Honours Final Project Report

An Assessment of Web Authentication Security and Usability

By

Student BB 11-12

Matriculation Number S090xxxx

Submitted for the Degree of BSc in Networking and Systems Support, 2011-2012

Project Supervisor: Peter Barrie
Second Marker: Dr. Richard Foley

Except where explicitly stated all work in this report, including the appendices, is my own

Signed: ________________________ Date: ________________________

Abstract

Authentication is central to almost everything a person does online on a daily basis. It is important to properly assess current password policies to evaluate their guidelines in terms of educating and equipping users with the knowledge of how to appropriately secure their online assets.

A key issue in this is the lack of an industry standard for password policies. Thus, web providers develop their own. In doing this an appropriate balance needs to be struck between password policies which are sufficient to ensure adequate security but not overly complex as to overburden the user and act as a deterrent from using the site.

This project aims to evaluate password policies through an experimental categorisation of the authentication rule sets of a significantly large number of popular websites across three commonly used internet business models. The experimental methodology analysed the authentication process of each individual site and evaluated its policies against a set of secure authentication attributes.

The results of the project indicate that a number of major commercial website providers have a lack of security and consistency in their policies across several key areas. These areas include password reset facilities, password strength and authentication consistency. Specifically no website in the sample met the criteria in all of these areas and most had specific failings in one or more areas. These findings imply that greater consideration should be given by the industry to the development and implementation of securer authentication policies as a means of protecting users.

Word count [247]

Acknowledgements

I would like to take this opportunity to thank my research supervisor Peter Barrie for all his support and guidance during the course of this project.

I would also like to extend my thanks to my second marker Dr Richard Foley for his input into the project and the additional guidance material provided throughout the entire honours year.

I wish to express my gratitude to my family for keeping me inspired and motivating me through my studies, I wish to extend a special thanks to my twin sister Joanne; I could not have done this without them.

Finally, I wish to thank my friend and colleague for their input into the project.

Contents

List Of Tables

List Of Figures

1.0 Introduction

1.1 Background

Authentication is at the heart of many activities that take place on the internet - banking, online shopping social media being core examples of user driven activities that require authentication. However, as explained by security expert Osawa (Osawa, 2011)data obtained from breaches in security is traded on the black market, a practice that could easily lead to unauthorised access to other online systems causing catastrophic results as typically systems that require authentication, hold more sensitive information than those that do not. . Traditionally security has been focused on physical, offline entities as opposed to online information assets. However a user's online information assets are increasingly becoming as important as those which are held offline (Abraham, 2011). This is apparent from new services (Questli, 2011) such as My Pass Will is a new service which gives users the ability to leave a will to relatives containing clues to their online assets and accounts upon their death. The fact that such services are becoming publically available clearly shows the level of importance that that password authentication has with so many activities now based online.

Alongside this increased level of online activities, there are the continual data compromises that are being seen in the environment at the moment. Earlier this year Comodo, a reseller of secure socket layer security certificates to enterprise companies, suffered a breach of their systems earlier this year. Reported by (O'brien, 2011) that the system involved used single factor authentication (password only authentication). This suggests that in this case it was not enough security clearly this calls for a better security solution. This attack to an organisation in the public eye is not exclusive to this organisation alone as even organisations as large as Sony are now being forced to revaluate their security systems (Osawa, 2011). A combination of weak passwords and an erudite program used to guess users' login details and passwords resulted in Sony suspending 93000 user accounts following them being compromised.

There are many ways to authenticate online; these methods include passwords, PIN-codes or smart card authentication, biometric or a combination of these - known as multifactor authentication. Multifactor authentication is often perceived as a more secure method of authentication, this perception is reflected in the fact that many organisations are beginning to employ this level of authentication. Google announced earlier this year that the company is now offering two-factor authentication in the form of texts, voice messages and smartphone apps (Quittner, 2011, Quittner, 2011). This increased adoption could help encourage other large organisations and web developers to also offer multiple factor authentication methods, hopefully paving the way for other organisations to do the same in hope of strengthening and providing consistency for web authentication. However, as found in a test carried out by (Pearce et al., 2010) using multiple authentication methods does not always produce authentication confidence. Although multifactor authentication seems more secure, key issues with this are that the method uses a rounding approach when adding up the authentication score from each factor. This may result in cancelling out a low score of one factor, thus giving false positive authentication. This shows multifactor authentication is not all it is perceived to be.

Conventional password authentication is still widely seen as effective (Sood, 2011). Furthermore, organisations still choose to use passwords alone regardless of the risks associated with this. Passwords are commonly defined into categories. An investigation into secure strong password authentication (Yang Jingbo& Shen Pingping, 2010) was carried out, this classified passwords into categories as either strong or weak. However it is not clear on what a password would need to constitute to be in either category. This is important to understand as studies have shown users will choose a password and use this across 5 or more different websites (Florêncio, 2007) ; this is an insecure practice as compromise of one site could lead to a breach of others associated with that same password. It has been shown that a user can have up to 25 separate password accounts to maintain making individual and unique passwords more difficult to manage and remember. Further investigations conducted users were found to have forgotten passwords to more than a quarter of sites they were registered with (S& E.W, 2006) illustrates this problem. Bad password habits are becoming more common place and are not limited to merely reusing of passwords. Often extremely simple passwords are also likely to be selected and accepted by site security policies. A report (Leesa-nguansuk, 2011) shows that approximately one percent of users used “123456” as their password as well as other equally insecure combinations following a breach to social application site Rock You in 2010. As such, from a purely secure authentication perspective it is unclear why users continually fail to employ securer practices around the passwords they select.

It is not entirely clear why some users continue to take such a relaxed stance on protecting their online information with many online users often taking the approach of ‘it will never happen to me’. A study (Kabay, 2010) explains that risk reality and risk feeling vary between each individual, which goes some way to explaining users’ decision to take a passive approach in securing their online identity, others may not be clear of the risks involved where as others simply may not care. This technical naivety can clearly be seen through research that found novice users to be those most at risk from security threats (Furnell et al., 2008) based on their inexperience with web systems and the methodology to secure their identity. Therefore rather than a lack of actual risk, it is instead a lack of perceived risks to users, potentially indicating that users need to either be educated to understand the risks or policies should be enforced that recognise these risks.

The risks of improper password practice can be seen in security breaches ranging from Denial of service (DOS) attacks, phishing, replay attacks and identity theft. However, a balance must be struck between security and usability which is an incredibly difficult balance to achieve. This is particularly true when the pressure is on the user to ensure a secure password and a protocol is adhered to, rather than being provided with a secure password. Research into 154 different organizations websites found a password length of 8 characters was generally mandated, yet most users would prefer a shorter password (Barra et al., 2010a) which let the burden of maintaining a secure password remains with the user.

Over the years many different password protocols have been suggested to address common issues with web authentication. In a study (Me et al., 2006, Me et al., 2006) designed a protocol using time stamps to prevent relay attacks guaranteeing that no multiple authentication requests can occur. In addition to this a web authentication protocol designed by (Thiruvaazhi& Divya, 2011) using zero proof of knowledge which aim is to prevent impersonation attacks on password. The differentiating factor in this protocol was the clients password is never know by the server. These studies show that there are many new ways to address the common problems with password authentication, but they also suggest that new authentication protocols are not able to address all the issues. This situation is further compounded as web systems have developed and hacker's methods have become more sophisticated. While numerous password protocols have been designed, and many are successful and have individual merits, none have been selected as a widely adopted standard. The first, and one of the few criteria published to aid users with password selection, was produced by Microsoft. (Microsoft, 2005) gives examples of both strong and weak passwords and details about common attacks. By providing users with this information it allows users, particularly those less technically competent on Internet security threats, the ability to make an informed choice about securing their identity online. However, although users may be inexperienced it is still their right to be informed about what they are at risk of and what could be a best practice solution for their security needs.

The consideration of a balance with usability is important; however it is dependent upon the individual user to determine where this balance rests with them. While guidelines for measuring password usability have been established over the years, they have never been mandated or widely adopted (DOD, 1985). This may be because it is commonly felt amongst the majority of user groups that the responsibility of web systems security lie with the web systems providers, therefore assessment into web systems password policies is long overdue and could be useful to a wide range of stakeholders detailed below.

1.2 Project Outline and Research Question

The main aim of this project is to assess protocols in relation to security vs. usability by characterising the attributes of password protocols.

To do this an experimental project will be carried out; 150 web authentication systems will be accessed via a laptop and registration will be attempted with each of the websites. Attributes about each of the password protocols will be collected from both the registration page and the password reset pages of each website to ensure a complete view of all the guidance a user would receive is collected. These will be measured using the length, composition, and strength of the password. Additional metrics will also be assessed to evaluate the guidance on each website to determine how beneficial this is to the user's ability to implement effective security measures. The results will be analysed and compared against predefined metrics and recommendations will be made for secure and usable password implementation for the future of password security.

1.2.1 Objectives

The following objectives have been identified as key to the completion of the project:

- To research and gain greater understanding into password based authentication implemented as part of current web systems

- To research and gain greater understanding of the varying risks associated with password based authentication
- To research and gain a greater understanding of issues found in the varying implementation of password protocols online
- To research into the potential impact of poor guidance for users
- To research and investigate metrics currently used to assess security and usability within the industry
- To identify a range of websites that require authentication, and qualify the validity of these to be used in the experiment
- To characterise the attributes of password protocols
- To collect data of required password length and store this in a database
- Evaluate the data collected from each site and taking each of the password protocols and assessing these in relation to industry best practice.
- To derive a scheme for benchmarking the security and usability for each password protocol
- To analyse the data collected and provide a current benchmark for the password protocol
- To propose a solution to improve consistency in the industry and to improve the current practice

1.2.2 Research Question

Are current password protocols and their guidelines clearly articulated to allow users to make best use of and strengthen their security credentials?

1.2.3 Initial Hypotheses

Following initial research, the following hypotheses have been generated:

1. Web authentication systems are not universal in their application of password policies which reduces security in certain authentication environments

2. Web authentication systems are not universal in the information, guidance and policies provided to users to ensure strong passwords are selected

These hypotheses are based on the findings of experiments to password practices. (Furnell, 2007) found that password restrictions were not constant across a range of web authentication systems. This can be evaluated easily as if there is variation in this data can be collected within the experiment and the results can be evaluated to reflect if there is consistency or not.

1.2.4 Rational

The main outcome of this project will be an analysis of the suitability of existing password protocols to determine if these are suitable in assisting a user to choose a strong and secure password. In addition to this the project will aim to propose a secure and usable universal password protocol or a solution which will address the issues which have been identified with others and to address changes in technology. It is hoped that this project highlights the need for a more widely understood password protocol which can be understood and implemented by users with varying degrees of computer literacy.

2.0 Literature review

A review of literature pertaining to methods of online authentication is presented, providing a foundation and understanding of existing characteristics of secure authentication methods. In addition a range of implementations for password policies is identified and discussed analysing various examples of contrasting information. The thread going through the literature review discussing authentication methods as these

Evaluation methods are discussed within the review of literature so an understanding is achieved of suitable candidate methods that informed the methodology.

The key areas informing the literature review are:

- Risks associated with password authentication
- Varying implementation of policies
- Impact of poor guidance on users
- Methods to assess security and usability

2.1 Password Policies

This section will focus on the special features and attributes of password policies that allow users to make best use of the guidelines that polices provide as well as identifying any additional usability attribute which help to enable users to strengthen their credentials. Understanding the literature that surrounds this subject is crucial for the project as it is dependent on establishing what the typical problems and key issues that is associated with password protocols that realistic experiment can be defined. further to understanding the key issues it is imperative to the project to identify what the typical existing methods of strengthening password authentication are which should be appropriately detailed in literature to design an appropriate methodology. Thus currently guides web system developers on the design of web authentication systems and users on how to use web authentication system.

2.1.1 Password Usability and Security Problems

Extensive research into the problems with password protocols has been carried out since information systems have become prevalent within society. Through this research many problems have been identified with this type of authentication, despite it being the most commonly used form of authentication to date. This is reflected in statistics that show that it is generally the home user who accounts for most of these passwords, with 95% of targeted attacks on home users (Symantec, 2012). One of the most obvious issues with password authentication is human-memory. Memory issues are clearly demonstrated from a the security breach against well-known social networking site RockYou where 32 million passwords were exposed. This revealed that around one per cent of users used '12345' as their passwords along with other equally insecure combinations (Leesa-nguansuk, 2011). The reasoning behind these insecure selections is not clear although it would seem that users do not feel capable or desire to remember a more secure combination. Alongside this challenge of user engagement, new ways to overcome the issues with traditional password problems are proposed all the time. Such technologies are already reaching the market with technology companies Fujitsu and Oracle coming together to produce new biometric authentication technology for enterprises. In a recent study (Pirro, 2006) highlighted is a new technology which is focused on addressing the limitations of authentication through the human memory along with the issues associated with traditional passwords. What differentiates this technology is that it relieves users of the burden of memorability, in return requiring an attribute of their physical being to authenticate themselves. While this proves to be a possible solution for enterprises to employ there is no equivalent solution for home users, particularly through web based usage scenarios. This shows that in the current environment, it is still critically important that users are aware of the importance of selecting a secure password as this is likely to remain the core authentication method for the foreseeable future.

Other studies have identified that data mining (the processing of gathering data from online sources about a potential target) is the biggest weaknesses of password authentication. (Laudau, 2010) implemented a study aiming to develop a new approach to password authentication by authenticating the user based on their personal preferences as opposed to challenge questions. The study found that commonly used answers to these challenge questions can easily be found online through such data mining activities. This is supported by an experiment carried out (Nicholson, 2011) highlighting how easy it is to steal an identity in seven easy steps. The experiments findings proved that by gaining access to an email account, only by collecting random pieces of information. As a result of this initial access, the researchers were able to reset and gain access to the user's bank account which shows the clear potential for cross-site attacks. Furthermore, as the availability of personal data from social networking sites increases, the potential for guessing and data mining techniques also increases, this makes it all the more easier for attackers that can research answers to these questions via a simple online search to gain increasingly accurate information. These results show that in order to maintain the security of their passwords, users need to be educated into thinking about what they post or blog about themselves online, as this can be used against them gain access to their account.

More research into password habits by (Florêncio, 2007) determined that users will reuse a password 5 times on average. This increases the chance of a user's account being compromised through an increase in the number of attack vectors that are available to a third party. This risk is reflected through the fact that if an attacker manages to gain access to one account then the issue is not restricted to that account alone, as all of the accounts with the same password are now compromised. From this practice it is clear that users need to understand the consequential effects of other reusing passwords on multiple accounts to reduce this cross-site attack vector.

2.1.2 Trends

New trends in computing are factors which have been felt to contribute to problems with password authentication. (Lynch, 2011) in a study into identity management acknowledges the issues password authentication on newer services is not as robust as the overall market. This is supported by (Ely, 2010) who proposes that password management complexity will increase with the new trends in computing. This would mean that that there is a requirement for guidance on the issue and the release of some standards on the topic to allow users the chance to be more secure. Another trend in computing that has been identified by (Kikusema, 2011) that may have an effect on password authentication is with new slate devices and the loss of keyboards it may be time for a new way to authenticate. One of these new methods introduced is finalists for the Global Security Challenge 2011 method called pattern logins. Convinced this is the next generation of authentication method, CEO of Kikusema suggests the implications for the computing practice could be huge but although the password concept is very different from current methods, in order for the new technology to be adopted then users must be educated with this technology.

Research beyond the technological aspects has been focused on in a behavioural analysis of passphrase design carried out Keith et al., (2009). This identified the problems areas as memory related issues, typing issues and user perception of authentication credentials. These findings draw attention to the fact that the failings of password authentication are not purely down to passwords as a concept or the technology utilised to hold them, but how they are used by the password-holder.

2.2 Varying Implementation of Password Policies

This section discusses the variation in implementation of password policies and what the implications of this are for password security. It also identifies the effects on users and how the varied implementation of password policies modified or otherwise in order to allow users to make best use and strengthen their credentials. The majority of previous research within this field shows that the guidance given to users is generally varied and inconsistent.

This is further complicated when considering that it has been shown that a user can have up to 25 separate password accounts to maintain (Florêncio, 2007).Therefore if a different password policy for each of these websites is required, then the burden of password selection becomes too cognitively challenging for users to manage and remember. Whilst different accounts will have different requirements for security based on what the system is protecting, there is still vast variation in guidance which can negative effect on user's memorability. This shows the need for a unified password protocol or at the minimum industry recognised and accepted best practices to be defined and implemented widely to reduce this challenge to users.

2.2.1 Multifactor

Multifactor authentication is viewed as a more secure authentication method and is perceived as more secure. (Landau, 2010) describes multifactor authentication as offering more security then passwords and addressing previous issues with this method of authentication. Yet in a study on assessing and improving authentication confidence management (Pearce et al., 2010)the findings indicate that multifactor authentication provides users with false confidence. Despite users being told that this method of authenticating is more secure, it has been proven that it may give false confidence when authenticating. This shows variation in what users are told around the success of differing authentication methods. For a user this renders making a decision regarding password policies more confusing and potentially impossible due to conflicting information, this could explain the insecure password selections highlighted in 2.1.1.

2.2.2 Passphrases

Passphrases as a concept work in the same way as passwords but by definition is a textual-phrase and consequently are usually longer that a typical single-word password. Guidance shows that in recent reports users are instructed to choose passphrases as opposed to passwords. In a recent report (Abraham, 2011) implies that the passwords are decreasing as a favourable method of authentication and advises users to use passphrases as a more method of practice. This is contrasted by findings in an extensive behavioural analysis of passphrase design and effectiveness. It is noted that (Keith et al., (2009) while passphrases are easier to remember (and therefore helps to address the selection of insecure combinations referred to in 2.1.1), passphrases may increase typographic errors as more material is entered and reduce usability for the user. These findings show that passphrases may help to combat security versus memorability which is a common issue with password authentication often complex longer password may increase the strength of the password yet difficult for the user to remember. Therefore, reduce usability if the user encounters typographic errors which are more likely to occur the longer the password is. This is yet another demonstration of the ambiguity in password policies which further highlights the importance of evaluating current password policies in order to evaluate what guidance users are supported with.

