Password Policies Adopted by South African Organizations: Influential Factors and Weaknesses

Pardon Blessings Maoneke[1(✉)] and Stephen Flowerday[2]

[1] Namibia University of Science and Technology, 13 Storch Street, Windhoek 9000, Namibia
blessings83@gmail.com
[2] Rhodes University, Prince Alfred Street, Grahamstown 6140, South Africa
s.flowerday@ru.ac.za

Abstract. Organizations worldwide are revisiting the design of their password policies. This is partly motivated by the security and usability limitations of user-generated passwords. While research on password policies has been ongoing, this has taken place in the Global North. Accordingly, little is known about the strengths and weaknesses of password policies deployed in the Global South, especially Africa. As such, this study researched password policies deployed on South African websites. Password policies of thirty frequently visited websites belonging to South African organizations were analyzed. Our observations show diverse password requirements. Even though the desire for strong passwords is the dominant motivator of complex password policies, South African organizations often adopt obsolete measures for attaining password security. The ten most common passwords in the literature were considered acceptable on most sites. In addition, some sites did not explicitly display password requirements and only a few sites adopted measures for providing real-time feedback and effective guidance during password generation.

Keywords: Password · Password usability · Password security
Password policy · Password strength meter

1 Introduction

Research findings from the analysis of more than 100 million English and Chinese passwords that were leaked into the public domain exposed various security limitations associated with user-generated passwords. In response, organizations are adjusting their password policies while institutions responsible for the promulgation of authentication guidelines are revising their perceptions on password strength and usability [1–3]. However, the literature reports inconsistency between the complexity of deployed password policies and prescribed best practices [1, 3]. For example, institutions that are expected to adopt complex password policies have simple policies and vice versa. In addition, passwords assumed strong by one password policy may be considered weak by another [3]. This is exacerbated by research that is focused on password policies (password strength meters and rule-based policies) deployed on Global North websites

H. Venter et al. (Eds.): ISSA 2018, CCIS 973, pp. 30–43, 2019.
https://doi.org/10.1007/978-3-030-11407-7_3

[3]. Little is known about password policy implementation in other countries, especially the Global South with a focus on Africa. As such, this study investigated password policies deployed by South African based organizations. The aim of this study was to identify factors motivating the adoption of password policies, as well as to evaluate the strengths and weaknesses of deployed password policies [4]. It was deemed important to establish the influence of international best practices and previous research findings on South African organizations' adoption of password policies. South Africa is Africa's most industrialized economy. It was therefore worth researching how the adoption of password policies is comparable to international trends. Such findings can play a leading role in informing authentication policy designs and implementation.

2 Background and Related Work

This study used the National Institute of Standards and Technology's (NIST) Digital Identity Guidelines and a study by Florêncio and Herley [1] to identify factors influencing the adoption of complex password policies. The NIST, a United States based research institute, has published various editions of Special Publications (SPs) on password guidelines that have been influential in shaping the design of password policies since 2006. In addition, guidelines in the NIST SPs complement propositions in prominent international electronic authentication frameworks for Australia, India and the European Union [5]. While the NIST SPs consider security to be the major factor influencing password policy design, Florêncio and Herley [1] propose a holistic approach for understanding the factors influencing the design of password requirements. Thus, the NIST SPs and Florêncio and Herley's [1] study give a balanced view on the factors that influence password policies.

2.1 NIST SP: 800-63-3 Digital Identity Guideline

The NIST SPs on electronic authentication guidelines have been influential in guiding password policies. Early versions of the NIST SP on electronic authentication guidelines were inspired by Shannon entropy to estimate password strength. It was assumed that the use of different character sets would enhance password strength. Studies conducted a few years later, starting with Wier et al. [6], proved that entropy was not a good measure of password strength. In response to these findings, NIST made modifications to its conceptualization of password strength and usability as reflected in the SP editions released in 2013 and 2017 [2, 7]. In 2017, NIST released an SP 800-63-3, which is considered a "suite of volumes" with the following three documentations for guiding user authentication:

- SP 800-63A Enrolment and Identity Proofing,
- SP 800-63B Authentication and Lifecycle Management
- SP 800-63C Federation and Assertions [2].

