Facebook, Google, and Twitter as a Single Sign-on Service:

To Use or Not to Use

A Master Thesis

Submitted to the Faculty

of

American Public University

by

Adam B. Hall

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

September 2015

American Public University

Charles Town, WV

The author hereby grants the American Public University System the right to display these

contents for educational purposes.

The author assumes total responsibility for meeting the requirements set by the United States Copyright Law for the inclusion of any materials that are not the author’s creation or in the public domain.

© Copyright 2015 by Adam Bruce Hall

All rights reserved.

# DEDICATION

I dedicate this thesis to my parents Spencer and Elayne, wife Elisha, and kids Shameek, Kiara, and Aaliyah; your support throughout every day is what allowed me to complete this goal. To Robert Nunley and Ian Davis who gave me the pushes I needed when I became stagnant in my current career. Lastly, I also dedicate this to my Grandmother Evelyn, Uncle Colin, and Aunt Sharon. You all are the best family and friends anyone can ask for!

# ACKNOWLEDGMENTS

I wish to thank all the faculty of APUS for their support, patience, and willingness to help with any questions I have had over the past year. Dr. Denise D. Eggersman was exceptional in her help with the capstone course and her continual follow-up with me with all of my questions and mistakes. Lastly, American Public University provided me with all the tools that I needed to succeed in all of my course and the knowledge that I will need to be successful in the now and future in my career.

# ABSTRACT OF THE THESIS

FACEBOOK, GOOGLE, AND TWITTER AS A SINGLE SIGN-ON SERVICE:

TO USE OR NOT TO USE

by

Adam B. Hall

American Public University, September 15, 2015

Charles Town, West Virginia

Dr. Denise D. Eggersman, Thesis Professor

Over the past few years, there has been a growing trend in using sites such as Facebook, Google, and Twitter as a single sign-on method to login into other websites (Wang, Chen, & Wang, 2012, p. 365). This is a great idea to be able to use a single login credential to access multiple accounts. This is the same principal as the single sign-on method. However, people tend to use insecure passwords and/or reuse passwords and are not fully aware of phishing attacks... so trying to be safe while using the single sign-on method is difficult. These three issues are common amongst average users and even for those with knowledge of these kinds of issues as phishing attacks can be difficult to detect. Lastly, even though weak passwords, password reuse, and phishing attacks are not an exclusive threat to the single sign-on method, they make the use of sites like Facebook, Google and Twitter as a single sign-on an unsafe option.

Keywords: Phishing, Password Cracking, Single Sign-On, Hacking, Two-Factor Authentication

TABLE OF CONTENTS

CHAPTER PAGE

[DEDICATION ii](#_Toc428813875)

[ACKNOWLEDGMENTS iii](#_Toc428813876)

[ABSTRACT OF THE THESIS iv](#_Toc428813877)

1. [Introduction 1](#_Toc428813878)

[Background 1](#_Toc428813879)

[Statement of Problem 3](#_Toc428813880)

[Statement of Purpose 4](#_Toc428813881)

[Research Questions 4](#_Toc428813882)

[Significance of the Study 4](#_Toc428813883)

[Definition of Unclear Terms 5](#_Toc428813884)

[Limitations 6](#_Toc428813885)

[Delimitations 7](#_Toc428813886)

[Assumptions 7](#_Toc428813887)

[Theoretical Framework 8](#_Toc428813888)

1. [Literature Review 8](#_Toc428813889)

[Breaches 8](#_Toc428813890)

[Living Social. 8](#_Toc428813891)

[FNF. 9](#_Toc428813892)

[Jimmy Johns. 9](#_Toc428813893)

[Partners HealthCare. 10](#_Toc428813894)

[Stolen Credentials. 10](#_Toc428813895)

[Passwords 11](#_Toc428813896)

[Password Quantities. 11](#_Toc428813897)

[Password Complexity. 12](#_Toc428813898)

[Password Cracking. 13](#_Toc428813899)

[Password Reuse. 16](#_Toc428813900)

[Phishing 17](#_Toc428813901)

[Phishing Basics. 17](#_Toc428813902)

[Phishing Attack. 18](#_Toc428813903)

[Phishing Detection/Prevention. 23](#_Toc428813904)

[Phishing Technologies. 23](#_Toc428813905)

[Phishing Training. 28](#_Toc428813906)

[Single Sign-On 30](#_Toc428813907)

[Single Sign-On Basics. 30](#_Toc428813908)

[Web SSO. 31](#_Toc428813909)

1. [Methodology 34](#_Toc428813910)

[Subjects and Settings 34](#_Toc428813911)

[Data Collection Techniques 35](#_Toc428813912)

[Phishing. 35](#_Toc428813913)

[Passwords. 36](#_Toc428813914)

[Breaches. 36](#_Toc428813915)

[Statistical Analysis 37](#_Toc428813916)

1. [Results 38](#_Toc428813917)

[Overview 38](#_Toc428813918)

[Password Analysis 38](#_Toc428813919)

[Breach Analysis 42](#_Toc428813920)

[Phishing Analysis 43](#_Toc428813921)

[Correlation 44](#_Toc428813922)

1. [Discussion 44](#_Toc428813923)

[H1 Review 44](#_Toc428813924)

[H2 Review 46](#_Toc428813925)

[H3 Review 47](#_Toc428813926)

[H4 Review 48](#_Toc428813927)

[Summary 49](#_Toc428813928)

1. [References 52](#_Toc428813929)
2. [Appendices 62](#_Toc428813930)

[Appendix A: Sample Phished Email 62](#_Toc428813931)

[Appendix B: Available Aapus.edu Domain 63](#_Toc428813932)

[Appendix C: SAML Flow Chart 64](#_Toc428813933)

[Appendix D: Janrain Flow Chart 65](#_Toc428813934)

LIST OF TABLES

TABLE PAGE

[*Table 1.* Phishing Technologies 24](#_Toc428037531)

[*Table 2.* Phishing Rules 26](#_Toc428037532)

[*Table 3.* Empirical research into average password length 39](#_Toc428037533)

[*Table 4.* Average password length of several websites 39](#_Toc428037534)

[*Table 5.* Empirical Recommended Minimum Password Length 40](#_Toc428037535)

[*Table 6.*  Empirical Results of Unique Password Usage 41](#_Toc428037536)

[*Table 7.*  Empirical Results of Password Based Accounts 41](#_Toc428037537)

[*Table 8.* Corporate and Individual Breaches due to Stolen User Credentials 42](#_Toc428037538)

[*Table 9.* Empirical Results of Average Successful Phishes 43](#_Toc428037539)

LIST OF FIGURES

FIGURE PAGE

[*Figure 1.* Hulu login page with Facebook option 2](#_Toc429298706)

[*Figure 2.* Expedia login page with Facebook recommended 2](#_Toc429298707)

[*Figure 3.* John the Ripper password crack on Kali Linux 16](#_Toc429298708)

[*Figure 4.* Phished APUS Login Page 20](#_Toc429298709)

[*Figure 5.*  Real APUS login page 21](#_Toc429298710)

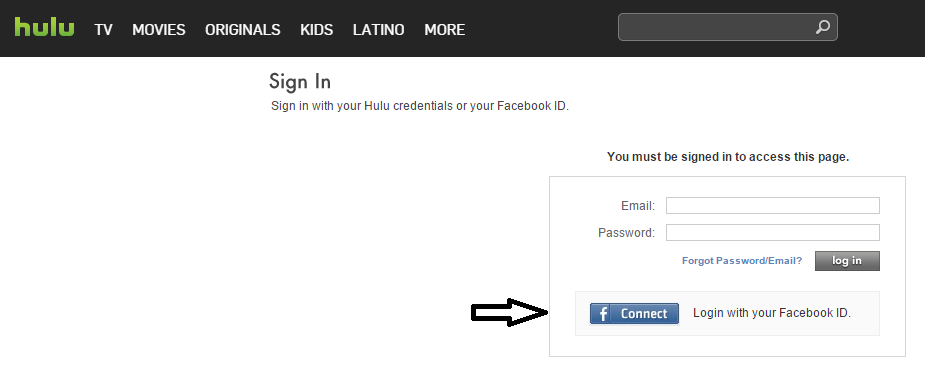
[*Figure 6.*  URL of Anchor Text 22](#_Toc429298711)

[*Figure 7.*  Tacacs and Radius Authentication Flow 31](#_Toc429298712)

# Introduction

## Background

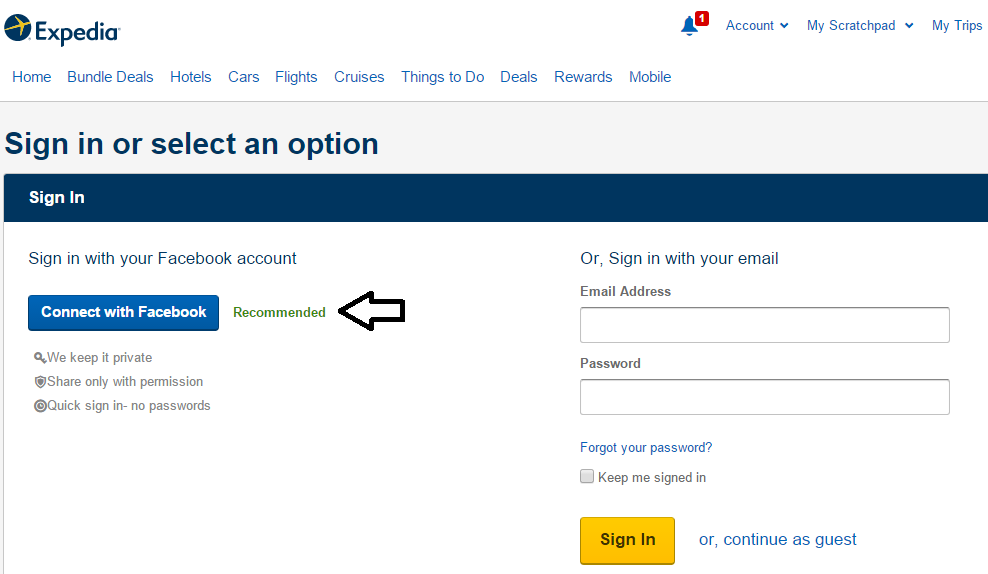
The breach of Community Health Systems in 2014 was an attack that spanned between April of 2014 and June of 2014 (Bosshart, n.d., para. 4). The attackers were able to get through their network security and were able to steal patient data to include patients’ names, addresses, birthdates, social security numbers, telephone numbers, and the names of employers or guarantors (Bosshart, n.d., para. 7). Another breach occurred at Sourcebooks, which is an online book-purchasing website, in October of 2014. Visa notified Sourcebooks of multiple fraudulent charges concerning purchases on Sourcebooks.com (Sourcebooks, 2014, p. 1). Sourcebooks found a security vulnerability in their shopping cart software which allowed attackers to steal personal and credit card information when customers where completing their purchase (Sourcebooks, 2014, p. 1). This breach reportedly affected nearly 5,000 customers (Sourcebooks, 2014, p. 1). Next, there was a breach of Home Depot in September of 2014 in which attackers stole nearly 53 million email addresses as well as credit card data (The Home Depot, n.d., para. 5). According to Home Depot, the attackers used a compromised third-party vendors login credentials to break into the Home Depot network (The Home Depot, n.d., para. 2). Home Depot also suggested going to a website to help educate users about phishing attacks to prevent against frauds that had been going around after the breach trying to get users to divulge personal data. Lastly, Target reported a breach in their network in December of 2013. They advised all shoppers who used a credit card at their stores between November 27th and December 15th to replace the credit cards used at their stores and to monitor their account transactions closely... numbers of possible affected people ranged close to 70 million (Target, n.d., p. 1).



*Figure 1.* Hulu login page with Facebook option

Hulu. (n.d.). *Sign In*. Retrieved from secure.hulu.com: https://secure.hulu.com/account/signin

This figure shows the option to login using a button for authentication with Facebook.



*Figure 2.* Expedia login page with Facebook recommended

Expedia. (n.d.). *Sign In*. Retrieved from expedia.com: https://www.expedia.com/user/login

This figure show the option to login using Facebook and recommends to use that option.

Sites like hulu.com, pinterest.com, groupon.com, and usatoday.com offer the option to be able to login to their sites using another site to authenticate the user like Facebook, Google, or Twitter. This option provides a quick way to be able to log into your account using either the main sites login credentials or one of the authenticating sites logins if you use that site. This can allow a user to have to remember one sites password for access to multiple sites. Sites such as podbean.com and expedia.com even recommend using your Facebook login over your local site login.

On March 23 of 2014, the site twitch.tv released a blog stating that there was unauthorized access to some of their user’s accounts (Twitch Interactive Inc., 2015, para. 1). The author of this paper received an email the next day at 2000 hours Eastern Time from Twitch informing him about this breach. Two hours later, the author received an email from PayPal concerning an issue with the author’s account. After contacting PayPal, they informed the author that someone attempted access to the author’s account from outside of the United States and PayPal blocked the login. The two events may be related, but there is no tangible proof of that. However, the author did use the same password ‘inadvertently’ on both accounts.

## Statement of Problem

Businesses are moving to online logins allowing more access for users to their personal information and access to company information. With users having to remember an increasing amount of passwords, users are using other methods to keep track of passwords. A current method involves using websites such as Facebook, Google, and Twitter as a method to login to other sites. While some sites even say this method is the ‘recommended’ method, is the use of the single sign-on method using sites such as Facebook, Google, and Twitter to authenticate a user for a different website a safe option to use?

## Statement of Purpose

The purpose of this study is to show the ease of acquiring user’s login credentials using phishing attacks and password attacks, and how leveraging the single sign-on method through sites such as Facebook, Google, and Twitter, can quickly gain access to multiple accounts of a user.