2.2.3 Single sign on

One commonly proposed solution to stronger web authentication is to have one authentication method for all or multiple sites that a user is registered with. There is a trend towards authentication through Facebook or other trusted identity provides such as Hotmail and Gmail. Facebook logins are increasingly common as users can trust these identity providers and it reduces the end provider’s requirement to manage security. Example sites that use Facebook authentication are Netflix and Spotify this is commonly thought of as a more usable method as it requires less memory and effort for the user. There are a number of variations to this method. One approach, to log into multiple websites with the one password, has been developed by Qiang. (Qiang Wang& Zhiguang Qin, 2010) solution works by capturing users input into the password field, securely hashes the password and sends it to a remote site. As only the one change is made to the client side by initially installing a browser plugin, this makes this authentication method more convenient for the user and easier to deploy than other methods. However, what must be considered is that fact that whilst this may be more convenient for users, if compromised the results could be more catastrophic than that of one password for one site (Qiang Wang& Zhiguang Qin, 2010) the same issue would occur for any single sign on route.

2.2.4 Security Perception

When considering the perception of security, contrasting information is shown in an article on re-evaluation into authentication systems; (Moss, 2011) this indicates that later in 2012 the National Credit Union Association (NCUA) will evaluate the controls of credit unions who offer electronic services. The new policies are expected to include risk assessments, member authentication for high-risk transactions and layered security programs and authentication techniques. The aim of these new policies is to cater for more sophisticated hackers who may target credit unions for financial gain. The issues with this are that when users see this tightening of security measures it can be confusing as to why increased security is required. Users may think that there is a current security risk, and that their accounts are not as secure as an account with the new policies. Consequently, users think of their password for these systems are of less importance as they're perceived as less secure anyway. More importantly, internet services providers need to be acutely aware of the perception portrayed via their choice of password policy. In a report (Quittner, 2011) it is explained that banks have concerns about putting extra security measures in place and having customers feel they are being inconvenienced. Users need to feel secure and as a consequence may become worried if they feel slacker measures are taken in situations where they feel there should be more rigorous protocols in place e.g. online bank accounts. This is shown as (Ernst et al, 2006) explains workplaces need to promote security practices in relation to the consequences of these systems being breached. The findings discussed in this section show that variation of password policies impacts the perception of security.

2.3 Impact upon Users of Poor Guidance

This section discusses several studies that have identified potential impacts of password protocols on usability and security, and what could be done to improve this.

Despite the findings discussed in 2.2.4 another assessment of password practices found that (Furnell, 2007) in some cases websites such as Amazon and EBay provided no initial guidance to the user when setting up their credentials. This indicates that even some of the world's largest website providers are not taking the time to educate users; this could result in a negative impact to users, who could use an existing personal password thus increasing the likelihood of an attack on their accounts.

In a study of password preferences (Barra et al., 2010b) demonstrated what users password preferences are. Findings of the study showed that users felt organizations that required users to use alphanumeric passwords were less usable opposed to character based passwords. This implies that the burden of password creation is the responsibility of the users and not that of organisations that are merely providing advisory information.

Furthermore a study into password protocols (Adams& Sasse, 1999) findings revealed that users resulting in making up their own assumed guidelines regarding what constitute a secure password this shows the impact poor guidance has on users when users of a varying IT literacy make up their own guidelines. Users have had to make a best guess at what makes a password secure. This ambiguity highlights the need for more clarity on password policies showing that more can be done to educate users.

In a recent study into the influence of awareness and training on cyber security (McCrohan et al., 2010) investigates the effectiveness of user training has on online security. Findings of this study show how impactful awareness can be for individual users and their organisations. This highlights the potential negative impact lack of guidance can be on users and organisations.

2.3.1 Impact of poor Usability to users

This section alludes to several of the consequences of poor usability in web authentication systems, a study into the challenges faced with future security systems (Joyce, 2008) it is noted that if a user is cannot use a system it will cease to be adopted. This suggests that web providers should not take a more relaxed stance of guidance they provide to users but improve this to facilitate the use of new systems and adoption of new technologies. The risk of poor usability to users could mean a standstill in the adoption of new technologies and systems. This alludes to the importance of usability to ensure continual adoption and advancement.

2.3.2 Responsibility for password policy education

Establishing which entities are responsible for educating users must be concluded in order to inform the methodology. A core issue with password authentication systems is that it is felt that users are ultimately responsible for keeping their online assets safe, but most users lack support and guidance from those more informed sources. In an investigation into security obstacles for users (Furnell et al., 2008) aimed to determine the views of users around who held responsibility for protection, and the obstacles that exist to achieving it. Findings revealed subjects of the interviews felt the responsibility of password policy education lay with users themselves, software companies and government bodies. As discussed in section 2.2.3 this is contrasted by (Ernst et al, 2006) who suggests the responsibility lies with workplaces that have the overall responsibility for educating users on secure password policies.

It is clear that the responsibility for password policy education lies with more than one entity. As these different entities will have different priorities, views and consideration this provides explanation as to why there is such ambiguity and variation in passwords policies (to reflect these differences in priorities).

2.4 Current password policy standards

This section will identify suitable methods for assessing the effectiveness of password protocols. In this section of the literature review many ways have been identified and discussed that are commonly used to qualify a password as secure or otherwise.

2.4.1 DOD

Historically the Department of Defense (DOD) has been used as one of the main industry standard. In 1985 the Department of Defense (DOD, 1985) required that users take a "common sense" approach to establishing password protocol thus, leaving it up to the user to decide what this is. As this has been adopted as industry best practice for a period of time it would be useful to incorporate this into the method of assessing if current password policies mandate that users take a common sense approach to establishing their passwords, however it is important to realise that 'common sense' is difficult to measure and qualify.

Furthermore, industry-wide recommendations and guidelines have also been difficult to implement with limited examples of success in a consistent way. One example can be seen in the new guidelines from the US Federal Financial Institutions Examination Council (FFIEC) (Moss, 2011) which shows that the financial services industry is moving to strengthen authentication in light of the fact that older guidelines were no longer relevant to modern threats and technologies. However, these are not definitive guidelines and are not used as common practice across all web systems users.

2.4.2 Personal Preferences

As highlighted in a study (Patent Bridge, 2008) explains the new technology authenticates users based on their likes and dislikes as it has. It has found through well-known psychology research that users' passwords based on personal preferences are a more stable choice than passwords that are based on long term memory. This is supported by (Christie Nicholson, 2011)which states it is wiser to use questions that ask about preferences or obscure things as opposed to data that can be looked up via a simples internet search. Based on these findings it would be useful from the primary methodology to assess if users are required to selecting a password based on a personal preference or otherwise

2.4.3 Microsoft

Further to the ways outlined above one other way of assessing the effectiveness is by investigating if current password policies comply with Microsoft's published guidelines which aim to guide users on what constitutes a strong and weak password. (Microsoft, 2005) suggests password fall under the following two concepts and comprised of the attributes outlined below. It is important to consider Microsoft's best practice guidance as they are the leader in software and online services as well as providing one of the largest online authenticated services, Hotmail. Microsoft propose the following;

A weak password:

- Is no password at all.
- Contains your user name, real name, or company name.
- Contains a complete dictionary word. For example, Password is a weak password.

A strong password:

- Are at least seven characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete dictionary word.
- Is significantly different from previous passwords.
- Passwords that increment (Password1, Password2, Password3 ...) are not strong.
- Contains characters from each of the following four groups: uppercase letters, lowercase letters, numerals and symbols found on the keyboard.

2.4.4 Strong and Weak

The strong and weak password concepts defined in Microsoft's guidance is supported by (Jiang Huiping, 2010)a study into strong password authentication protocols which aims to modify current authentication protocols to make password resistant to common attacks. Further to (Microsoft, 2005) guidance (Jiang Huiping, 2010) categorises password protocols as strong and weak. It would be effective from the primary methodology to investigate which concept the password policies used in the experiment would be categorised as. Hence as Microsoft is such a well-known organisation, and 'strong' and 'weak' are terms which are commonly referred to when discussing passwords, this guidance would be useful when assessing strength of password policies. It is noted that there is no guidance used that suggests users should consider using their personal preferences for password selection as mentioned above in this section thus highlighting the need for a more comprehensive method of assessing passwords.

Furthermore one way of assessing the effectiveness of password protocols is to investigate if current password policies require a user to use security questions. As reported by (Kearns, 2010)the use of security questions within a password policy can unveil important information about the user therefore not aiding to privacy and security. Hence it will be useful to investigate if password policies used in the experiment warn users against the use of security questions which may be exploited by attackers or otherwise.

In a study into mnemonic password practices (Oghenerukevbe,E., DME,BSc, MSc, 2010)analyses the strength of character based passwords in comparison to mnemonic passwords. Findings suggests that mnemonic passwords although perceived as more secure, are similar to character based password in that they are susceptible to human attackers and automated tools. Thus it would be useful to assess current password policies establishing which of these require user mnemonic passwords. As a way of determining which password policies are more effective.

In addition there have been guidelines published by the United States Government as guidelines for assessing usability (William E. Burr Donna F. Dodson W. Timothy Polk, 10/01/2012)details four levels of password strength.

For password (or PIN) based Level 1 authentication systems (William E. Burr Donna F. Dodson W. Timothy Polk, 10/01/2012), the probability of success of a targeted on-line password guessing attack by an attacker who has no a priori knowledge of the password, but knows the user name of the target, shall not exceed 2-10 (1 in 1024), over the life of the password. There are no min-entropy requirements for Level 1.

For password based Level 2 authentication systems (William E. Burr Donna F. Dodson W. Timothy Polk, 10/01/2012), the probability of success of an on-line password guessing attack by an attacker who has no a priori knowledge of the password, but knows the user name of the target, shall not exceed 2-14 (1 in 16,384), over the life of the password. Level 2 passwords shall have at least 10 bits of min-entropy.

Files of long-term shared secrets used by CSPs or verifiers at Level 3 (William E. Burr Donna F. Dodson W. Timothy Polk, 10/01/2012) shall be protected by discretionary access controls that limit access to administrators and only those applications that require access.

Files of long-term shared secrets used by CSPs or verifiers at Level 4 (William E. Burr Donna F. Dodson W. Timothy Polk, 10/01/2012)shall be protected in the same manner as long-term shared secrets for Level 3

Although a limited number of guidelines and recommendations have been published, no formal definition has been defined despite web authentication being the forefront of the internet (Yang Jingbo& Shen Pingping, 2010)

2.5 Overview of Literature

The objectives of the literature review were to provide a foundation and understanding of existing methods of online authentication is presented, provide a foundation and understanding of existing characteristics of secure authentication methods today. The literature review highlights a range of implementations for password policies and the impact it has on users is discussed. Various examples of contrasting guidance users are given is discussed. The review also discusses the responsibility of informing users about secure password policies. The rule sets are the essence of the research. Perhaps the most significant conclusion that can be drawn from the review of literature is that password policies need to promote security requirements. Hence, this is the reason why these key areas have been taken into the projects method**.**

3.0 Methods

3.1 Experiment Environment

A number of security factors have been discussed within the review of literature, following this discussion a set of variables that should be tested as part of this experiment have been defined. These variables will be used to determine the security and usability of password policies across the sample data set. The variables the experiment will assess are a combination of Microsoft's guidance and additional usability and security attributes.

The reason for this choice to focus on Microsoft's guidance as a primary source for the variables in this experiment are due to the fact that Microsoft has one of the largest online authentication systems in the industry through their Windows Live ID infrastructure and Hotmail services. Furthermore, due to Microsoft's longevity and experience in this field, it is reasonable to believe that newer less experienced web authentication systems are likely to recognise Microsoft's leadership in this area and follow such published guidance. As a summary, Microsoft proposes the following recommendations for all passwords that authenticate a user. Whilst this has not initially been defined as for online systems, no specific guidance exists for requiring different online and offsite authentication processes.

- Passwords must be at least seven characters long.
- Password does not contain your user name, real name, or company name.
- Password does not contain a complete dictionary word.
- Password is significantly different from previous passwords.
- Passwords that can be incremented are not advised.
- Passwords should contain characters from each of the following four groups: uppercase letters, lowercase letters, numerals and symbols found on the keyboard.

Alongside this guidance from Microsoft, literature and further industry recommendations have been collated into the thirteen variables that this experiment will test for on 150 sites across each of the three business model groups.

The following sections explain each of the individual variables and seek to justify and validate the use of each of these variables. Furthermore, these sections explain the individual variables suitability to be included in this experiment along with the source of each variable.

To assist for easy discussion and identification with each of the thirteen variables, each of the variables has been assigned a variable code such as V1, V2 or V3. These are defined below and will continue to be referenced throughout the analysis and conclusions to ensure consistency.

3.2 Security Variables

3.2.1 V1 passwords should be at least 7 characters

The first variable we will examine in this experiment is a guideline proposed by Microsoft, the purpose of which is to help a user select a password of an appropriately secure length. As discussed in the literature in section 2.1.1users commonly have difficulty in remembering passwords as they feel they are not able to remember long combinations for authentication. However while this is a usability issue, it is widely known that user accounts are more vulnerable with a shorter password (Leesa-nguansuk, 2011). As part of their recommendations, Microsoft propose a strong password that is at last seven characters in length, for the purpose of the experiment this was felt to be a realistic number, and also while the issue of usability was considered, it was felt that seven characters was not a high enough level which would overburden the user therefore V1 will be assessed within the experiment to help determine the secureness of the sample set of sites.

3.2.2 V2 Passwords should not contain real name, username or company name and

In section 2.4.3 of the literature review, guidelines proposed by the United States Government are discussed. In these discussions, a ranking system is proposed for the levels of security required for different types of systems from US Government; these levels are proposed to range from 1 to 4. Level 1 is said to be the least secure with a probability of access if the attacker knows the username of the user, Burr et al (2012). This research suggests that advising users not to use their username as a password correlates to an increased level of security regarding their account. Therefore, it is important to assess the presence of this variable in websites to help determine their security practices with regard to end users passwords.

3.2.3 V3 Passwords should not contain a complete dictionary word

As discussed in the literature review users often use passwords which are easy for them to remember to improve usability of authentication. However, whilst the use of dictionary words as a password is common amongst users, one of the most common password hacking attacks is the dictionary attack Zhang et al (2009) which can crack any password that can be found in the English dictionary. The non-use of dictionary words in passwords is one which is proposed by Microsoft; therefore as the use of dictionary words within passwords has such a detrimental effect on the security of passwords, the presence of this variable is important to assess and therefore this will be assessed within the experiment to help determine the overall security of the password policies as the third variable.

3.2.4 V4 Passwords should be significantly different from a previous password and

As discussed in section 2.1.1 of the literature review, it is commonly known that users often develop bad password habits by using previous passwords again (Florêncio, 2007). It is proposed by Microsoft that secure password users use significantly different passwords and do not increment these, sites that do this are more are risk from cross site attacks therefore to assess the overall security of the password policies the presence of this variable will be tested in the sample set.

3.2.5 V5 Do not increment passwords

Similar to the experiment variable discussed in 3.2.4, users often develop bad password habits by using incrementing an old password e.g. password, password1, password2 etc. (Florêncio, 2007). It is proposed by Microsoft that secure password users use significantly different passwords and do not increment these, sites that do this are more are risk from cross site attacks therefore to assess the overall security of the password policies the presence of this variable will be tested in the sample set.

3.2.6 V6 Do not use animal pet names as passwords

In section 2.4.2 of the literature review it is proposed that users use personal preferences when constructing passwords as opposed challenge data e.g. animal pet names which can easily be found online (Nicholson, 2011). It is felt that websites that notify users of this risk are more likely to take suitable precautions and in turn less likely vulnerable to data mining and socially engineered attacks, therefore this variable will be assessed within the experiment to help determine the overall security of the websites password policies.

3.2.7 V7 Composition - uppercase, lowercase, numerals and symbols

As mentioned in the above sections, a dictionary attack is the most common type of password attack. However the way to increase security of a password from a dictionary attack is to use a mix of composition within the password. This reduced the capabilities of a dictionary attack by increase the potential adaptations that a dictionary word could be formed as. As composition can help to increase password security (Microsoft, 2005) the project will assess the presence of the Microsoft guideline to help gauge how secure the guidelines advised by the sample set of sites within this experiment are.

3.2.8 V8 Instructions after a failed login attempt

This variable will be used to help indicate how a password policy may impact upon usability of the authentication method. This links to the fact that It is widely understood that for a technology to be successful users must understand it (Ernst, 2006), this principle is applicable to users and websites also and therefore influences the authentication practices of a website. From a usability perspective it is important to assess if a user's is given feedback on how to proceed should they provide an incorrect password, without this the security and authentication of the site has hugely reduced the usability of this site. This will be assessed within the experiment to help indicate whether this security policy has impacted the usability of the site.

3.2.9 V9 Presence of Strength meter when choosing a password

It has been discussed within the literature review that users have taken to making up their own password guidelines when they need to (Adams& Sasse, 1999), this is an insecure practice particularly for users that have less IT literacy skills. Therefore, it is important to determine whether website providers are providing an easy and accessible route for users to understand what poor passwords are, and how to improve these. As a means of providing instant feedback on a user's selected password a strength meter is a commonly utilised method, therefore this variable will determine the presence of this functionality and therefore indirectly understand the impact this has on improving the strength of a password selected by the user following the strength meters recommendations.

3.2.10 V10 Password must not be user ID

This variable will also be assessed within the methodology but unlike V2 discussed in section 3.2.2 this variable is limited to guidance around just the users ID.

3.2.11 V11 CAPTACHA

The project will assess if users are required to enter a CAPATCHA code, this is known to prevent against scripting attacks. From a security perspective it is important to assess that it is indeed a user attempting to sign in and not a machine programmed to guess a number of password. To assess all the websites for this security attribute to understand the presence of this variable within the websites.

3.2.12 V12 Password sent directly to user on registration

The project will assess if users are sent their passwords in plain text to their email account, as this is clearly a security challenge. This is known to compromise password security as the email can be intercepted or the password obtained from the user's computer via a socially engineered attack or a cross site attack whereby the unauthorised access is gained to a user's email account then allowing access to all other passwords sent in plain text. The foundations of a password are that it is something you know and is maintained tacitly within the user. By sending the users password to them in email this changes to something a user has in a digital item and therefore makes it more vulnerable to these types of attacks. The project will assess which of the sites send their passwords directly to users and use this information to understand the presence of this variable within the sample set.

3.2.13 V13 Secret Question

Many websites utilised security questions as an alternative way users can authenticate themselves to a site should they forget their password or user credentials. Whilst this is a useful feature that gives a user another option should they forget their details, it is highlighted within section 2.4.3 that security questions can also reveal to an attacker what information they need to obtain about a user via data mining or other attacks to gain access to their account (Kearns, 2010). For the purpose of the experiment the interpretation of this variable is that while it provides usability for users, it must be understood the presence of this variable to understand the risk associated with a security question.