NIST indicated that the SP 800-63A and 800-63B could be used in the private sector while US federal agencies are required to also incorporate specifications in the SP 800-63C. This study focuses on authentication; hence, it is limited to the 800-63B

of the SP 800-63-3 Digital Identity Guideline. According to NIST, service providers should evaluate the risks associated with their online transactions to establish assurance levels that will guide choices regarding authentication complexity [2]. Memorized secrets such as passwords are among the authentication measures considered by NIST. Propositions in SP 800-63B suggest a shift from NIST's view of password strength that was traditionally centered on the use of different character sets. Today, system designers are encouraged to make use of a blacklist with common passwords and dictionary words [2]. The use of keyboard patterns and personal information during password generation is strongly discouraged. In addition, user-generated passwords should be at least eight characters long. Password policies are to be designed in such a way that they provide feedback and guidance to users as they generate new passwords. These propositions to some extent concur with suggestions in the literature that are being advanced with the aim of enhancing password security and usability. For example, Dropbox's zxcvbn algorithm for guiding password generation makes use of a blacklist, guards against the use of keyboard patterns, personal information and gives real-time feedback on the reasons for password rejection [7]. Similarly, Shay et al. [8] found that using a blacklist promotes password strength even though it is less usable. Furnell [9] suggests a need to provide feedback and guidance during password generation. Password feedback make provisions for ratings on password strength, while password generation guidance goes on to provide "more explanatory detail about how well the resulting password would serve" users [10, p. 5].

2.2 Factors Influencing the Adoption of Complex Password Policies

Florêncio and Herley [1] researched factors influencing the adoption of different password policies. Their analysis of seventy-five websites found that websites are adopting diverse password policies. This finding was corroborated by research findings from studies conducted in the Global North [3, 4, 9]. Florêncio and Herley [1] observe that factors assumed to be of importance when deciding on the complexity of password policies were irrelevant. The "size of the site, the number of user accounts, the value of the resources protected, and the frequency of non-strength related attacks all correlate very poorly with the strength required by the site" [1, p. 1]. These findings suggest that security-related factors may not inspire the adoption of complex password policies. Other studies found the security requirements determined by potential risks not sufficient to motivate the adoption of complex password policies [3, 4]. Rather, these organizations are mainly influenced by the usability of adopted password policies with the aim of encouraging users to sign up irrespective of security implications [9].

3 Methodology

This study adapts and modifies an approach used by Florêncio and Herley [1] and Wang and Wang [3] in which sites are selected for analysis, measuring the strength of password policies. These are explained next.

3.1 Selecting Sites and Password Policy Analysis

Considerations of popular sites were based on online traffic ranking using Alexa's top sites list (www.alexa.com/topsites/countries/ZA). This approach is widely used in the literature [3, 9, 11]. Accordingly, South African websites that appeared among the first one hundred and fifty (150) on Alexa's list were considered. The focus was on websites owned by companies with headquarters based in South Africa. The idea was to establish the perception of South African organizations on password strength and usability. Besides, password requirements on websites of most multinational companies such as Dropbox, Google, YouTube and Yahoo have received wide research [1, 3, 5, 9, 11]. Limiting websites to those appearing among the top one hundred and fifty allows this study to base its conclusions on the most visited [11] South African sites. It is expected that these sites influence a number of end-users and may set a standard [9] on password requirements for South African sites. In addition, their popularity might inspire a desire to conform to international password requirement best practices.

Once the websites were identified, they were categorized according to different themes based on web services. For each site, password requirements were investigated focusing on "length limits, charset requirement, whether rules are explicitly stated, whether allowing special characters, whether using a blacklist, whether deterring the use of personal data" [3, p. 10], password creation guidance and the use of a password strength meter. An attempt to generate a password or create an account was made where possible to enhance the understanding of password requirements [1].

3.2 Password Policy Strength

The strength of passwords generated through the guidance of a password policy determines the strength of the policy [1, 3]. The literature suggests two common password strength measures, namely, entropy and password guessing [3, 6, 8]. This study adopts a formula in Florêncio and Herley [1] that is inclined towards ascertaining password entropy to measure password policy strength. The formula expresses password strength in terms of bits. The formula is stated as follows:

$$N_{min} Log_2 C_{min} \tag{1}$$

Where:

N_{min} is the minimum password length and

C_{min} is the cardinality of the minimum character set required [1, p. 2].

