https://doi.org/10.48009/1_iis_2010_256-265

AN EMPIRICAL STUDY OF USER AUTHENTICATION: THE PERCEPTIONS VERSUS PRACTICE OF STRONG PASSWORDS

Lisa Z. Bain, Rhode Island College, lbain@ric.edu
Michael Hayden, Rhode Island College, mhayden@ric.edu
Sandra Sneesby, Community College of Rhode Island, sluzzisneesby@ccri.edu

==========

ABSTRACT

Computers are an essential aspect of our lives, storing and transmitting a variety of personal and private information. Unwanted parties threaten the security of this information making strong passwords vital for its protection. This research paper examines the perceptions versus the practice of strong password use among students at a medium-sized, 4-year, public college. The results show the use of some strong password principles but the overall use of weak passwords for most Information Systems. Conclusions are drawn and suggestions are made for increasing password awareness and strength.

Keywords: Strong Passwords, Computer Security, Information Systems, User Authentication

INTRODUCTION

Computers are an integral part of the daily lives of millions of people, especially college students. According to the U.S. Census Bureau, the majority (77%) of college students are between the ages of 15 and 24 years old [24]. This makes them part of Generation Y, also known as Gen Y, Echo Boomers, the Net Generation, and Millennials. Although the dates range among researchers and authors, Generation Y generally includes those born between 1977 and 2002 [11, 16, 18]. They use computers more than any previous generation and for a variety of reasons, considering themselves knowledgeable about and comfortable with technology [18]. This includes, but is not limited to, educational projects, business tasks, and personal activities [18]. Electronic mail, online shopping, social networking, and cyber banking are just a few examples of common and daily applications [18].

Many of the software applications used by college students require them to store information that is personal and private, making it vulnerable to unwanted parties. Data and information, such as social security and credit card numbers, is highly coveted by criminals and therefore susceptible to theft. Cyber crime is a term used to describe any illegal activity conducted over a computer network, especially the Internet. The number of Internet security vulnerabilities has significantly increased over the last 15 years [3]. Vulnerabilities include any possible threat that could cause harm to a computer or computer network. The Computer Security Institute (CSI) conducts an annual survey of computer crime, publishing statistics not only on attacks but also their impact. The 2009 survey indicates that attacks increased in most areas, including an 8% increase in password sniffing [7]. Sniffing allows computer criminals, or hackers, to steal passwords from other users on a computer or computer network. This is just one of the many methods and techniques employed by criminals to conduct cyber crime, making computer security essential for protecting confidential information. Fortunately, there are many types of information security controls that can help prevent such attacks, including passwords.

Passwords are a common method used for allowing and restricting access to computers and computer networks. They are a type of access control that performs authentication in order to verify the identity of the user. Passwords vary from simple words like a pet's name to more complex acronyms of sayings or phrases [13]. Hackers, computer criminals, and others have ways to figure out simple or weak passwords [5]. The more complex the password is, the harder it is for unwanted parties to crack or steal. Complex or strong passwords are harder to guess and therefore more difficult to break. Computer security experts recommend the use of strong passwords, but do not necessarily agree on their exact characteristics. However, the majority of strong password recommendations do include the combination of letters, numbers, and symbols or special characters [5].

Current computers and Information Systems support the use of strong passwords. Users, including college students, have the capability to use strong passwords. Users may not use strong passwords for a variety of

reasons, like the lack of awareness of what constitutes a strong password or the impact a weak password may have on security [10]. Understanding the awareness and use of strong passwords can identify areas for improvement, with the end result of increased security. Security education is important at the college level, especially for students majoring in business disciplines [14]. Although students tend to be computer savvy, they are a threat to computer security [25]. Businesses and organizations rely on Information Systems and their employee's proper use of these systems, making computer security essential for daily operations and sustained viability.

This research paper will define the term strong password and identify the awareness (perceptions) versus the use (practice) of strong passwords by college students. The next section conducts a review of the existing literature on strong passwords. The methodology section describes the development of the strong password model and the survey used to collect data on the types of passwords currently used by college students. The results section discusses the data collected, including demographics. The conclusion section summarizes the findings and makes recommendations.

