. For example, even though most of the websites set the password minimum length to 6 characters, they allowed common passwords like “123456” and “password” as well as common dictionary words as passwords. If such websites used a password meter or tips, their users will be able to know that such passwords are weak and still vulnerable to being cracked. The fact that only 3 websites (8%) use both a password meter while also providing password tips clearly indicates the lack of password guidance practices among these websites. This is a cause for concern as it indicates the existence of minimal efforts to improve the password security behaviors of their users. When password strength meters and password tips are implemented on a website, even novice users tend to effectively use the guidance to create strong passwords as they tend to feel in control of the situation.

5 Conclusion

Despite the criticisms of passwords, they have remained the primary authentication choice for most websites. Generally, end users are often criticised for misuse of passwords due to their poor password security behaviors. However, putting the blame on end-users is somewhat overstated, especially when service provides totally ignore the role they play in promoting poor password security practices. Indeed, many online service providers have highly overlooked essential lessons on how to improve the password security posture of their users. As highlighted above, the provision of password support and guidance mechanisms on websites can significantly improve the password security behaviors of users. Yet, many service providers continue to deploy e-commerce websites without providing any support/guidance or enforcing relevant restrictions that can enhance the security behaviors of end-users. As such, documenting the extent of this problem is the first step in creating awareness for service providers so that they can review and improve their current password practices. The present study is the first to document the extent of this problem among SA e-commerce websites.

The evaluation of SA e-commerce websites clearly showed the need for such studies as many of the websites are yet to adopt good password security practices. The implications of the findings are threefold. Firstly, evidence from SA shows that online consumers have poor password security behaviors. It is highly probable that their poor password behaviors could be a direct result of the lack of support and guidance in the password creation process as argued by many researchers. As such, e-commerce service providers need to play an active role in enhancing the security behaviors of their consumers by implementing good password security practices. Secondly, the extent of the problem suggests the need for training of website developers and designers in the country on the need for and implementation of good password security practices. Lastly, policymakers are also encouraged to consider enforcing legislation that mandates e-commerce websites to maintain a minimum set of password practices as this will be imperative in enhancing end-user security behaviors. Also, e-commerce websites owners should be encouraged to adopt multi-factor authentication as a means to limit the weaknesses of password mechanisms.

The study has two key limitations that also offer avenues for future studies. Firstly, the evaluation of password practices was limited to password practices during the initial registration with an e-commerce website. As such, other stages like password recovery and changing existing passwords were not covered. Future studies can also examine password practices at these other stages. Secondly, the study was limited to 37 e-commerce websites in South Africa. This only depicts a fraction of e-commerce websites in SA. As such, future studies can conduct an evaluation using a more comprehensive list of e-commerce websites in the country.

Appendix

Website Name	Website URL
Action Gear	https://www.actiongear.co.za/
Bidorbuy.co.za	https://www.bidorbuy.co.za/
Esque	https://www.esque.co.za/
Flook Sporting Deals	https://www.flook.co.za/
Futurama	https://www.futurama.co.za/
Gemboree	http://www.gemboreeshop.com/
Groupon South Africa	https://www.groupon.com/
HomeChoice	https://www.homechoice.co.za/home.aspx
iToys	https://www.itoys.co.za
Juniva.com	https://www.supps365.co.za/
Kapas Baby & Toddler	https://www.kapasbaby.com
Legwear Safari	http://www.legwearsafari.co.za
LekkeSlaap	https://www.lekkeslaap.co.za/
Loot.co.za	https://www.loot.co.za/welcome
Macaroon Collection	https://macarooncollection.co.za/
Mantality	http://www.mantality.co.za/
Norman Goodfellows	https://www.ngf.co.za/
Orms Direct	https://www.ormsdirect.co.za
Port2Port	https://www.port2port.wine/
Quicket	https://www.quicket.co.za/
Raru	https://raru.co.za/
Red Square	https://www.redsquare.co.za/
RunwaySale	https://www.runwaysale.co.za
SassyChic.co.za	https://www.sassychic.co.za
Seeds for Africa	https://www.seedsforafrica.co.za/
Simplicity	https://simplicity.co.za
Spree	https://www.spree.co.za/
Superbalist.com	https://superbalist.com/
Takealot.com	https://www.takealot.com/
TravelGround	https://www.travelground.com/
Travelstart	https://www.travelstart.co.za/
WebAntics Online	https://www.webantics.com/
Wellness Warehouse	https://www.wellnesswarehouse.com/
Wootware	https://www.wootware.co.za/
Yuppiechef.com	https://www.yuppiechef.com/
Zando	https://www.zando.co.za/
ZumbaWear South Africa	http://zumbawearsouthafrica.co.za