This study used a US standard keyboard with an ASCII character set that includes twenty-six letters (lower or upper case), ten digits, and thirty-three non-alphanumeric special characters [12]. For example, the bits of a password rule that requires at least six characters is computed as follows:

$$6. \log_2 26 = 28.2 \text{ bits}$$

4 Findings and Results

This section reports on the findings from the reviewed sites.

4.1 Reviewed Sites

Alexa's top one hundred and fifty list shows that there are forty-seven websites matching this study's definition of websites owned by South African organizations. The remaining sites are owned by multinational organizations. However, seventeen of the selected forty-seven sites were not considered for further analysis in this study. The reason being that eight had no provisions for password generation, while two could not be opened as the Uniform Resource Locator was not found. The password generation requirements of the remaining sites (seven) could not be accessed as they were restricted to clients only. In the end, the password policies of thirty websites were analyzed. An attempt to create passwords was done on twenty-four of the thirty websites considered for this study. The reviewed sites were categorized according to themes based on web services as follows: e-Commerce (5), universities (4), news (4), banks (3), job vacancies (3), sites of Information and Technology (IT) corporations (2), television services (2), real estate (2), classified adverts (2), electronic mail (email) site (1), betting site (1) and an electronic government (e-Government) site for tax filing. Section 5 and the Appendix provides an overview of findings on the full set of the analyzed sites.

4.2 The Diversity of Password Policies and Strength

Data analysis shows that South African organizations deploy diverse password policies. These include password strength meters and rule-based password policies. Of all the sites analyzed, 10% used password strength meters and 90% used rule-based password policies. In addition, 85.2% of the sites using rule-based password policies had password composition rules requiring different character sets. Only 7.4% of sites of those assuming a rule-based password policy had a provision for a Single Sign-On (SSO), while the remaining 7.4% had provisions for users to either use a user-generated rule-based password or SSO. Findings in this study concur with the literature on the dominance of rule-based password policies and the diversity of password policies [1]. Table 1 shows the minimum password policy strength according to entropy that was computed using the formula in Sect. 3.2. Password policy strength varied across and within the analyzed categories, as shown by the entropy in the least and highest password policy strength columns.

Entropy was computed for sites with rule-based password policies. Table 1 reports on the lowest, median and highest minimum password policy strength observed for each password category analyzed. For example, the lowest password policy strength observed on all e-Commerce sites could encourage users to generate a password that is at least 23.5 bits. However, an e-Commerce site with the highest minimum password policy strength could see users generating passwords of at least 41.4 bits. Only the lowest password policy strength was reported in cases where the computed entropy was

Table 1. Password policy strength of researched categories of sites

Site Category	Minimum password policy strength (bits)		
	Least password policy strength	Median password policy strength	Highest password policy strength
*e-Commerce	23.5	31.03	41.4
Universities	28.2	55.3	78.8
*News site	23.5	33.1	47.6
Bank	37.6	46	52.7
*Job vacancies	4.7	4.7	4.7
IT corporations	47.6	47.6	47.6
Television services	28.2	28.2	28.2
*Real estate	28.2	32	35.7
Classified adverts	4.7	18.8	32.9
email	23.5	–	–
Betting site	31	–	–
e-Government	37.4	–	–

Note: *Some of the sites use SSO or a password strength meter, hence the strength of their policies was not computed.

for a single website, as shown in Table 1. Table 1 shows that sites of universities, IT corporations and banks had, on average, the strongest password policies.

It should be noted that there was a keen interest in testing the guessing resistance of candidate passwords generated under different policies. This study used an open source zxcvbn password-guessing algorithm. Zxcvbn is an outstanding password strength measure deployed today [4]. However, the majority of passwords that were found acceptable on researched policies have already been found weak and easy to guess in other studies. For example, passwords that were found acceptable by researched password policies include 1234567, password, qwerty, iloveyou and 12345678 and are, in fact, among the top ten of millions of leaked passwords [13]. These passwords were considered relevant on more than 60% of the researched sites to which the researchers had access to generate a candidate password. The Appendix shows candidate passwords found acceptable at each site researched.

