Investigating customer-facing security features on South African e-commerce websites

Deen Brandreth
Jacques Ophoff

This is the Author Accepted Manuscript of a conference paper published in Information and Cyber Security: 19th International Conference, ISSA 2020, Pretoria, South Africa, August 25–26, 2020, Revised Selected Papers

The final authenticated publication is available online at Springer via
http://dx.doi.org/10.1007/978-3-030-66039-0_10

Investigating Customer-Facing Security Features on South African E-commerce Websites

Deen Brandreth[1] and Jacques Ophoff[1,2][0000-0003-0634-5248]

[1] University of Cape Town, Cape Town, South Africa
[2] Abertay University, Dundee, United Kingdom
deen.brandreth@uct.ac.za, j.ophoff@abertay.ac.uk

Abstract. E-commerce websites often store sensitive customer information and there is the impression that customers are not as concerned about protecting their data as they should be. Instead they often choose convenience over security. There are those who argue that e-vendors do not provide the necessary environment to adequately protect their customers' data by utilizing multi-factor authentication and by providing customer support that educates and encourages customers to follow security best practices. This study develops criteria to evaluate website security and goes on to investigate how the top 20 South African e-commerce websites perform against this. The results show that multi-factor authentication is underutilized and security in the form of password-based authentication can be improved. Furthermore, despite many customer support channels and resources, there is little emphasis placed on educating and encouraging customers to follow security best practices. The results suggest areas for security improvement in order to build trust in e-commerce websites.

Keywords: E-commerce, Security Features, Account Creation, Login, Security Management.

1 Introduction

Despite its growth, e-commerce is still relatively new to many people [1]. An e-commerce customer tends to accept far more risk during a transaction than a traditional offline customer [2]. There are those who believe that e-commerce has yet to reach its full potential and one of the major factors impeding this is a lack of trust between the customer, the system facilitating the transaction and the e-commerce business [2-4].

For a website to be considered secure data should be transmitted securely between the customer and the website. Customer data stored on the website should also be stored in a secure manner so that only authorized entities have access to it [5]. These two categories can be called transactional data and customer information. A typical solution for securing transactional data would be encryption while customer information is often protected using authentication and verification [5, 6].

Customers' perception of security is one of the biggest factors that determine whether they will transact online [3, 6-8]. This perception of security lies in the risk of

sensitive personal and payment information being compromised [6, 7]. Regular and consistent security reviews with the implementation of solutions is thus a prerequisite to success in e-commerce [9].

Based on security literature, this paper proposes criteria for evaluating the level of security that an e-commerce website provides customers. Instead of a purely technical analysis of security features the criteria consider a broader range of issues and aims to give a typical customer several indicators of trust for the e-vendor. The criteria are separated into three phases which include account creation, login, and security management.

A sample consisting of the top 20 South African e-commerce websites is then evaluated against the criteria, to determine the perception of security and trust a customer may have of the website. Purchase of goods or services is specifically excluded from the evaluation, as security during this process is more standardized (e.g. PCI-DSS) and technical features may be less visible to the customer.

The remainder of this paper proceeds as follows. Section 2 provides a background discussion leading to the proposed criteria. Next, Section 3 reviews the research methodology and how the sample was selected. This is followed by analysis and a discussion of the findings in Section 4, after which the paper concludes with a brief summary.

2 Background

E-commerce plays a pivotal role in the global economy and particularly in developing countries, where there is a growing middle class and companies from around the world serving the need for better quality and more convenient shopping [2]. The significant growth of e-commerce can partly be attributed to the fact that the internet has become ingrained in our daily lives [3]. However, given the rise in targeted phishing and other social engineering attacks [10], data security should be a primary concern for both e-commerce businesses and the customers who use their platforms.

A customer, a vendor, one or more third parties such as certification authorities or payment systems and the technological system facilitating the trade, are the various actors in an e-commerce transaction and since the customer decides whether or not to transact, you could consider them to be the most important of the four [3]. Trust needs to be established between these actors but of utmost importance is the level of trust experienced by the customer [3, 6]. The customer should, therefore, believe that the e-vendor will act in their best interest during and after the transaction or exchange. To define trust is not easy as there are many considerations of which context is very important. Trust has been studied in the context of psychology, economics, sociology and management studies but for the purpose of this paper, trust will be defined simply as “a belief that one party (the trustee) will behave in a manner which is in the interest of another party (the trustor), through transactions or exchanges” [2].