The methods section outlines the experiment environment and the metrics used to undertake the experiment.

This section will describe the methods used to evaluate the effectiveness of the password protocol. The primary research method in this experimentally based project will be stated and justified as to why this method has been selected to investigate whether password protocols are articulated clearly by giving the user enough information to construct a secure usable password. A detailed outline of the precise nature of the intended experiment will be given including an explanation and justification of the selected websites to be used within the investigation. As this is an experimentally based evaluation project that involves human computer interaction and the collection of password attributes additional explanation will be provided as to why these attributes were considered appropriate to act as evaluators for the demonstrating of effectiveness of Password Protocols and any limitations these attributes may impose on the ability to generalise.

3.3 Primary Research Methods

3.3.1 Site Selection

In order to draw statistically valid conclusions the project aimed to identify and collect data of a large number of sites across the major use cases for password authentication. By exploring Alexa traffic ranking websites it was found that the project could utilise a 150 of the listed sites that provided a method of password authentication. The sample of sites were reviewed and classified into one of three internet business models so a comparative analysis can be carried out on the experiment results. The three categories of password collecting websites are:

- E-commerce sites
  Websites that's purpose is to sell and goods to a user, websites that fall under this category have a relationship with the merchant and not with other users.

- Identity sites
  Sites which allow a user to create an online identity or profile to interact with other users with this persistent identity
- Content sites
  This category is not specific to news websites; this category largely classifies any site where user can control what they see e.g. one which they can save their preferences on.

It must be noted that these categories are not exclusive for all purposes of the experiment.

There was some limitation at this stage of the experiment as the project could only utilise sites offering free accounts and not member only sites. Therefore, banking websites alongside websites not in English, pornographic websites and premium websites such had to be excluded for the purpose of the experiment.

3.3.2 Procedure

Each site was evaluated by a manual process of physically opening the webpage and attempting three features of the website. Firstly, registering with the site, then attempting to login with an incorrect password and finally attempting to reset the password. The presences of the variables were assessed throughout this procedure. The data was recorded in a database in the form of a “1” or a “0”, a 1 was assigned in the website used this variable and a 0 was assigned if website did not implement this variable.

3.3.3 Registration

On each website all sign up was done with an identical set of user data. All of the password advice given to the user at registration stage was recorded; the majority of the variables were collected from this user interface.

3.3.4 Attempted failed login

The project attempted to login to each of the sites with an incorrect password. The data collected at this stage was purely to help determine usability, if a user is given advice or provided with an option to move forwards and are not essentially locked out of their account with no advice on what to do next.

3.3.5 Password reset

The project attempted to reset each of the sites passwords. The data collected at this stage was mostly on whether or not the site advised the user to change their password from their previous selection.

3.4 Method Analysis

This section aims to give an analysis of the primary research methods given in this report.

3.4.1 Primary Method

The project aims to evaluate password policies in relation to security vs. usability through an experimental categorisation of the authentication rule sets. The project is an experimental project as defined in (Oates, 2006) where typical experimental studies include repetition, observation and measurement, proving or disproving a relationship between factors and explanation and prediction.

3.4.2 Analysis

Data collection from the websites is stored in a database. The database contains output based on the variables set out for the experiment. Each website will have 11 results as outlined in section 3.1.1 and further justified in the following sections. The data presented for conclusions will be based on the average and median calculations take for all websites and separately for sites within the different categories. The hypothesis will be analysed. Data will be presented in graphical format with detailed analysis of the findings.

3.4.3 Conclusion

The data can be analysed and the different business models compared against one another to see if trends in one type of business model can be identified. The data collected and the results of the analysis will show the variance in variables in password protocols of different types of internet business models. This data can be used to identify the weaknesses and strengths of the protocols depending on the environment. The results of this research also provide insight into which password policy variables are commonly used and which are least used.

4.0 Analysis of Results

This section of the report will evaluate and document the findings of the primary data gathered from the execution of the experiment as documented in the methods section 3. The password policy index rating will be identified and aims to evaluate across different business models which websites follow best practice and give users more opportunity to strengthen their credentials. Graphical representation of these results will be provided along with discussion as to what they mean in terms of password security within this section.

4.1 Introductory overview

The purpose of the experiment is to evaluate password policies through an experimental categorisation of the authentication rule sets of a significantly large number of popular websites across three commonly used internet business models. The three business models defined to be used in the experiment as content, e-commerce and identity.

This project is a large scale categorisation where by assessing actual websites password policies to see if the employ best practice security features to allow users to make best use of and strengthen their credentials.

Experimental categorisation was deemed the best way to evaluate the strength of the password policies as all the data required of each of the variables outlined was obtainable from doing so. By following the methodology of register on the site and reset the password on the site this was the most realistic method of collecting information about the variables as this is what a real user would experience.

4.2 Variable analysis

4.2.1 V1 passwords should be at least 7 characters

Based on the guidance provided by Microsoft (Microsoft, 2005) it is stated that strong passwords should have at least 7 characters in length as this helps contribute to password strength.

Overall 35 websites advised users to choose a password of 7 characters or above this is a fairly low portion of the 134 sample set. The result is that users are less likely to choose passwords of a suitable secure length. As can be seen from Graph 1 there is little variation in the type of site that implements this, although a slight trend can be seen in that slightly more e-commerce websites implement this variable.

This security attribute is proposed so as the longer the password the more difficult it is for a hacker to guess. Therefore, this shows us that as the websites that returned a negative result there users are more likely to choose passwords of a shorter length thus making it easier for attackers to guess. These websites are not contributing to helping users build up password strength.

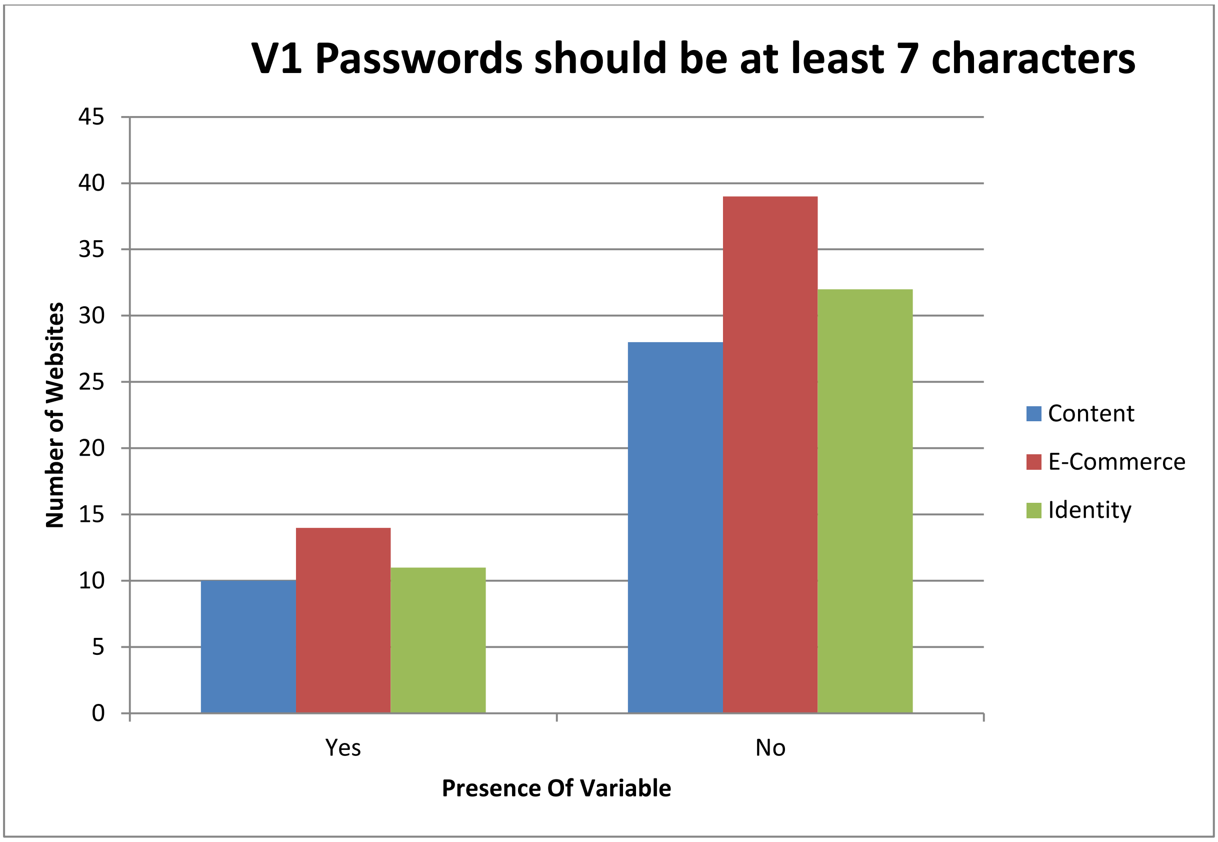


Figure 1 V1 passwords should be at least 7 characters

4.2.2 V2 Passwords should not contain real name, username or company name

Whether or not users were advised not to use their real name, username, or company name in the construction of their password was assessed within the experiment. The results can be seen in Figure 2, identity websites returned the highest number of positive results showing which suggest this type of site is more likely to implement V2. A trend can also be seen in e-commerce type sites as 43 of 53 websites returned a negative result for this variable. As e-commerce websites returned the highest number of negative values on assessment it shows that these websites are less likely to implement V2 which is worrying. Section 2.1.1 of the literature review discusses data mining techniques which are made exploitable by using freely available information online about a user e.g. real name, username and company name.

From the graph we can see that those sites that more than 75% of sites did not do this it is conceivable to conclude that as these sites have taken less responsibility for educating users on secure password policies users passwords strength will be reduced.

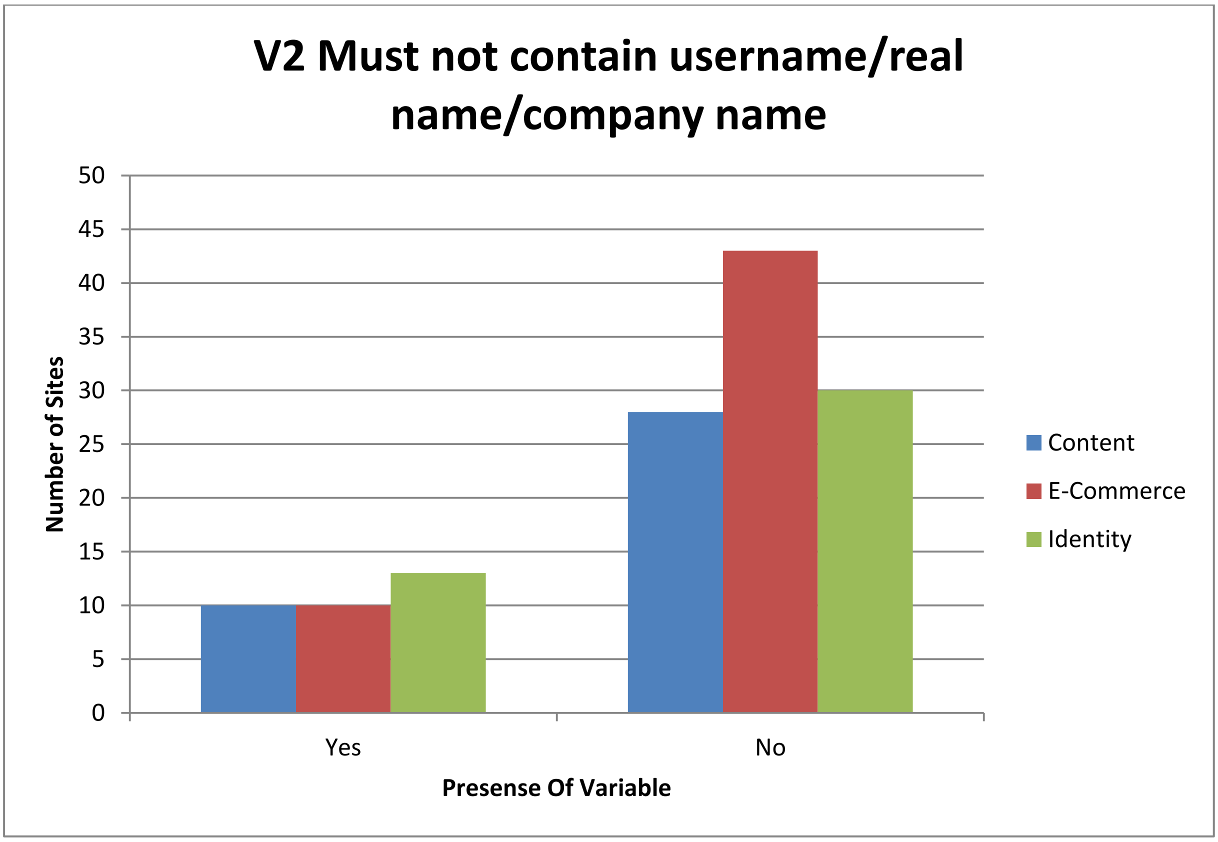


Figure 2 V2 Passwords should not contain real name, username or company name

4.2.3 V3 Passwords should not contain a complete dictionary word

As is discussed in section 2.1.1 of the literature review, passwords that contain dictionary words are easily obtainable via dictionary attacks. The presence of this variable was assessed in the experiment and results can be seen from Figure 3. From the results of the analysis it is evident that this advice is more frequently provided within e–commerce sites as these sites returned the highest number of positive results which was 20 out of 53 sites. Content websites also returned a large number of positive values from the sample set with 14 sites out of 38 using this variable. V3 was less likely to be used by identity websites as only 13 of 43 used this as part of the policy.

Overall this variable scored highly with 47 of 134 websites provided this advice to users while it is good to understand that overall there is a strong variation between the different categories of site.

It can be conceived that the sites who did not promote this variable take less of a responsibility when it comes to educating users with information on how to enhance their credentials and therefore users of these sites are more likely to be victims of dictionary attacks than users of sites that do not promote this aspect of password security.

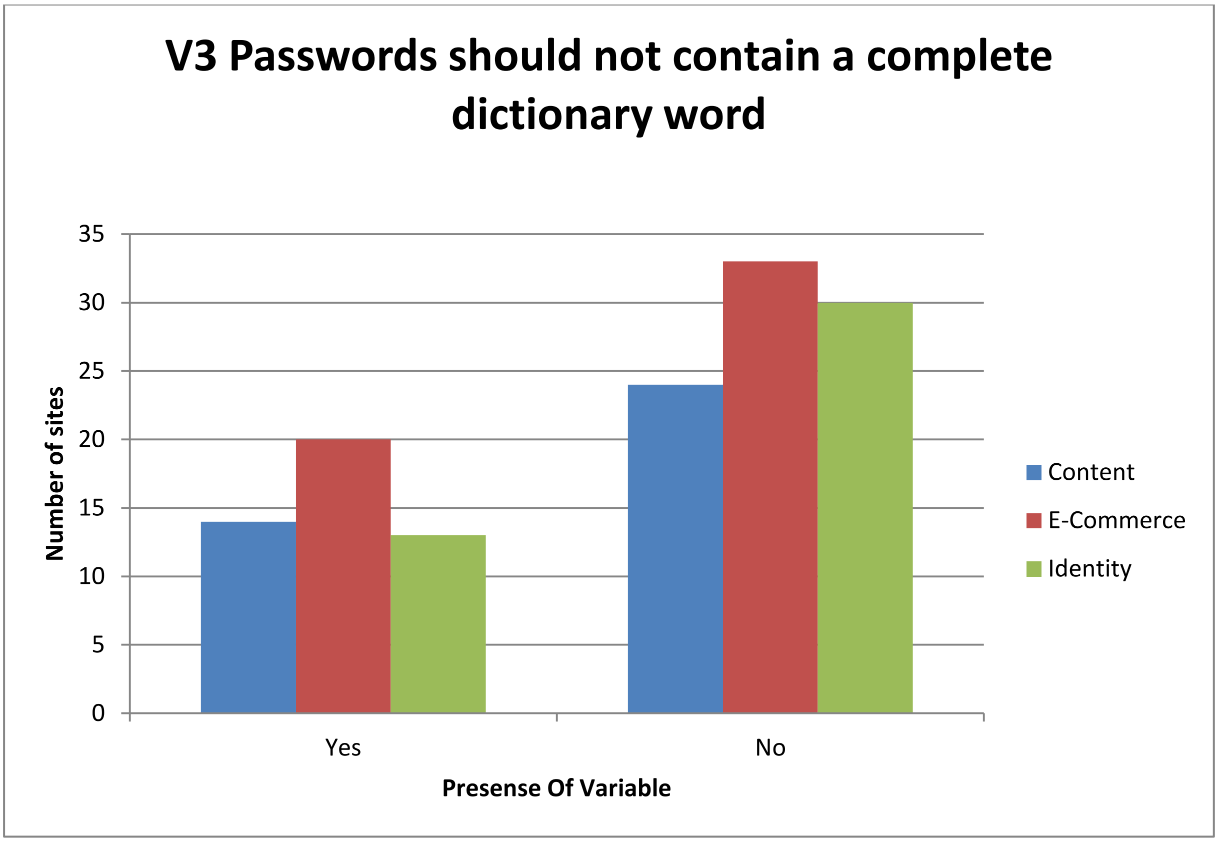


Figure 3 V3 Passwords should not contain a complete dictionary word

4.2.4 V4 Passwords should be significantly different from a previous password

In the literature review it is discussed that users often do not change their passwords and are known to reuse the same password up to five times (D. Florêncio, 2007). This variable was assessed within the experiment as graph 4 shows there was little variation in the presence of this security attribute across the three different business models from the sample set with identity websites marginally more likely to impose this as part of their password policy. The results indicate that the users of websites that do not promote this advice are more likely to use passwords multiple times across multiple sites - lack of V4 has the same negative effect that the absence of V1 provides they are make it easier for an attacker to guess particularly in the user has had the same password for a number of years.