4.3 Password Policies and Influential Factors

This section reports on the characteristics of researched password policies according to specifications in Sect. 3.1. An analysis of factors influencing the adoption of complex password policies is included. The analysis and findings are presented according themes based on web service:

University Sites. All the analyzed university websites had rule-based password policies together with a strict password minimum length requirement. All the sites clearly indicated password rules in advance. For example, one of the university websites

required that passwords be at least six characters long with no additional requirements for character sets. Another university recommended passwords of at least eight characters with three additional character set requirements involving the use of lowercase and uppercase letters, a number and symbol. On the other hand, the other two university sites recommended long passwords of at least twelve and fourteen characters. The twelve-character password policy had additional requirements that users include upper and lowercase letters together with a number and special characters. However, the fourteen-character password policy does not require the inclusion of different character sets but the use of user identity details and keyboard patterns is restricted.

The analysis of password policies in this study was limited to university accounts for students. These accounts provided access to personal information including student results and emails. Accordingly, the Authentication Assurance Level (AAL) for university sites was considered to be AAL2 according to NIST. Our observations suggest that password policies on university sites are influenced by a desire to enhance password security. Florêncio and Herley [1] reason that, once enrolled at a university, students have no alternative source of services except from the institutions they are enrolled at. Hence, such institutions often have complex password requirements.

Bank Sites. The analyzed sites belong to commercial banks and had rule-based password policies. User-generated passwords are expected to be at least eight characters long, have a number and uppercase and lowercase letters. One of the three bank sites had additional requirements for users to include a special character in their passwords, as well as blacklisting passwords based on keyboard patterns. All the researched banks published their password rules for users to see during password generation. Researchers managed to generate a password under one of the researched bank site's password policy. While the bank had provisions for real-time feedback during password generation and blocking certain keyboard patterns, there was no provision for password guidance. In addition, none of the bank sites used a blacklist to prohibit passwords based on common dictionary words or personal information.

A review of the online banking services offered suggests that the AAL for the reviewed banks is at level three (AAL3) according to NIST [2]. Security breaches of passwords for accessing online banking services have potentially high financial loss and inconvenience. Hence, strong passwords should be used for accessing online services classed AAL3. Accordingly, complex password policies on bank sites reflect that the value of protected resources has an influence on password policy complexity.

e-Commerce Sites. One of the five researched e-Commerce sites had a password strength meter with the remaining sites using a rule-based password policy. In particular to the site with a password strength meter, the implemented meter appeared sensitive to the use of different character sets when determining password strength. For example, password *"passwo"* was considered very weak while *"Password12"* was considered better. The password *"P@55word"* was regarded as strong. Three e-Commerce sites with rule-based password policies insisted on the creation of passwords that are at least five or six or eight characters long. Only one e-Commerce site used a Facebook SSO. Diversity in rule-based password policies for this category saw some sites recommending a minimum password length without any other additional requirements. However, one of the researched e-Commerce sites using a rule-based

password policy required that users mix numbers with any other character set. In addition, a small blacklist was included that blocked the use of the word *"password"* in user-generated passwords. Hence "*password1*" and "*pa55word*" were not acceptable. However, the policy succumbed to other practices of character replacement, use of common words, keyboard patterns and personal information. For instance, *"111111p", "p@55word"* and *"iloveyou1"* were considered relevant passwords.

An analysis was carried out to establish the influence of password strength and usability on e-Commerce password policies. Given that there is a potential for financial loss and inconvenience as a result of compromised passwords, e-Commerce authentication assurance was classed AAL2 according to NIST. However, even though e-Commerce sites implemented password strength requirements, these requirements are fairly stringent, which points towards a need to maximize password usability. Florêncio and Herley [1] suggests that e-Commerce businesses thrive on the high volumes of clients that visit their sites; hence, password requirements are likely to be relaxed in order to reduce the chances of dissatisfaction.