2.1 Increasing Customer Trust

Some researchers argue that trust cannot exist without doubt [3]. It stands to reason then, that the factors that increase risk and doubt in an online environment must be dealt with before trust can be established. In a traditional context, the customer may have the opportunity to observe the vendor in person through a handshake or reading body language [6] but in an online context, this is not possible.

Oliveira et al. [1] point to three properties of trust, namely "competence, integrity and benevolence". These are said to be established by the character of both the customer and the e-vendor and by the website functionality. McCole et al. [3] also include properties of compassion, aptitude and certainty along with those mentioned by Oliveira et al., but do not consider the website and its functionality as needing trust. Instead, they consider that trust in the entire system that facilitates the transaction along with the e-vendor and other third parties involved in the transaction is required.

Steyn and Mawela [2] have found that trust is formed based on the customer's own core beliefs of what is normal and acceptable, technological aspects and due to experiences with the e-vendor and system over a period. They have also identified further categories such as cognitive, institutional, calculative, knowledge based and reputational trust where trust is based on factors that fall under these descriptions. For example, cognition-based trust occurs when the customer considers aspects such as privacy and security or the quality of the system, they are interacting with whereas institutional trust speaks to aspects of laws, regulations and third-party guarantees and certification [2]. Thus, it stands to reason that for a customer to trust an e-vendor or their website, some of the important considerations lie around privacy, security, quality of the user interface, website functionality and the use of trusted third parties. As such, these concepts, as they relate to e-commerce websites, were considered as key factors in this study.

2.2 Privacy in E-commerce

Privacy in e-commerce refers to the right of customers and organizations to have control over how their personal data is stored and transmitted to others [4, 11, 12]. Privacy is a growing concern, specifically for customers who transact online in fear of their information being used fraudulently [7, 8]. Customer privacy is not new or specific to e-commerce but in order to thrive, e-vendors do have to provide assurance that customer data is secure. Chatterjee [8] argues that privacy and security issues can determine whether a business succeeds or fails. These privacy fears are further fueled because of aggressive data collection by both public and private sector organizations with some companies using collected data for marketing and monitoring purposes [4]. As such, many e-vendors include privacy policies on their websites to remove customers' fears about how their information is managed [11]. Privacy policies are an indication to the customer that the e-vendor is concerned about privacy [4] which should positively influence trust in the e-vendor [11].

Regardless of privacy policies and assurance about how data is managed, caution should still be exercised when transacting online. Customers are encouraged to only

share information that is required and only use secure websites that utilize encryption [4, 8].

2.3 Security from a Customer's Perspective

Customers may have sensitive financial and health data stored/exchanged with e-commerce servers or accounts, which makes security even more imperative [13]. When it comes to securing online accounts, authentication is the primary means of doing so [14].

Passwords are the most common means of end user authentication to protect data on computer systems. At an early stage in the evolution of computer security the end user was identified as a major weakness in the use of passwords as a means of authentication [15]. Many years later research still identifies the end user as a weak link in password-based authentication systems, e.g. "password-based authentication is frequently criticized on the basis of the ways in which the approach can be compromised by end users" [16]. Furnell et al. [17] go so far as to call the end user "the weakest link in the information security realm". The end user, unfortunately, is not the only weakness to be exploited when it comes to password-based authentication systems. Technically incorrect or insufficient security implementations can be equally problematic.

Researchers have found numerous ways of mitigating the potential exploitation of these weaknesses. Some suggest adding additional layers of authentication, known as multi-factor authentication [18-21] while others point out that supporting the end user by providing information and feedback to increase security awareness, is another means of improving the success of password-based authentication systems [17, 22].

Supporting the user is typically done in an active or passive manner. Passive support simply provides information and advice to aid the user in making better security related decisions. This could take the form of a frequently asked questions webpage, games, educational programs and self-assessment checklists [17]. Although effective in bringing about change in user actions and attitude, passive support is not resolving the issue in its entirety and so active intervention is gaining popularity. This would include a more direct approach of coaxing users to comply with security policies through interactive feedback such as highlighting poor choices and things like password meters [17].