LITERATURE REVIEW

Multiple sources provide computer security recommendations for passwords and strong passwords. They vary in detail, but are consistent in their promotion of the necessity for information and network security. Some estimates put the cost of computer security at billions of dollars per year [23]. Others just say it is expensive and difficult to calculate the exact cost [21]. Regardless, passwords are a key element in this protection even if they are not completely secure [4]. Other technology is currently available, like biometrics, and further research continues on more secure alternatives [23]. Nevertheless, password use continues as a common and widely used method of security because of their low cost and ease of use. Therefore, recommendations for strong passwords exist to increase the level of security provided by passwords. These recommendations consist of two primary areas. There are general guidelines on *how* to choose a password and specific details on *what* components to choose for the characters in the password.

General guidelines outline basic rules for identifying and choosing strong passwords. Passwords should be difficult to guess [9, 19, 20]. The word "password" is still considered one of the most commonly used and easily guessed passwords [12]. Passwords should not use names of any type, especially names of family, friends, and pets [5, 8, 13, 20, 22]. They should not use any type of personal information such as addresses, dates, social security and telephone numbers [5, 20, 22]. Some suggest that passwords should be unrecognizable to anyone except the owner [9]. These general guidelines mean that someone other than the user would not be able to login just by trying commonly known information about the user. One study showed that many people use personal information as passwords because it is convenient and easy to remember [2]. In addition, passwords should not be any word that is found in a dictionary [5, 8, 13, 19, 20, 22]. There are many programs freely available on the Internet that can figure out these types of passwords if a hacker gains access to the system or to the information on the network.

Other general guidelines deal with the use of the passwords for multiple systems and how the passwords are stored and shared. Many experts recommend that users create a different password for each computer system [8, 9, 12, 19, 22]. This reduces the overall security impact if one password becomes compromised. However, users should keep passwords private by not writing them down or sharing them with anyone, especially by email [8, 9, 12, 19, 22]. Last, users should change their passwords on a regular basis, with recommendations ranging anywhere from 30 to 120 days [8, 19, 22].

Beyond the general guidelines, there are specific recommendations as to what specific components should be used for the characters in the password itself. These focus primarily on the type and number of characters and password length. Most experts agree that the characters in a password should be a combination of letters, numbers, and symbols [5, 8 9, 12, 13, 15, 17, 20, 22]. In most cases, security experts recommend that these characters should use both upper case and lower case letters [1, 5, 12, 13, 15, 20, 22]. Passwords should also include a number but not one placed at the beginning or end [5]. In addition, passwords should include symbols [1, 5, 12, 13, 15, 20, 22]. Symbols are also called special characters and are typically available on most keyboards (@#$%^&*).

The recommendations on password length ranges between 7 and 15 characters [5, 8, 9, 12, 17, 19, 22]. Microsoft's online password checker recommends at least 14 characters, while three other password

checkers Password Meter, Geek(Wisdom), and Yet Another Password Meter recommend a minimum of 8 characters. In fact, passwords that are the same as the username and less than 8 characters can be cracked be within minutes [19]. However, most of these recommendations do not identify the exact amount of upper case letters, lower case letters, numbers, or symbols that should exist in a strong password.

Other experts recommend that users create a passphrase or some type of acronym to make strong passwords easier to remember [9, 5, 12, 13, 17, 20, 22]. Microsoft recommends creating passwords this way and provides examples on their web site [17]. A common way to do this is to use the first letter of each word in the passphrase making sure to add numbers and symbols. Others recommend even more specific items like not using a regular password with a number at the beginning or at the end or backward spellings [5]. There are also recommendations for specific operating systems and computing environments [19]. In some cases, the computer system requires or forces the users to create passwords with certain characteristics [19].

Although the literature suggests some varying information on strong passwords, there is a core of similar information in terms of the general guidelines and the specific components of the password. The results section summarizes these, developing a strong password model.