## Research Questions

H1. Phishing attacks are not hard to detect due to their ability to look like a normal email or website.

H2. Many users do not use simple passwords for their accounts.

H3. Many users do not reuse the same passwords on multiple accounts.

H4. Compromised user accounts have not occurred through stolen login credentials.

## Significance of the Study

This study will help to create an understanding of what the single sign-on method is and that this method is the same as websites offering a login option to their site through sites such as Facebook, Google, or Twitter. The importance of this understanding is due to websites as well as mobile applications offering the use of those sites as an option to login and not associating the negative consequences that could happen if there is a compromised login credential. There are even sites that mention using the single sign-on method with Facebook, Google, or Twitter as the recommended option, or the faster option (Expedia, n.d., p. 1; Podbean.com, n.d., p. 1). Even though the method is faster and an easier option, this option is less secure than others.

Many people may be more inclined to use the single sign-on method because they feel that there is no significant information available about them from that site (Sun, Pospisil, Muuslukhov, Dindar, Hawkey, & Beznosov, 2011, p. 3). However, every painted picture ever made started off as a single brush stroke of paint. Getting your address or a previous address, a different email account, your birthday, how many children you have and their names, and many other small pieces of information can quickly build your life. Furthermore, once these small pieces have started to come together… the bigger more important pieces become available.

The intent for this research is to help foster more knowledge concerning this issue and add new measures into the current methodology of this framework making this method more reliable. Some new ideas to include are website checks that can match the current link you want to visit to the intended site to ensure there is no discrepancy between the spellings of the two sites. Secondly, password checks between single sign-on sites and sites using them for access to their website to ensure that the password is not the same on both sites, and allowing only limited access to your account if logging in with your Facebook, Google, etc. account. Other ideas include allowing tracking and notification of any site that access is attempted using one of those methods; removing the ability to create a password for an account if logged into by one of those methods; and lastly tying in IP based logins to the new site from the last IP of the single sign-on method.

## Definition of Unclear Terms

Cleartext/Plaintext – This is human readable data prior to or after encryption (non-unintelligible) (Merriam-Webster, n.d.d, p. 1).

E-Commerce – Refers to the buying and selling of goods online (Merriam-Webster, n.d.a, p. 1).

Encryption – To change the form of data with the intent to hide the meaning (Merriam-Webster, n.d.b).

Hacker/Cracker – A person that tries to access illegally computers, networks, systems, and files (Dictionary.com, n.d., p. 1).

Phishing – a type of fraud in which an e-mail user is tricked into revealing personal or confidential information to a party that is not who they claim to be (Merriam-Webster, n.d.c, p. 1).

Single Sign-On (SSO) – systems that help reduce the amount of login credentials a user has to remember, by replacing those credentials with one credential which they can authenticate themselves to multiple different web sites (Cao, Shoshitaishvili, Borgolte, Kruegel, Vigna, & Chen, 2014, p. 1).

Two-Factor authentication – A second step of verification to log into an account that can include something you have (phone) or something you are (fingerprint) (Google, n.d., p. 1).

URL – Short for universal resource locator; refers to the address source of an object on the internet and the protocol used for communication (Merriam-Webster, n.d.e, p. 1).

User Credentials – Objects needed to identify a user to a system such as a password, username, email address, and biometrics

## Limitations

One limitation concerning this research is the lack of credible subjects. Many of the studies found were performed in controlled testing environments with limited people. To truly get an idea of the strengths or weakness of users passwords and reuse of passwords as well as susceptiblity to phishing attacks… one would need to be able to perform these attacks against the general public with them unaware of the attack which is illegal (Reinhard, 2012, p. 1). Furthermore, there have been some database breachs such as Myspace and Rockyou where their password database was dumped out onto the public internet. This gives us some idea concerning a general publics password methodology… but that is only in regards to that site and the restrictions on the passwords for that site. One would also need to test password reuse and strength versus multiple types of restrictions across multiple sites. Such examples to include sites that have no restrictions on password length, to sites that require a certain amount of characters as well as upper and lowercase characters, digits, and special characters. Furthermore, one would also need to perform the same tests against sites that contain little to no personal information versus sites that contain sensitive information to include medical, banking, and other private information.

## Delimitations

For this research, the author will not go into the security of the SSO devices themselves. Many applications can have patches applied to them and there are less SSO devices than there are users using the device. Secondly, the author will not deal with the various types of encryption or hashing in the password process. The author will be concerned about getting the password in any form… but particularly in cleartext through means of phishing attacks. Thirdly, the author will not discuss the differences between SSO and web SSO, as the methodologies of the two are nearly the same. Lastly, this research will focus on phishing attacks through embedded links in emails, which will try to send the user to an impersonated site, and the structure of the impersonated sites.

## Assumptions

This study includes the following assumptions: (a) all passwords are crackable given enough time; (b) the methodology of SSO and web SSO are the same; (c) the methodology of phishing, spear phishing, and whaling are all the same.

## Theoretical Framework

There is already a myriad of research available concerning password complexity, password cracking/hacking, and best password practices. There is also a plethora of knowledge concerning phishing attacks such as how phishing attacks work, and best practices on how to detect phishing attacks. Next, there is also a large availability of material concerning SSO and varying weaknesses concerning if a user’s login credentials become compromised, then every account associated to that users login can also be compromised (Sun, et al., 2011, p. 10; Ives, Walsh, & Schneider, 2004, p. 76; Mpafe, 2013, p. 13). This research will fill a gap dealing with the association of password issues, phishing attacks, SSO, and their interrelation to logging into online sites using another site as an authenticator… also known as web SSO.

Current research into web SSO deals primarily with the actual method of how the web SSO works. Current research lacks the direct linking of a button on a website that allows a user to login to that site using another sites login credentials and the associated threat that the method possess which are those of SSO. While this study will not modify the SSO/web SSO method, password implementations, or phishing attacks; the author hopes the research will add extra deployable security measures to make SSO safer. Finally, this research will also help to educate the public on what the method they are using for authentication is, and an associated risk with that method.

# Literature Review

## Breaches

Living Social. Sometime around April 12 of 2013, there was a data breach of the site livingsocial.com (McNicholas, 2013, para. 1). LivingSocial is an online site for the purchasing of goods similar to groupon.com. This data breach resulted in the theft of names, email addresses, dates of birth, and ‘hashed’ or ‘salted’ passwords (LivingSocial Inc., n.d., p. 1). The breach was determined to have occurred through the use of stolen user credentials that allowed the attackers to gain access to parts of LivingSocials environment which included where user information was stored (McNicholas, 2013, para. 1). The affected amount of people due to this breach was over 29 million (para. 1). According to McNicholas, “Regarding the passwords at issue, although they were hashed and salted, given time, it would conceivably be possible for the intruder to reverse-engineer them” (p. 3).

FNF. In April of 2014, there was a data breach of the company Fidelity National Financial (FDF) (Perez, 2014, para. 1). This data breach resulted in the possible theft of Social Security Numbers (SSN), bank account numbers, credit/debit card numbers, and driver’s license numbers (para. 3). Through investigations provided internally as well as through a third party group, the investigators determined that the attackers performed a targeted phishing attack which compromised a small number employees and were able to login through the phished accounts (para. 3). Concerning the amount of affected consumers, there is no clear number of the amount of people that may have been affected by this breach. The ongoing investigation has so far determined that the breach was not intended to steal consumer information, but to monitor ongoing business related traffic in hopes to disrupt the scheduled flow of money transfers (para. 3).

Jimmy Johns. On July 30 of 2014, there was a data breach of the fast food restaurant chain Jimmy Johns (Jimmy Johns Franchise LLC., 2014, para. 1). This data breach resulted in theft of credit and debit card data (para. 1) and possibly cardholders names, verification code, and/or expiration date (Ventrone, 2014, para. 2). The attackers managed to steal login credentials from a point-of-sale vendor which were used to remotely access Jimmy Johns systems (para. 2). Jimmy Johns estimates nearly 216 stores were affected (para. 3).

Partners HealthCare. On November 25 of 2014, there was a data breach of the healthcare provide Partners HealthCare (Anonymous, 2015, para. 1). This data breach resulted in the potential theft of names, addresses, SSN, dates of birth, phone numbers, e-mail addresses, bank account numbers, and bank routing numbers in regards to the affected workforce members (para. 1). Workforce members beneficiaries and dependents had a potential loss of names, addresses, dates of birth, phone numbers, and SSN (para. 1). The attackers performed a phishing campaign against Partners Healthcare associates of which several thought the emails were ‘legitimate’ (para. 1). This lead to the attackers being able to access the Partners Healthcare network through the compromised login credentials.

Stolen Credentials. While Partners Healthcare, Jimmy Johns, Fidelity National Financial, and LivingSocial breaches all occurred through user credentials being stolen to gain access to the corporate network, there are similar attacks that occured only on individual accounts. Around December of 2014, American Airlines detected several unauthorized access’s of user accounts (American Airlines Inc., 2015, para. 1). American Airlines determined that their own systems had not been breached. Furthermore, they believed the users accounts had been breached by the users login credentials being stolen in breaches from other companies. The accounts that were compromised could have had stolen names, email addresses, phone numbers, postal addresses, dates of birth, last four or credit/debit card and expiration date, AAdvantage number, information about the users miles, mileage activity, points acrued, and last four digits of passport (para. 1). Furthmore, just like the American Airlines breach; Intuit (Turbo Tax), Toys R US, and Nordstroms were all affected similarly. They all found that their own systems had not been breached and an investigation determined the users account credentials had been taken from other various breaches or methods and were used on their site (Dawson, 2011, para. 3; Meighan, 2015, para. 1; Toys R Us, 2015, para. 1). Through the Nordstom investigation, customers had admitted to using non-complex passwords and to reusing the same passwords on multiple sites (Dawson, 2011, para. 5).

## Passwords

Password Quantities. One of the problems that users have to deal with today is the amount of passwords that they have to remember. According to Ives, Walsh, and Schneider as well as Cazier and Medlin, this is in part due to the large growth of e-commerce and the need for password protected sites (2004, p. 76; n.d., p. 1; Cao, et al., 2014). Even non tech-savvy individuals will still require a few passwords that they have to remember; email accounts, online billing accounts, debit card pin numbers, and special passwords when talking to certain businesses on the phone. Zhang, Luo, Akkaladevi, and Ziegelmayer show on the smaller side of passwords that need to be remembered, the average employee would require nearly three different job-related login credentials (2009, p. 166). Chitalia, Sanghavi, Iyer, Shah, and Jyotinagar state that the average user has to remember about six point five passwords (2013, p. 207). Lastly, on the higher end, there was evidence shown that users needed to remember passwords for nearly twenty-five different accounts (Florencio & Herley, 2007, p. 1). Another issue increasing the amount of passwords to remember is due to password expiration (Adams & Sasse, 1999, p. 42). While not every site requires passwords to expire, any site that does require it, forces a user to have to create and remember another password. Furthermore, when dealing with accounts that a user has forced password expirations, some sites will require a unique password for every new password on their site further adding to the library of passwords for a user to remember.

The amount of passwords is not just limited to websites or e-commerce. Users must also remember passwords for their cell phones, laptops, tablets, computers, and may have to remember multiples of these determining how many of the same type of devices that they have. Many companies are having multiple parts of the company moved to the cloud to include organizational data, computation tasks, and even business operations (Wang, Chen, & Wang, 2012, p. 1). With so many types of personal equipment that a person can own that needs to be password protected, coupled with the amount of passwords required for the various methods of access to tasks at people’s jobs, users have to remember an ever-growing amount of passwords.

Password Complexity. There is no defined legal standard for the complexity of a password. Generally outlined in a company’s security policy is the metrics for the complexity of a password. This becomes an issue for users, as not only do users have to remember multiple passwords, but also remember different complexities of passwords. Multiple sites may require different minimal lengths, different mandatory characters, and different maximum lengths. One site may require a minimum password length of eight characters; require two uppercase characters, two lowercase characters, two digits, and one special character; and have no maximum length. Another site may require a minimum length of six characters, a maximum length of twelve characters, and have no other requirements. Furthermore, some sites may only allow a subset of characters, which is occasionally seen in special characters such as not allowing single or double quotes, and less than or greater than symbols. Those symbols can potentially cause vulnerabilities for SQL databases and web pages.

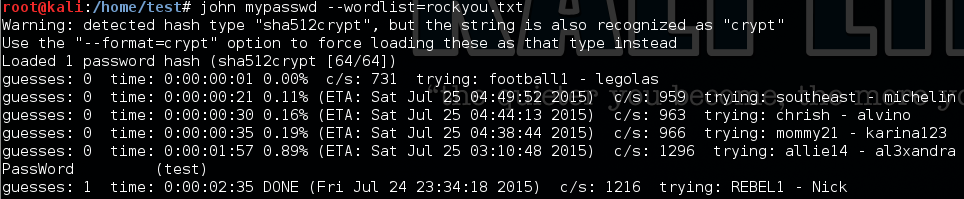
Most users tend to use weak passwords despite any complexity standards (Walters & Matulich, 2011, p. 3; Zhang, Luo, Akkaladevi, & Ziegelmayer, 2009, p. 166; Cazier & Medlin, 2006, p. 3). This is in part due to the fact that humans can only store a small amount of random information in their short-term memory, roughly five to nine random bits (Cazier & Medlin, 2006, p. 3). Because of this issue, users tend to select passwords that have personal meanings to them that are easy to associate with objects in their long-term memory (para. 1). This tends to lead people to more straight forward words like family members names and basic dictionary words that are normally used on a regular basis rather than complicated strings of letters, numbers, and special characters. Lazar, Tikolsky, Glezer and Zviran explained a revolving scale dealing with password memorization in which the more complicated the password, the harder the password is to remember and to possibly be hacked/cracked; and the less complicated a password is, the easier the password is to remember and the easier the password is to be hacked/cracked (2011, p. 28).