2.4 Security Evaluation Criteria

There is little research documenting the extent of multi-factor authentication or how end-users are supported and guided by those who have implemented it. Studies around password practice and user support have shown that there are tangible benefits to providing support and guidance to end-users, with the aim of improving the security and protection of user accounts and data. It therefore makes sense that e-vendors who offer online accounts should provide support with the aim of educating their customers in order to mitigate the likelihood of unauthorized access to customer data.

It is agreed that there is no silver bullet to resolve these issues but using a layered approach to security is certainly better than not doing anything at all.

The key concepts identified in the literature review were privacy, security, website functionality, and the use of trusted third parties. These were then considered when designing the criteria in the *Website Security Analysis Criteria,* as shown in Table 1.

Table 1. Website Security Analysis Criteria

Criteria	Account Creation	Login	Security Management
Security			
Does the site use HTTPS? (Is the connection secure?)	X	X	
Is the HTTPS certificate valid?	X		
What are the password requirements (if any)?	X		
Does the account get locked after entering the incorrect password?		X	
Is there a forgot password option? / Is there an option to change the password?		X	X
How is the password reset, i.e. use of account recovery questions, new password auto-generated, link provided to change password, or OTP sent?		X	
What are the communication options when resetting pin, i.e. email, SMS, app, etc.?		X	
What are the password requirements when changing passwords?		X	X
Is multi-factor authentication offered?	X	X	
What multi-factor authentication settings are available?			X
What other settings are available for securing the account?			X
Are you required to verify any information, e.g. email address? (How is this done?)	X		
Does the website allow for third-party login?	X	X	
Privacy			
What personal information is required to sign up?	X		
What additional personal information is requested (but not compulsory) when signing up?	X		
What additional personal information can be added in account settings?			X
Support / Awareness			
Are there any security prompts, e.g. password strength indicators?	X		
Are security indicators explained in more detail or are there links for additional information?	X		X
What are the various types of help resources available?	X	X	X
Does the site have a privacy policy?	X		X
Is there a link to terms and conditions?	X		

The criteria consider three distinct phases of security analysis, namely account creation/registration, the login process, and after gaining access to the site as a registered user while browsing the site for available account settings and support resources (security management). In each phase the focus is on information which would be visible to the customer. While additional technical criteria (such as HTTPS certificate issuer, cryptographic settings, etc.) could be considered important, the criteria is aimed at non-technical users and information readily obtained on a website. Criteria to consider are separated into security, privacy, and support or awareness issues. The applicability of each criteria within the three phases is indicated with an *"X"*.

The next section explains how the criteria was used to evaluate actual security settings on a relevant sample of e-commerce websites.

3 Methodology

This study used documentary secondary data in the form security-related settings, text, and video found in the help sections of the various e-commerce websites, as well as potential external sources that the websites refer customers to. Settings related to multi-factor authentication and account security in general were also noted for analysis. Data was reduced into content categories before being analyzed qualitatively. Referred to as content analysis, this technique aims to "quantify and describe aspects of textual or visual data after coding and categorizing them" [23]. Content analysis is based on objective observation of factual objects and analyzing what is clear and obvious, as opposed to interpreting the data subjectively.

3.1 Sampling

A well-known longitudinal study used ten popular websites, as ranked by Alexa (https://www.alexa.com/topsites), to identify how these websites managed password security [16, 20]. Similarly, this study uses the Alexa ranking system to identify the top 20 South African e-commerce websites. The rankings are calculated using a combination of average daily visitors and pageviews. The sample was determined using website traffic at a specific point in time: in this case the top 500 websites were retrieved in July 2019. A set of selection criteria were applied to identify the final list of e-commerce websites, which included:

- The website is used to conduct business.
- The website facilitates transactions for the sale of goods or services. Some online marketplaces or classifieds allow free advertising and viewing of adverts. In this manner, an entire transaction is free of charge and the website was disqualified.
- The website requires an account to be created in order to transact. Websites that allow free viewing of adverts but required an account and payment to advertise was included.