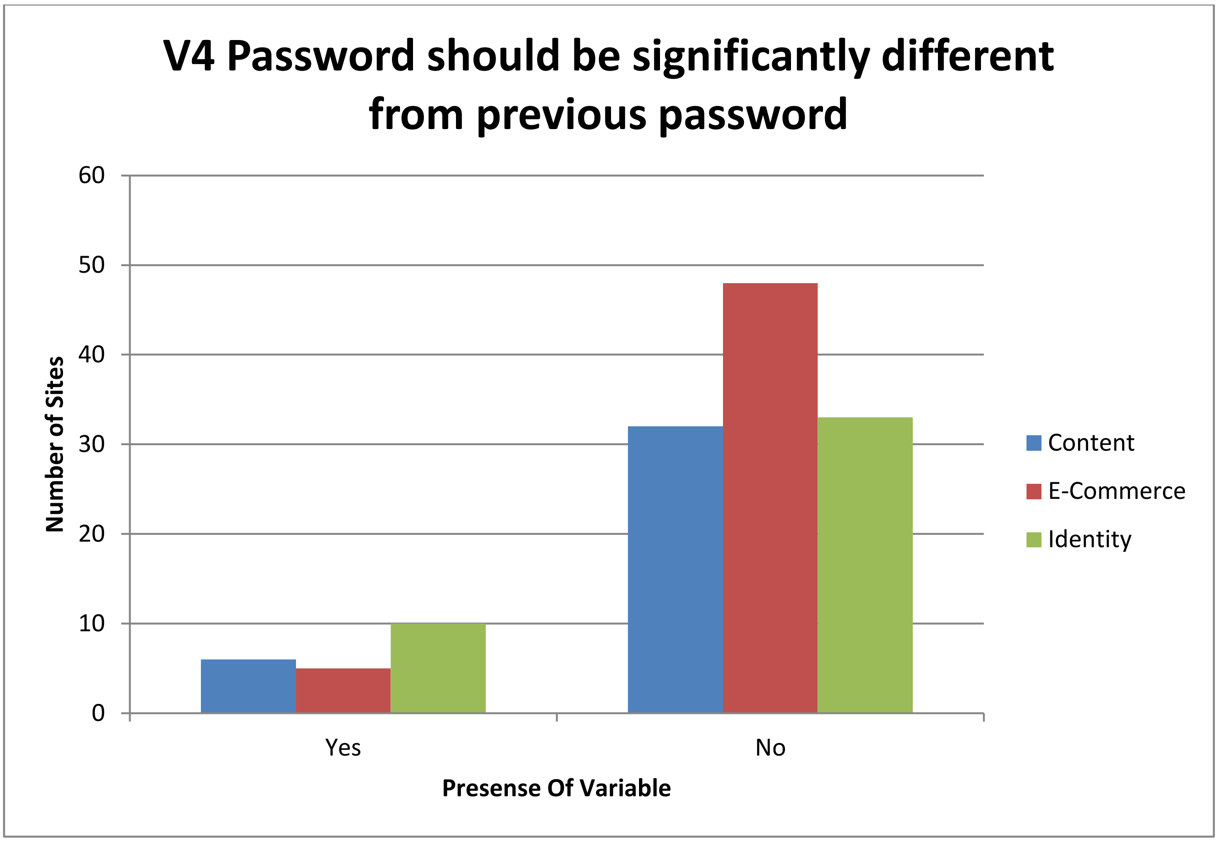


Figure 4 V4 Passwords should be significantly different from a previous password

4.2.5 V5 Do not increment passwords

The results of V5 analysis show the industry is not following the guidance published by Microsoft discussed in section 2.4.2 which advises users not to increment their passwords. As illustrated in Figure 5 only a limited number of websites used this security variable as part of their sites password policy. This is particularly present in the fact that no content site users and only small numbers of identity and e-commerce. Therefore, results we can see only a small number of users are being advised not to increment their passwords which as discussed in the literature review is not a secure way of securing online assets. This shows that as the majority of the sample set of sites are not taking the responsibility of highlighting this to users, it is likely that users are uneducated to the risks associated with incrementing passwords.

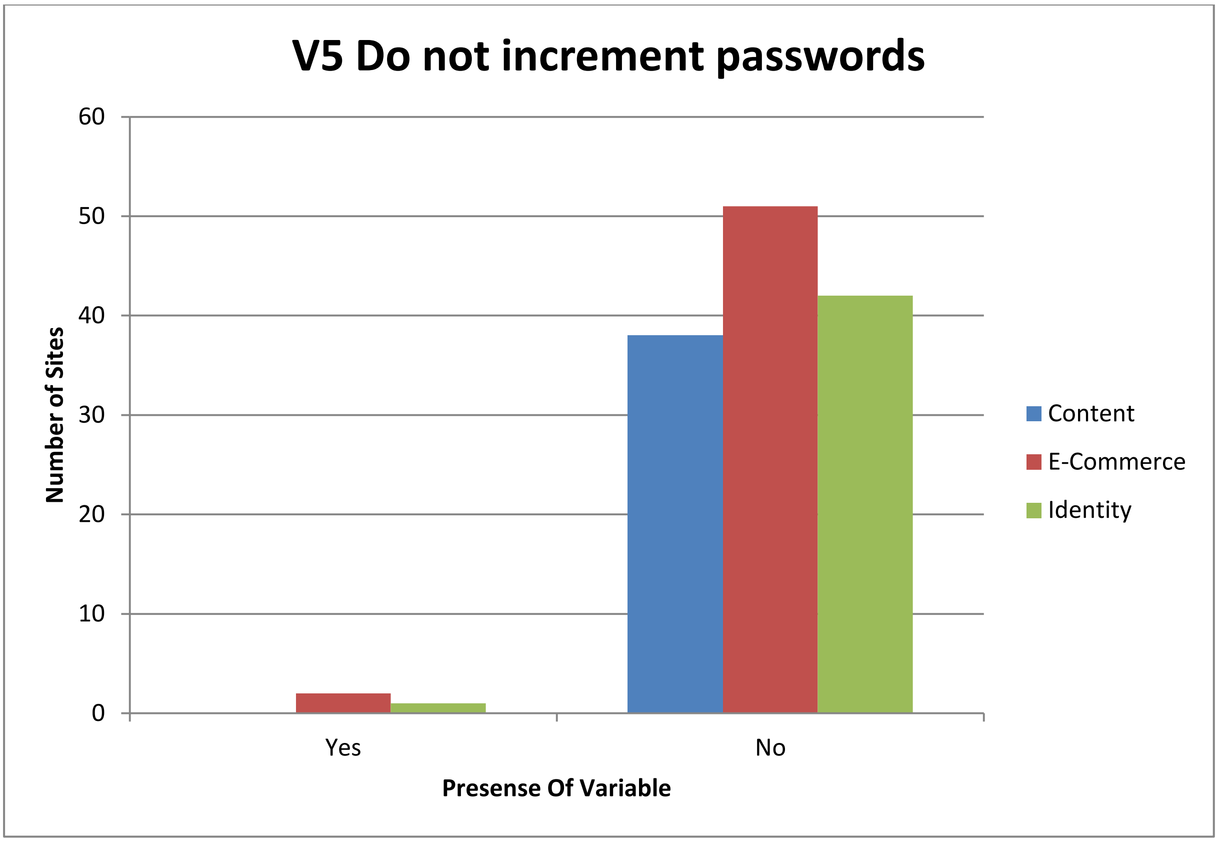


Figure 5 V5 Do not increment passwords

4.2.5 V6 Do not use pet names as passwords

Based on guidance also proposed from a study into password security (Nicholson, 2011) it is suggested that users do not use challenge data as passwords. E.g. pets names as this is easily researchable and could compromise the strength of the password. As Graph 6 shows there is no variation in the presence of this variable as a recommendation of password security in the different categories of websites assessed. This security attribute is proposed so as the password is not found easily found out by a hacker using external research or socially engineered attacks. This result shows us that the sites that returned a negative result in relation to this variable are more susceptible to data mining attacks. It is anticipated that the large sample of sites that do not publish this guidance on their websites do not take as much responsibility to educate their users as the websites that do advise this within their policy. This is a variable that when not present also contributes to preventing user's building the strength of their passwords due to this reduced level of user education.

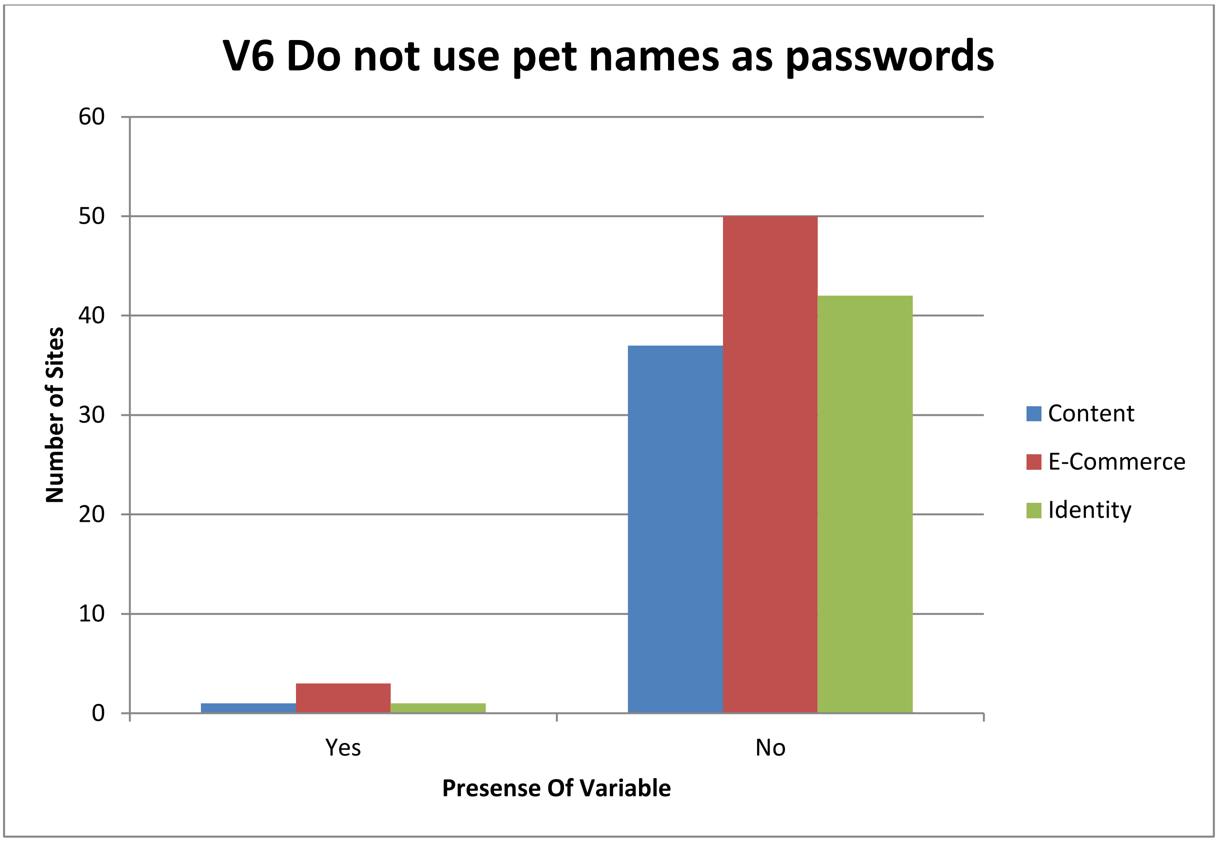


Figure 6 V6 Do not use pet names as passwords

4.2.7 V7 Composition - uppercase, lowercase, numerals and symbols

Based on guidance proposed Microsoft (Microsoft, 2005) it is proposed that user should use a mix of composition when to construct a secure password, this is supported by (Barra, 2010)who suggests passwords should be alphanumeric to protect them from dictionary attacks password guessing attacks. As can be seen from Graph 7 this variable is more commonly used by sites than the others assessed. It is clear that instruction to use composition is more commonly advised by e-commerce websites which shows that whilst content and identity websites scored reasonably well and there was marginal variation between the two categories; e-commerce type websites take more responsibility of educating users about this particular security variable. The presence of V7 aids somewhat to helping to defend against dictionary attacks due to users avoiding this composition of their passwords. The difference in presence of this guidance between the samples continues to highlight the lack of consistency of advice provided to users.

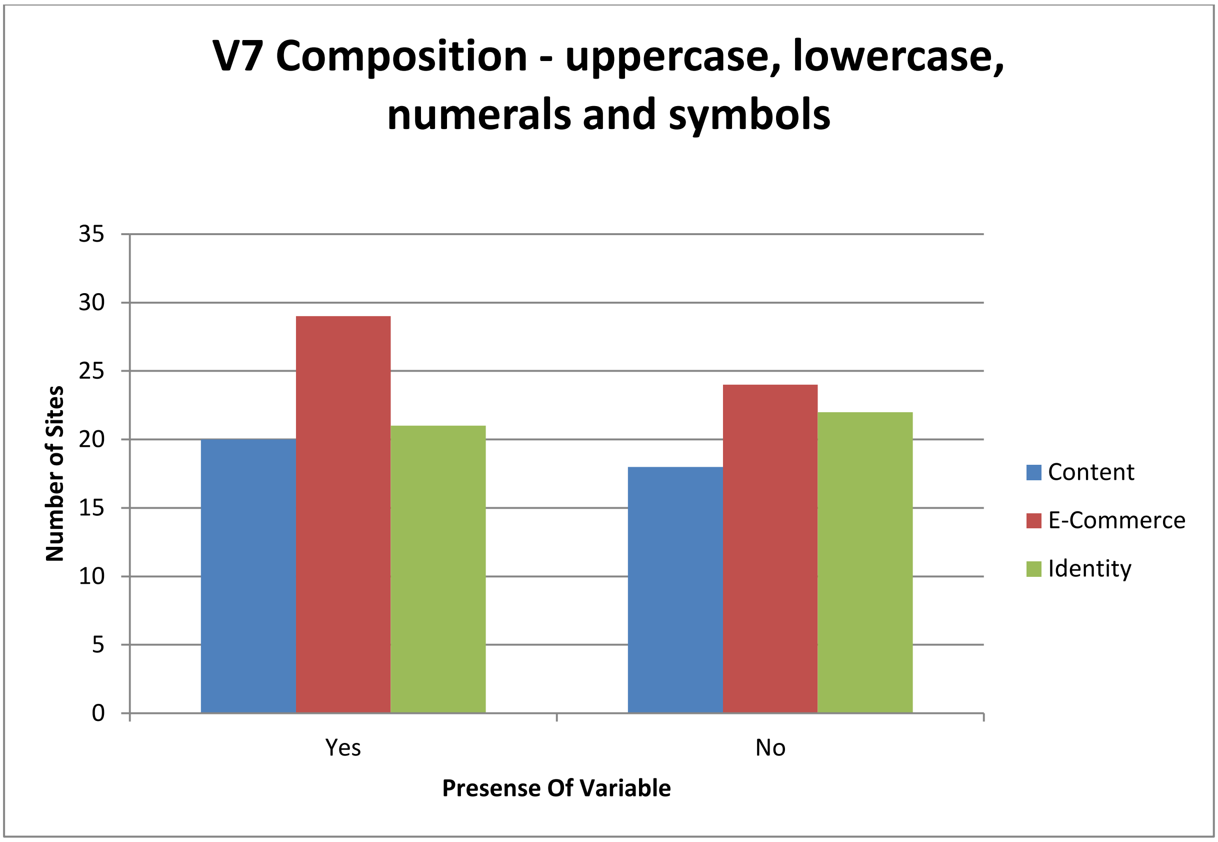


Figure 7 V7 Composition - uppercase, lowercase, numerals and symbols

4.2.8 V8 Instructions after a failed login attempt

Based on studies into password usability (Ernst, 2006) it is suggested that password security is a burden that has been offloaded onto users with web providers doing less to promote security requirements. However, from Figure 8 the result of this variable can be seen that a large majority of the sites do provide instructions to a user they have entered an incorrect password which is a positive for usability and promotes a closer engagement with users into the authentication progress by providing clear feedback and responses when there has been an error. However, while the results show that only a marginal amount of sites do not provide users with this usability the sites that do not should consider this carefully from a user engagement perspective as it is a highly reduced level of usability.

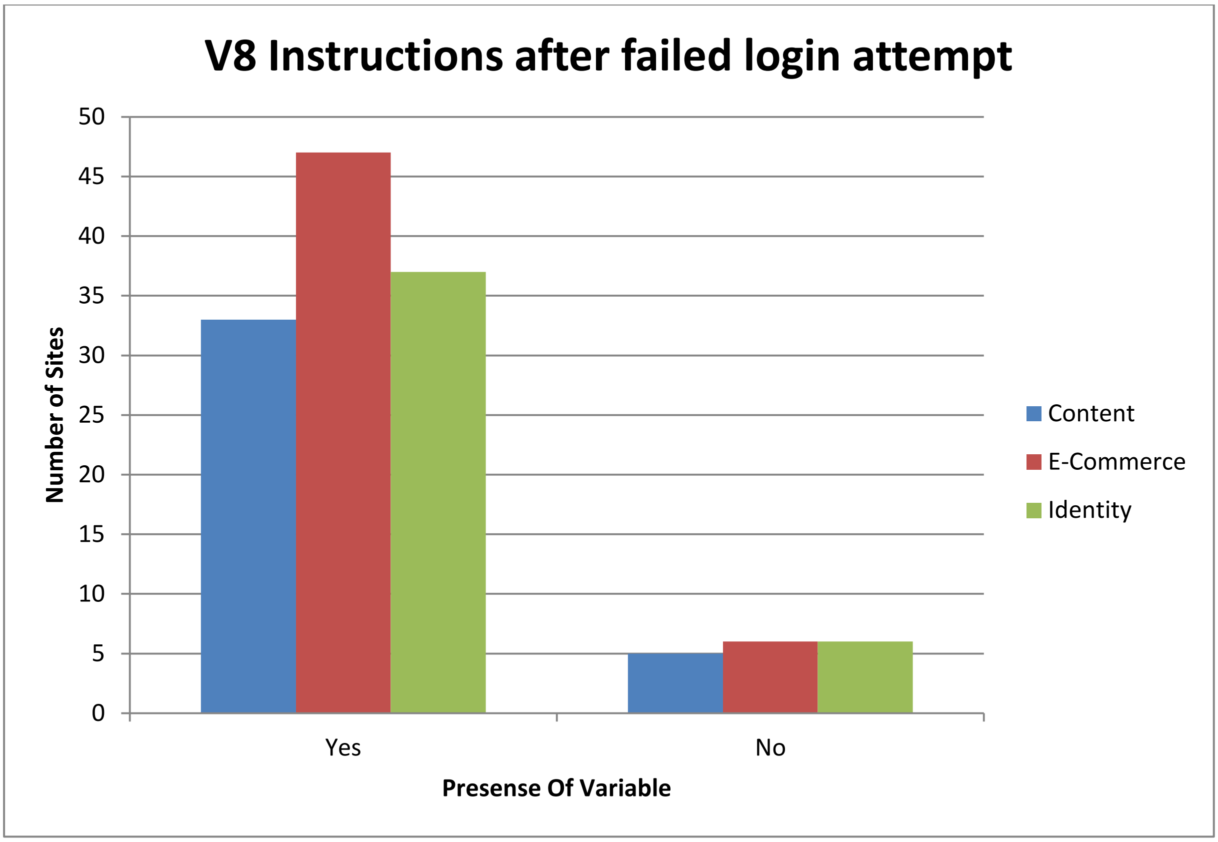


Figure 8 V8 Instructions after a failed login attempt

4.2.9 V9 Presence of Strength meter when choosing a password

In the interest of usability and as a way of providing feedback to users on the strength of their password choice strength meters was assessed the results of which can be seen in Figure 9. The results shown in Figure 9 show that strength meters are not widely used by sites with only 26 in the 135 sample set with a strength meter in place. Variation can be seen across the 3 types of sites with this V1 being most popular in e-commerce and identity websites and least likely to be used in content websites. As discussed in the literature review particularly novice users may be unaware of the range and sophistication of password attacks therefore it is in therefore it is in the users interest to have a form of feedback. The majority of websites do not provide this feedback in form of a strength meter to user allowing users to make their own assumptions as to what constitutes secure.