Password Cracking. Password complexity plays an important part in the amount of time that is needed to crack a password. Password cracking refers to any method used to obtain a password through non-approved methods. An approved method is generally those of a password reset or a forgotten password request that can reissue a password. Passwords contain a mathematically defined amount of space. Even a password with no password requirements only has a finite amount of combinations that the password can contain. A password can be broken down into password content and password length. Password content referring to what is the password made of: uppercase letters, lowercase letters, numbers, and special characters. Those four sets break down into a defined space of 26 uppercase letters (ABCDEFGHIJKLMNOPQRSTUVWXYZ), 26 lowercase letters (abcdefghijklmnopqrstuvwxyz), 10 numbers (0123456789), and 32 special characters (~`!@#$%^&\*()\_-+={[}]|\:;”’<,>.?/) combining for a total of 94 possibilities for a single character. If your password had only one character, the password could be cracked within 94 guesses at the password. The next part deals with the length of the password, of which the possible single character combination will be raised to the power of the amount of characters. If a password contained only uppercase and lowercase letters, and had a length of eight characters, the password would have a mathematical formula of 528 which is equal to 53,456,728,531,456 possible combinations. Increasing a password length by one increases the possible combinations greatly. 529 has 2,779,905,883,635,712 combinations which is five times larger than that of the password length of 8. This would make cracking a nine character password much harder than cracking an eight character password. While these numbers seem very large, these are not uncrackable lengths.

Many authors have referenced a password cracking tool called ‘John the Ripper’ for offline cracking of passwords (Bonneau & Preibusch, 2010, p. 4; Bonneau, 2012, p. 539; Amico, Michiardi, & Roudier, 2010, p. 3; Chou, Lee, Yu, Lai, Huang, & Hseuh, 2013, pp. 16-17). The author performed research using the tool to evaluate the tools ease of use and effectiveness. A three-part walk through was found on youtube.com under the user ‘Live Hacking’ (https://www.youtube.com/watch?v=QqCeHk1yf3k) entitled ‘John the Riper’. Several other examples of how to use the tool were also available on youtube.com.

On July 13 of 2015, the author performed a test of the tool John the Ripper. The author created a user named ‘test’ and gave this user the password ‘PassWord’. This password was chosen as an example for the previously mentioned password complexity of 528 which involves only eight characters and only uppercase and lowercase letters. This test was also performed on a default install of Kali Linux 1 which has John the Ripper 1.7.9 built in and on Ubuntu Linux 14.04 with the newest version of John the Ripper installed, 1.8.0. A database of passwords must be used for the application to try and break a password with. For both tests, the Rockyou database was used as a wordlist to attempt to crack the password. This database was retrieved from (https://wiki.skullsecurity.org/index.php?title=Passwords). The /etc/passwd and /etc/shadow file from both systems were used for the contents of the user password. This test is designed to simulate an attacker that managed to steal the /etc/passwd and /etc/shadow files off of a Linux system.

Following the instructions provided by Youtube as well as the help page from the application, the author successfully cracked the password on both systems. The password crack on the Kali Linux system completed in two minutes and 35 seconds, which was faster than the attempt on the Ubuntu Linux system which completed in three minutes and 11 seconds. These two times resulted in an average cracking time of similar passwords to two minutes and 53 seconds. With the wide availability of free directions on how to use the tool, as well as free password databases that can be used with the tool, John the Ripper is an effective tool to be used with offline password cracking. Not only is the tool effective, but the tool does not require much skill to install or use as the directions are very detailed and the application does not require many steps to install. Lastly, these results also confirm the claims made by the authors mentioned above concerning the effectiveness of the tool.



*Figure 3.* John the Ripper password crack on Kali Linux

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

This figure illustrates John the Ripper password cracker on Kali Linux.

There are many password cracking tools available: John the Ripper (http://www.openwall.com/john/), OphCrack (http://ophcrack.sourceforge.net/), l0phtcrack (http://l0phtcrack.com), hashcat (http://hashcat.net/oclhashcat/), and Aircrack-NG (http://www.aircrack-ng.org/) just to name a few. These tools employ several different methods to crack passwords. One of the methods most commonly used and effective at cracking weak passwords is known as a dictionary attack (Amico, Michiardi, & Roudier, 2010, p. 3; Martin & Tokutomi, n.d., p. 5). This attack is designed to match the password with commonly occurring words within a language (Raza, Iqbal, Sharif, & Haider, 2012, p. 440). Other methods of attack are: brute force attacks, replay attacks, and phishing attacks.

Password Reuse. The ability to remember easy passwords coupled with the large amount of passwords that people need to remember will eventually cause password reuse (Bonneau & Preibusch, 2010, p. 34). As people become familiar with another password, that password will now be a memorable word that can be used as a password somewhere else. According to Ives, Walsh, and Schneider, people are not strong enough on a ‘cognitive level’ to remember multiple passwords and this causes users to reuse passwords (2004, p. 76). This can cause both a less sensitive site such as a place that contains no credit card information or personal information, just a login and password; and a site containing personal information and credit card information to have the same login credentials. If the site with the personal information were to expire the user’s password and force the user to create a new password, the user may use the password of the less sensitive site since that login credential is memorable to them now.

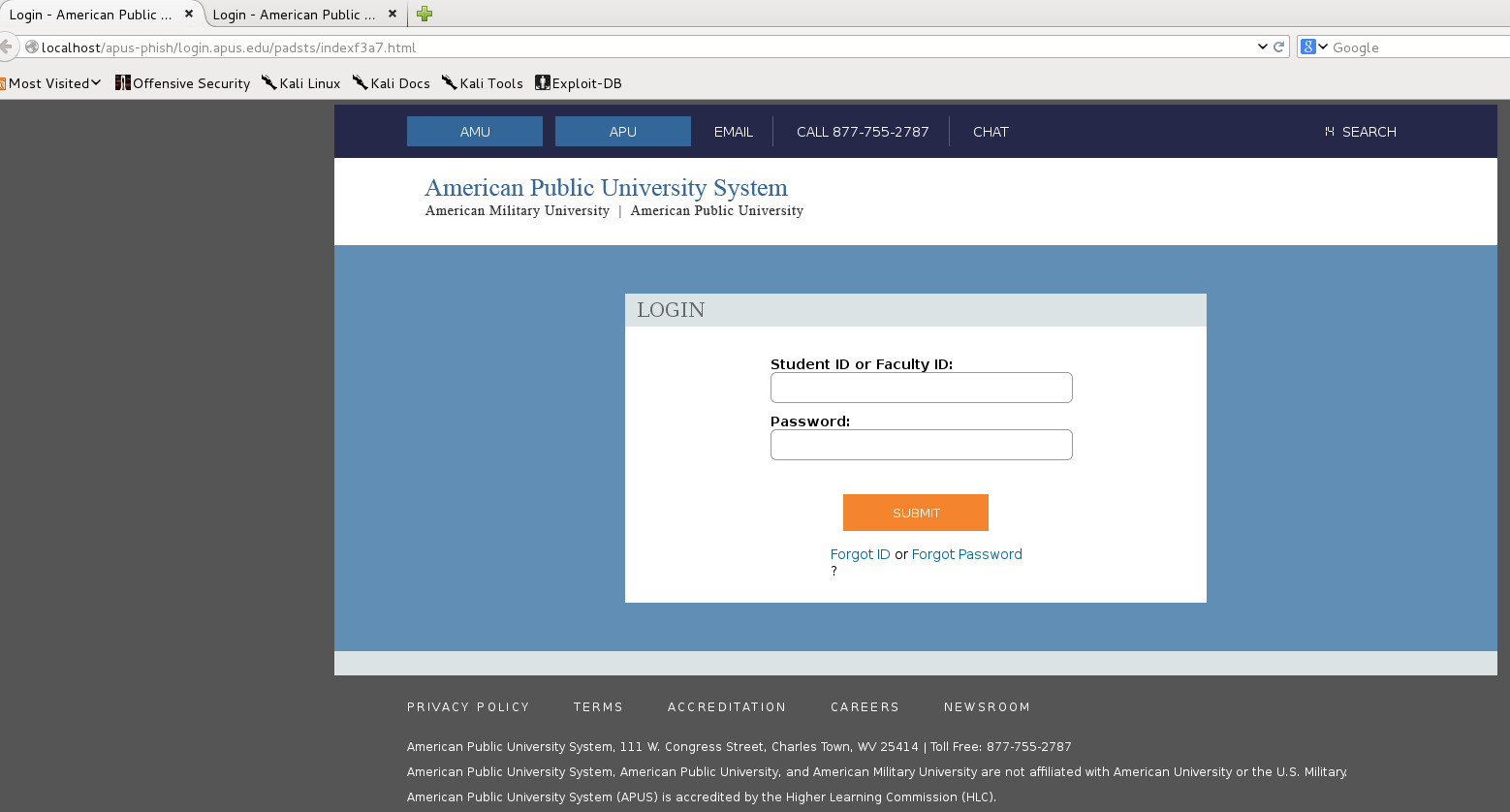
## Phishing

Phishing Basics. Phishing is a method of attack designed to steal a user’s personal data generally through deceptive emails and websites (Hong, 2012, p. 74; Halevi, Lewis, & Memon, 2013, p. 1). This has been a method that has grown in usage, deceptiveness, and lucrativeness over the past few years (Halevi, Lewis, & Memon, 2013, p. 1; Marchal, Francois, State, & Engel, 2014, p. 458; Kontaxis, Polychronakis, & Markatos, 2012, p. 321). The attack is designed to primarily trick the user into either clicking on a link in an email, or visiting a fradulent website. The intent of the attack is to try and get the user to input some personal information (Halevi, Lewis, & Memon, 2013, p. 2). With sites like Facebook having over 900 million users (p. 3), there is no foreseeable decline with these kinds of attacks.

Phishing attacks range in their level of deceptiveness which is what can make them rather obvious all the way to nearly undetectable, even for experienced users (Parno, Kuo, & Perrig, 2005, p. 5). On the less deceptive side, phishing attacks may be an email asking you to login to an account for a company of which you have no account with. They could also address you as ‘customer’ instead of using your name and use other vague terms that never actually identify you. While on the more targeted side, phishing attacks may take a user having to check all hyperlinks and the actual URL address itself to determine whether or not a site or email is real. Furthermore, if another user or company you deal with regularly emails you, an attacker could change their email address to say that the address is from an entity you regularly converse with giving you more incentive to click on the link in the email or going to a website that they suggest. In a phishing experiment conducted on students at West Point Academy, nearly 80 percent of the students clicked on an embedded link in an email sent to them that was actually a phishing email (Ferguson, 2005, p. 56). When the students were asked for feedback as to why they clicked on the link, some of their responses were “The e-mail looked suspicious but it was from an Army Colonel so I figured it must be legitimate” and “Any email that contains the word ‘grade’ in it gets my immediate attention and action!” (p. 56). Knowing that these were military cadets and students allowed the attacker to craft the phishing email in a way that would get their attention and deceive them enough to click on the link. In a study performed by Jagatic, Johnson, Jakobsson, and Menczer, they had a seventy-two percent success rate in users clicking on embedded links which is close to the same results that Ferguson (p. 56) came up with.

Phishing Attack. One thing to understand about phishing attacks is that they do not require expert knowledge in phishing attacks to perform the attack, nor do they require large amounts of money to perform the attack. As the phishing attack performed on West Point Academy shows, one could perform the same attack easily with just a name. Most colleges have a directory where faculty member’s information is available. This can include just names, or names, pictures, and even bios. Some examples can be located at http://www.usma.edu/bsl/SitePages/Faculty.aspx, http://www.harvard.edu/faculty, and https://www.nyu.edu/about/leadership-university-administration/office-of-the-president/office-of-the-provost/redirect/faculty/new-faculty.html, where various types of instructor information is available. From there, an attacker can find the email address structure for the school and will now have the means to make an email appear to come from a legitimate person. The structure is in reference to how the schools email address looks such as; are they first-name period last-name @school.edu, or last-name period first-initial @school.edu. Next will be to find the type of class the instructor teaches. This will allow the email to be accurate with respect to something that the teacher would send in an email. The hard part that will require some research is how to find students that are currently taking that instructors course, or are still in the program and might respond to an email from that teacher. However, with the amount of information that may be present about the faculty members, the attacker may be able to get around the limitation of a class.

Appendix A demonstrates an attacker’s ability to target all students by acting as the Student Services Advisor. With the information gained from the faculty page, the actual Student Services Advisor information is available for that spot to allow this email to appear as if the email is legitimate since someone could lookup that person and the information would match the actual Student Services Advisor information. The student would then click on the link which could take them to a login page and they would then attempt to login with their username and password for the school at which time that information would be sent to the attacker and now that attacker has phished the users login and password for that account.