METHODOLOGY

This research project consisted of two main items, a strong password model developed from the literature and a password survey completed by college students. First, the research project analyzed each strong password recommendation, compared it to the others and organized each into groups. Multiple similar recommendations were combined and unique recommendations were separated. Recommendations that included a specific amount or number of characters were specified using ranges instead. For example, the length of a strong password varied between 7 and 15 characters. In some cases, a common word or phrase was used for differing terminology. This summarization provided a more comprehensive and easier to use list of the recommendations. The results section provides two tables detailing the strong model, one for the general guidelines and a second one for the specific components.

Second, the research project developed a password survey that collected data about the awareness (perceptions) and the actual use (practice) of strong passwords by college students. The survey was distributed to students in the introductory and intermediate Information Systems classes in the business school at a medium-sized, four-year, public college in southern New England. The majority of the students in these courses major in the business disciplines of Accounting, CIS (Computer Information Systems), Economics, Finance, Management, and Marketing. The survey also included the basic demographics of age, college level, gender, and college major/minor.

The awareness (perceptions) portion of the survey asked the students to list any characteristics of strong passwords that they currently use or that they currently know. These characteristics would then be combined and compared against actual strong password recommendations from computer security experts. The use (practice) portion of the survey asked the students to test and record the strength of their passwords. This required each student to spend approximately one week recording a list of each Information System they used that required a password, including the system type, then testing the password using an online password checking tool. The survey did not require the students to record their passwords. The online tool, by default, keeps all passwords hidden.

The password portion of the survey provided space to record detailed information about each password. This included the name of the Information System that required the password and the type of system by category. It also included the Complexity and Strength of each password and the specific password Requirements used by the password checking tool. The names of the Information Systems were provided by the student and primarily consisted of email systems, online shopping sites, financial institutions, and social networking sites. The survey instrument dictated the categories for the system types and included Business, Education, Entertainment, Financial, Medical, Shopping, and Other (Specify).

The online password checking tool used for the survey was The Password Meter at www.passwordmeter.com. Again, this tool identifies the Complexity, Score, and Requirements for each password entered. The Complexity values range from Very Weak, Weak, Good, Strong, and Very Strong based on the Score. The Score value uses a

percentage from 0 to 100. The Requirements evaluate each component of the password and include a section for Additions and Deductions to the Score (Table 8). The Additions include: Number of Characters; Uppercase Letters; Lowercase Letters; Numbers; Symbols; Middle Numbers of Symbols. The Deductions include: Letters Only; Numbers Only; Repeat Characters; Consecutive Uppercase Letters; Consecutive Lowercase Letters; Consecutive Numbers; Sequential Letters; and Sequential Numbers. The online tool uses symbols to indicate the result for each of the Requirements. The symbols include a Star for Exceptional, Checkmark for Sufficient, Exclamation Point for Warning, and an X for Failure.

The survey used the same terminology as the online tool to make it easy for the students to record the results. In addition, the online tool was demonstrated in class to the students. The results section discusses the results of the password survey, including the demographics of the students, their awareness of strong password recommendations and the use of these recommendations in their actual passwords.

RESULTS

Strong Password Recommendations – Model

Summarizing the strong recommendations from the literature resulted in two types of recommendations, one set for the general guidelines and one set for the specific components of a password (Table 1). In general, strong passwords should be difficult to guess, kept private, changed regularly, and unique. This means passwords should not use names, personal information or dictionary words of any type. Pets, friends, family, interests, birthdays and phone numbers are all examples that violate this recommendation. Users should keep their passwords private by not writing them down or sharing them with anyone, especially through email. Security experts also recommend that user change their passwords on a regular basis, preferably every 30 to 120 days. And lastly, passwords should be unique in that they are different for each Information System.

The specific components of strong passwords include recommendations for length and the type of characters used in the password itself. Passwords should be at least 7 to 15 characters in length. Characters representing both uppercase and lowercase letters, numbers, and symbols. As for the amount of these characters, the literature suggests that passwords consists of a combination of all these characters and include at least one uppercase letter, lowercase letter, symbol, and number. There was not a strong consensus on passphrases, nonconsecutive numbers/letters, or middle numbers/letters. Table 1 summarizes these recommendations.