It is important to note that while a strength meter is assessed here this does not assess directly what the site classes as strong. Therefore whilst strength meter provide instantaneous feedback to users it will not solve all the problems as it also requires the site to determine what is strong (following the other variables).

From carrying out the experiment it was found that there was inconsistency across what each of the strength meters classified as “strong” and “weak”. A password of Thirty!1 was tested on all of the strength meters, Sky’s website gave the feedback “fair” whilst this is contradicted by the feedback from the site Sales force who deemed the password “strong”. This is example of inconsistency extends further as Drop box gave differing feedback on this password of “good”.

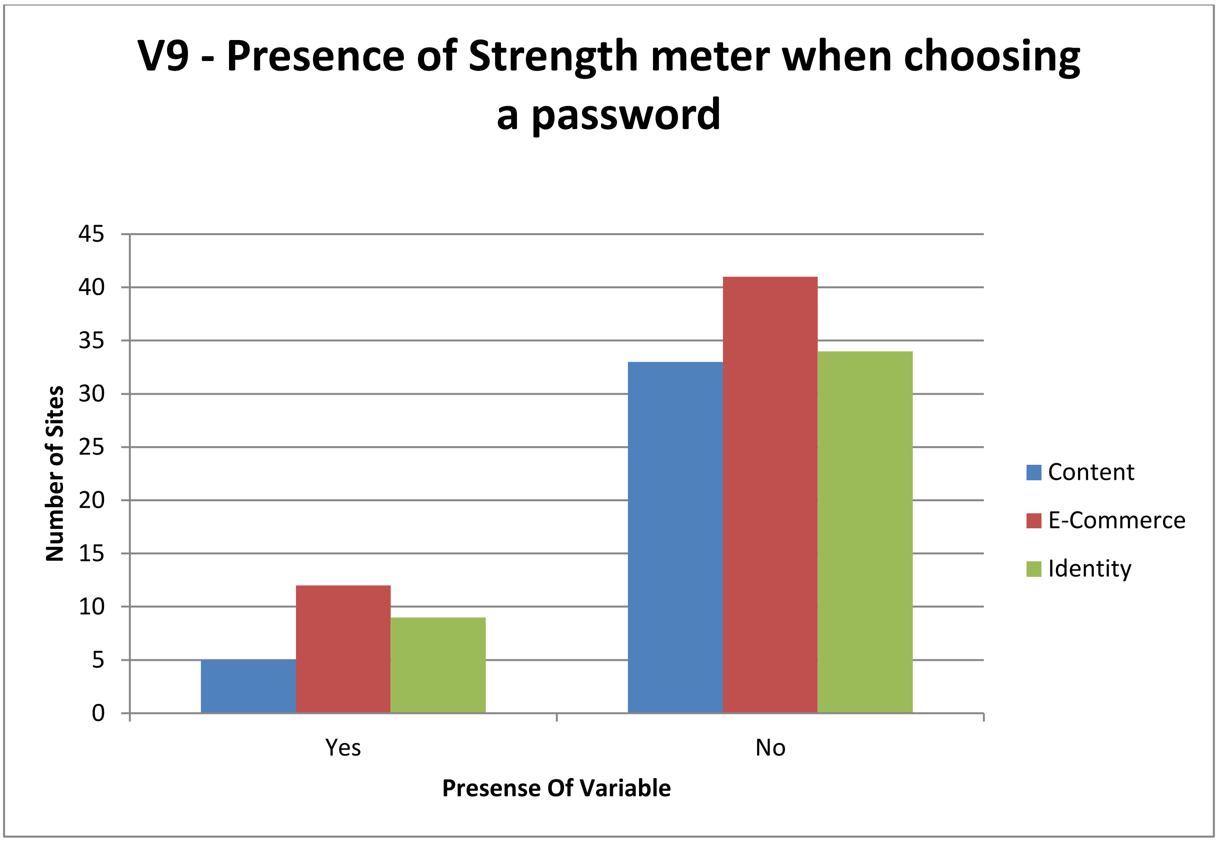


Figure 9 V9 Presence of Strength meter when choosing a password

4.2.10 V10 Password must not be user ID

Based on guidance also proposed by Microsoft (Microsoft, 2005) to allow a secure password should be different from the user ID. A total of 32 sites out of 134 included this within their password policy. This is a fairly low result for a variable that is relatively easy to implement from a technological and usability perspective. Furthermore, there is little variation between them all, but E-Commerce sites are strongly less likely to show this which is worrying. The set of websites who do not advise their users on V10 allow users to choose to use their username as their password weakening the strength of the password as once one aspect of the authentication method is determined the other is greatly reduced or compromised. Furthermore, implementing this variable does not impact on usability greatly as users should expect to configure a password and user ID separately as the most basic of authentication measures. See note.

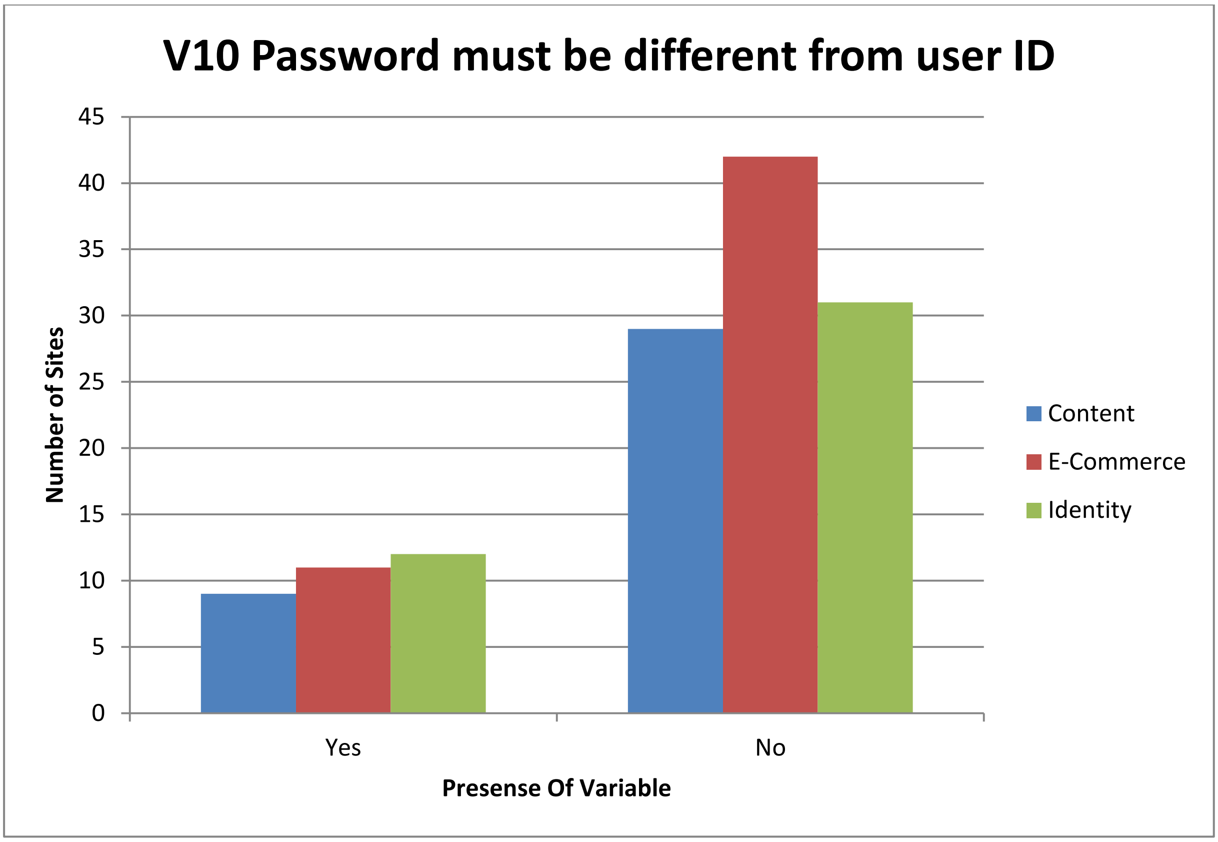


Figure 10 V10 Password must not be user ID

4.2.11 V11 CAPATCHA Code

As discussed in section 2 of the literature review a CAPATCHA code helps to prevent against scripts signing up to websites or logging in as another user. As can be seen from the results in Figure 11 this security practice is not one which is largely deployed. Figure 11 shows that 49 out of 134 websites required a user to enter a CAPTCHA code, there was little variation across the different business models however a slight trend can be seen of e-commerce websites in that they less likely to use CAPTCHA codes as method of security with only 18 of 53 sites implementing this variable. Whilst content websites were most likely to do so as 15 of the 38 mandated this as part of the registration phases. Following this was identity sites with 16 out of 43 sites requiring users to use CAPATCHA codes. Overall the sites that did not use CAPATCHA code are more vulnerable to scripting attacks.

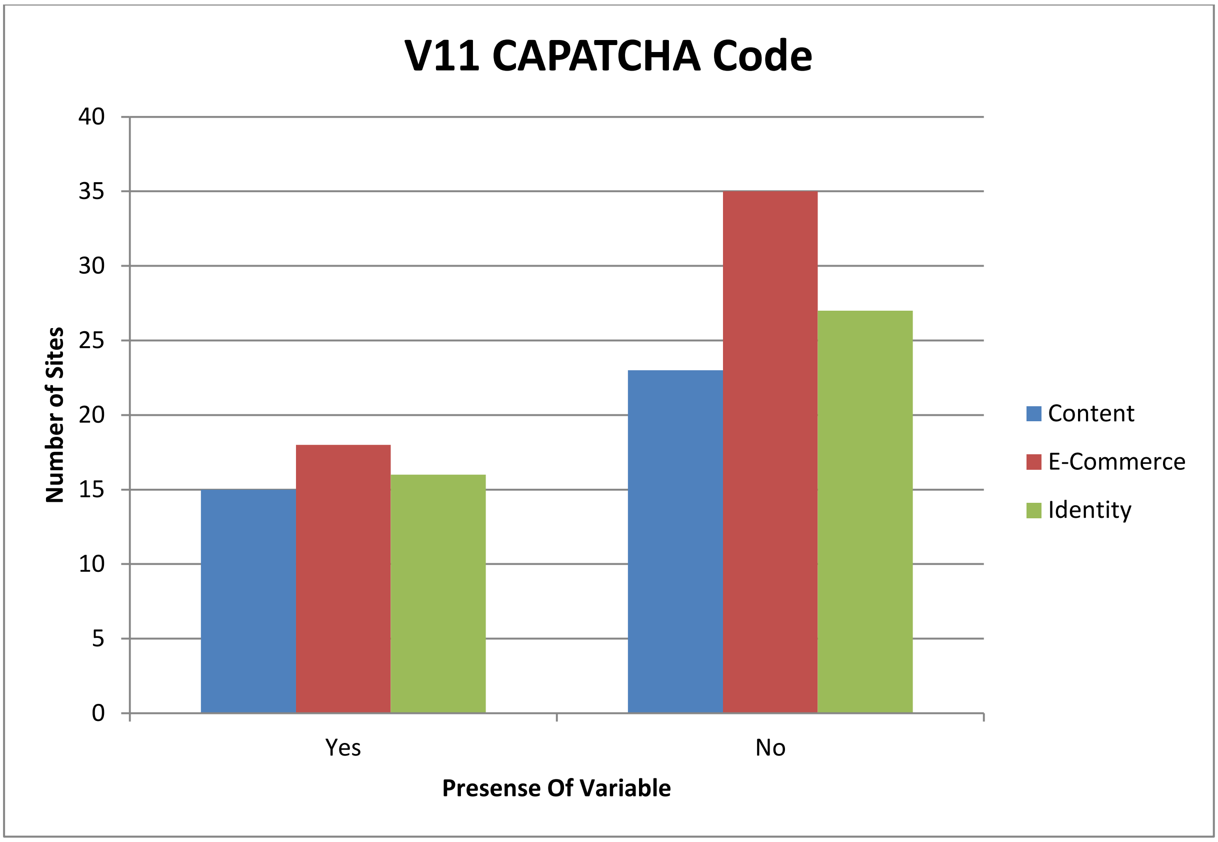


Figure 11 V11 CAPATCHA Code

4.2.12 V12 Password sent directly to user on registration

Based on various studies into authentication security it is recognised that emailing a password to users in plain text compromises security as this email can be intercepted on the wire or indeed compromised via a socially engineered attack.

From the results shown in Figure 12 it is clear that almost all of the sites do not send users' passwords to them via email in plain text format. This is a positive for password security and also opposes habits that users have been found to be akin to – physically writing their password down to remember them. It transforms the password from being something you have to something you know which is by definition of password how it should be. Only a small number of sites do email users with their password, the sites that do this should consider this carefully from a password security perspective as when a password is stored in plain text in email there are a number of ways it can be compromised.

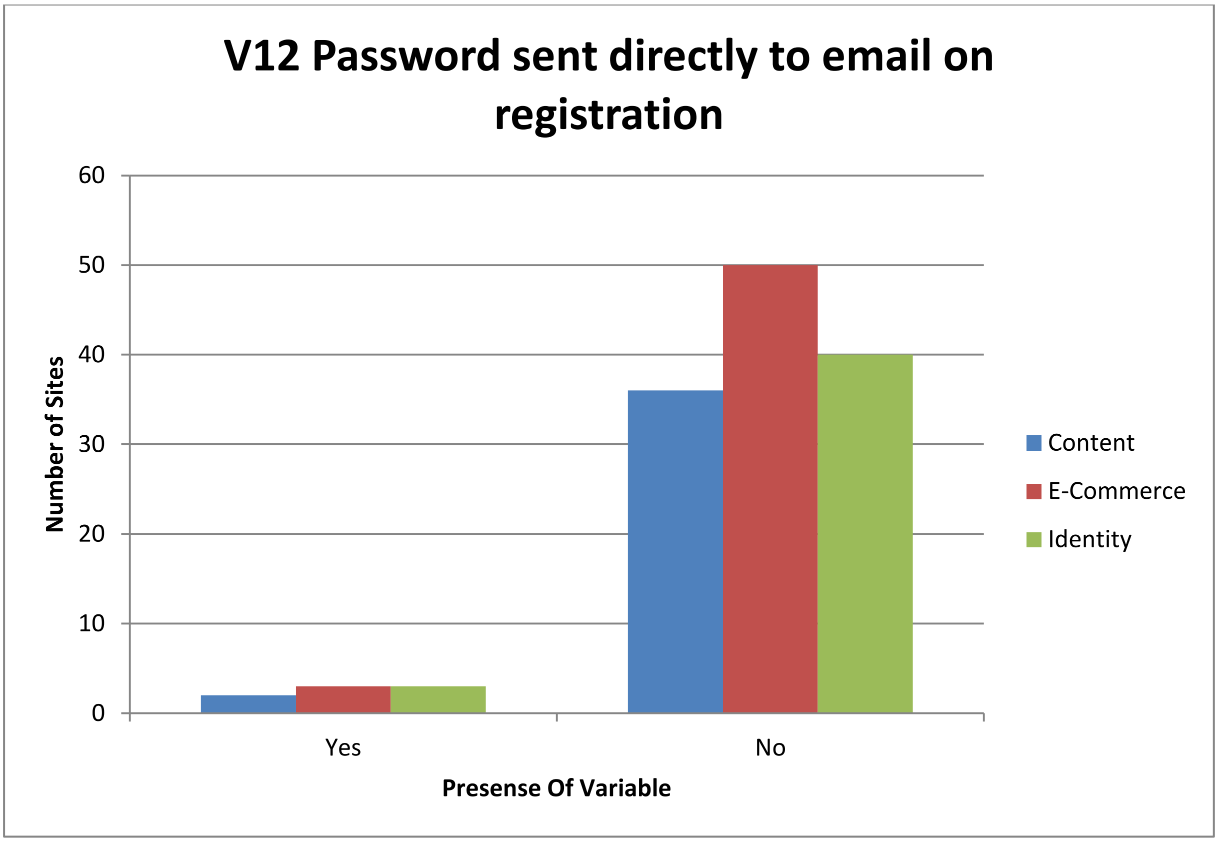


Figure 12 V12 Password sent directly to user on registration

4.2.13 V13 Secret Question

In the interest of usability as discussed in the literature review when a user cannot remember their password they are often asked to authenticate themselves by answering a secret question which they will have setup with the site when they registered. Figure 13 shows that there is a variation in the use of secret questions across the 3 business models. 14 out of 43 identity websites required users to setup a security question. This was followed by content sites where 9 out of 38 provided this functionality for users. Finally, e-commerce websites are least likely to use security questions as can be seen only 6 out of 53 websites used secret questions which are considerably less than the other two business models. This suggests that e-commerce websites do not want their users to be able to provide their users with an alternative method of authenticating themselves to the site should they need to.