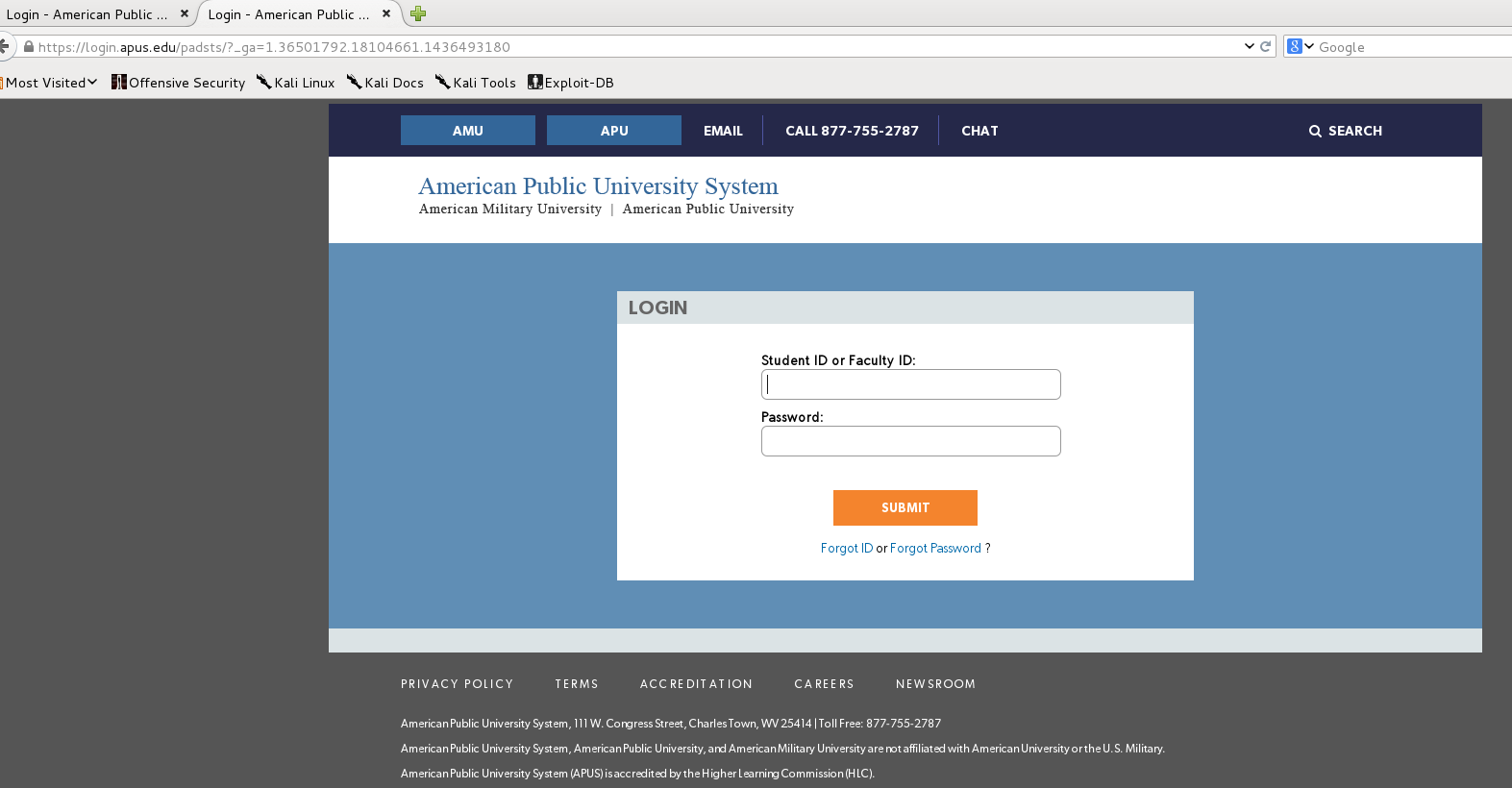
While the email is a big part in a phishing attack, the email is not the only part (Parno, Kuo, & Perrig, 2005, p. 4). The phishing site must also be convincing enough to a user for them to use the site. For this research, not only must the site be convincing, the site must also be easy to create. The author has used the American Public University System (APUS) login page for an example attack. Figure 4 below shows a phished version of the APUS login page. This attack started by first downloading, installing, and booting into Kali Linux 1. There are several walk-throughs on YouTube on how to install the Kali Linux Operating System that is available by searching for ‘Kali Linux install’. Next the author updated the system to ensure everything was up to date by running ‘apt-get update && apt-get upgrade –y’. Once the system was up to date, the author installed Httrack by running ‘apt-get install Httrack’. After this, the author searched YouTube for ‘Httrack Kali Linux’ to find directions on how to run Httrack. Next, the author ran Httrack and copied the login page for APUS which was located at ‘https://login.apus.edu/padsts/?\_ga=1.36501792.18104661.1436493180’. Httrack had access for the directory to store the copied website in which was /var/www/ and all settings stayed at their defaults. 

*Figure 4.* Phished APUS Login Page

APUS. (n.d.). Login. Retrieved from login.apus.edu:

https://login.apus.edu/padsts/?\_ga=1.36501792.18104661.1436493180

This is a phished version of the APUS student login page.



*Figure 5.*  Real APUS login page

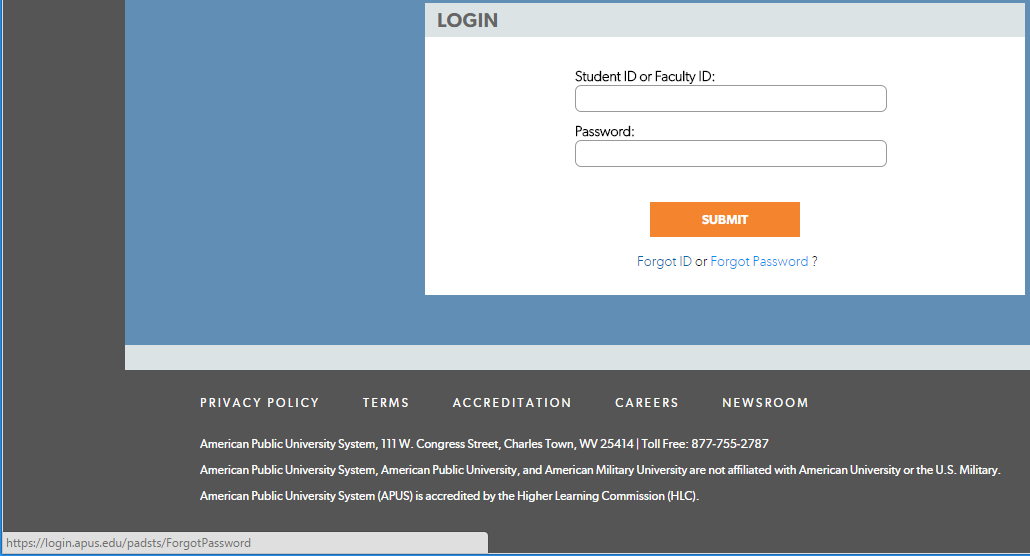
APUS. (n.d.). Login. Retrieved from login.apus.edu:

https://login.apus.edu/padsts/?\_ga=1.36501792.18104661.1436493180

This illustration is of the real APUS login page.

Running just the defaults and not trying to fix any discrepancies upon completion, the two sites are mostly identical. You should have noticed in the URL bar that the two addresses are different, but an attacker could register a domain similar to apus.edu such as aapus.edu and the URL could be identical aside from the extra ‘a’ in Apus. As of the time of this research, the domain for aapus.edu was available according to net.educause.edu as seen in Appendix B. Once the domain was registered, the attacker can tie the domain name to the cloned apus.edu site and would be able to attempt to fool anybody who did not detect the aapus.edu in the URL bar instead of apus.edu.

Now that the attackers have their site up and running as a clone of the real site, the next step is to ensure that all data stays within the phished site. One way of performing this task is through changing the underlying hyperlink of all embedded links on the page. In our phished site from Figure 4 above: Forget ID, Forget Password, and Submit all have an underlying embedded link that will redirect the user to a webpage somewhere. Most are visible simply by hovering over the link as in Figure 6 below. From here, you can see in the bottom left corner of the image a URL that would redirect the user to the https://login.apus.edu/padsts/ForgotPassword page if you hovered over the anchor text ‘Forgot Password’. The attacker would change all of these links to say aapus, instead of apus. Being able to see these links is extremely difficult to perform if the site was on a mobile device, as there is no ‘hover over’ function on many mobile devices for you to see the underlying link of the anchor text. In addition, there may not be enough room for you to see the entire link on the screen if there was.



*Figure 6.*  URL of Anchor Text

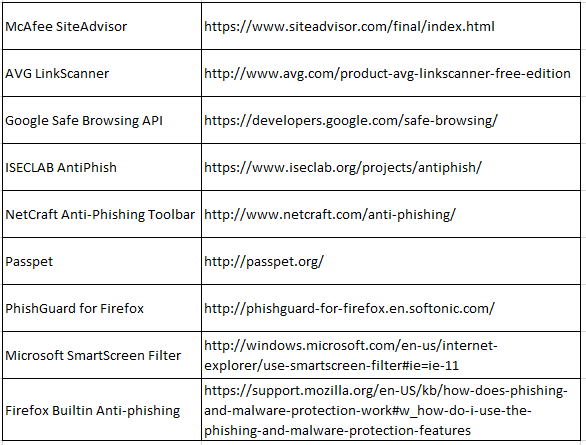
APUS. (n.d.). Login. Retrieved from login.apus.edu: https://login.apus.edu/padsts/?\_ga=1.36501792.18104661.1436493180

This illustration shows the Forgot Password anchor text button and the buttons underlying URL.

Now that the attacker has their phished emails setup, and their cloned site completed, the phishing attack is now ready to launch. All emails will have real embedded links that will take the user to what looks like the real school site. All links on the lookalike school site will direct them to a page on the phished site that looks just like the real site. Lastly, the attacker can just leave this and see how many students would try to log into their account on the phished site after sending out the emails to any students for the school. The attacker could also use just the login page and not have to create the phishing site even deeper. To be more deceptive, the attacker could have your credentials sent to another site as you login as well as send you to the legitimate site at the same time. This way the attacker could steal your credentials and you would be on the real site after you logged in. If you did not know that the named changed from aapus.edu to apus.edu after you logged in, you may have no idea that you were phished.

Phishing Detection/Prevention. At first glance, the issue of phishing may seem fixable by deploying anti-phishing technologies, and/or to provide users phishing training. However, this is not as easy of an issue to fix even with those two methods. There is no security application currently available that can provide ‘complete protection’ against phishing attacks (Parno, Kuo, & Perrig, 2005, p. 6). Furthermore, most users cannot tell the difference between phished sites and legitimate sites (Khonji, Iraqi, & Jones, 2013, p. 2097).

Phishing Technologies. Several technologies are available to help aid in the detection and prevention of phishing attacks. While prevention of phishing attacks would be the preferred method, since most users lack the ability to tell the difference between a phished site and a legitimate one, there must be a method for detection and a plan for remediation. Many of the technologies for phishing perform either detection, prevention, or a combination of both. Table 1 below outlines the name and locations of several phishing technologies.



*Table 1.* Phishing Technologies

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

This table illustrates Phishing technologies that can aid in the detection and prevention of phishing attacks.

Many of the phishing technologies listed in Table 1 use either heuristics or blacklists as their primary source of detecting phishing attacks since they are the most common methods to use (Hong, 2012, p. 78). Heuristics when used with phishing attacks refers to the ability to find patterns matching phishing websites (Parno, Kuo, & Perrig, 2005, pp. 13-14). Blacklists are lists of URL’s of known phishing sites (Purkait, 2012, p. 395). When a user attempts to access a site, the URL of the site is checked against the blacklist. If a site is found in the blacklist, a warning will pop up informing the user that they are attempting to access a phished site, or the technology may not allow the connection to the site at all. However, the problem with blacklists is that they can only list a URL as being a phising URL once the site is deemed a phishing site which is usually after someone has fallen for the phishing attack and reported the phished site (p. 395). Unfortunately, heuristics is susceptible to the same short comings as heuristics takes multiple phished sites to be analyzed and for a correlatable heuristic measure to be found among those sites before a heuristic can be made. Another issue is that these lists must be regularly updated for them to be effective. The built-in anti-phishing software used in the Mozilla Firefox browser performs blacklist and heuristic updates every 30 minutes (Mozilla, n.d.). However, there are technologies that will require the user to update these lists themselves.

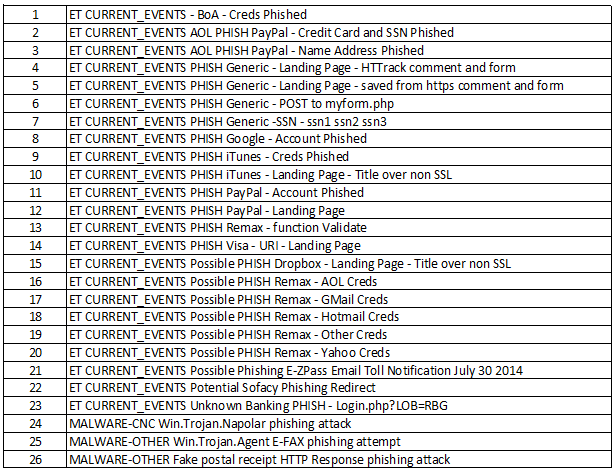
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are technologies that are found commonly in enterprise environments (Ashoor & Gore, 2011, p. 2). IDS is designed to detect issues like phishing and alert on them once they are detected. IPS can do the same, but also has the ability to prevent a connection from happening or continuing. These systems can use multiple methods to try to detect and prevent phishing attacks. Even though they have the ability to use multiple methods of detection and prevention, they require regular maintenance to keep them up to date. Products like Bro IDS (https://www.bro.org/), Sagan IDS/IPS (https://quadrantsec.com/), and Snort IDS/IPS (https://www.snort.org/) all work off of special heuristics and blacklists to detect malicious attacks that must be regularly maintained for them to be effective.

Bro IDS is an open-source, network traffic analyzer (The Bro Project, 2015, para. 1). Bro can monitor all traffic on a network link and perform tasks based off of the traffic that is detected (para. 1). Signatures (heuristics) can be created that will allow Bro to alert a user if certain types of traffic are detected (para. 5). Furthermore, Bro is open source and free to use.

Sagan is a product by the Manged Security Services Provider (MSSP) Quadrant Information Security based out of Jacksonville, Florida. Sagan uses ‘Snort like’ rules to perform heuristics to detect malicious activity (Quadrant Information Security, n.d., para. 1). According to Quadrant Information Security their product contains over 7,500 internally developed attack signatures that are used to detect malicious activity (para. 1). Sagan is also open source and free to use, but also offers a paid managed side for larger deployments.