Company details were confirmed on the appropriate domain registration authority's website. It was also confirmed that the company is registered in South Africa by searching the Companies and Intellectual Properties Commission website. The final list of included websites is shown in Table 2. The table shows the e-commerce rank, website URL, as well as overall country (South African) ranking.

Since the rankings are based on site traffic, it can be said that these are the most frequented South African e-commerce websites as visited by South Africans. This does not imply that these are the most successful e-commerce websites or that they have the most online accounts, but it does allow the researcher to comply with the principles of scientific research in that it contributes to making the study replicable.

Table 2. Websites Selected for Analysis

Rank	Website	Overall	Rank	Website	Overall
1	Takealot.com	9	2	Property24.com	19
3	Hollywoodbets.net	34	4	Showmax.co.za	46
5	Bidorbuy.co.za	52	6	Privateproperty.co.za	68
7	Makro.co.za	73	8	Sageone.co.za	92
9	Afrihost.com	101	10	Vodacom.co.za	104
11	Builders.co.za	136	12	Nationallottery.co.za	137
13	Superbalist.com	149	14	Loot.co.za	155
15	Evetech.co.za	159	16	Game.co.za	167
17	Onedayonly.co.za	179	18	Clicks.co.za	184
19	Zando.co.za	188	20	Altcointrader.co.za	197

3.2 Data Collection

The data was collected by assuming the role of a customer. An account was created on each of the websites using an email account created specifically for this study. This process was documented using the Website Security Analysis Criteria (Table 1) as a guide, screen captures, notes about the experience (sequence of processes, type and timing of communications), information such as security prompts and restrictions that are applied (restrictions related to enforcement of security features such as multi-factor authentication and password strength, etc.), built-in tools that assist and advise the customer, links to help/support resources (including the data they contain whether in the form of text, audio or video) and all other available security options.

After the initial account creation, all security options, related to the account, were documented in the same way that the account creation process was documented. Here the researcher looked for replication of settings, additional options and settings that were not presented during the account creation process and whether password requirements were enforced or if they differed from the account creation stage. This was followed by collecting data on all the support options related to security. These took the form of help sections with knowledge base articles, frequently asked questions (FAQ) pages, documentation related to multi-factor authentication and account security, video and other interactive help tools. Data pertaining to support provided on the actual website and support that is provided offsite, for which links are provided, was also collected.

4 Analysis and Discussion

Analysis focused on three stages: account creation/registration, the login process, and after gaining access to the site as a registered user by observing available account security settings. The first step in data analysis was to clean up and sort the data because different websites use different terms to describe the same data. For example, one website would use the term surname where a different website would request your last name when registering an account. Similarly, some sites had a password reset feature, while others would refer to this as a forgot password option. Similar

terms were renamed to standardize the terminology used. Settings were grouped into the following categories:

- Security
    - Account security: Multi factor authentication, password requirements, account lockout for entering the incorrect password, are the password requirements enforced and other account security settings.
    - Website security: Use of HTTPS, validity of certificate, and a secure connection between the customer device and website.
- Privacy
    - Types of information stored as part of the account. These include personally identifiable information such as first name, last name, identity number, passport number or contact information such as the mobile number and email address.
    - The use of privacy policies and/or terms and conditions.
- Customer support options (considered to be a function of the website)
    - Any method of contact between the e-vendor and the customer which allows the e-vendor to provide support information through direct communication (email, telephone, etc.) and indirect communication (videos, social media posts, help articles, FAQs, interactive website features, etc.).
- The use of third parties
    - Allowing third-party login, for example using Facebook, Google, Microsoft, etc.
    - Using a third-party to facilitate security. An example would be Takealot.com and OneDayOnly.co.za who use GoDaddy.com to facilitate site security and their payment system.

4.1 Privacy

Given the diverse offering of services and products, it stands to reason that there is a similarly diverse range of information stored on these platforms, making them a potential target for cyber criminals. It is no surprise that the most common information required on these websites are first name, last name, email address and mobile number. What is surprising is that half of these websites potentially store customers' ID numbers while about a third store home phone numbers, work phone numbers and physical addresses of customers. Potentially sensitive data includes: Mobile/Home/Work Phone Number; Date of Birth; ID/Passport Number; Physical/Postal Address; Credit Card Details; Bank Account Number; Type of Income; E-vendor Account Number; FICA Documents (ID and Proof of Address).