Table 1. Strong Password Model

General Guidelines
Passwords should be difficult to guess
- Should not use names
- Should not use personal information
- Should not be a word found in a dictionary
Passwords should be private
- Should not be written down or stored
- Should not be shared
- Should not be emailed
Password should be changed on a regular basis
- Should be changed every 30 to 120 days
Passwords should be different for each system
Specific Components
Passwords should have a minimum length
- Should be 7-15 characters
Passwords should use a combination of characters
- Should include at least one uppercase letter
- Should include at least one lowercase letter
- Should include at least one number
- Should include at least on symbol

Password Survey Results – Demographics

The results of the password survey included 65 usable responses. The demographics of the sample are summarized in Table 2. The responses included slightly more females (35) than males (30), primarily business majors (88%), and mostly juniors (55%). The non-business majors represented a very small percentage and were therefore combined. The average age of 22.05 fell within the typical range.

Table 2. Demographics

Item	**Count**	**Per**
Male	30	46%
Female	35	54%
Total	65	100%
Major		
Accounting	10	15%
CIS	10	15%
Economics	1	2%
Finance	5	8%
Management	26	40%
Marketing	5	8%
Total Business Majors	57	88%
Total Non-Business Majors	8	12%

Total All Majors	65	100%
Level		
Freshmen	0	0%
Sophomore	5	8%
Juniors	36	55%
Seniors	24	37%
Average Age	22.05	100%

Password Survey Results – Perceptions

The results of the perception portion of the password survey showed that the students use some, but not all, of the recommended strong password guidelines and specific components. The survey did not provide any suggestions or recommendations. It simply asked the students to record any type of strong password characteristic that they use or know. The results were reviewed for terminology and related to the Strong Password Model and summarized in Table 3. About a third of the students still use passwords that could be guessed (36%) but almost half (44%) know that they should not. A very small percentage (3%) keeps their passwords private or knows (3%) that they should. They also do not change them regularly (0%) or know (3%) to do so. A few more students (6%) do use different passwords for each system but twice as many more (14%) know they should. For the length, only about a quarter of the students (26%) use passwords that are eight or more characters, while slightly more (32%) know they should.

As for the specific components of their passwords, there are mixed results that vary from the recommendations. However, numbers (83%) are used more than any other character. Only about a quarter of the students (22%) use symbols but about 3 times as many (62%) know they should. As for the letters, about half of the students use (51%) and know (49%) about using uppercase letters. A majority use (66%) and know (65%) about using lowercase letters. Students also included other items on their surveys that were more specific that the recommendations. These included the use and knowledge of nonconsecutive numbers/letters, passphrases, and middle numbers or symbols. These combined resulted in a small percentage of students that use (18%) versus know (25%). It was encouraging to see the use and awareness of numbers, symbols, and uppercase letters in passwords. However, the lack of awareness for keeping passwords private, changing them regularly and using different passwords for each Information System was cause for concern.

Table 3. Perceptions – You Use versus You Know

Password Should:	Use	Know
Be difficult to guess		
Names	6%	0%
Birthdays	3%	0%
Something easy to remember	8%	0%
No predictable words/phrases	17%	44%
Multiple ending letters	2%	0%
Be private		
Do not share/record	3%	3%
Be changed on a regular basis		
Change regularly	0%	2%
Be different for each system		
Unique	6%	14%
Have a minimum length		
Length (6 or more characters)	8%	20%
Length (8 or more characters)	18%	12%
Use a combination of characters		
Numbers	83%	62%
Symbols/Special Characters	22%	62%
Uppercase Letters	51%	49%
Lowercase Letters	66%	65%
Nonconsecutive numbers	5%	9%
Nonconsecutive letters	5%	11%
Passphrase	3%	2%
Middle numbers or symbols	5%	3%

Password Survey Results – Password Strength

The password survey also captured data about each individual password used by the students. Table 4 summarizes this data. The 65 returned surveys included a total of 613 passwords with an average of 9.58 passwords per student. However, one student responded with only two passwords and seven responded with 15 passwords each. The most common number of passwords among the students was seven. One of the recommended strong password guidelines from the literature and added to the strong password model is that passwords should be kept private and different for each system. With the increased use of Information Systems, the number of passwords a user must maintain has increased. This may also increase the likelihood that users will write down their passwords or use them for more than one system.