Snort performs real-time packet logging and traffic analysis and is a free and available open source IPS (Cisco, n.d.c, p. 1). Snort has a free version of their rules as well as a subscriber based version of their rules that can be used with their product. Snort is also open source and free to use, but offers a paid version of their rule sets that will allow users to receive rule updates either as soon as they are created, or 30 days after they are created (Cisco, n.d.a, p. 1). Sourcefire (Snort) was founded in 2001 and was acquired in 2013 by Cisco to deliver what they claim to be the most effective real-time network defense solution (Cisco, n.d.b, p. 1).

Emerging Threats claims that in the world of open source and commercial threat intelligence, that they are the leaders of this field (Emerging Threats Pro LLC., n.d., p. 1). Emerging Threats is also an open source product that is free to the public. While Emerging Threats is not an IDS/IPS, they contain many signatures that can be integrated with those systems. Emerging Threats contains various threat feeds of rules (heuristics). They contain several rules for phishing attacks which are listed in Table 2 below.



*Table 2.* Phishing Rules

Emerging Threats Pro LLC. (n.d.). Index of /open-nogpl/snort-2.9.0. Retrieved from emergingthreats.net: http://rules.emergingthreats.net/open-nogpl/snort-2.9.0/emerging.rules.tar.gz

This table shows 26 signatures in Emerging Threats rules that can detect phishing attacks.

The rules for Table 2 are built on heuristic patterns such as the ‘ET CURRENT\_EVENTS PHISH Google - Account Phished’ which has a heuristic of ‘flow:established,to\_server; content:"POST"; http\_method; content:"continue="; http\_client\_body; content:"followup="; http\_client\_body; content:"checkedDomains="; http\_client\_body;’ (Emerging Threats Pro LLC., n.d., p. 1). This heuristic looks for a POST request to a web browser that contains ‘continue=’, ‘followup=’, and ‘checkedDomains=’. However, these rules do not mean that all phishing attacks triggered are accurate! Many rules can generate false positives, which are when an alert triggers, but the event is not the intended event. An example would be a rule that looks for the word ‘trickery’ in a certain spot in a packet and the rule says that this is a particular kind of attack. However, the word ‘trickery’ was in that spot, but was in reference to a newspaper article about a magic show from last night. Therefore, this was positive as a match for the word, but false because the event was not the intended event.

Phishing Training. Another method to detect and prevent phishing attacks is through training the end users. The end user is the one that is ultimately responsible for the phishing breach. The end user will be the one to open the phishing email, click a phished link on a webpage, or visit the phishing site and input personal credentials. The end user is the most important part for the prevention of phishing attacks (Larcom & Elbirt, 2006, p. 54; Kirda & Kruegel, 2006, p. 560; Whitlock, 2008, p. 31). Furthermore, there are techniques that end-users can learn to help them avoid falling for phishing attacks. Even though no technique can guarantee to detect all phishing attacks, many of these can avoid most vectors of phishing attacks.

When dealing with possible phishing emails, there are best practices that can help to protect the user. One such technique is never to use the links within an email (Kirda & Kruegel, 2006, p. 560; Whitlock, 2008, p. 31; Fu-an, 2015, p. 6). The anchor text that a user clicks on does not mean that is the actual site a user will visit. To ensure that an anchor text of facebook.com is safe, have the user manually type in facebook.com. One such example of why this is the case is due to visual deception. A user may know of the site planet.com and click on the link to go there. However, the spelling of planet.com is with a one (1) instead of an l (L) and they went to the phished site planet.com. Many times users can be tricked due to letters looking like other letters such as l (L) and 1 (one) or O (o) and 0 (zero) (Dhamija, Tygar, & Hearst, 2006, p. 3).

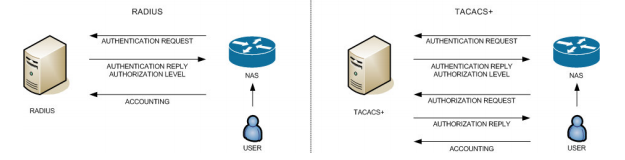
If a user goes to a website, there are techniques that can verify the site for phishing. Just because a user went to a phished site does not guarantee that anything has happened yet. So taking the time to check where the user is at can still prevent the phishing from happening. Typing the URL that you are currently at into a URL blacklist checker can help to determine if the site that the user is at is possibly a phishing site or not. Sites like virustotal.com, ipvoid.com, and urlquery.net can perform these types of checks free on a URL or IP address. Another reason for this check is that many users do not understand URL structures (Dhamija, Tygar, & Hearst, 2006, p. 2). The user may be familiar with planet.com and know that the site is safe. However, the site planet.com and planet-security.com are not part of the same site.

Aside from checking the URL when at a website, that are also indicators that can be noticed within the website. Users should check for security indicators on secure web pages and be aware of where these security indicators should be. Some users may be aware that a secure site has a padlock that is locked on the website. Consequently, unless they know the exact location of where that padlock should be, they may be fooled if an attacker put a padlock anywhere on the page and said the site was SSL protected (Dhamija, Tygar, & Hearst, 2006, p. 3).

## Single Sign-On

Single Sign-On Basics. Most users today have multiple systems that they must maintain login credentials for (Cao, et al., 2014, p. 1; Radha & Reddy, 2012, p. 134; Sun, et al., 2013, p. 1). One of the largest methods to deal with this issue both within the corporate world and out is with using the single sign-on method (SSO) (Mpafe, 2013, p. 8). “SSO is an identity management solution which is facilitated by the cooperation between enterprises. SSO involves sharing user authentication credentials, thereby, allowing permitted users to login just once when accessing their account with any of the businesses” (p. 8). There are several different types of SSO models. Furthermore, as you can see from Figure 7 below and in Appendix C and D: while Security Assertion Markup Language (SAML) and Janrain have seven and eight steps, Radius and Terminal Access Controller Access Control System (Tacacs) have only three and five steps. However, while many of these authentication methods use different steps, they all have the same underlying method. The same underlying steps they share are:

1. A user attempts to connect to a site or device.
2. That device sends the authentication attempt to an authenticating device.
3. The authenticating device verifies the user credentials.
4. The authenticating device tells the original device whether the user’s credentials are valid or not.
5. The original device will allow the user in or disallow access.



*Figure 7.*  Tacacs and Radius Authentication Flow

TACACS.net. (2011, April). The Advantages of TACACS+ for Administrator Authentication.

Retrieved from tacacs.net: http://www.tacacs.net/docs/TACACS\_Advantages.pdf

The illustration shows the steps used in both Radius and Tacacs for authentication.

Web SSO. Web SSO refers to the SSO method specifically used in browser based authentication. This method “separates the role of Identity Provider (IdP) from that of Relying Party (RP). An IdP collects user identity information and authenticates users, while an RP relies on the authenticated identity to make authorization decisions” (Sun, et al., 2011, p. 1). An example of this is a user using an IdP such as Facebook to connect to an RP such as wingstop.com. Using this method, a user can use their Facebook account through Facebook to authenticate themselves to a site that uses Facebook as an IdP. Not only can the user use their Facebook to login to wingstop.com, but they could also use their login to log into any other site offering Facebook as an IdP so that the user only needs to remember one login credential.

This offers many advantages in the corporate realm as employees can use the same sign on for local systems as well as web based applications. Furthermore, should a user’s account become compromised, a password is forgotten, or a password needs to expire, only a single password needs to be changed rather than multiple passwords across multiple devices (Radha & Reddy, 2012, p. 134). This in turn makes changes of credentials for administration easy to manage as there is only one place that needs to be changed. Not only does management benefit from this, but help centers will only have to deal with one location where passwords can be changed. This can greatly reduce the amount of time help desk’s spend when attempting to change user login credentials (Radha & Reddy, 2012, p. 138; Xiong, 2005, p. 68).

While SSO for the corporate world may sound like the method has no downside, there are disadvantages to using SSO in a corporate setting. The primary disadvantage is the fact that the SSO method has a single point of both failure and compromise (Chitalia, Sanghavi, Iyer, Shah, & Jyotinagar, 2013, p. 212; Gouda, Liu, Leung, & Alam, 2005, p. 11). If an attacker can breach the site or device acting as the authenticator, then all users account credentials can be stolen. Also, now all accounts belonging to a user can be compromised from the single login credential that was stolen. Furthermore, if the authenticating site or device should loose connectivity, there is no other method for the users to be able to authenticate to connect to where they were going.

Web SSO also offers advantages to non-corporate users. With sites that do offer a separate login option that a user has a valid account for; a user can use that other sites credentials to log into the intended site. This can be helpful when dealing with multiple login credentials for multiple sites. If a user forgets their login credentials for a site, they can simply use another site’s login credentials to be able to log into the intended site and from their change their password or perform whatever task they were originally going to perform. However, this differs from a ‘pure SSO’ setup. A ‘pure SSO’ setup refers to a user only having a ‘single sign-on’, hence the acronym SSO. However, if a user can use an SSO method such as using Google to log into their pizzahut.com account and use their local pizzahut.com account, this is not a pure SSO method due to the user having two logins for the same account.

A disadvantage to non-corporate users using web SSO is that the availability of the technology is not everywhere, so a ‘pure SSO’ environment is not available. While there are sites such as vimeo.com and Spotify.com and many others that offer this service, unless a user only used these sites and never added login credentials to these sites, they would have two logins for the same site. This negates the SSO as the user no longer has a single sign on. The user now faces the issue of multiple accounts with multiple login credentials causing password reuse (Bonneau & Preibusch, 2010, p. 34) and creating less secure passwords that are easily cracked (Zhang, Luo, Akkaladevi, & Ziegelmayer, 2009, p. 166).

The Literature Review has gone over four main areas: breaches, passwords, phishing attacks, and SSO. First involved a review of breaches that have occurred due to phishing attacks or other means in which user credentials were stolen and access was gained to either the corporate network or individual accounts. In the review concerning passwords, the author has demonstrated an offline password attack on credentials taken from a Linux password file using a password cracker called John the Ripper. The review has also shown that when dealing with passwords, users tend to use weak passwords due to complexity issues (Cazier & Medlin, 2006, p. 3), and the large quantities of passwords that a user needs to remember (Florencio & Herley, 2007, p. 1). Finally, password reuse is a product of bad password management due to the large quantity of passwords users have to remember (Bonneau & Preibusch, 2010, p. 34).

Next involved reviewing phishing attacks to provide a clear understanding of how to perform a phishing attack and how to make a phished site. A phishing email and phishing site were created as well as a walk through was provided on the steps an attacker would need to follow to perform a similar attack. Furthermore, the process of creating phishing sites or phishing emails does not require a large skill set to perform such an attack. There are phishing prevention technologies and phishing training methods currently used to try to combat phishing attacks. While no method of detection or prevention can completely solve the issue of phishing; through equipment such as Intrusion Detection Systems and Intrusion Prevention Systems, blacklists in browsers, and training the users, you can greatly reduce the possibility of users being phished.

Lastly was a review of the single sign-on method (SSO). The basics of the single sign-on method was reviewed to provide an understanding that different methods such as SAML and Tacacs may use different steps when authenticating in SSO, but they still use the same basic structure for performing the authentication. SSO has different advantages and disadvantages if you were a corporate user or non-corporate user. One difference shown was the lack of a ‘pure SSO’ method for non-corporate users as SSO refers to a single sign-on and users may have more than one sign on to the same account.

# Methodology

## Subjects and Settings

To answer the author’s question of whether using sites such as Facebook, Google, and Twitter to login into other sites is a safe method to use, there needs to be four questions answered. These questions, if all are true, pose a threat to the single sign-on method. This is the same process of using Google and other sites to authenticate to another site such as expedia.com. To determine the answer to the four questions as listed below, there will require a use of qualitative deduction, and empirical data.

* Are phishing attacks hard to detect?
* Do users use simple passwords?
* Do users reuse the same passwords on multiple accounts?
* Has comprised user accounts occurred through stolen login credentials?

There are situations where companies do not have to notify the public of breaches to corporate information. Due to this issue, gathering statistics on corporate breaches totals is not a reliable source metric, as the exact total for a given year of all companies cannot be determined against companies that a breach did not occur. Furthermore, individual users who had their accounts breached do not have dedicated governmental forms to fill out concerning their personal breach of an account for a given company. This causes an issue in determining individual user accounts that also incurred a breach. Next, there are no laws concerning a defined minimum or maximum password length or password reuse across multiple accounts. Lastly, the ability to detect phishing attacks rests on a user’s knowledge of phishing attacks and phishing detection/prevention technologies in place. These issues will require a historical research design involving gathered evidence of phishing attacks, password complexities and reuse, and compromised accounts through stolen login credentials.

## Data Collection Techniques

Phishing. To begin collecting phishing data, previous phishing research and dedicated phishing statistics will be required. Material concerning types of phishing attacks, frequency of attacks, successful and unsuccessful attacks, phishing sites and phishing email types, will require gathering. Another large component for phishing attacks will require research on how to perform a phishing attack. Furthermore, companies dedicated to network detection or phishing detection that publish reports concerning what they have seen should be collected and can be found at Anti-Phishing Working Group (APWG), Symantec, Kaspersky, and PhishTank. These companies provide monthly, quarterly, and/or yearly statistics concerning the volume of phishing traffic. The data gathered from all the different sources will require compiling and assessment to determine the feasibility of performing a phishing attack. The results should have a qualitative result of whether a phishing attack is easy to perform and have a reasonable expectation of success.