All but one of the sites have a privacy policy. The privacy policy explains how e-vendors manage customers' information. Privacy policies detail, to the customer, which personal information is collected, how the data is processed, who the data is shared with and also lists the type of information collected that the customer may not be aware of such as IP addresses, browsing data, location information, website preferences, operating system information and all electronic communications between e-

vendor and customer. Another common theme, found within the privacy policies, is the assurance that the e-vendors try and convey to their customers that their data is safe, that the e-vendor is compliant from a legal perspective, that their systems are safe and of course that they have the customers' best interest at heart, e.g. *"we are committed to protecting and respecting your privacy"*.

4.2 Account Security

All the websites, except one, use password-based authentication to restrict access to customer accounts. This is in line with many researchers who point out that password-based authentication is still the most widely used form of authentication despite the many known weaknesses. The odd one out is Nationallottery.co.za which only re-quires a five-digit pin in conjunction with the customer's mobile number for authentication.

Since most of the e-vendors opt to use password-based authentication systems, it is interesting to note how many of them configure their systems in a way that would mitigate the many pitfalls associated with passwords. Unfortunately, only half of the websites investigated require a complex password consisting of a mix of upper- and lower-case letters, numbers and special characters. The other half allow the creation of simple passwords by only requiring a minimum amount of characters. In all cases where only the minimum number of characters were specified as a requirement, the researcher could create a password of a string of consecutive numbers such as *"123456"* for example. One of the websites, however, did not even enforce the minimum requirements of five characters. Once an account was registered, the researcher was able to change the password to a single digit on Evetech.co.za, log out and log back in with the password *"1"*.

The next examined setting was account lockout for incorrect password attempts. The researcher made 20 incorrect attempts before trying the correct password if no prompts were received. Again, the results were not positive. Only four out of the ten websites that allow simple passwords, locked the account after several unsuccessful login attempts. In total, seven websites utilized this security measure. Table 3 describes the minimum password requirements and the account lockout security feature for each website.

Only two of the websites have opted to use multi-factor authentication for securing their customers' accounts. Altcointrader.co.za have made multi-factor authentication, using Google's Authenticator app, optional on their site. Afrihost has taken the decision out of their customer's hands and appear to re-quire a one-time pin (OTP) for login at their own discretion. This notably caused some concern as the feature took customers by surprise when first introduced, as can be seen by a post on the Afrihost forum [24]:

"I received the following notice from Afrihost: 'An OTP has been requested on your Afrihost Account' What is an OTP?" asked Nov 26, 2018 in General by Swart (190 points)