News Site. All the news sites researched in this study use rule-based password policies. Only one site uses a Facebook SSO facility while the remaining sites make use of a password composition policy. Password composition policies require that users generate a password that comprises of at least five or six or eight characters. There are no character class restrictions on the five and six-character password sites, hence *"passw"* and *"password"* are seen as good passwords. However, the eight-character password policy insists that users include numbers, uppercase and lowercase letters. Attempts to generate a password showed that the inclusion of an uppercase letters in the password was not enforced despite it being one of the requirements.

Further analysis on news sites shows that users can log into these sites to make comments "and personalize news, weather and listings". Our evaluation of these websites suggests that there are very limited consequences for the organization and users as a result of password security breaches. Hence, an AAL for this category was set at AAL1. As suggested by Florêncio and Herley [1], the implementation of authentication on the news sites appears to be motivated by password usability. The news site accepts third-party adverts; hence, the need for increased readership and the presence of alternative online news sources further emphasize the need for usable authentications.

Television Service Sites. The companies involved in television broadcasting implement a password strength meter and a rule-based password policy for guiding password generation. The password strength meter has provisions for real-time feedback and password generation guidance. The password generation algorithm can warn users if the password is found among popular passwords and names or passwords are based on keyboard patterns and simple character replacement such as L33T. Password length has an effect on password strength as long as the phrases or words used are not among those blacklisted. It was observed that one could only fill the strength bar if the password was at least twelve characters long. The other television site required users to generate a password that is at least six characters long with no specific character class requirements. Users have an option for an SSO using Facebook account.

Our observations show that password breaches on the television service provider site may expose users' personal information and grant access to online television viewership. Accordingly, the authentication assurance requirements of this site were rated AAL2. Observations show that the password policies of the researched sites attempt to find a balance between usability and security. One of the sites implemented password generation requirements according to recent suggestions by NIST and zxcvbn.

Real Estate Sites. The real estate sites make use of a rule-based password policy: SSO using a Facebook or Google account and provisions for user-generated passwords of at least six characters. Of the two researched real estate sites, one has additional requirements for including upper and lowercase letters together with a special character or number in a password. However, these password rules are not displayed for users to see. Password rules only appear after one has failed to generate a password that meets any of the requirements upon clicking the register button. Further, some of the common passwords such as *"passwords"* or *"Password5@"* are blacklisted by one of the real estate sites while the other site found the passwords acceptable. However, the password policy with a blacklist succumbs to character replacement, passwords based on keyboard patterns and common words. For example, *"Ilove1995"; "P@s5word"* and *"Qwerty123"* were found acceptable.

Further analysis showed that there are limited consequences of password security breaches on the real estate sites. As such, real estate sites were classed AAL1 in terms of authentication assurance level. This explains the more usable password requirements employed on the researched sites.

IT Corporation Sites. The IT corporation sites researched in this study have rule-based password policies. Users are required to generate a password that is at least eight characters long with at least one upper or lowercase letter or a number. Password requirements are displayed prior to password generation. The password policy demonstrated good use of feedback during password generation. For example, one of the sites had ticks appearing after each password generation rule was met so that users are provided with instant feedback and are guided on their progress. However, no reason was given for including different character sets. Users create accounts for updating their profile, managing telecommunication services subscriptions, redeeming vouchers and purchasing data bundles. Based on these observations, we rated authentication assurance for these sites at AAL2.

Password requirements suggest that password security has a great influence. Further, there is a desire for usability, as reflected by real-time feedback on progress regarding the meeting of password requirements during password generation.

Sites for Job Vacancies. Password policies on three sites in this category were analyzed. These sites show that a password strength meter and rule-based password policies are in use. The implemented password strength meter recommends passwords that are at least six characters long using alphanumeric characters. However, the password strength meter does not seem to offer adequate feedback to guide users during password generation. During password generation attempts, the password strength meter identified the password "123456" as very weak. Moreover, changes in character

classes and length to candidate passwords did not reflect any movement on the password strength meter suggesting improvements in password strength. Furthermore, the other two sites did not explicitly display password requirements. Password generation attempts show that a single character password such as "1" is accepted.