Passwords. Password collection techniques will require multiple empirical research results. Data compiling involved statistics concerning user’s password length, password complexity, and password reuse. Password focus was on web based and computer based passwords, and not on data concerning the history of passwords. User’s ability to remember passwords, number of remembered passwords, complexity of the remembered passwords, and number of accounts requiring passwords primarily composed the data.

These results were broken down into three areas: password complexity, password reuse, and password quantities. The author used a comparative analysis on the literature that is available for and against the above password areas to determine the average for the results. From the data collected concerning password complexity, a qualitative result came from whether users tend to use weak passwords. In addition, a similar determination did arise as to whether users reuse passwords. This determination will result in true, if in general; users reuse one or more passwords. Lastly, users average password length came from the results of previous research into password lengths and the average of all the materials results.

Breaches. Data collection concerning breaches will require research material as well as reputable source material of breaches. The focus concerning breaches is through those breaches that occurred with the use of stolen credentials. Credentials obtained through phishing attacks will further support phishing attack data. However, any breach so long as the breach involves stolen credentials to gain illegal access will be sufficient. There are 47 States including several territories that have legislation requiring private and government entities to notify people involved in breaches where personally identifiable information (PII) is stolen (National Conference of State Legislatures, 2015, p. 1). Some states contain resources concerning notices sent to residents of the state such as California (https://oag.ca.gov/ecrime/databreach/list) and New Hampshire (http://doj.nh.gov/consumer/security-breaches/). The states that provide notices of user breaches are the primary source for the historical data for breaches.

## Statistical Analysis

After compiling the results of all the data, the final analysis for each area will be determined. Then, the author’s question of whether the use of the single sign-on method using sites such as Facebook, Google, and Twitter to authenticate a user for a different website is a safe option to use will be determined. For hypotheses one (Phishing attacks are not hard to detect due to their ability to look like a normal email or website.) to be false; the results of phishing attacks must show that phishing attacks require little skill to perform and have a reasonable expectation of success. For hypotheses two (Many users do not use simple passwords for their accounts) to be false; the results for passwords must show that findings of multiple previous research results conclude that users do tend to use weak passwords. For hypotheses three ( Many users do not reuse the same passwords on multiple accounts) to be false; the results for passwords must show that the previous research results conclude that uses do reuse passwords. For hypotheses four (Compromised user accounts have not occurred through stolen login credentials) to be false; the research must show that there is valid data of user accounts being compromised through stolen login credentials.

# Results

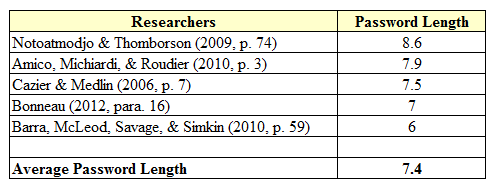
## Overview

Concerning the author’s question of whether using sites such as Facebook, Google, and Twitter as a single sign-on is a safe method to use, the results paint a compelling picture. The results will show why the areas of phishing, passwords, and breaches are important issues to consider when contemplating on whether using the method in question is viable. Each area will show the results of the data and provide clarity for each hypotheses. Lastly, the correlation will show how these areas tie together to form the author’s result.

## Password Analysis

After reviewing the empirical data concerning passwords, the results concerning the authors H2 and H3 statements are now clear. Concerning the H2 hypothesis of whether users use simple passwords, the data shows that users do use simple passwords. A review of the five studies in Table 3 below resulted in a mean password length for users to be seven point four characters long. Next, the average minimum password length for Google, TDAmeritrade, Hulu, Facebook, and Wal-Mart came out to be six point six characters long as seen in Table 4. This concluded that user’s average about one character longer than the mean minimum length for a website. Furthermore, of the five sites, only TDAmeritrade required any special conditions enforced upon password length. This results in a minimum complexity of 106, or one million combinations, for Wal-Mart, Facebook, and Hulu. Google has a minimum complexity of 108, or one hundred million combinations. Lastly, TDAmeritrade with the most complex password has a complexity of 367, or 78,364,164,096 combinations.

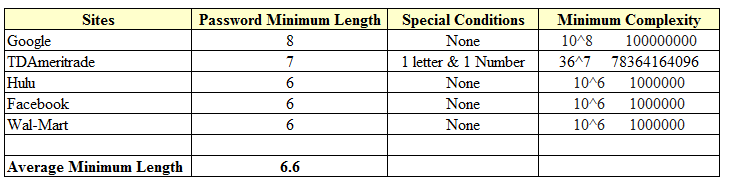
Using the cracking results from the authors testing of the password cracking tool John the Ripper (JTR), which averaged a cracking speed of about 4,000 cracks per second; JTR can feasibly crack the three least complex passwords, using the users average length of seven, in about 41 minutes (4,000 cracks p/s \* 60 sec. = 240000 cracks p/m). Google has a feasible time of seven hours to crack a password (4,000 cracks p/s \* 60 sec. = 240,000 cracks p/m & 240,000 cracks p/m / 100,000,000 = 416 minutes of cracking & 416 minutes / 60 minutes in an hour = 6.94 hours). Lastly, TDAmeritrade has a feasible cracking time of 226 days.



*Table 3.* Empirical research into average password length

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 3 contains researchers and their average user password length

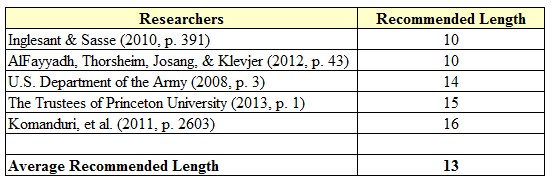


*Table 4.* Average password length of several websites

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 4 contains websites and their minimum password length requirements.

The empirical research outlined in Table 5 below shows a recommended safe length for passwords of 13 characters. The recommended character length provides a minimum mathematical value of 1013 or 10,000,000,000,000 combinations. Using the formula of (4,000 cracks p/s \* 60 sec. = 240000 cracks p/m), the password would require 79 years to crack. This would take roughly 922,720 times longer to crack than the complexity of 106. In addition, the password would take nearly 109 times longer to break than the most complex minimum password length from TDAmeritrade of 367.

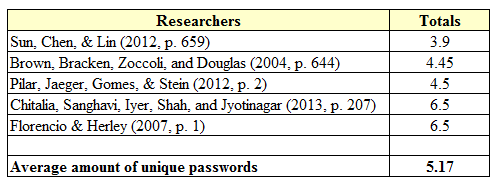


*Table 5.* Empirical Recommended Minimum Password Length

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 5 contains researchers and their recommended minimum password length.

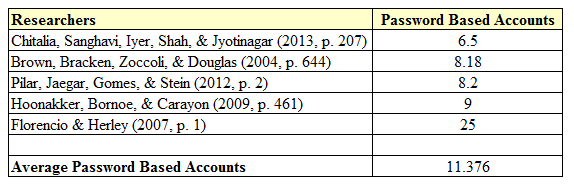
Concerning hypothesis three, do users reuse the same passwords on multiple accounts; the research showed that users do reuse passwords on multiple accounts. The mean result of empirical studies showed users average 5.17 unique passwords as shown in Table 6 below. The primary determination concerning the amount of passwords belonging to users occurred through surveys. When comparing the amount of unique passwords versus the amount of password-based accounts as shown in Table 7 below, there is a shortage of unique passwords for the average amount of accounts. The Table 7 results show that users have around 11.376 accounts. These two results show that users on average will reuse just over two of their unique passwords.



*Table 6.*  Empirical Results of Unique Password Usage

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 6 contains researchers and their participant’s average unique password amounts.



*Table 7.*  Empirical Results of Password Based Accounts

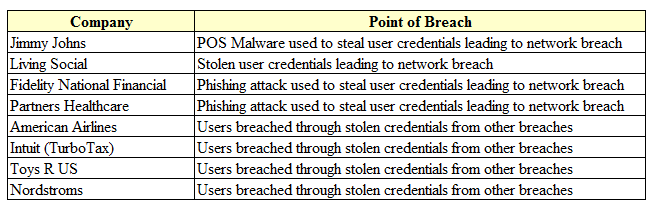
Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 7 contains researchers and their participant’s average amount of password based accounts.

## Breach Analysis

Concerning the research performed on confirmed breaches, the authors H4 hypothesis has been determined. The H4 hypothesis, have user accounts been compromised through stolen user credentials, has found that user accounts have been breached due to stolen user credentials. A compilation of breaches directly related to stolen user credentials is located in Table 8 below. As shown in Table 8 below, Jimmy Johns, Living Social, Fidelity National Finance, and Partners Healthcare all had their networks breached through stolen user credentials. After attackers gained access to the user’s credentials, the attackers successfully managed to penetrate their networks using the stolen credentials.

The findings show that on an individual basis, accounts owned by users are broken into with credentials stolen from breaches as seen in Table 8 below. American Airlines, Intuit (Turbo Tax), Toys R US, and Nordstrums found no breaches of their own internal networks. Investigations in all four cases concluded that the users had their user credentials stolen in other company breaches or other methods and then used on the above-mentioned four sites of which the attackers were successful in gaining access to their accounts due to the users using the same credentials on multiple accounts.



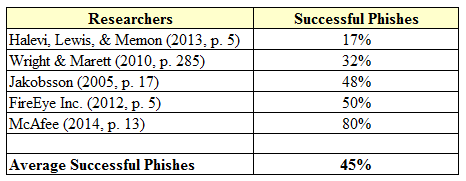
*Table 8.* Corporate and Individual Breaches due to Stolen User Credentials

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 8 contains the breach method of several companies.

## Phishing Analysis

Analysis of empirical data into the authors H1 question, phishing attacks are not hard to detect due to their ability to look like a normal email or website, shows that phishing attacks are hard to detect. Analysis of previous research shown in Table 9 below has shown that an average of 45% of phishing attacks are successful. The breach results from Table 8 above show that Fidelity National Financial and Partners Healthcare had users fall for phishing attacks, which is what provided the attackers the credentials they needed to gain illegal access to the network.



*Table 9.* Empirical Results of Average Successful Phishes

Hall, A. (2015). Facebook, Google, and Twitter as a Single Sign-On Service: To use or not to use. Jacksonville, FL, United States of America.

Table 9 contains researchers and phishing success rates based off testing and analysis.

## Correlation

These three areas are significant as they prove the inherent weakness in the SSO method when using sites like Twitter… the user. The user creates their password and chooses simple passwords that are easy to break. Furthermore, the user clicks on links that sends them to phished sites. Determining how an attacker obtains users credentials, they can feasibly break an encrypted password and attempt to login to other accounts owned by those credentials in a matter of minutes. The research into breaches proves that an attacker will attempt to use users stolen login credentials by going to other sites and trying to login with them. With the speed in which an attacker can break the average user’s password, and the fact that the average user reuses their password at least twice, this proves that the method is not a safe method to use. Lastly, the attacker can retry user credentials on other accounts even faster if they can obtain a user’s credentials through phishing attacks ,which have a nearly 50% success rate, and do not have to decrypt the password.

# Discussion

## H1 Review

The authors H1 question dealt with the effectiveness of phishing attacks. In both the research of breaches as well as phishing, this was determined to be false. Concerning the results of Table 9 in which the average successful phishing attack was 45%, this is primarily comprised of spear phishing attacks. Spear phishing attacks are attacks in which the attacker knows some information about the victim prior to the attack. These become increasingly more successful as more information about the victim is available to the attacker. The attacker can construct an email or web site that the victim may have already visited or contains information about the user making them think the site or email is legitimate.

To provide a more accurate numbers into phishing attacks, research into blind phishing attacks versus targeted phishing attacks would be required. The research would need the ability to separate phishing attacks where information was available about the victim prior to the attack. To elaborate on the prior knowledge, inclusion of what information was known before the attack should be added to determine how targeted the attack was and the effectiveness based on the amount of prior knowledge.

Training the user is an important part of preventing phishing attacks. However, the knowledge provided to the user may not always be accurate. According to Whitlock, users should check for discrepancies such as misspelling and poor grammar (Whitlock, 2008, p. 30). However, this does not mean that an attacker with little skill created the phished email or website. Cormac Herley (2012) performed research on phishing attacks with the intent of answering the question, why do Nigerian scammers say they are from Nigeria. In his study, he concluded that there is a cost in performing these frauds, and these attackers need to try to weed out people who might not fall for the entire attack (Herley, 2012, pp. 2,11-12). One way to weed out bad phishing victim results could be through intentionally adding errors into phished emails and web sites. If they are able to detect the phishing attack, then the attack is not worth the attacker’s time to continue after the victim. This can also give an attacker more insight into future attacks though. If a user does not respond to certain attacks, but then does respond to one, this could inform the attacker of the types of attacks that the user may be more susceptible too.

As breaches continue to occur in companies and individuals, attackers will have access to more information about users. With that information, they can design better blind phishing attacks with a much higher chance of success. With so many breaches in the past two years that have resulted in stolen user information and credentials, the need for public education of phishing attacks is important. While this is not a guaranteed method, this will greatly help to decrease the possibility of falling for phishing attacks.

## H2 Review

The authors H2 question dealt with the complexity of passwords. Phishing is a severe threat as an attacker can get your login credentials in cleartext. However, passwords caught encrypted on the wire or in a stolen database are decodable in a matter of time. As shown in the results section, many users have a password length of about seven characters. The most complex password at this length is 947, or roughly 69 trillion combinations. This password would require all four sets of complexity: digits, uppercase letters, lowercase letters, and special characters. However, a password of 2610, which would comprise of either uppercase or lowercase letters, and be ten characters long, would be double the strength of the 947 complexity and half as difficult for users to remember as it only uses half the complexity variations.

The author has drawn a conclusion that a better method to stronger passwords will require an overall standard of password minimum length. A mandate to all businesses with user authentication to require a minimum length of 2610, or 10 characters with one letter, should help to increase overall password strength. This conclusion is the result of the average password length of users and the average minimum password length of sites. If the user average password length is a direct result of the average password length of the sites they use; then enforcing a longer minimum password length on all sites should increase a user’s ability to remember and use stronger passwords.