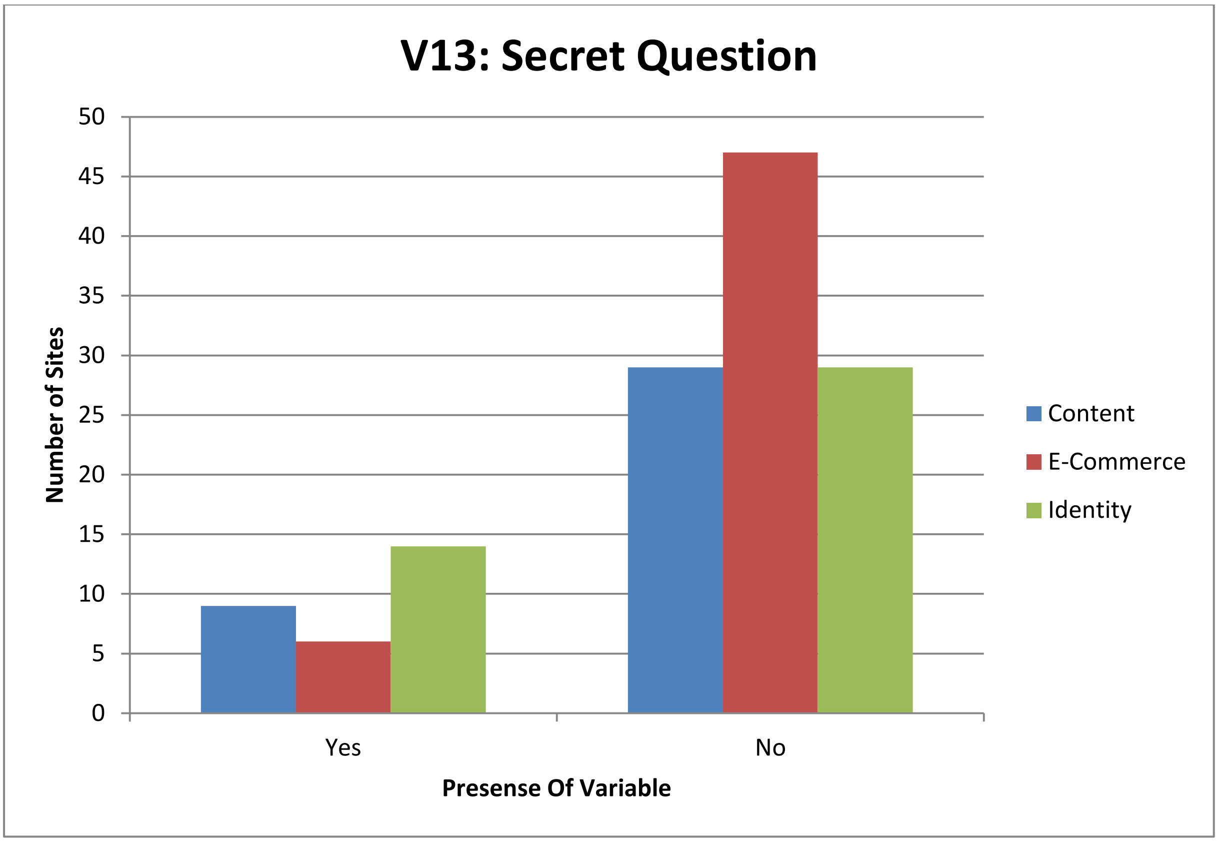


Figure 13 V13 Secret Question

4.3 Overview of Results

Huge variation in the scores, a lot of sites only had 1 or less which is not a positive for password strength. There was a lot of authentication inconsistency with many security policies are internally inconsistent, specifically with regards to the guidance given on the registration page to the guidance a user is faced with when resting their password. Many examples of this were seen during the experimental stage of the project e.g. identity website Hootsuite provided no password guidance at the registration stage and did not provided any guidance until the password reset interface, another example of this can been in websites Sourcecloud who accepted a password of “password” at the registration stage yet at the reset interface employed a strength meter which gave the feedback that a password of “password” was weak.

4.4 Recommendations

Clearly there is a lack of consistency and users would benefit from a unified understanding of the levels of security. The project proposes that web providers carry out a self-assessment using the variables discussed throughout section 3.2 and publicise this figure on their websites calling this their Password Policy Index Rating (PPIR). This will help address the issues of inconsistency amongst the industry and also raises awareness amongst users driving greater password strength and consistency.

4.5 Hypothesis testing

1. Web authentication systems are not universal in their application of password policies which reduces security in certain authentication environments
2. Web authentication systems are not universal in the information, guidance and policies provided to users to ensure strong passwords are selected

Web authentication systems are not universal in their application of password policies which reduces security in certain authentication environments

Result: Confirmed

Based on the results from the experiment in sections detailed in the results chapter it is confirmed that web authentication systems do not apply the same password policies across different authentication environments.. The application of password policies differ cross site as from the analysis of results some sites provide no password policy while there other vary greatly in complexity using a mix of one or up to 12 security variables..

Web authentication systems are not universal in the information, guidance and policies provided to users to ensure strong passwords are selected

Result: Confirmed

The variation of security variables from site to site across the business models show that variables used in across the sites are different, the difference in average and median results also reflects this. It is evident from the results of V1 - V13 there there is a difference in security variables used in different password policies. This shows that the information provided to users is not universal.

5.0 Conclusion

This section will present the final overall conclusions of the project based on the results collected during the experiment phase, as detailed in section 4. A brief summary of the project will be presented along with a final discussion on the findings identified in the experiment in relation to the research question and hypotheses. Finally, this chapter will conclude with the learned project limitations and any associated future works.

5.1 Brief Summary of Project

As authentication is crucial to most things that a user does online it is important to evaluate password policy guidelines in terms of providing users with sufficient knowledge of how to appropriately secure their online assets. It is believed that guidance on password security should come from the web providers themselves. There is no documentation nor has there been little research into how much guidance users are given by web providers when opening an account. This is something which all users would benefit from when choosing which sites to register their credentials with. Therefore a thorough investigation into a very large sample set of popular websites was required. This led to the following research question:

Are current password protocols and their guidelines clearly articulated to allow users to make best use of and strengthen their security credentials?

To answer this question, an investigation into security and usability issues of password authentication was carried out; this was followed by further investigation into implications and threats to users of poor password guidance. Secure and usable variables attributed to password policies were identified as well as metrics currently used to assess security and usability within the industry. Upon review of the investigations, an experiment was conducted to assess which of the variables were present in a large number of sites across three business models. After conclusion of the experiment the resulting data detailed in section 4 helped critically analyse how password guidelines in relation to the research question, project objectives and hypotheses, are articulated to allow users of a varying IT literacy to make best use of and strengthen their credentials.

5.2 Discussion of Results

5.2.1 Research Question Results

The results available in section 4 indicated that there is a huge variation in the password policy index rating across all sites with some sites scoring 1 or less while others scored 12. This variation is evident from the average password policy index rating average which was 3.5 for all sites. However, it is also important to recognize that no single website scored the maximum index rating available to them of 13. The highest index scoring of 12 was awarded to only one site which must be noted somewhat skewed the average of the scores as most sites scored 1 or less which is reflected in the median of 3.

These poor findings would suggest that password protocols that there is room for considerable improvement in how password protocols and their guidelines are articulated to users with the intention of strengthening their security credentials. Only 3 sites of the sample set scored an index rating of 10 or above, these can be considered comprehensive guidelines for users. Never the less, due to the large variation in guidance users are faced with increases users' uncertainty on best practices for password security thus collectively they are not clearly articulated to users.

When a user wishes to register on a website they are looking for guidance on how to do this securely. However, with the lack of guidance on a lot of sites and the variance it cannot be considered clear or secure, thus leaving the user confused as to what best practice actually is, thus not selecting passwords of appropriate security and leaving themselves vulnerable to attacks. Therefore, it is not appropriate that there is such variance in password policies, if other more unified solutions are available such as websites publicising their password policy index ratings allowing users to make an informed choice before registering their details with that site.

The main advantage of secure and clearly articulated password guidelines is the ability to equip users with the knowledge of how to eliminate the threat of various password hacking techniques. The average and median PPIR for the different categories of sites can be seen in Figure 14. Not only do e-commerce websites on average use more security variables the median PPIR was greater than that of the other business models tested in this experiment.

Table 1 Business Model Categorised Experimental Data Statistics

	Content	**E-commerce**	**Identity**
Average	2.71	3.79	3.07
Median	1	3	2.5
Total Number of Sites	38	53	43

A more unified approach to password guidance such as publicising password policy index rating (PPIR) so as to eliminate confusion amongst the industry is required. By publishing this clearly on each site this provides an industry benchmark that users can compare against. It must be noted that one negative of sites publishing their PPIR is that hackers can then adapt their password hacking skills and derive information about each site the sites password policy based on their PPIR, if they are able to find out what they need to know about a user to gain access to their account this would have the opposite effect in increasing security and make users accounts with that site more vulnerable. Also the implications of only some sites publishing their rating could have a positive effective, if the most popular sites identified in the sample set begun to do this other sites would hopefully want to follow their example. One key advantage of publishing this rating is that is has the ability to drive competitive advantages between sites that are either competing for business or competing for users.

5.3 Project Limitations

Despite the fact that both of the hypotheses were found to be confirmed based on the graphical representation and results discussed in section 4 the project is not without its limitations which could possibly have provide a restraint on the results.

One of the major limitations of the project as discussed in the methods section was that the project did not compare actual password data it is not reasonable to expect a website to give out password data to an undergraduate student. Therefore, we are assuming that the clear articulation of password policies and the education of users lead to increased password security. To defeat this problem if an unlimited budget was available and time constraints were not an issue each of the websites could be approached and anonymised password data could be asked for from all 150 sites , then correlate between little recommendations and unsecure passwords being set by users.

Secondly, as the security variables identified through the literature review were based on several studies and guidelines from different organisation and were not manipulated within the study it is possible that similar results may not be found should a different set of security variables be investigated. As this study only focuses on the implementation of 13 security variables it is not able to provide comment on the presence or otherwise of a different subset implementation of variables.

Thirdly, as the samples set of websites were based on Alexa traffic rankings top most 150 websites that use password authentication similar results may not be found should a different sample set of websites be used.

Whilst during the experiment it was found that some websites would accept a password of lesser criteria than it had advised it is recommended that testing the entire sample of sites to establish how many would accept password that contradicts the criteria it has advised.

Finally, the business model groupings were based on the criteria identified within the methods section. The placement of site within each category may be different if there placing was determined by someone who had an opposing opinion over what each of these categories of site consisted of.

5.4 Future Work

To address the limitations of this study and to explore the issues in more depth further it is proposed that further research could be carried out in this area.

In order to further validate how clearly the guidelines of password policies are articulated to users it is proposed that users could be interviewed or a survey completed to rate their experience when registering with a set of websites. The verbatim this type of method would generate would provide more detailed results as opposed to confirming or denying the presence of a security variable and so more detailed conclusions can be drawn.

Secondly, the research performed within this study could be conducted on a project which assesses a greater range of security variables that were used within the primary methodology to determine if these are more popular in

It is suggested that contacting sites to ask for password data and comparing this anonymised password data from the sites to see if user education/password policies do actually create stronger passwords, or if actually users do this of their own accord simply because they know how to.

Another area of work which could be conducted would be an investigation into the key areas lack security and inconsistency as a result of the analysis section - password reset, password strength and authentication consistency could be investigated separately to gather evaluate which area has the largest number of failings and equally which area has the least number of failings. As this study has only investigated password policies generally and not specifically these key areas.

Another area of future work which could be conducted would be to investigate the smallest number of security variables a website would need to implement in order to obtain full security coverage. As this study has only investigated the presence of the determined security variables on these sites as advised by other parties. By implementing future work it may be possible to determine a smaller number of variables a site can implement to receive the same coverage in terms of security. The results could then be used to reduce the security configuration time of site should a smaller number of variables be recommended for optimum use. In addition, this would decrease registration, login and password reset times for user's thus increasing usability.

5.5 Conclusions

This study has investigated the effectiveness of current password protocols and if their guidelines are sufficiently articulated to allow users to make best use of and strengthen their security credentials in order to determine if enough is being done to educate users on how to secure their assets online. The study has involved a large scale categorisation of a set of security variables identified through a review of literature.

As discussed in the literature review, the responsibility for password security has historically been thought of as residing with web providers. However now that authentication is so pervasive throughout the online world, it may be time for users to take ownership of this aspect of security through wider education.

This is however a challenge as it is clear that currently websites have a lack of security and inconsistency in their policies across several key areas. These key areas are the password reset function, password strength and authentication consistency which are all core areas that a user interacts with on a regular basis whilst authenticating with online services. Therefore this frequency of interaction, with varying levels of security policies is likely to cause further confusion. As all of the websites assessed provide failings in one or more of these key areas, there is clearly a large amount of improvement to be made in the online authentication industry.

Furthermore, there are themes in what websites see as important across the three internet business models; the most commonly found variable is V8 (Instructions after a failed login attempt), which is a positive for usability, as usability is such a core driver for website usage, this is not surprising that it is widely adopted. However it should be questioned whether this higher level of adoption is through a desire to improve security, or through the desire to not negatively impact on user adoption of a website. In contrast to V8, the least commonly found variable in password policies across all sites is V5 (do not increment passwords), which is clearly a negative result for both password strength but also for user education as if a user is not aware they should not increment passwords, they're unlikely to avoid this behaviour and therefore security will remain at a reduced level. Furthermore, websites are unlikely to implement this security policy as it may cause a decrease in usability and therefore adoption which is a risk website providers must balance as previously discussed.

Alongside this balance that website providers must determine, this experiment shows that user education is crucial when it comes to password security. This is because while websites are only successful if people use them, people will only us websites if they know how to. Therefore reducing the level of security policies and barriers to usability may increase the easy of which users can utilise a site; however this is likely to lead to a reduced level of security. Furthermore, it is users who have low levels of computer literacy that are unlikely to already be educated about how to implement a strong password, while they're also the least likely to understand how to utilise a site. Therefore it could be suggested that for novice users, password security may be better implemented not through advice, guidelines and education on sites but policies enforcing users to increase password security to ensure users strengthen their credentials. This will then ensure that all users must meet a minimum level of security; however it is important that any site should understand the usability impact of this.

Finally, it can be concluded that there should be a wider index used across the industry to improve consistency and reduce confusion amongst users around password complexity and security policies. It is therefore proposed that all websites publish a Password Policy Index Rating on their site for users to review publically. This wider implementation of a password policy related index should be published on sites to drive a competitive advantage between websites as sites currently value security, as they do not want their users information to be gained through unauthorised access. While this is currently true, it is crucially important for users to have visibility of the Password Policy Index Rating publically so they can make informed choices about which sits they sign up to. If the Password Policy Index Rating is displayed publically, then the website will have to consider improved security a positive competitive advantage (with a higher index attracting users), rather than only a risk (having a lower level of security resulting in a security breech in the future). However while in conclusion the responsibility for password security may need to switch over to the user, the web services industry must also take this seriously to address key issues identified in the project and implement its recommendations to complement this change in responsibility and ownership, to improve password security overall.

References

Adams and Sasse, 1999 “Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures, *Communications of the ACM*, 42(12):40-46.

Anonymous, 2010, "Fujitsu and oracle partner to develop palm vein biometric identity management solution", *Entertainment close - up,* .

Abraham, N. 2011, How to keep passwords secure [internet], *The Economic Times (Online),* Oct 13, .

Alexa 2012, *Alexa: The web information company* [online]. Available at: http://www.alexa.com/topsites/countries/GB [Accessed February/2 2012].

Anon, 2005, *Microsoft TechNet strong passwords* [online]. Available at: http://technet.microsoft.com/en-us/library/cc756109(WS.10).aspx [Accessed October, 28 2011].

Barra, R., McLeod, A., Savage, A. & Simkin, M. 2010a, "Passwords: Do user preferences and website protocols differ from theory?", *Journal of information privacy & security,* Vol. 6, no. 4, pp. 50.

Barra, R., McLeod, A., Savage, A. & Simkin, M. 2010b, "Passwords: Do user preferences and website protocols differ from theory?", *Journal of information privacy & security,* Vol. 6, no. 4, pp. 50.

Bonneau, J. & Preibusch, S. 2010, "The password thicket: Technical and market failures in human authentication on the web", *The ninth workshop on the economics of information security* Boston, June, 2010, Cambridge, USA.

Christie Nicholson. 15/12/2011, Re "
How to steal an identity in seven easy steps ", *Smart Planet* [online]. Available at: 14/01/2012 [Accessed 15/12/2011].

D. Florêncio, C.H. 2010, "Where do security policies come from?", , ed. Micorsoft Research, Washington, July 14-16, 2010, Symposium On Usable Privacy and Security, Washington.

D. Florêncio, C.H. 2007, "A large scale study of password habits.", *Proceedings of the sixteenth international world wide web conference* New York, May 8-12, ACM, USA, pp. 657.

DOD 1985, *Password management guideline* [online]. Available at: http://www.nipc.gov/publications/nipcpub/password.thm [Accessed February, 2 2012].

Ely, A. 2010, "Identity crisis", *InformationWeek,* no. 1266, pp. 38.

Ernst, Young, 2006 "Making it real", pp. 12

Furnell, S. 2007, "An assessment of website password practices", *Computers & security,* Vol. 26, no. 7/8, pp. 445.

Furnell, S., Tsaganidi, V. & Phippen, A. 2008, "Security beliefs and barriers for novice internet users", *Computers & security,* Vol. 27, no. 7/8, pp. 235.

Jiang Huiping 2010, "Strong password authentication protocols", *Distance learning and education (ICDLE), 2010 4th international conference on*, pp. 50.

Kabay, M.E. 2010, "Security reality vs. feelings: Steinberger on schneier", *Network world (online),* .

Kearns, D. 2010, "Lie your way to password security", *Network world (online),* .

Keith, M., Shao, B. & Steinbart 2009, "A behavioral analysis of passphrase design and effectiveness*", *Journal of the association for information systems,* Vol. 10, no. 2, pp. 63.

Kikusema, 2011, " FABULAROSA named top 10 european finalists for the global security challenge 2011", *News of science,* , pp. 676.

Landau, J. 2010, *Tata communications introduces managed 2-factor authentication as cloud-based service*, Anonymous edn, Entertainment Close - Up, Jacksonville: Jan 28, 2010.

Leesa-nguansuk, S. 2011, "We have to do better than '123456'", *McClatchy - tribune business news,* .

Lynch, L. 2011, "Inside the identity management game", *IEEE internet computing,* Vol. 15, no. 5, pp. 78.

McCrohan, K., Engel, K. & Harvey, J. 2010, "Influence of awareness and training on cyber security", *Journal of internet commerce,* Vol. 9, no. 1, pp. 23.

Me, G., Pirro, D. & Sarrecchia, R. 2006, "A mobile based approach to strong authentication on web", *Computing in the global information technology, 2006. ICCGI '06. international multi-conference on*, pp. 67.