Further observations show that security breaches on job vacancy sites could expose personal information. As such, authentication assurance for these sites was rated AAL2. The password policies implemented suggest less caution in relation to password security. More interest is invested in designing simple and usable password policies, although the lack of adequate feedback may negatively affect usability. The desire for usable policies could be motivated by competition from other sites with vacancies.

Classified Adverts. The two researched sites make use of rule-based passwords. The password policy on one of the two sites recommends passwords of at least seven characters. Users could generate a password such as "1234567". However, the other researched site did not display password requirements. Password generation attempts revealed that a single character password was acceptable.

Further observations show that there is little risk that could affect users with compromised passwords. These sites make provision for subscriptions to the latest adverts and uploading adverts. As such, sites for classified adverts are classed AAL1 according to NIST. This rating is reflected by simple password policies implemented on the sites.

Betting Site. A single betting site was researched. The site recommends that users generate an alphanumeric password that is at least six characters long. One of the limitations of the site's password generation policy design is that password requirements only appear after a user has failed to generate a suitable password. In addition, the policy is open to weak passwords such as *"password123"*. Our observations show that the site gathers personal user data such as name, address and identity number. Password breaches could lead to the exposure of personal information; hence, this site is rated AAL2, suggesting relatively complex password requirements. However, the password policy on the betting site is more inclined towards usability. This could be explained by a need to attract more users.

E-Government Site. The password policy of the e-Government site recommends the generation of a password that is at least six characters long with upper and lowercase letters, a number and a symbol. Password requirements are displayed in advance for users to see. The use of special characters is limited to: ~!@#$%^&*()_+. Users are also warned against the use of personal information in passwords. Our observations suggest that security breaches could lead to the exposure of personal information. Hence, the researched e-Government site is classed AAL3 according to NIST. However, this suggestion is not in line with the site's implementation of a password policy which appears to be leaning towards usability rather than security.

5 Discussion

Popular South African sites have diverse password requirements even for institutions in the same type of industry. Rule-based password policies are the most popular policies when compared to the use of password strength meters. This study made the following key observations:

- There are cases where password policies are limited to a few permissible password characters.
- Password requirements are not always explicitly displayed for users to see.
- There is very limited use of effective guidance and feedback during password generation.
- The use of a blacklist is often poorly implemented. Most blacklists did not block the ten most common passwords in the public domain.
- Some password policies allow the generation of very short passwords (one-character password).
- There are instances where password requirements are not enforced.
- Sites that are expected to have strong password policies sometimes have weak policies.
- Most password policies are based on practices that were found to be obsolete in the literature – the use of different character sets and a limited use of blacklists.
- Sites with strict password policies are more likely to display their password rules explicitly.

However, there are some encouraging observations. For example, one of the deployed password strength meters appears to use the zxcvbn password generation algorithm coupled with a long blacklist and real-time interactive fear appeals such as *"names and surnames by themselves are easy to guess"* or *"this is a top-10 common password"*. The use of "interactive fear appeals" significantly increases password strength compared to simple password strength meters with bars that change in colour [14, p. 2988]. Similarly, a few sites that enforced a rule-based password policy gave real-time feedback and guidance during password generation. Password rule enforcement, real-time feedback and effective guidance are some of the most effective methods that have the potential to reduce password generation errors, inform and support users to generate strong passwords [8, 10, 15].

The study findings suggest an attempt to increase password security. However, the password strength measures implemented on most of the researched sites have since been rendered obsolete. Tremendous emphasis is placed on using different character sets to enhance password strength. Very few sites (four) appeared to have effectively implemented proposed best practices of using a blacklist, blocking keyboard patterns, or encouraging long passwords. This is also common in the literature [9]. In addition, there appears to be a general belief that short passwords are easy to generate. Little effort is made to explicitly display password requirements, feedback and guidance, something that could enhance usability [3, 10, 15].