Programs such as Keepass and Lastpass can assist users with remembering passwords. Both Keepass and Lastpass are password mangers that offer users the ability to store passwords within their application. The user can then remember a single password to access the application and then get all their passwords from there. This can also allow users to create passwords with lengths larger than 20 characters long and include a new set of complexity, those that require multiple key presses at the same time to create the character. Characters such as High-Ansi can require two or more keys be pressed at the same time, i.e. (ALT + 338) which equals Œ.

## H3 Review

The authors H3 question dealt with user’s reuse of passwords. This issue does not have a simple answer to help prevent this. There are system implementations such as password remembering, which will remember a certain amount of passwords for a user and make sure a user does not reuse a password that they have used before. However, different companies are not checking passwords against each other’s passwords, so this method is defeated with multiple accounts. Even if password remembering is set up across every site a user uses, they could still use the same password on all sites. One method mentioned earlier is to have the SSO method, when using sites like Google for SSO, to check the password against whichever site the user is trying to access to determine if the user is using the same password on both sites. Furthermore, if the user is doing this, then inform the user that their passwords are the same on both accounts and that they must change one of the passwords to use this method.

The author reviewed several empirical articles to determine the average amount of unique passwords a user has to be around 5.17 as seen in Table 6 above. Furthermore, a user has on average 11.376 accounts requiring passwords as shown in Table 7 above. With users reusing just over two of their unique passwords, this is a severe issue. There are some tools, such as Keepass and Lastpass, which can help with password remembering. While these tools can help with generating stronger passwords and remembering them, even these tools still lack the ability to prevent a user from reusing the same password on the same site.

From the review of the empirical evidence, two-factor authentication appears to be the best method to mitigate this issue. While two-factor authentication will not prevent password reuse, the method will require a second form of authentication to access a user’s account. Therefore, even if an attacker were to get a user’s credentials, they would have to get the second factor of authentication. This is available in some sites such as Google and Yahoo. When a user attempts to access their account, they will receive an email or text message with a code that they will also have to enter, along with the correct password, to gain access to their account.

## H4 Review

The authors H4 question dealt with the illegal reuse of stolen credentials to gain access to the users accounts. This is available in Table 8 with respect to both individual user accounts and business related accounts. The attacker may or may not know whose credentials they have stolen. However, an email can be a roadmap of where to attack. If a user’s login credentials are somebody@gmail.com or somebody@company.com, this can tell the attacker where exactly to use the credentials. Furthermore, the attacker can formulate a better idea of where to attack next. A person might not use their business email address for non-business related tasks, so the email that ended in company.com may be business related and only attackable there. Therefore, the email address that ended in gmail.com is a Google account, so performing further password reuse attacks on Google, as well as sites that offer Google as a SSO would be vectors of attack.

This is probably the hardest type of attack to detect. If an attacker has valid credentials, how can the security devices in place and the people monitoring the network know that user Bob is not really user Bob? This again is another candidate for two-factor authentication. Using the example for Google where users were sent a text or email message with a code, an attacker would not only need the users login credentials and passwords, they would also have to steal the users phone to get the code from the text, or have access to the users email account also. This when coupled with the issue of password reuse does raise an issue that sending a security code to an email address may not be safe either as a user may have used the same login credentials on both accounts and the attacker could have access to the second factor of authentication.

## Summary

The intention of this research was to determine if using sites like Facebook, Google, and Twitter to authenticate to other websites is a safe method to use. Through empirical research, this study has concluded that this is not a safe method to use. The author noted several instances of breaches performed through stolen user credentials to both individuals and businesses. The collecting of user credentials occurred through multiple methods, but of note, with phishing attacks. After the attacker managed to either decrypt a user’s login credentials, or received the credentials in plaintext, the attacker then proceeded to reuse the user’s login credentials on other sites. This lead to theft of other people’s information in the cases involving user credentials that allowed network access to a company. Furthermore, the breach lead to the access of other accounts belonging to the same user.

There are current methods in place that can help to mitigate some of the risk involved in this process. Using programs like Keepass and Lastpass to manage passwords and store highly complex passwords can help to mitigate the ability of a user decrypting a user’s credentials if stolen. This can also help with the issue of password reuse, as a user does not technically need to remember their password for every account. They only need to remember the password to the application and then they can get the password to the site from there. However, this do not solve the issue of password reuse as a user can still have the same password for multiple accounts while still using those applications. Lastly, the use of two-factor authentication, whenever possible, will further mitigate the issue of illegal access to an account even if an attacker has the login credentials for the users account. However, as shown with the issue of using a second factor of authentication as a user’s email address. An attacker could already have access to the users email account and could intercept the second factor authentication message. Ensuring that whatever the second method is, the user has physical access to other method will increase the odds that the second factor is also safe. Examples of such safe methods include text message to a phone, text message to a pager, or a physical token.

The author also mentioned several methods to help make the use of sites like Google as an SSO a safer option to use. These methods include password checks between single sign-on sites and the sites using them for access to their website to ensure that the password is not the same on both sites. Allowing only limited access to your account if logging in with your Facebook, Google, Twitter, etc. account. Allowing the user the ability to choose which sign-on methods are available on a site (i.e. local sign-on, Facebook or Google or Twitter). Having the option to turn off the single sign-on method on the site the user is trying to access, or the SSO allowed on the site.

[Blank Page]

# 

# References

Adams, A., & Sasse, M. A. (1999). Users are not the Enemy. *Communications of the ACM, 42*(12), 41-46.

AlFayyadh, B., Thorsheim, P., Josang, A., & Klevjer, H. (2012). Improving Usability of Password Management with Standardized Password Policies. *Proc. of the 7th Conference on Network and Information Systems Security (SAR-SSI)*, (pp. 38-45).

American Airlines Inc. (2015, January 1). *American Airlines Notice.* Retrieved from oag.ca.gov: https://oag.ca.gov/system/files/American%20Airlines%20Notice\_0.pdf?

Amico, M., Michiardi, P., & Roudier, Y. (2010). Password Strength: An Empirical Analysis. *Infocom* (pp. 1-9). San Diego: IEEE.

Anonymous. (2015, February 13). *partners-healthcare-system-20150212.pdf.* Retrieved from doj.nh.gov: http://doj.nh.gov/consumer/security-breaches/documents/partners-healthcare-system-20150212.pdf

APUS. (n.d.). *Login*. Retrieved from login.apus.edu: https://login.apus.edu/padsts/?\_ga=1.36501792.18104661.1436493180

Ashoor, A., & Gore, S. (2011, January). Importance of Intrusion Detection System (IDS). *International Journal of Scientific & Engineering Research, 2*(1), pp. 1-4.

Barra, R., McLeod, A., Savage, A., & Simkin, M. (2010). Passwords: Do User Preferences and Website Protocols Differ from Theory? *Information Privacy & Security, 6*(4), 50-69.

Bonneau, J. (2012). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. *Security and Privacy* (pp. 538-552). San Franciso: IEEE.

Bonneau, J., & Preibusch, S. (2010). *The Password Thicket.* Retrieved from weis2010.econinfosec.org: weis2010.econinfosec.org/papers/session3/weis2010\_bonneau.pdf

Bosshart, A. (n.d.). *Data Breach Notification.* Retrieved June 26, 2015, from chs.net: http://www.chs.net/media-notice/

Cao, Y., Shoshitaishvili, Y., Borgolte, K., Kruegel, C., Vigna, G., & Chen, Y. (2014). *Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel.* Retrieved June 27, 2015, from cs.ucsb.edu: https://www.cs.ucsb.edu/~vigna/publications/2014\_RAID\_WebSSO.pdf

Cazier, J., & Medlin, D. B. (2006, April). *How Secure is your Password? An Analysis of E-Commerce Passwords and thier Crack Times.* Retrieved from isy.vcu.edu: http://www.isy.vcu.edu/~gdhillon/Old2/secconf/pdfs/21.pdf

Cheswick, W. (2013). Rethinking Passwords. *Communications of the ACM, 56*(2), 40-44.

Chitalia, U., Sanghavi, M., Iyer, S., Shah, S., & Jyotinagar, V. (2013). Single Sign On (SSO) Application for Websites. *International Journal of Advances in Engineering Science and Technology, 2*(9), 207-212.

Chou, H., Lee, H., Yu, H., Lai, F., Huang, K., & Hseuh, C. (2013). Password Cracking Based on Learned Patterns from Disclosed Passwords. *International Journal of Innovative Computing, Information and Control, 9*(2), 821-839.

Cisco. (n.d.a). *How are rules distributed?* Retrieved from snort.org: https://snort.org/faq/how-are-rules-distributed

Cisco. (n.d.b). *What is the relationship between Snort and Cisco?* Retrieved from snort.org: https://snort.org/faq/what-is-the-relationship-between-snort-and-cisco

Cisco. (n.d.c). *What is Snort?* Retrieved from snort.org: https://snort.org/faq/what-is-snort

Dawson, K. (2011, September 1). *nordstrom-20110901.pdf.* Retrieved from doj.ng.gov: http://doj.nh.gov/consumer/security-breaches/documents/nordstrom-20110901.pdf

Dhamija, R., Tygar, J., & Hearst, M. (2006, Aug 14). *Why Phishing Works!* Retrieved from escholarship.org: http://escholarship.org/uc/item/9dd9v9vd

Dictionary.com. (n.d.). *hacker.* Retrieved August 05, 2015, from dictionary.reference.com: http://dictionary.reference.com/browse/hacker

educase.edu. (n.d.). *Ready to Request a New .edu Domain Name.* Retrieved from educause.edu: http://net.educause.edu/edudomain/request.asp

Emerging Threats Pro LLC. (n.d.). *About Emerging Threats.* Retrieved from emergingthreats.net: http://www.emergingthreats.net/about-us

Emerging Threats Pro LLC. (n.d.). *Index of /open-nogpl/snort-2.9.0.* Retrieved from emergingthreats.net: http://rules.emergingthreats.net/open-nogpl/snort-2.9.0/emerging.rules.tar.gz

Expedia. (n.d.). *Sign In*. Retrieved from expedia.com: https://www.expedia.com/user/login

Ferguson, A. (2005). Fostering E-Mail Security Awareness: The West Point Carronade. *Educause Quarterly*, 54-57.

FireEye Inc. (2012). *Spear Phishing Attacks: Why they are Successful and How to Stop them.* Retrieved from fireeye.com: https://www2.fireeye.com/WP-Spearfishing-Attacks\_LP.html

Florencio, D., & Herley, C. (2007). *A Large-Scale Study of Web Password Habits.* Retrieved from research.microsoft.com: http://research.microsoft.com/pubs/74164/www2007.pdf

Fu-an, Z. (2015). Phishing Sites and Prevention Measures. *International Journal of Security and Its Applications, 9*(1), 1-10.

Google. (n.d.). *2-Step Verification.* Retrieved August 5, 2015, from google.com: https://www.google.com/landing/2step/#tab=how-it-protects

Gouda, M., Liu, A., Leung, L., & Alam, M. (2005). *Single Password, Multiple Accounts.* Retrieved from msu.edu: http://www.cs.msu.edu/~alexliu/publications/Password/password.pdf

Halevi, T., Lewis, J., & Memon, N. (2013, Feb 08). *Phishing, Personality Traits and Facebook.* Retrieved from arxiv.org: http://arxiv.org/pdf/1301.7643

Herley, C. (2012). *Why do Nigerian Scammers say the are from Nigeria?* Retrieved from microsoft.com: http://research.microsoft.com/pubs/167719/WhyFromNigeria.pdf

Hong, J. (2012). The Current State of Phishing Attacks. *Communications of the ACM, 55*(1), 74-81.

Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. *53rd Annual Proceedings of the Human Factors and Ergonomics Society* (pp. 459-463). Copenhagen: Human Factors and Ergonomics Society Inc.

Hulu. (n.d.). *Sign In*. Retrieved from secure.hulu.com: https://secure.hulu.com/account/signin

Inglesant, P., & Sasse, M. (2010). The True Cost of Unusable Password Policies: Password Use in the Wild. *Proc. of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 383-392). New York: ACM.

Ives, B., Walsh, K., & Schneider, H. (2004). The Domino Effect of Password Reuse. *Communications of the ACM, 47*(4), 75-78.

Jagatic, T., Johnson, N., Jakobsson, M., & Menzer, F. (2007). Social Phishing. *Communications of the ACM, 50*(10), 94-100.

Jakobsson, M. (2005). Modeling and Preventing Phishing Attacks. *9th International Conference on Financial Cryptography and Data Security*, (pp. 1-19). Roseau, The Commonwealth of Dominica.

Janrain Inc. (n.d.). *Deploy Identity Services.* Retrieved from janrain.com: http://developers.janrain.com/how-to/identity-services/integrate-identity-services/#prerequisites

Jimmy Johns Franchise LLC. (2014, September 24). *Data Security Incident.* Retrieved from jimmyjohns.com: https://www.jimmyjohns.com/datasecurityincident/

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials, 15*(4), pp. 2091-2121.

Kirda, E., & Kruegel, C. (2006). Protecting Users against Phishing Attacks. *The Computer Journal, 49*(5), pp. 554-561.

Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., Egelman, S. (2011). Of Passwords and People: Measuring the Effect of Password-Composition Policies. *Proc. CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595-2604). New York: ACM.

Kontaxis, G., Polychronakis, M., & Markatos, E. (2012). Minimizing Information Disclosure to Third Parties in Social Login Platforms. *International Journal of Information Security, 11*, 321-332.

Larcom, G., & Elbirt, A. (2006). Gone Phishing. *IEEE Technology and Society Magazine*, pp. 52-55.