Moss, V. 2011, "Re-evaluate authentication systems", *Credit union magazine,* Vol. 77, no. 9, pp. 54.

Oates, B.J. 2006, *Researching Information Systems and Computing,* Sage Publications.

O'brien, D. 2011, Web security breaches show better solutions are necessary, *Irish Times,* Mar 25, p. 8.

Oghenerukevbe,E., DME,BSc, MSc 2010, "Mnemonic passwords practices in corporate sites in nigerian", *Journal of internet banking and commerce,* Vol. 15, no. 1, pp. 1.

Osawa, J. 2011, PlayStation takes new hit; sony suspends 93,000 user accounts after suspicious activity on network, *Wall Street Journal (Online),* Oct 13, .

PatentBridge, 2008, "new "likes and dislikes"- based RavenWhite password protection technique helps consumers and businesses thwart email hackers", *Psychology & psychiatry journal,* , pp. 28.

Pearce, M., Zeadally, S. & Hunt, R. 2010, "Assessing and improving authentication confidence management", *Information management & computer security,* Vol. 18, no. 2, pp. 124.

Qiang Wang & Zhiguang Qin 2010, "Stronger user authentication for web browser", *Advanced computer theory and engineering (ICACTE), 2010 3rd international conference on*, pp. V5-539.

Questli 2011, Http://passmywill.com/ [Accessed November,4 2011].

Quittner, J. 2011, "Two-factor authentication has one big endorsement: Google", *Cardline,* Vol. 11, no. 7, pp. 2.

S, G. & E.W, F. 2006, "
Password management strategies for online accounts", *SOUPS '06 proceedings of the second symposium on usable privacy and security* New York, July 12 - 14, ACM, USA, pp. 44-55.

Sood, S. 2011, "Cookie-based virtual password authentication protocol", *Information security journal,* Vol. 20, no. 2, pp. 100.

Symantec, 2012 http://www.symantec.com/index.jsp [Accessed February 3, 2011]

Thiruvaazhi, U. & Divya, R. 2011, "Web authentication protocol using zero knowledge proof", *Information security journal,* Vol. 20, no. 2, pp. 112.

William E. Burr Donna F. Dodson W. Timothy Polk 10/01/2012, *Electronic authentication guideline* [online]. Available at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf [Accessed 10/01/2012 10/01/2012].

Yang Jingbo & Shen Pingping 2010, "A secure strong password authentication protocol", *Software technology and engineering (ICSTE), 2010 2nd international conference on*, pp. V2-355.

Zhang, J, Luo, X. Akkaladevi, S & Ziegelmayer, J. 2009, “Improving multiple-password recall: An empirical study”, European journal of information systems, Vol.18, no. 2, pp. 165.

Appendices

Appendix 1 – Sample Website List

Website	**Category**
www.archive.org	Content
www.imdb.com	Content
www.tfl.gov.uk	Content
www.thesun.co.uk	Content
www.tripadvisor.co.uk	Content
www.w3schools.com	Content
www.wikimedia.org	Content
www.yell.com	Content
www.192.com	Content
www.cnet.com	Content
www.dailymail.co.uk	Content
www.deviantart.com	Content
www.digitalspy.co.uk	Content
www.dropbox.com	Content
www.ft.com	Content
www.independent.co.uk	Content
www.newsnow.co.uk	Content
www.nytimes.com	Content
www.photobucket.com	Content
www.premierleague.com	Content
www.putlocker.com	Content
www.reed.co.uk	Content

www.reference.com	Content
www.skysports.com	Content
www.stumbleupon.com	Content
www.telegraph.co.uk	Content
www.wikipedia.org	Content
www.cnn.com	Content
www.ehow.com	Content
www.findaproperty.com	Content
www.outbrain.com	Content
www.reuters.com	Content
www.rightmove.com	Content
www.sourceforge.net	Content
www.statcounter.com	Content
www.totaljobs.com	Content
www.tvguide.co.uk	Content
www.xe.com	Content
www.alibaba.com	E-Commerce
www.asda.com	E-Commerce
www.avg.com	E-Commerce
www.ebuyer.com	E-Commerce
www.expedia.co.uk	E-Commerce
www.oneandone.co.uk	E-Commerce
www.paypal-business.co.uk	E-Commerce
www.play.com	E-Commerce
www.talktalk.co.uk	E-Commerce
www.three.co.uk	E-Commerce

www.tradedoubler.com	E-Commerce
www.vodafone.co.uk	E-Commerce
www.123-reg.co.uk	E-Commerce
www.888.com	E-Commerce
www.affiliatewindow.com	E-Commerce
www.amazon.co.uk	E-Commerce
www.apple.com	E-Commerce
www.asos.com	E-Commerce
www.aws.amazon.com	E-Commerce
www.betfair.com	E-Commerce
www.booking.com	E-Commerce
www.clickbank.com	E-Commerce
www.ebay.co.uk	E-Commerce
www.fiverr.com	E-Commerce
www.godaddy.com	E-Commerce
www.groupon.co.uk	E-Commerce
www.ikea.com	E-Commerce
www.istockphoto.com	E-Commerce
www.lovefilm.com	E-Commerce
www.next.co.uk	E-Commerce
www.paypal.com	E-Commerce
www.pistonheads.com	E-Commerce
www.salesforce.com	E-Commerce
www.sparkstudios.com	E-Commerce
www.tesco.com	E-Commerce
www.themeforest.net	E-Commerce

www.adobe.com	E-Commerce
www.argos.co.uk	E-Commerce
www.bet365.com	E-Commerce
www.birtishairways.com	E-Commerce
www.cj.com	E-Commerce
www.domaintools.com	E-Commerce
www.easyjet.com	E-Commerce
www.etsy.com	E-Commerce
www.heartinternet.co.uk	E-Commerce
www.hotukdeals.com	E-Commerce
www.johnlewis.com	E-Commerce
www.ladbrokes.com	E-Commerce
www.marksandspencer.com	E-Commerce
www.microsoft.com	E-Commerce
www.nationalrail.co.uk	E-Commerce
www.thetrainline.com	E-Commerce
www.virginmedia.com	E-Commerce
www.addthis.com	Identity
www.answers.com	Identity
www.aol.co.uk	Identity
www.channel4.com	Identity
www.dailymotion.com	Identity
www.google.co.uk	Identity
www.guardian.co.uk	Identity
www.hubpages.com	Identity
www.imgur.com	Identity

www.live.com	Identity
www.msn.com	Identity
www.national-lottery.co.uk	Identity
www.reddit.com	Identity
www.stackoverflow.com	Identity
www.typepad.com	Identity
www.vimeo.com	Identity
www.wordpress.com	Identity
www.yahoo.com	Identity
www.autotrader.co.uk	Identity
www.download.com	Identity
www.hootsuite.com	Identity
www.ign.com	Identity
www.linkedIn.com	Identity
www.mashable.com	Identity
www.mediafire.com	Identity
www.myspace.com	Identity
www.soundcloud.com	Identity
www.squidoo.com	Identity
www.blogger.com	Identity
www.blogspot.com	Identity
www.bt.com	Identity
www.conduit.com	Identity
www.ebay.com	Identity
www.facebook.com	Identity
www.pof.com	Identity

www.seomoz.org	Identity
www.sky.com	Identity
www.skype.com	Identity
www.tumblr.com	Identity
www.twitter.com	Identity
www.warriorforum.com	Identity
www.wikia.com	Identity
www.wordpress.org	Identity

Appendix 2 Raw Data Results

Appendix 2.1 V1 to V4

Website	V1: Must be at least 7 Characters in length	V2: Must not contain username/real name/company name	V3: Does not contain a complete dictionary word	V4: Significantly different from previous password
www.192.com	0	0	1	0
www.archive.org	0	0	0	0
www.cnet.com	0	0	0	0
www.cnn.com	0	0	0	0
www.dailymail.co.uk	0	0	0	0
www.deviantart.com	0	0	1	0
www.digitalspy.co.uk	0	0	0	0
www.dropbox.com	0	0	0	0
www.ehow.com	0	0	0	0
www.findaproperty.com	0	0	0	0
www.ft.com	0	0	0	0
www.imdb.com	1	0	0	0
www.independent.co.uk	0	0	0	0
www.newsnow.co.uk	1	0	0	0
www.nytimes.com	0	0	0	0
www.outbrain.com	0	0	0	0
www.photobucket.com	1	0	1	0
www.premierleague.com	0	0	0	0
www.putlocker.com	0	0	0	0
www.reed.co.uk	0	0	0	0
www.reference.com	0	0	0	0
www.reuters.com	0	0	0	0
www.rightmove.com	0	0	0	0
www.skysports.com	1	1	1	1
www.sourceforge.net	0	0	0	1
www.statcounter.com	0	0	0	0
www.stumbleupon.com	1	0	1	0
www.telegraph.co.uk	0	0	0	1
www.tfl.gov.uk	0	0	1	0
www.thesun.co.uk	0	0	0	0
www.totaljobs.com	0	0	0	0
www.tripadvisor.co.uk	0	0	0	0
www.tvguide.co.uk	0	0	0	0
www.w3schools.com	0	0	0	0
www.wikimedia.org	0	0	0	0

www.wikipedia.org	0	0	0	0
www.xe.com	1	0	0	0
www.yell.com	0	0	0	0
www.123-reg.co.uk	1	0	0	0
www.888.com	0	1	1	0
www.adobe.com	0	0	0	0
www.affiliatewindow.com	1	0	1	0
www.alibaba.com	0	0	0	0
www.amazon.co.uk	0	0	0	0
www.apple.com	1	1	1	1
www.argos.co.uk	0	0	1	0
www.asda.com	0	0	0	0
www.asos.com	0	0	0	0
www.avg.com	0	0	0	0
www.aws.amazon.com	0	0	0	0
www.bet365.com	0	1	1	0
www.betfair.com	1	0	1	0
www.birtishairways.com	0	0	0	0
www.booking.com	0	0	0	0
www.cj.com	0	0	1	0
www.clickbank.com	0	0	1	0
www.domaintools.com	1	0	0	0
www.easyjet.com	0	0	0	0
www.ebay.co.uk	0	1	0	0
www.ebuyer.com	0	0	0	0
www.etsy.com	0	0	0	0
www.expedia.co.uk	0	0	0	0
www.fiverr.com	0	0	0	0
www.godaddy.com	0	0	0	0
www.groupon.co.uk	0	0	0	0
www.heartinternet.co.uk	1	0	0	1
www.hotukdeals.com	0	0	0	0
www.ikea.com	1	1	1	0
www.istockphoto.com	0	0	1	0
www.johnlewis.com	0	0	0	0
www.ladbrokes.com	0	1	1	1
www.lovefilm.com	0	0	0	0
www.marksandspencer.com	0	0	0	1
www.microsoft.com	0	1	1	1
www.nationalrail.co.uk	0	0	0	0
www.next.co.uk	0	1	1	0
www.oneandone.co.uk	0	0	1	0
www.paypal.com	1	1	1	1
www.paypal-business.co.uk	1	1	1	1

www.pistonheads.com	0	0	0	0
www.play.com	0	0	1	0
www.salesforce.com	1	1	1	1
www.sparkstudios.com	1	0	1	0
www.talktalk.co.uk	1	1	1	1
www.tesco.com	0	1	1	0
www.themeforest.net	1	1	1	0
www.thetrainline.com	0	0	0	0
www.three.co.uk	1	1	0	0
www.tradedoubler.com	1	0	0	0
www.virginmedia.com	1	1	1	1
www.vodafone.co.uk	1	1	1	1
www.addthis.com	0	0	0	0
www.answers.com	0	0	0	0
www.aol.co.uk	0	0	1	1
www.autotrader.co.uk	1	0	1	0
www.blogger.com	1	1	1	1
www.blogspot.com	1	1	1	1
www.bt.com	1	1	1	0
www.channel4.com	0	0	0	0
www.conduit.com	0	1	1	1
www.dailymotion.com	1	1	1	0
www.download.com	0	0	0	0
www.ebay.com	0	1	0	0
www.facebook.com	0	0	0	0
www.google.co.uk	1	0	0	0
www.guardian.co.uk	0	0	0	0
www.hootsuite.com	0	0	0	0
www.hubpages.com	0	0	1	0
www.ign.com	0	0	0	0
www.imgur.com	0	0	0	0
www.linkedIn.com	0	0	0	0
www.live.com	0	1	1	1
www.mashable.com	0	0	0	0
www.mediafire.com	0	0	1	0
www.msn.com	0	1	1	1
www.myspace.com	0	0	0	0
www.national-lottery.co.uk	0	0	0	0
www.pof.com	0	0	0	0
www.reddit.com	0	0	0	0
www.seomoz.org	0	0	0	0
www.sky.com	1	1	1	1
www.skype.com	0	0	0	0
www.soundcloud.com	0	0	0	0

www.squidoo.com	0	0	0	0
www.stackoverflow.com	1	1	1	0
www.tumblr.com	1	1	1	0
www.twitter.com	1	1	0	0
www.typepad.com	0	0	0	0
www.vimeo.com	0	0	0	0
www.warriorforum.com	1	0	0	0
www.wikia.com	0	0	0	0
www.wordpress.com	0	1	1	0
www.wordpress.org	0	1	1	0
www.yahoo.com	1	1	1	0

Appendix 2.2 V5 to V8

Website	V5: Do not increment passwords	V6: Cannot use pet names	V7: Composition - uppercase, lowercase, numerals, symbols	V8: Instructions for after failed login attempt
www.192.com	0	0	1	0
www.archive.org	0	0	0	1
www.cnet.com	0	0	0	1
www.cnn.com	0	0	0	1
www.dailymail.co.uk	0	0	0	1
www.deviantart.com	0	0	0	1
www.digitalspy.co.uk	0	0	0	1
www.dropbox.com	0	0	1	1
www.ehow.com	0	0	0	0
www.findaproperty.com	0	0	0	0
www.ft.com	0	0	1	0
www.imdb.com	0	0	0	1
www.independent.co.uk	0	0	0	1
www.newsnow.co.uk	0	0	1	1
www.nytimes.com	0	0	0	1
www.outbrain.com	0	0	0	1
www.photobucket.com	0	0	1	1
www.premierleague.com	0	0	0	1
www.putlocker.com	0	0	0	1
www.reed.co.uk	0	0	1	1
www.reference.com	0	0	0	1
www.reuters.com	0	0	0	1
www.rightmove.com	0	0	0	1
www.skysports.com	0	0	1	1
www.sourceforge.net	0	0	0	1
www.statcounter.com	0	0	0	1
www.stumbleupon.com	0	0	1	1
www.telegraph.co.uk	0	0	0	1
www.tfl.gov.uk	0	0	1	1
www.thesun.co.uk	0	0	0	0
www.totaljobs.com	0	0	1	1
www.tripadvisor.co.uk	0	0	0	1
www.tvguide.co.uk	0	0	0	1
www.w3schools.com	0	0	0	1
www.wikimedia.org	0	0	0	1
www.wikipedia.org	0	0	0	1
www.xe.com	0	0	1	1
www.yell.com	0	0	0	1

www.123-reg.co.uk	0	0	1	0
www.888.com	0	0	1	1
www.adobe.com	0	0	0	1
www.affiliatewindow.com	0	0	1	1
www.alibaba.com	0	0	1	1
www.amazon.co.uk	0	0	1	1
www.apple.com	1	1	1	1
www.argos.co.uk	0	0	1	1
www.asda.com	0	0	0	1
www.asos.com	0	0	0	1
www.avg.com	0	0	0	1
www.aws.amazon.com	0	0	1	1
www.bet365.com	0	0	1	1
www.betfair.com	0	0	1	1
www.birtishairways.com	0	0	0	1
www.booking.com	0	0	0	1
www.cj.com	0	0	1	1
www.clickbank.com	0	0	1	1
www.domaintools.com	0	0	0	1
www.easyjet.com	0	0	0	0
www.ebay.co.uk	0	0	1	1
www.ebuyer.com	0	0	0	0
www.etsy.com	0	0	0	0
www.expedia.co.uk	0	0	0	0
www.fiverr.com	0	0	0	0
www.godaddy.com	1	0	1	0
www.groupon.co.uk	0	0	0	0
www.heartinternet.co.uk	1	0	1	1
www.hotukdeals.com	0	0	0	1
www.ikea.com	0	0	1	1
www.istockphoto.com	0	0	1	1
www.johnlewis.com	0	0	1	1
www.ladbrokes.com	0	0	1	1
www.lovefilm.com	0	0	0	1
www.marksandspencer.com	0	0	0	0
www.microsoft.com	0	0	1	1
www.nationalrail.co.uk	0	0	1	1
www.next.co.uk	0	1	1	1
www.oneandone.co.uk	0	0	1	1
www.paypal.com	0	1	1	1
www.paypal-business.co.uk	0	1	1	1
www.pistonheads.com	0	0	0	1
www.play.com	0	0	1	1
www.salesforce.com	0	0	1	1

www.sparkstudios.com	0	0	1	1
www.talktalk.co.uk	0	0	1	1
www.tesco.com	0	0	1	1
www.themeforest.net	0	0	1	1
www.thetrainline.com	0	0	0	1
www.three.co.uk	0	0	1	1
www.tradedoubler.com	0	0	0	1
www.virginmedia.com	0	0	1	1
www.vodafone.co.uk	0	0	1	1
www.addthis.com	0	0	0	1
www.answers.com	0	0	0	1
www.aol.co.uk	0	0	1	1
www.autotrader.co.uk	0	0	1	1
www.blogger.com	0	0	1	1
www.blogspot.com	0	0	1	1
www.bt.com	0	0	1	1
www.channel4.com	0	0	0	1
www.conduit.com	0	1	1	1
www.dailymotion.com	0	0	1	1
www.download.com	0	0	0	1
www.ebay.com	0	0	1	1
www.facebook.com	0	0	0	0
www.google.co.uk	0	0	1	0
www.guardian.co.uk	0	0	1	0
www.hootsuite.com	0	0	0	1
www.hubpages.com	0	0	1	1
www.ign.com	0	0	0	1
www.imgur.com	0	0	0	1
www.linkedIn.com	0	0	0	1
www.live.com	0	0	1	1
www.mashable.com	0	0	1	1
www.mediafire.com	0	0	1	1
www.msn.com	0	0	1	1
www.myspace.com	0	0	0	1
www.national-lottery.co.uk	0	0	1	1
www.pof.com	0	0	0	1
www.reddit.com	0	0	0	1
www.seomoz.org	0	0	0	1
www.sky.com	0	0	1	1
www.skype.com	0	0	0	1
www.soundcloud.com	0	0	0	1
www.squidoo.com	0	0	0	1
www.stackoverflow.com	0	0	1	1
www.tumblr.com	0	0	1	1

www.twitter.com	0	0	1	1
www.typepad.com	0	0	1	1
www.vimeo.com	0	0	0	1
www.warriorforum.com	0	0	1	1
www.wikia.com	0	0	0	1
www.wordpress.com	0	0	1	1
www.wordpress.org	0	0	1	1
www.yahoo.com	0	0	1	1