References

1. Kim, Y., Peterson, R.A.: A meta-analysis of online trust relationships in e-commerce. J. Interact. Mark. **38**, 44–54 (2017)
2. Verkijika, S.F.: Factors influencing the adoption of mobile commerce applications in Cameroon. Telematics Inform. **35**, 1665–1674 (2018). https://doi.org/10.1016/j.tele.2018.04.012
3. Mybroadband.co.za: Takealot's plan to grow its R2.3-billion annual revenue (2017). https://mybroadband.co.za/news/business/229775-takealots-plan-to-grow-its-r2-3-billion-annual-revenue.html. Accessed 26 Apr 2018
4. Fin24.Com: Spree records 500% growth (2014). https://www.fin24.com/Companies/Retail/Spree-records-500-growth-20140221. Accessed 26 Apr 2018
5. Smith, C.: How e-commerce is exploding in SA (2018). https://www.fin24.com/Economy/how-ecommerce-is-exploding-in-sa-20180316. Accessed 26 Apr 2018
6. Ndyali, L.: Adaptation and barriers of e-commerce in Tanzania small and medium enterprises. Dev. Country Stud. **3**(4), 100–105 (2013)
7. Herley, C., Van Oorschot, P.: A research agenda acknowledging the persistence of passwords. IEEE Secur. Priv. **10**, 28–36 (2012)
8. Shen, C., Yu, T., Xu, H., Yang, G., Guan, X.: User practice in password security: an empirical study of real-life passwords in the wild. Comput. Secur. **6**, 130–141 (2016)
9. Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S., et al.: Sp 800-63-1: electronic authentication guideline. In: National Institute of Standards and Technology (2011)
10. Furnell, S.: An assessment of website password practices. Comput. Secur. **26**, 445–451 (2007)
11. Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., Li, N.: Enhancing security behaviour by supporting the user. Comput. Secur. **75**, 1–9 (2018)
12. Furnell, S.: Password practices on leading websites–revisited. Comput. Fraud Secur. **12**, 5–11 (2014)
13. Butler, R., Butler, M.: The password practices applied by South African online consumers: perception versus reality. S. Afr. J. Inf. Manage. **17**(1), 1–11 (2015). Art. #638
14. Clover, J.: Celebrity iCloud accounts compromised by weak passwords, not iCloud breach (2014). www.macrumors.com/2014/09/02/apple-no-celebrityicloud-breach/. Accessed 28 Apr 2018
15. Verkijika, S.F.: Evaluating and improving the usability of e-government websites in Sub-Saharan Africa for enhancing citizen adoption and usage. Ph.D. thesis, University of the Free State, Bloemfontein, South Africa (2017)
16. Greene, S.S.: Security Program and Policies: Principles and Practices. Pearson, Indianapolis (2014)
17. Guo, Y., Zhang, Z.: LPSE: lightweight password-strength estimation for password meters. Comput. Secur. **73**, 507–518 (2018)
18. Splashdata: Worst passwords of 2017: Top 100 (2017). https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf. Accessed 8 July 2018
19. Segreti, S.M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., et al.: Diversify to survive: making passwords stronger with adaptive policies. In: Symposium on Usable Privacy and Security (SOUPS) (2017)
20. Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., et al.: Design and evaluation of a data-driven password meter. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 3775–3786. ACM (2017)

21. Stuart, T.: 50 of South Africa's top e-commerce sites (2015). http://ventureburn.com/2015/08/50-south-africas-top-ecommerce-sites/. Accessed 1 Apr 2018
22. Rankin, K.: Why final passwords are at least 12 characters (2016). https://getfinal.com/company-news/2016/03/08/why-final-passwords-are-at-least-12-characters/. Accessed 2 May 2018
23. Gamby, R.: Minimum password length best practices: are 14-character passwords necessary? (2012). https://searchsecurity.techtarget.com/answer/Minimum-password-length-best-practices-Are-14-character-passwords-necessary. Accessed 2 May 2018
24. Cross, M.: Social Media Security: Leveraging Social Networking While Mitigating Risk. Syngress, Waltham (2014)
25. Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., et al.: Of passwords and people: measuring the effect of password-composition policies. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2595–604 (2011)
26. Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., et al.: Encountering stronger password requirements: user attitudes and behaviors. In: Proceedings of the Sixth Symposium on Usable Privacy and Security, pp. 1–20 (2010)