Table 3. Website Account Security

Site	Password Requirements	Account Lockout
Takealot.com	Minimum 5 characters.	Yes. Warning after 7th incorrect attempt that there are 3 attempts left.
Property24.com	Minimum 6 characters. Password must have both upper- and lower-case letters and a symbol or number.	No. 20 incorrect attempts and then successful login with correct password.
Hollywood-bets.net	Minimum 4 characters.	Unable to log in as I have not submitted FICA documents.
Showmax.com	Minimum 6 characters.	No. 20 incorrect attempts and then successful login with the correct password.
Bidorbuy.co.za	Minimum 8 characters, minimum 1 upper case letter and minimum 1 number.	No. 20 incorrect attempts and then successful login with correct password.
Privateproper-ty.co.za	6-50 characters.	No. 20 incorrect attempts and then successful login with correct password.
Makro.co.za	8-32 characters, no spaces, must have upper- and lower-case letter, must have at least 1 number.	Yes. Correct password did not work after 20 incorrect attempts. Had to reset password before gaining access to account.
Sageone.co.za	Minimum 6 characters, 1 lower case letter, 1 upper case letter, 1 number, 1 special character.	No. 20 incorrect attempts and then successful login with correct password.
Afrihost.com	Minimum 6 characters. Could use 5 characters in password once registered.	Yes. Had to reset password after 20 incorrect attempts. The account becomes active after 5 minutes.
Vodacom.co.za	Minimum 8 characters, 1 number, 1 upper case and 1 lower case letter. Password reset from profile doesn't require old password.	Yes. Have to reset password after 3 incorrect attempts. OTP sent to email to allow password reset.
Builders.co.za	Minimum 6 characters, 1 upper and 1 lower case letter and 1 number and no spaces.	No. 20 incorrect attempts and then successful login with correct password.
Nationallot-tery.co.za	5-digit pin.	No. 20 incorrect attempts and then successful login with correct pin.
Superbalist.co.za	Minimum 6 characters.	No. 20 incorrect attempts and then successful login with correct password.
Loot.co.za	Minimum 6 characters.	No. 20 incorrect attempts and then successful login with correct password.
Evetech.co.za	Minimum 5 characters at account creation but single digit password accepted after registration.	No. 20 incorrect attempts and then successful login with correct password.
Game.co.za	Minimum 6 characters.	Yes. Correct password did not work after 20 incorrect attempts. Had to reset password before gaining access to account.
Onedayonly.co.za	Minimum 6 characters.	No. 20 incorrect attempts and then successful login with correct password.
Clicks.co.za	Minimum 6 characters.	Yes. Correct password did not work after 20 incorrect attempts. Had to reset password before gaining access to account.
Zando.co.za	Minimum 6 characters.	No. 20 incorrect attempts and then successful login with correct password.
Altcoin-trader.co.za	Minimum 8 characters, at least 1 letter and at 1 number and a 24-hour hold is placed on withdraw-als when password is changed.	Yes. Account blocked after 3 failed attempts. Blocked for 30 minutes.

The answer to which was: *"An OTP is a one time pin - they sometimes send you one when you try to access your account to make sure that no one has stolen your login details" answered Dec 5, 2018 by FearsomePiratePete (180 points)*

Some customers were clearly not informed about the introduction of multi-factor authentication or missed the communication. Other customers were unable to access their accounts as they could not receive the OTP for various reasons. One such post on the forum reads [25]:

"Look, this is an obvious question and one that affects me greatly (and inconvenient also !!) is that ibn [sic] my area my Vodacom signal is frequently down or too weak to even carry a bar for SMS delivery. How can Afrihost be so careless of clients needs as to introduce a silly SMS verification system for login to Client Zone??" asked Mar 20, 2019 in Client Zone by GarethG (120 points)

4.3 Website Security

The use of a secure, encrypted connection between customer and e-vendor was found to be standard practice on all the top 20 South African e-commerce websites and all website certificates were valid. Hollywoodbets.net was the anomaly in this case though. Although their website is secure, uploading of FICA documents is not done over a secure connection when following links via their website support section. However, when viewing a how-to video the URL indicated in the video did display as HTTPS and when navigating to it the upload could be done securely.

Third-Party Login. Third-party logins are allowed on seven of the 20 websites. These were restricted to Google and Facebook. Both Facebook and Google have the option of using multi-factor authentication for enhanced account security.

Furthermore, most of the websites actively advertise secure payments. These are provided by third parties such as PayU, MasterCard, Visa, GoDaddy, Thawte and MyGate. Sageone.co.za are the only e-vendor who have their own payment gateway. Showmax is one of the few sites who don't actively advertise transaction security, but they do offer an extensive range of payment options. These include PayPal, the option to add the subscription to one of several other subscriptions such as DSTV, Telkom, Vodacom, MTN and by purchasing vouchers from third parties.

Support. There is a myriad of support resources that e-vendors can use to interact with and provide support to their customers. Social media is the most utilized means of communicating with customers as all the studied e-vendors make use of YouTube and Facebook while 19 have a Twitter account. A dedicated FAQ section follows as the most popular means of providing support with a total of 17 websites utilizing this support resource. Telephone contact is also supplied for 19 websites but not all of them indicate this as a means of support. Other electronic forms of support such as blogs and email are also well utilized. Forums and live chat, which are a more immediate forms of support are only used by five and four of the e-vendors respectively. It is no surprise that fewer e-vendors provide a physical address as a means of contact.

Of the eight websites that provide this type of detail, five are major retailers with stores countrywide.