Table 4. Password Survey Responses

Item	Results
Total Surveys Returned	65
Total Passwords Tested	613
Average Passwords per Student	9.58
Minimum Passwords per Student	2
Maximum Passwords per Student	15
Common Passwords per Student (Mode)	7

Fortunately, only a small percentage of the students (14%) write down their passwords, but only about a third (31%) use a unique password for each system. This could be related to the fact that only 23% of the systems used by the students required a strong password. Table 5 summarizes the results for these three items.

Table 5. Passwords Privacy, Uniqueness, Required

Item	Yes	No	Blank
Password Written Down	8	530	
	14%	31%	
Password Unique	192	384	37
	31%	63%	6%
Strong Password Req	142	420	70
	23%	63%	11%

Next, the survey asked the students to type their actual passwords into a password checker. The results of the password checker provided a Score, Complexity, and details about the specific components (characters) of the password. Table 6 summarizes the Complexity rating of the 613 passwords, Table 7 summarizes the Score by System Type and Table 8 summarizes the Password Components. The possible Complexity ratings based on the numerical score included Too Short, Very Weak, Weak, Good, Strong, and Very Strong. The average score for all the passwords was 36.53, a score that the password checker rated as Weak. Over half of the passwords (57%) received one of the weak Complexity ratings. Only a few of the passwords (4%) received the Very Strong rating. However, there were 264 passwords that were rated as Good, Strong, or Very Strong. This provided some basic evidence that students really were using some of the strong passwords guidelines they specified in the perceptions sections of the survey.

Table 6. Password Complexity

Complexity	Count	Per
Too Short	2	0.3%
Very Weak	165	27%
Weak	182	30%
Good	124	20%
Strong	114	19%
Very Strong	26	4%
Average Password Score	36.53	(Weak)
Too Short, Very, Weak, Weak	349	57%
Good, Strong, Very Strong	264	43%

The password survey also asked the students to provide a category for the type of Information System for which the password was used. The original system types included Business, Education, Entertainment, Financial, Medical, Shopping, and Other. After reviewing the surveys, the three additional categories of Computer Access, Email/Messenging and Social Networking were added. The Entertainment category was expanded to include Information. All passwords marked with the Other category were either removed from the results or changed to another category. For example, passwords for non-Information Systems like PDAs and cell phones were removed. Table 7 summarizes the results by System Type. The System Type with the highest score (76.00) was the Medical category, but it received only one password. A score of 76.00 has a complexity rating of Strong. Obviously, this is not a common area for college students. The next highest score (52.19) is in the Education category, which has a complexity of Good. This category included many of the Information Systems the student use at the college like the registration and learning management systems. The remaining categories all received average scores in the Weak complexity ranges of 24.68 to 39.42. Other than the Medical outlier, there was little to distinguish among the System Types. This could indicate the use of the same password across multiple systems, with the exception of the Education systems.

Table 7. Password Score by System Type

System Type	Count	Per	Ave Score
Business	54	9%	32.57
Computer Access	19	3%	24.68
Education	73	12%	52.19
Email/Messenging	156	25%	39.42
Entertainment/Info	72	12%	30.57
Financial	103	17%	38.31
Medical	1	0%	76.00