Lazar, L., Tikolsky, O., Glezer, C., & Zviran, M. (2011). Personalized Cognitive Passwords: An Exploratory Assessment. *Information Management & Computer Security, 19*(1), 25-41.

LivingSocial Inc. (n.d.). *LivingSocial Security Notice.* Retrieved from livingsocial.com: https://www.livingsocial.com/createpassword

Marchal, S., Francois, J., State, R., & Engel, T. (2014). PhishStorm: Detecting Phishing with Streaming Analytics. *Transactions on Network and Service Management, 11*(4), 458-471.

Martin, S., & Tokutomi, M. (n.d.). *Password Cracking.* Retrieved from cs.arizona.edu: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic7-final/report.pdf

McAfee. (2014, August). *McAfee Labs Threats Report August 2014.* Retrieved from mcafee.com: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2014.pdf

McNicholas, E. (2013, April 26). *livingsocial-20130426.pdf.* Retrieved from doj.nh.gov: http://doj.nh.gov/consumer/security-breaches/documents/livingsocial-20130426.pdf

Meighan, B. (2015, February 5). *Sample Consumer Notification.* Retrieved from oag.ca.gov: https://oag.ca.gov/system/files/Sample%20Consumer%20Notification%20Letter\_0.pdf?

Merriam-Webster. (n.d.a). *e-commerce.* Retrieved August 05, 2015, from merriam-webster: http://www.merriam-webster.com/dictionary/e-commerce

Merriam-Webster. (n.d.b). *encrypt.* Retrieved August 05, 2015, from merriam-webster.com: http://www.merriam-webster.com/dictionary/encrypt

Merriam-Webster. (n.d.c). *phishing.* Retrieved June 27, 2015, from merriam-webster.com: http://www.merriam-webster.com/dictionary/phishing

Merriam-Webster. (n.d.d). *plaintext.* Retrieved August 05, 2015, from merriam-webster.com: http://www.merriam-webster.com/dictionary/plaintext

Merriam-Webster. (n.d.e). *url.* Retrieved August 5, 2015, from merriam-webster.com: http://www.merriam-webster.com/dictionary/url

Mozilla. (n.d.). *How does built-in Phishing and Malware Protection work?* Retrieved from mozilla.org: https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work#w\_how-does-phishing-and-malware-protection-work-in-firefox

Mpafe, B. (2013, August). *Single Sign-On the Internet: Trust and Ethical Issues.* Retrieved from academia.edu: http://www.academia.edu/6484830/Single\_Sign-on\_Trust\_Issues

National Conference of State Legislatures. (2015, June 11). *Security Breach Notification Laws.* Retrieved from ncsl.org: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Notoatmodjo, G., & Thomborson, C. (2009). Passwords and Perceptions. *7th Australian Information Security Conference* (pp. 71-78). Wellington, New Zealand: Australian Computer Science Inc.

OASIS. (2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview.* Retrieved from oasis-open.org: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

Parno, B., Kuo, C., & Perrig, A. (2005, December 3). *Phoolproof Phishing Prevention.* Retrieved from cmu.edu: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1068&context=cylab

Perez, P. (2014, September 23). *Consumer Notification Letter.* Retrieved from oag.ca.gov: https://oag.ca.gov/system/files/Consumer%20NotificationLetter%20Proof\_2014%20Incident\_0.pdf?

Pilar, D., Jaeger, A., Gomes, C., & Stein, L. (2012). Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. *PLoS ONE, 7*(12), pp. 1-7.

Podbean.com. (n.d.). *login*. Retrieved from podbean.com: http://www.podbean.com/site/user/login

Purkait, S. (2012). Phishing Counter Measures and their Effectiveness - Literature Review. *Information Management & Computer Security, 20*(5), pp. 382-420.

Quadrant Information Security. (n.d.). *Sagan Technology.* Retrieved from quadrantsec.com: https://quadrantsec.com/services\_technology/product\_technology/

Radha, V., & Reddy, D. (2012). A Survey on Single Sign-On Techniques. *Procedia Technology*, 134-139.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal, 19*(4), 439-444.

Reinhard, C. (2012, June 28). *Penalties for Computer Hacking.* Retrieved from cga.ct.gov: http://www.cga.ct.gov/2012/rpt/2012-R-0254.htm

Sourcebooks. (2014, October 7). *Data breach FAQ Sourcebooks.com.* Retrieved from sourcebooks.com: http://www.sourcebooks.com/company/payment-card-issue-faq.html

Sun, H.-M., Chen, Y.-H., & Lin, Y.-H. (2012, April). oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 7*(2), pp. 651-663.

Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2013, November). Investigating Users' Perspectives of Web Single Sign-on: Conceptual Gaps and Acceptance Model. *ACM Transcations on Internet Technology, 13*(1), pp. 1-35.

Sun, S.-T., Pospisil, E., Muuslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). What Makes Users Refuse Web Single Sign-On? An Empirical Investigation of OpenID. *Symposium on Usable Privacy and Security (SOUPS)*, (pp. 1-20). Pittsburgh.

TACACS.net. (2011, April). *The Advantages of TACACS+ for Administrator Authentication .* Retrieved from tacacs.net: http://www.tacacs.net/docs/TACACS\_Advantages.pdf

Target. (n.d.). *data breach FAQ.* Retrieved June 26, 2015, from corporate.target.com: https://corporate.target.com/about/shopping-experience/payment-card-issue-faq

The Bro Project. (2015, July 21). *Introduction.* Retrieved from bro.org: https://www.bro.org/sphinx/intro/index.html

The Home Depot. (n.d.). *The Home Depot Reports Findings in Payment Data Breach Investigation.* Retrieved June 26, 2015, from corporate.homedepot.com: https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf

The Trustees of Princeton University. (2013, July 2). *Password Composition Best Practices.* Retrieved from princeton.edu: http://www.princeton.edu/itsecurity/policies/password-policy/

Toys R Us. (2015, February). *Rewards "R" Us - February 2015 Security Update Email.* Retrieved from oag.ca.gov: https://oag.ca.gov/system/files/Notifications\_2.pdf?

Twitch Interactive Inc. (2015, March 23). *Important Notice about your Twitch Account.* Retrieved from blog.twitch.tv: http://blog.twitch.tv/2015/03/important-notice-about-your-twitch-account/

U.S. Department of the Army. (2008, May 1). *Army Password Standards.* Retrieved from militarycac.com: https://militarycac.com/files/army\_password\_standards.pdf

Ventrone, M. (2014, September 24). *jimmy-johns-20140924.pdf.* Retrieved from doj.nh.gov: http://doj.nh.gov/consumer/security-breaches/documents/jimmy-johns-20140924.pdf

Walters, M., & Matulich, E. (2011). Assessing Password Threats: Implications for Formulating University Password Policies. *Journal of Technology Research, 2*(1), 1-9.

Wang, R., Chen, S., & Wang, X. (2012). Singing me onto your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. *Security and Privacy*, 365-379.

Whitlock, D. (2008). Internet Fraud: Preventing and Responding to Phishing and Spoofing Scams. *New Hampshire Bar Journal*, 30-33.

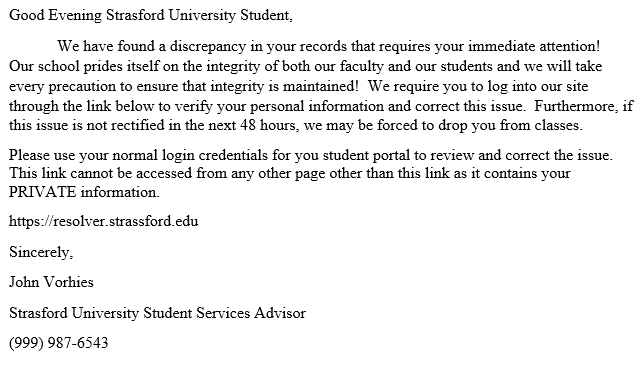
Wright, R., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, 273-303.

Xiong, S. (2005, June). *Web Single Sign-On System for WRL Company.* Retrieved from kth.se: http://people.kth.se/~johanmon/theses/xiong.pdf

Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving Multiple-Password Recall: An Emperical Study. *European Journal of Information Systems*(18), 165-176.

# Appendices

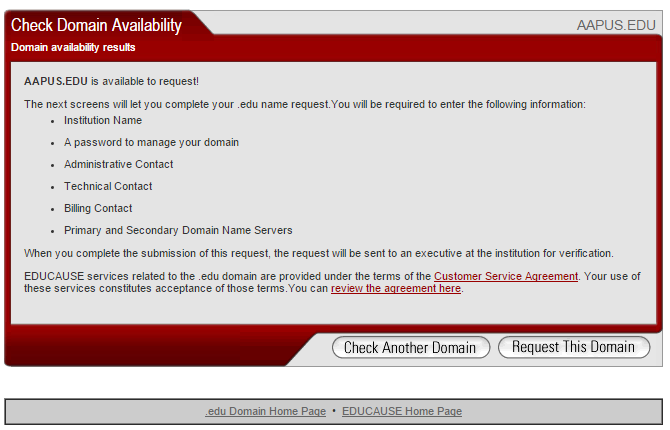
## Appendix A: Sample Phished Email



Example email created to demonstrate a phished email to university students.

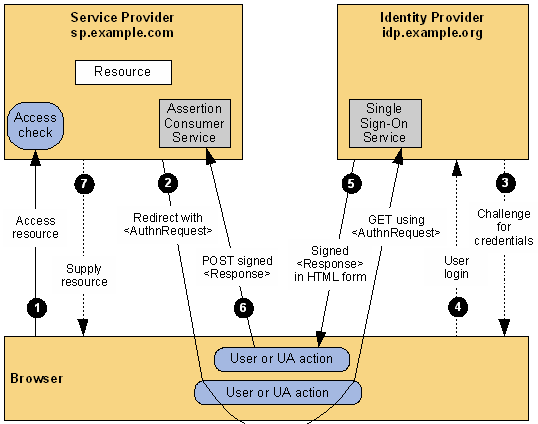
* The link for the students to click on contains strassford and not strasford.
* The Student Services Advisor information could be real and gathered from the schools site.
* The school informed the student that the link contains their personal information, but never addressed the student by their name.
* A time limit of 48 hours could force the student to respond quickly before contacting the school.

## Appendix B: Available Aapus.edu Domain



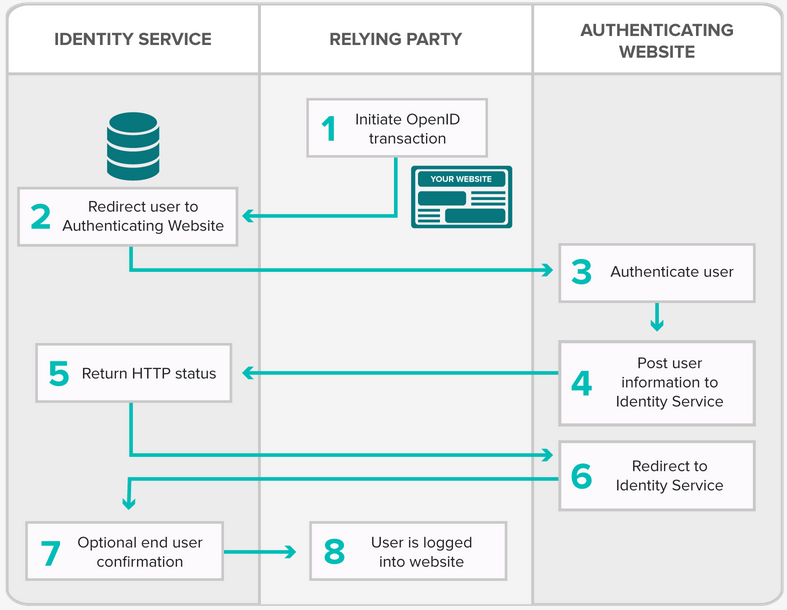
Educase.edu. (n.d.). *Ready to Request a New .edu Domain Name.* Retrieved from educause.edu: http://net.educause.edu/edudomain/request.asp

## Appendix C: SAML Flow Chart



OASIS. (2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview.* Retrieved from oasis-open.org: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

## Appendix D: Janrain Flow Chart



Janrain, Inc. (n.d.). *Deploy Identity Services.* Retrieved from janrain.com: http://developers.janrain.com/how-to/identity-services/integrate-identity-services/#prerequisite

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I, Adam B. Hall, owner of the copyright to the work known as Facebook, Google, and Twitter as a Single Sign-On Service: To Use or Not to Use hereby authorize

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to use the following material as part of his/her thesis to be

Submitted to American Public University System.

Page Line Numbers or Other Identification

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

School of Science, Technology, Engineering, and Math

MS in Information Technology

The thesis for the master’s degree submitted by

Adam B. Hall

under the title

Facebook, Google, and Twitter as a Single Sign-On Service: To Use or Not to Use

has been read by the undersigned. It is hereby recommended for acceptance by the faculty with credit to the amount of 3 semester hours.

(Signed, first reader)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Date) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Signed, second reader, if required) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Date) \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommended for approval on behalf of the program

(Signed) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Date) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommendation accepted on behalf of the program director

(Signed) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Date) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved by academic dean

This capstone has been approved by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ for submission, review, and

publication by the Online Library.

Author’s name: Adam B. Hall\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: Facebook, Google, and Twitter as a Single Sign-On Service: To Use or Not to Use

Professor: Dr. Denise D. Eggersman\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Second reader, if required: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Program: Master’s of Science in Information Technology with a concentration in Information Assurance and Security

Pass with Distinction:

YES NO

Keywords/Descriptive Terms: Phishing, Password Cracking, Single Sign-On, Hacking, Two-Factor Authentication

[ ] Contains Security-Sensitive Information