As mentioned above, social media is used extensively to provide support. Table 4 lists the number of videos that the e-vendors have uploaded to their official YouTube channels. The researcher could only find eight videos which mentioned security or privacy.

Table 4. Videos per e-Vendor

Site	Total YouTube Videos	Account Security/Privacy Videos
Takealot.com	73	0
Property24.com	64	0
Hollywoodbets.net	223	2
Showmax.com	857	0
Bidorbuy.co.za	50	0
Privateproperty.co.za	51 316	0
Makro.co.za	107	0
Sageone.co.za	43	1
Afrihost.com	20	2
Vodacom.co.za	1 471	1
Builders.co.za	743	0
Nationallottery.co.za	933	0
Superbalist.co.za	117	0
Loot.co.za	4	0
Evetech.co.za	265	0
Game.co.za	182	0
Onedayonly.co.za	14	0
Clicks.co.za	369	0
Zando.co.za	115	2
Altcointrader.co.za	27	0

A total of 25 different types of support resources were counted (social media not counted as a collective). Afrihost.com provide the largest number of support resources with six other e-vendors providing ten or more. The rest of the websites provide six to nine options for support. Active support in the form of password strength meters and other interactive functionality is lacking. Only eight of the 20 websites provide feedback to users while they enter their password.

4.4 Discussion

There is a considerable variety of data stored on e-commerce platforms. Some of the data can be considered more sensitive than others especially if accessed by criminals. Some data such as first and last names can be considered less critical than other pieces of information such as ID or passport numbers or contact information such as home and mobile phone numbers. Customers who register on e-commerce websites should ideally store as little information as possible and only divulge information of a more critical nature if absolutely required. The nature of some e-commerce sites requires their customers to submit sensitive information in which case it is the responsibility of the e-vendor to ensure that the information is stored and transmitted safely and securely. Privacy policies indicate how the e-vendor intends managing the customers'

information. All the websites investigated, except for one, have done so adequately thereby hopefully increasing the level of trust experienced by their customers.

The next step would be to follow through and provide a safe environment for customer's information. Somehow more emphasis is placed on transactional data security using encryption and third-party payment providers compared to the more basic approach applied to the protection of customer data stored in their accounts. Cost is certainly a consideration when e-vendors decide how to configure authentication on their websites and so is usability of the website. If cost were the only consideration, then one would expect the e-vendors to require more complex passwords or make more use of the account lockout feature as a means of re-enforcing account security. The researcher would argue that ease of use and convenience for the customer carries more weight than information security.

The lack of support aimed at educating and encouraging the customer from a security perspective also indicates that more can be done by the e-vendor to improve the protection of customer information. This is evident by comparing the amount of support that covers areas such as product support and advertising/marketing to the amount of content covering account security. One of the key support features were the forums of Bidorbuy.co.za and Afrihost.com. These forums provided an interactive platform where security was a hot topic and questions could be answered conveniently and in detail. Community powered support resources is an avenue that more e-vendors should utilize.

5 Conclusion

Security should be a primary concern for all e-vendors regardless of the size or nature of their business. Given the importance that cyber criminals place on data, customer information should be protected adequately. It was established that the top 20 South African e-commerce websites generally take a very basic approach to account security. Multi-factor authentication is said to improve account security by adding one or more additional steps to the authentication process. Only two of the websites investigated made use of this security feature. It was further established that many of the websites do not provide an environment within which customers can empower themselves. Many of the websites appear to favor convenience over security. There is a clear lack of education and encouragement within customer support resources. Emphasis is placed on providing support related to products and services with only a fraction of effort aimed towards account security. There is room for improvement in terms of how e-vendors configure authentication and the type and volume of support provided to address customer account security.