Shopping	54	9%	29.46
Social Networking	81	13%	29.52

The last part of the password survey recorded the results of the specific components of the passwords. Again, Table 8 summarizes the findings. The password checker divided these results into an Addition and Deductions section, both using rating of Star (Exceptional), Checkmark (Sufficient), Exclamation Point (Warning), and X(Failure). The Additions section rated the password on Number of Characters, Uppercase Letters, Lowercase Letters, Numbers, Symbols, and Middle Numbers or Symbols. The Deduction section rated the password on Letters Only, Numbers Only, Repeat Characters, Consecutive Uppercase Letters, Consecutive Lowercase Letters, Consecutive Numbers, Sequential Letters, and Sequential Numbers. This password checker provides a level of detail that other password checkers do not, allowing users to see what items they could use to increase the strength of their passwords. Most notable of all of this detail are the Failures in the Additions sections and the Warnings in the Deduction section. In the Additions section, over half (55%) of the passwords received a failure on the use of uppercase letters and over two-thirds (68%) received a failure on the use of symbols. In the Deductions section, over half (53% and 58%) received a warning for using repeat characters and using consecutive lowercase letters, respectively. This level of detail, along with the visual indicators, immediately shows the weak areas of a password and provides instant feedback for increasing password strength. (See Table 8 below).

CONCLUSIONS

Strong passwords are an important aspect of computer security, providing user authentication and helping to maintain privacy of user data. Passwords that are not strong pose a security threat to a multitude of Information Systems, ranging from E-mail and Online Shopping to Education and Business systems. Although the recommendations from computer experts vary, there are still many known and consistent guidelines for increasing the strength of weak passwords. There are also well-documented details on the specific components that constitute a strong password. In addition, these guidelines and components are relatively easy to use. They do not require any special type of software, computer, or Information System. Just making a few changes like adding a symbol or not using a common word can change a weak password into a very strong one.

The results of the password survey conducted for this research project showed the perceptions of strong passwords do vary from the actual use. The students did use some of the recommendation guidelines and knew of other guidelines that they did not always use, but were not aware of many significant others. In general, they used and were aware of using letters and numbers in their passwords. However, there was a strong lack of awareness in keeping their passwords private, changing them on a regular basis, and making them unique across systems. This could be caused by Information Systems that do not require strong passwords or it could simply be an awareness and education issue. It could also be related to the number of passwords they need to remember and use on a regular basis. With over half of the passwords rated as weak, this could be a significant security issue as these students move from the educational to the business environment where security plays an even more important role. An additional study into why students do not always make their passwords stronger could provide further insight.

The password strength by system type was also not encouraging. The passwords in all the categories, with the exception of Education and Medical, were rated as weak. This included Business, Computer Access, and Financial systems that presumably would contain more private information than Entertainment, Online Shopping or Social Networking systems. The students may not be distinguishing between the types of systems or they may be using the same passwords across all the categories, except for the Education and Medical systems. Again, this study focused on the current state of passwords not the process of selecting a password.

Although the results of the password components showed many weak areas, the details highlighted simple changes that could easily strengthen passwords. Knowing that a majority of weak passwords do not include an uppercase letter or symbols is an easy item to address with awareness and education. This applies to both students and users of any type of Information System. Information Systems courses at all levels can educate students on the use of strong passwords and the type of characters that increase a password's strength. Businesses can also educate and encourage their users to increase the strength of their passwords with these rather simple changes. This is especially important for systems that currently do not require strong passwords, with this survey showing that a majority still do not. Fortunately, there are many

resources available and opportunities to help educate users. Workshops, strong password generators, training sessions, and regular notices/emails are all examples of ways to increase the awareness and use of strong passwords.

As more of our daily life becomes automated and computerized, the need for security increases. User authentication provides us with access to this computerized world but it comes with a price. Users must be aware of the need for protecting their private data with strong passwords. The recommended guidelines for strong passwords provide users with the tools they need for choosing a better password and keeping it private. In some cases, the simple act of adding a symbol and an uppercase letter could mean the difference between identify theft and private data staying private.