A comparison of the findings of this study and those in the literature was done for each category researched, with a focus on categories that were previously researched in

the literature. Frequently visited South African IT corporation sites had comparable password policies to their Chinese counterparts [3]. Irrespective of country, IT corporations encouraged passwords that are at least eight characters long with numbers, special characters, uppercase and lowercase letters. None of the sites were found to be using a blacklist. However, the majority of Chinese IT corporations restrict the use of personal information. On the other hand, Chinese email service providers explicitly show password rules and use a blacklist, with some restricting the use of personal information [3]. Interestingly, South Africa's popular email site does not use any of these measures in its password policy. Furthermore, password policies of frequently visited South African e-Commerce sites were found to be comparable to those reported in the literature [1, 3]. e-Commerce sites recommend nearly the same character sets and minimum password length but do not always restrict user information in passwords and do not use a blacklist. However, frequently visited South African university sites encourage longer passwords compared to their Chinese counterparts [3]. In addition, two frequently visited South African university sites recommend a longer minimum password length than those in the US [1]. However, South Africa's popular e-Government site was found to have a short minimum length (6) requirement that translated to a relatively weaker password policy compared to its American counterparts [1]. Popular South African banks encourage the use of more character sets compared to their US counterparts [1]. It should be noted that banks often use a two-factor authentication [1, 3, 5]. Both South African and US frequently visited sites for classified adverts and news do not seem to emphasize the use of different character sets.

6 Conclusion

The literature suggests that the failure to implement measures that could influence user behavior towards using the technology correctly is one of the reasons behind the generation of weak passwords [1, 9, 16]. This has seen studies investigating password generation rules in use with others recommending corrective measures [9, 10, 15]. This study researched password policies deployed by South African organizations. It was found that security and usability factors play an important role in influencing the extent of password requirement complexity. The value of protected resources appears important to banks, universities and television broadcasting companies. However, e-Commerce, email, news sites, classified adverts and job sites appear to emphasize usability. It should be noted that the desire for secure passwords on South African sites is hampered by the use of obsolete password strength measures. Despite Wier et al.'s [6] ground-breaking research finding that using different character sets alone may not enhance security, the practice remains popular in South Africa. There are suggestions that leading international sites too have implemented minimal changes to their password requirements policies since 2011 [9]. This is so despite the literature suggesting different measures to enhance password generation [9, 16]. In addition, while some South African institutions prefer the usability of password requirements, they often do not provide real-time interactive feedback and guidance to users during password generation. Nevertheless, the majority of password policies deployed on popular South African sites are comparable to their global counterparts.

Appendix

Researched Sites, Password Policies and Accepted Passwords

Category	Password strength meter	Rule-based password policy	Minimum length limits	Character set	Blacklist	Deter personal data	SSO	Explicitly display password rules	Accepted passwords
Bank site	No	Yes	8	ULNS	No	No	No	Yes	P@s$word5
Bank site	No	Yes	8	ULN	No	No	No	Yes	N/A
Bank site	No	Yes	8	UN/ LN	No	No	No	Yes	N/A
Betting site	No	Yes	6	UN/ LN	No	No	No	No	password123
Classified adverts	No	Yes	No	No	No	No	No	No	1, we, pass
Classified adverts	No	Yes	7	N/ L/S/U	No	No	No	Yes	1234567
e-Commerce	Yes	N/A	N/A	N/A	No	No	No	Yes	P@55word
e-Commerce	No	Yes	5	L/N/S/U	No	No	No	No	ilove
e-Commerce	No	Yes	N/A	N/A	No	No	Yes	N/A	N/A
e-Commerce	No	Yes	8	UN/LN	Yes	No	No	Yes	111111p; p@55word; iloveyou1
e-Commerce	No	Yes	6	U/L/N/S	No	No	No	No	password
E-Government	No	Yes	6	ULNS	No	No	No	Yes	N/A
E-mail	No	Yes	No	U/L/N/S	No	No	No	No	12345
Job vacancies	Yes	Yes	6	U/L/N/S	No	No	No	Yes	pa55word
Job vacancies	No	Yes	No	U/L/N/S	No	No	No	No	pass
Job vacancies	No	Yes	No	U/L/N/S	No	No	No	No	pass
News site	No	Yes	N/A	N/A	No	No	Yes	N/A	N/A
News site	No	Yes	6	U/L/N/S	No	No	No	No	password
News site	No	Yes	5	U/L/N/S	No	No	No	No	passw
News site	No	Yes	8	ULN	No	No	No	Yes	password1
Real estate	No	Yes	6	U/L/N/S	Yes	No	No	No	Pa$5word
Real estate	No	Yes	6	U/L/N/S	No	No	No	Yes	password
IT corporations	No	Yes	8	ULN	No	No	No	Yes	Password@1
IT corporations	No	Yes	8	ULN	No	No	No	Yes	Password1
TV services	Yes	N/A	N/A	N/A	Yes	No	No	Yes	
TV services	No	Yes	6	U/L/N/S	No	No	Yes	No	password
University	No	Yes	6	U/L/N/S	No	No	No	Yes	password
University	No	Yes	12	ULNS	No	No	No	Yes	N/A
University	No	Yes	14	U/L/N/S	Yes	Yes	No	Yes	N/A
University	No	Yes	8	ULN/ UNS/LNS	No	No	No	Yes	password1#