References

1. Oliveira, T., Alhinho, M., Rita, P., & Dhillon, G. (2017). Modelling and testing consumer trust dimensions in e-commerce. Computers in Human Behavior, 71, 153–164. https://doi.org/https://doi.org/10.1016/j.chb.2017.01.050

2. Steyn, L. J., & Mawela, T. (2016). A Trust-based e-Commerce Decision-making Model for South African Citizens. In Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists (pp. 42:1--42:9). New York, NY, USA: ACM. https://doi.org/10.1145/2987491.2987496
3. McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. Journal of Business Research, 63(9), 1018–1024. https://doi.org/https://doi.org/10.1016/j.jbusres.2009.02.025
4. Udo, G. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. Information Management & Computer Security, 9(4), 165–174. https://doi.org/10.1108/EUM0000000005808
5. Mahadevan, L., & Kaleta, J. P. (2017). Consumer Perceptions about E-Commerce- The Influence of Public Internet Trust. In Southern Association for Information Systems Conference 2017. St. Simons Island. Retrieved from http://aisel.aisnet.org/sais2017
6. Kim, M.-J., Chung, N., & Lee, C.-K. (2011). The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. Tourism Management, 32(2), 256–265. https://doi.org/https://doi.org/10.1016/j.tourman.2010.01.011
7. Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. Information & Management, 46(7), 411–417. https://doi.org/https://doi.org/10.1016/j.im.2009.08.002
8. Chatterjee, S. (2015). Security and privacy issues in E-Commerce: A proposed guidelines to mitigate the risk. In 2015 IEEE International Advance Computing Conference (IACC) (pp. 393–396). https://doi.org/10.1109/IADCC.2015.7154737
9. Ladan, M. I. (2014). E-Commerce Security Issues. In 2014 International Conference on Future Internet of Things and Cloud (pp. 197–201). https://doi.org/10.1109/FiCloud.2014.39
10. Proofpoint. (2018). PROTECTING PEOPLE: A Quarterly Analysis of Highly Targeted Cyber Attacks. Retrieved from https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-protecting-people-autumn-2018.pdf
11. Chen, Y.-H., Hsu, I.-C., & Lin, C.-C. (2010). Website attributes that increase consumer purchase intention: A conjoint analysis. Journal of Business Research, 63(9), 1007–1014. https://doi.org/https://doi.org/10.1016/j.jbusres.2009.01.023
12. Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. Information Management & Computer Security, 10(4), 149–158. https://doi.org/10.1108/09685220210436930
13. O'Gorman, L. (2003). Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, 91(12), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611
14. Nag, A. K., Roy, A., & Dasgupta, D. (2015). An Adaptive Approach Towards the Selection of Multi-Factor Authentication. In 2015 IEEE Symposium Series on Computational Intelligence (pp. 463–472). https://doi.org/10.1109/SSCI.2015.75
15. Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770–772.
16. Furnell, S. (2007). An Assessment of Website Password Practices. Comput. Secur., 26(7–8), 445–451. https://doi.org/10.1016/j.cose.2007.09.001
17. Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. Computers & Security, 75, 1–9. https://doi.org/https://doi.org/10.1016/j.cose.2018.01.016

18. Albayram, Y., Khan, M. M. H., & Fagan, M. (2017). A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). International Journal of Human–Computer Interaction, 33(11), 927–942. https://doi.org/10.1080/10447318.2017.1306765
19. Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). ``It's Not Actually That Horrible'': Exploring Adoption of Two-Factor Authentication at a University. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 456:1--456:11). New York, NY, USA: ACM. https://doi.org/10.1145/3173574.3174030
20. Furnell, S. (2018). Assessing website password practices – over a decade of progress? Computer Fraud & Security, 2018(7), 6–13. https://doi.org/https://doi.org/10.1016/S1361-3723(18)30063-0
21. Yu, J., Wang, G., Mu, Y., & Gao, W. (2014). An Efficient Generic Framework for Three-Factor Authentication With Provably Secure Instantiation. IEEE Transactions on Information Forensics and Security, 9(12), 2302–2313. https://doi.org/10.1109/TIFS.2014.2362979
22. Furnell, S., & Esmael, R. (2017). Evaluating the effect of guidance and feedback upon password compliance. Computer Fraud & Security, 2017(1), 5–10. https://doi.org/https://doi.org/10.1016/S1361-3723(17)30005-2
23. Saunders, M., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students (Seventh Ed). Pearson.
24. Afrihost Answers, https://answers.afrihost.com/16427/received-following-notice-afrihost-requested-afrihost-account, last accessed 2020/07/28.
25. Afrihost Answers, https://answers.afrihost.com/17429/cannot-verify-clientzone-because-cellphone-network-signal, last accessed 2020/07/28.