Appendix 2.3 V9 to V13

Website	V9: Strength meter	V10: Password must be different from user ID	V11: CAPTACHA	V12: Password sent directly to email on registration	V13: Secret Question
www.192.com	0	0	0	0	0
www.archive.org	0	0	1	1	0
www.cnet.com	0	0	1	0	0
www.cnn.com	0	0	1	0	0
www.dailymail.co.uk	0	0	0	0	0
www.deviantart.com	1	0	1	0	0
www.digitalspy.co.uk	0	0	0	0	0
www.dropbox.com	1	0	0	0	0
www.ehow.com	0	0	0	0	0
www.findaproperty.com	0	1	1	0	0
www.ft.com	0	0	1	0	0
www.imdb.com	0	0	0	0	0
www.independent.co.uk	0	0	0	0	0
www.newsnow.co.uk	0	0	0	0	0
www.nytimes.com	0	0	0	0	0
www.outbrain.com	0	0	0	0	0
www.photobucket.com	0	0	0	0	0
www.premierleague.com	0	0	0	0	0
www.putlocker.com	0	0	0	0	0
www.reed.co.uk	0	0	0	0	0
www.reference.com	0	0	0	0	0
www.reuters.com	0	0	1	0	0
www.rightmove.com	0	0	0	0	0
www.skysports.com	1	1	1	0	0
www.sourceforge.net	0	0	0	0	0
www.statcounter.com	0	0	0	0	0
www.stumbleupon.com	1	0	1	0	0
www.telegraph.co.uk	0	0	1	0	0
www.tfl.gov.uk	0	1	1	0	0
www.thesun.co.uk	0	0	0	0	0
www.totaljobs.com	0	0	0	0	0
www.tripadvisor.co.uk	0	0	0	0	0
www.tvguide.co.uk	0	0	0	0	0
www.w3schools.com	0	0	0	0	0
www.wikimedia.org	0	0	0	0	0
www.wikipedia.org	0	0	0	0	0
www.xe.com	0	0	1	0	1

www.yell.com	0	0	1	0	0
www.123-reg.co.uk	1	0	0	1	0
www.888.com	0	1	1	0	1
www.adobe.com	0	0	0	0	0
www.affiliatewindow.com	1	0	0	0	0
www.alibaba.com	1	0	1	0	0
www.amazon.co.uk	0	0	1	0	0
www.apple.com	1	1	1	0	1
www.argos.co.uk	0	0	0	0	1
www.asda.com	0	0	0	0	0
www.asos.com	0	0	0	0	0
www.avg.com	0	0	1	0	0
www.aws.amazon.com	0	0	1	0	0
www.bet365.com	1	1	0	0	1
www.betfair.com	0	0	0	0	1
www.birtishairways.com	0	0	0	0	0
www.booking.com	0	0	0	0	0
www.cj.com	0	0	1	0	0
www.clickbank.com	1	0	1	0	0
www.domaintools.com	1	0	0	0	0
www.easyjet.com	0	0	0	0	0
www.ebay.co.uk	1	1	1	1	1
www.ebuyer.com	0	0	0	0	1
www.etsy.com	0	0	0	1	0
www.expedia.co.uk	0	0	0	0	0
www.fiverr.com	0	0	1	0	0
www.godaddy.com	0	1	1	1	1
www.groupon.co.uk	0	0	0	0	0
www.heartinternet.co.uk	0	0	1	1	1
www.hotukdeals.com	0	0	0	0	0
www.ikea.com	0	1	1	0	0
www.istockphoto.com	0	0	0	0	0
www.johnlewis.com	0	0	0	0	0
www.ladbrokes.com	1	1	0	0	1
www.lovefilm.com	0	0	0	0	0
www.marksandspencer.com	0	0	0	0	0
www.microsoft.com	0	1	0	0	1
www.nationalrail.co.uk	0	0	0	0	1
www.next.co.uk	0	1	0	0	0
www.oneandone.co.uk	0	0	0	0	0
www.paypal.com	0	1	0	0	0
www.paypal-business.co.uk	0	1	0	0	0
www.pistonheads.com	0	0	0	0	0
www.play.com	0	0	0	0	0

www.salesforce.com	1	1	0	0	1
www.sparkstudios.com	0	0	1	0	0
www.talktalk.co.uk	0	1	1	0	1
www.tesco.com	0	1	0	0	0
www.themeforest.net	1	1	1	0	0
www.thetrainline.com	0	0	0	0	0
www.three.co.uk	0	1	1	0	0
www.tradedoubler.com	0	0	1	0	0
www.virginmedia.com	0	1	1	0	1
www.vodafone.co.uk	0	0	1	0	1
www.addthis.com	0	0	0	0	0
www.answers.com	0	0	0	1	0
www.aol.co.uk	1	0	1	0	1
www.autotrader.co.uk	0	0	0	0	0
www.blogger.com	1	1	1	0	1
www.blogspot.com	1	1	1	0	1
www.bt.com	0	1	0	0	1
www.channel4.com	0	0	0	0	0
www.conduit.com	0	0	1	0	1
www.dailymotion.com	1	0	1	0	1
www.download.com	0	0	0	0	0
www.ebay.com	1	1	1	1	1
www.facebook.com	0	0	0	0	0
www.google.co.uk	1	0	0	0	0
www.guardian.co.uk	0	0	0	0	0
www.hootsuite.com	0	0	0	0	0
www.hubpages.com	0	0	1	0	0
www.ign.com	0	0	0	0	0
www.imgur.com	0	0	0	0	0
www.linkedIn.com	0	0	0	0	0
www.live.com	0	1	0	0	1
www.mashable.com	0	0	0	0	0
www.mediafire.com	1	0	0	0	0
www.msn.com	0	1	0	0	1
www.myspace.com	0	0	1	0	0
www.national-lottery.co.uk	0	0	0	0	1
www.pof.com	0	0	0	0	0
www.reddit.com	0	0	0	0	0
www.seomoz.org	0	0	0	0	0
www.sky.com	1	1	1	0	0
www.skype.com	0	0	0	0	0
www.soundcloud.com	0	0	0	0	0
www.squidoo.com	0	0	0	0	0
www.stackoverflow.com	0	1	1	0	0

www.tumblr.com	1	1	1	0	1
www.twitter.com	1	0	1	0	0
www.typepad.com	0	0	1	0	0
www.vimeo.com	0	0	0	0	0
www.warriorforum.com	0	0	1	0	0
www.wikia.com	0	0	0	0	0
www.wordpress.com	0	1	1	0	0
www.wordpress.org	0	1	1	0	0
www.yahoo.com	1	1	0	0	1

Appendix 3 - Password Policy Index Rating Data

Website	Password Policy Index Rating
www.192.com	2
www.archive.org	3
www.cnet.com	2
www.cnn.com	2
www.dailymail.co.uk	1
www.deviantart.com	4
www.digitalspy.co.uk	1
www.dropbox.com	3
www.ehow.com	0
www.findaproperty.com	2
www.ft.com	2
www.imdb.com	2
www.independent.co.uk	1
www.newsnow.co.uk	3
www.nytimes.com	1
www.outbrain.com	1
www.photobucket.com	4
www.premierleague.com	1
www.putlocker.com	1
www.reed.co.uk	2
www.reference.com	1
www.reuters.com	2
www.rightmove.com	1
www.skysports.com	9
www.sourceforge.net	2
www.statcounter.com	1
www.stumbleupon.com	6
www.telegraph.co.uk	3
www.tfl.gov.uk	5
www.thesun.co.uk	0
www.totaljobs.com	2
www.tripadvisor.co.uk	1
www.tvguide.co.uk	1
www.w3schools.com	1
www.wikimedia.org	1
www.wikipedia.org	1
www.xe.com	5
www.yell.com	2
www.123-reg.co.uk	4
www.888.com	7

www.adobe.com	1
www.affiliatewindow.com	5
www.alibaba.com	4
www.amazon.co.uk	3
www.apple.com	12
www.argos.co.uk	4
www.asda.com	1
www.asos.com	1
www.avg.com	2
www.aws.amazon.com	3
www.bet365.com	7
www.betfair.com	5
www.birtishairways.com	1
www.booking.com	1
www.cj.com	4
www.clickbank.com	5
www.domaintools.com	3
www.easyjet.com	0
www.ebay.co.uk	8
www.ebuyer.com	1
www.etsy.com	1
www.expedia.co.uk	0
www.fiverr.com	1
www.godaddy.com	6
www.groupon.co.uk	0
www.heartinternet.co.uk	8
www.hotukdeals.com	1
www.ikea.com	7
www.istockphoto.com	3
www.johnlewis.com	2
www.ladbrokes.com	8
www.lovefilm.com	1
www.marksandspencer.com	1
www.microsoft.com	7
www.nationalrail.co.uk	3
www.next.co.uk	6
www.oneandone.co.uk	3
www.paypal.com	8
www.paypal-business.co.uk	8
www.pistonheads.com	1
www.play.com	3
www.salesforce.com	9
www.sparkstudios.com	5
www.talktalk.co.uk	9

www.tesco.com	5
www.themeforest.net	8
www.thetrainline.com	1
www.three.co.uk	6
www.tradedoubler.com	3
www.virginmedia.com	9
www.vodafone.co.uk	8
www.addthis.com	1
www.answers.com	2
www.aol.co.uk	7
www.autotrader.co.uk	4
www.blogger.com	10
www.blogspot.com	10
www.bt.com	7
www.channel4.com	1
www.conduit.com	8
www.dailymotion.com	8
www.download.com	1
www.ebay.com	8
www.facebook.com	0
www.google.co.uk	3
www.guardian.co.uk	1
www.hootsuite.com	1
www.hubpages.com	4
www.ign.com	1
www.imgur.com	1
www.linkedIn.com	1
www.live.com	7
www.mashable.com	2
www.mediafire.com	4
www.msn.com	7
www.myspace.com	2
www.national-lottery.co.uk	3
www.pof.com	1
www.reddit.com	1
www.seomoz.org	1
www.sky.com	9
www.skype.com	1
www.soundcloud.com	1
www.squidoo.com	1
www.stackoverflow.com	7
www.tumblr.com	9
www.twitter.com	6
www.typepad.com	3

www.vimeo.com	1
www.warriorforum.com	4
www.wikia.com	1
www.wordpress.com	6
www.wordpress.org	6
www.yahoo.com	8

Appendix 4 – Variable Summary Data

Variable ID	Variable Description	Yes	No	Total
V1	Must be at least 7 Characters in length	35	99	134
V2	Must not contain username/real name/company name	33	101	134
V3	Does not contain a complete dictionary word	47	87	134
V4	Significantly different from previous password	21	113	134
V5	Do not increment passwords	3	131	134
V6	Cannot use pet names	5	129	134
V7	Composition - uppercase, lowercase, numerals, symbols	70	64	134
V8	Instructions for after failed login attempt	117	17	134
V9	Strength meter	26	108	134
V10	Password must be different from user ID	32	102	134
V11	CAPTACHA	49	85	134
V12	Password sent directly to email on registration	8	126	134
V13	Secret Question	29	105	134

Appendix 5 – Variable Data Displayed By Category

Appendix 5.1 - V1 Must be at least 7 Characters in length

Category	Yes	No	Total
Content	10	28	38
E-Commerce	14	39	53
Identity	11	32	43
Total	35	99	134

Appendix 5.2 - V2 Must not contain username/real name/company name

Category	Yes	No	Total
Content	10	28	38
E-Commerce	10	43	53
Identity	13	30	43
Total	33	101	134

Appendix 5.3 - V3 Does not contain a complete dictionary word

Category	Yes	No	Total
Content	14	24	38
E-Commerce	20	33	53
Identity	13	30	43
Total	47	87	134

Appendix 5.4 - V4 Significantly different from previous password

Category	Yes	No	Total
Content	6	32	38
E-Commerce	5	48	53
Identity	10	33	43
Total	21	113	134

Appendix 5.5 - V5 Do not increment passwords

Category	Yes	No	Total
Content	0	38	38
E-Commerce	2	51	53

Identity	1	42	43
Total	3	131	134

Appendix 5.6 - V6 Cannot use pet names

Category	Yes	No	Total
Content	1	37	38
E-Commerce	3	50	53
Identity	1	42	43
Total	5	129	134

Appendix 5.7 - V7 Composition - uppercase, lowercase, numerals, symbols

Category	Yes	No	Total
Content	20	18	38
E-Commerce	29	24	53
Identity	21	22	43
Total	70	64	134

Appendix 5.8 - V8 Instructions for after failed login attempt

Category	Yes	No	Total
Content	33	5	38
E-Commerce	47	6	53
Identity	37	6	43
Total	117	17	134

Appendix 5.9 - V9 Strength meter

Category	Yes	No	Total
Content	5	33	38
E-Commerce	12	41	53
Identity	9	34	43
Total	26	108	134

Appendix 5.10 - V10 Password must be different from user ID

Category	Yes	No	Total

Content	9	29	38
E-Commerce	11	42	53
Identity	12	31	43
Total	32	102	134

Appendix 5.11 - V11 CAPTACHA

Category	Yes	No	Total
Content	15	23	38
E-Commerce	18	35	53
Identity	16	27	43
Total	49	85	134

Appendix 5.12 - V12 Password sent directly to email on registration

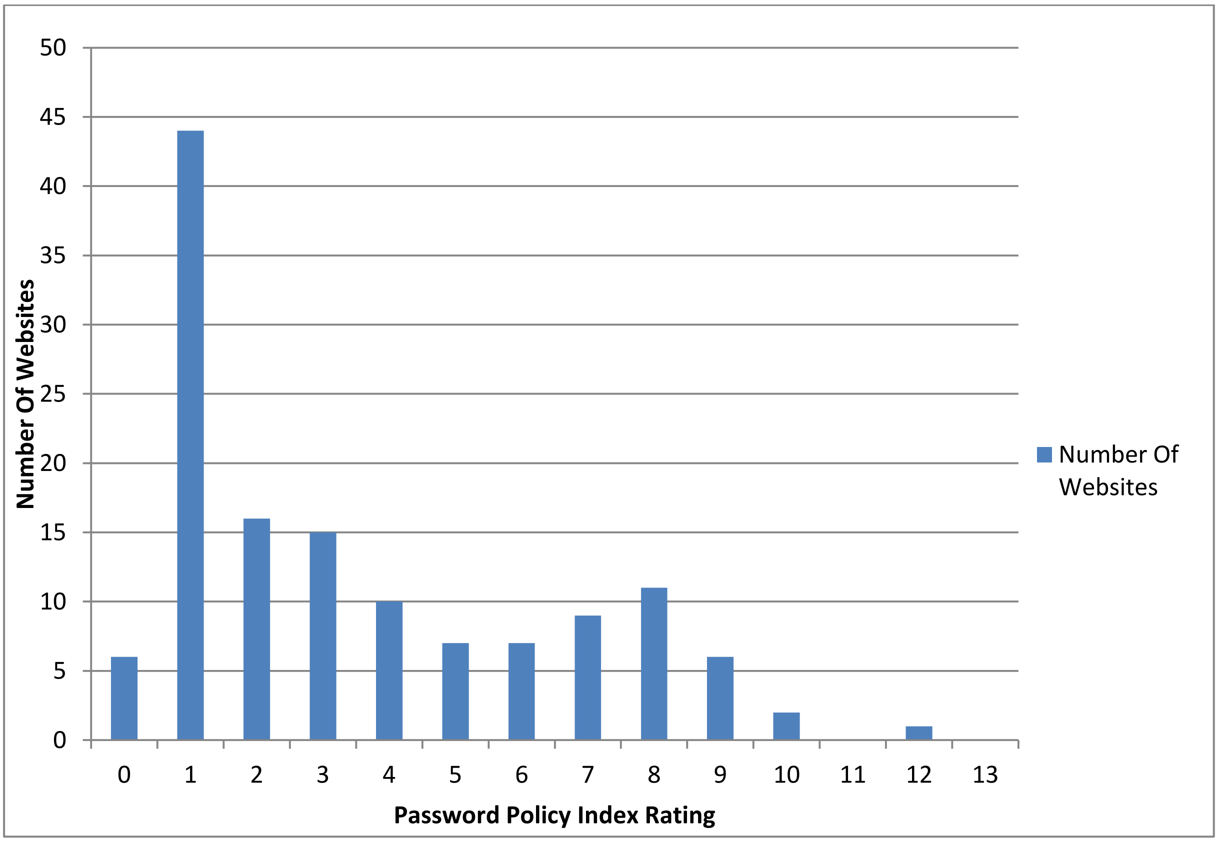
Category	Yes	No	Total
Content	2	36	38
E-Commerce	3	50	53
Identity	3	40	43
Total	8	126	134

Appendix 5.13 - V13 Secret Question

Category	Yes	No	Total
Content	9	29	38
E-Commerce	6	47	53
Identity	14	29	43
Total	29	105	134

Appendix 6 - Password Policy Index Rating Distribution Data

Password Policy Index Rating	Number Of Websites
0	6
1	44
2	16
3	15
4	10
5	7
6	7
7	9
8	11
9	6
10	2
11	0
12	1
13	0



Appendix 7 - Password Policy Index Rating Category Distribution Data

Appendix 7.1 – Content

Password Policy Index Rating	Number Of Sites
0	2
1	15
2	11
3	4
4	2
5	2
6	1
7	0
8	0
9	1
10	0
11	0
12	0
13	0
Total Number	38
Average	2.71
Median	1

Appendix 7.2 – E-Commerce

Password Policy Index Rating	Number Of Sites
0	3
1	13
2	2
3	8
4	4
5	5
6	3
7	4
8	7
9	3
10	0
11	0
12	1
13	0
Total Number	53
Average	3.79
Median	3

Appendix 7.3 – Identity

Password Policy Index Rating	Number Of Sites
0	1
1	16
2	3
3	3
4	4
5	0
6	3
7	5
8	4
9	2
10	2
11	0
12	0
13	0
Total Number	43
Average	3.07
Median	2.5