Key: U: Uppercase letters; L: Lowercase letters; N: Number; S: Symbol.
N/A: Not applicable

References

1. Florêncio, D., Herley, C.: Where do security policies come from? In: Proceedings of a Symposium on Usable Privacy and Security (SOUPS), pp. 1–14. ACM, Redmond (2010)
2. Grassi, P.A., Garcia, M.E., Fenton, J.L.: Digital Identity Guidelines. NIST Special Publication 800-63-3, pp. 1–62. NIST (2017)

3. Wang, D., Wang, P.: The emperor's new password creation policies: In: Pernul, G., Ryan, P. Y.A., Weippl, E. (eds.) ESORICS 2015. LNCS, vol. 9327, pp. 456–477. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24177-7_23
4. de Carnavalet, X., Mannan, M.: From very weak to very strong: analyzing password-strength meters. In: NDSS, vol. 14, pp. 23–26 (2014)
5. AlFayyadh, B., Thorsheim, P., Jøsang, A., Klevjer, H.: Improving usability of password management with standardized password policies. In: Proceedings of the Seventh Conference on Network and Information Systems Security (SAR-SSI), pp. 7983–7999. Kolkata, India (2012)
6. Weir, M., Aggarwal, S., de Medeiros, B., Glodek, B.: Password cracking using probabilistic context-free grammars. In: Proceedings of the 30th IEEE Symposium on Security and Privacy, pp. 391–405. IEEE, Washington (2009)
7. Wheeler, D.L.: zxcvbn: Low-Budget Password Strength Estimation. In: Proceedings of the 25th USENIX Security Symposium. pp. 157–173. USENIX Association, Austin (2016)
8. Shay, R., et al.: A spoonful of sugar? The impact of guidance and feedback on password-creation behavior. In: Proceedings of the Human Computer Interaction (HCI) Conference, pp. 2903–2912. ACM, Seoul (2015)
9. Furnell, S.: Password practices on leading websites – revisited. Comput. Fraud Secur. **12**, 5–11 (2014)
10. 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)
11. Ur, B., et al.: How does your password measure up? The effect of strength meters on password creation. In: Proceedings of USENIX Security Symposium, pp. 65–80. USENIX, Bellevue (2012)
12. Yang, C., Hung, J.-L., Lin, Z.: An analysis view on password patterns of chinese internet users. Nankai Bus. Rev. Int. **4**, 66–77 (2013)
13. Wang, D., Cheng, H., Gu, Q., Wang, P.: Understanding Passwords of Chinese Users: Characteristics, Security and Implications. CACR Report, China (2015)
14. Vance, A., Eargle, D., Ouimet, K., Straub, D.: Enhancing password security through interactive fear appeals: a web-based field experiment. In: Proceedings of the 46th Hawaii International Conference on System Sciences, pp. 2988–2997. IEEE, Wailea (2013)
15. Furnell, S., Esmael, R.: Evaluating the effect of guidance and feedback upon password compliance. Comput. Fraud Secur. **1**, 5–10 (2017)
16. Althubaiti, S., Petrie, H.: Instructions for creating passwords: how do they help in password creation. In: Proceedings of the 31st British Computer Society Human Computer Interaction Conference, pp. 55–65. BCS Learning & Development Ltd, Sunderland (2017)