REFERENCES

1. Apple (2010). Password Builder 1.0. Retrived January 6, 2010 from Apple Inc. Web site: http://www.apple.com/downloads/macosx/networking_security/passwordbuilder.html
2. Brown, A. S., Bracken, E., Zoccoli, S., and Douglas, K. (2004). Generating and Remembering Passwords. *Applied Cognitive Psychology*, 18, 641-651.
3. CERT(2009). *CERT Statistics (Historical)*. Retrieved January 4, 2010 from CERT Web site: http://www.cert.org/stats/
4. Charoen, D., Raman, M., & Olfman, L. (2008). Improving End User Behaviour in Password Utilization: An Action Research Initiative. *Systemic Practice and Action Research*, 21(1), 55. Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 1413108821).
5. Ciccarelli, P., Faulkner, C., Fitzgerald, J., Dennis, A., Groth, D., & Skandier, T. (2008). *Networking basics*. Hoboken, NJ: John Wiley & Sons.
6. Chien, H. & Jan, J. (2003). Robust and Simple Authentication Protocol. *The Computer Journal*, 46(2), 193. Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 332888321).
7. CSI (2009). *CSI Computer Crime and Security Survey 2009*. Retrieved January 4, 2010 from Computer Security Institute Web site: http://www.gocsi.com/2009survey/;jsessionid=Z14DF5YZLDF4ZQE1GHRSKHWATMY32JVN
8. Dean, T. (2006). Network+ guide to networks (4th ed.). Boston, MA: Thomson Learning, Inc.
9. Fordham, D. (2008). How Strong Are Your Passwords? *Strategic Finance*, 89(11), 42-47. Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 1553566021).
10. Gibbs, M. (2008, April). Fighting off strangers bearing candy. *Network World*, 25(16), 50. Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 1473998791).
11. Glossary (2009). *Generation Y, Definition(s) of*. Retrieved January 4, 2010 from Boston College Web site: http://wfnetwork.bc.edu/glossary_template.php?term=Generation%20Y,%20Definition(s)%20of&topic=6&area=all
12. Kennedy, D. (2007). Power Passwords. *ABA Journal*, 93, 59. Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 1411468971).
13. Kroenke, D. M. (2007). Using MIS. Upper Saddle River, NJ: Pearson Education, Inc.
14. Lawler, J.P., Li, Z., & De Leon, Y. (2005). A Study of Security Education in the Era of Cyber-Terrorism. *Journal of College Teaching & Learning*, 2(10), 61-72.
15. Lindenmayer, G. (2007). Information Security Standards: The 10 Keys to Protecting Your Network. *Risk Management*, 54(12), 11. Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 1399142721).
16. Meskauskas, J. (2003). *Millennials Surfing: Generation Y Online*. Retrieved January 4, 2010 from iMedia Connection Web site: http://www.imediaconnection.com/printpage/printpage.aspx?id=2027
17. Microsoft (2010). *Create strong passwords*. Retrieved January 6, 2010 from Microsoft Web site: http://www.microsoft.com/protect/fraud/passwords/create.aspx
18. Nicholas, A. (2009). Generational Perceptions: Workers And Consumers. *Journal of Business & Economics Research*, 7(10), 47-52. Retrieved January 5, 2010, from ABI/INFORM Global. (Document ID: 1913274401).
19. NSA (2006). *The 60 Minute Network Security Guide*. Retrieved January 8, 2010 from National Security Agency Web site: http://www.nsa.gov/ia/_files/support/I33-011R-2006.pdf
20. Rainer, K. (2009). Introduction to information systems (2nd ed.). Hoboken, NJ: John Wiley & Sons.

21. Rose, C. & Gordon, J. (2003). Internet security and the tragedy of the commons. Journal of Business & Economic Research. 1(11), 67-72.
22. SANS.org (2010). *SANS Password Policy*. Retrieved January 4, 2010 from SANS Institute Web site: http://www.sans.org/resources/policies/Password_Policy.pdf
23. Summers, N. (2009, October). Building a Better Password :Tough to remember but easy to crack, passwords are the weak link in computer security. Billions hang in the balance. *Newsweek*, 154(16). Retrieved January 6, 2010, from ABI/INFORM Global. (Document ID: 1879746471).
24. U.S. Census Bureau (2008). *School Enrollment--Social and Economic Characteristics of Students: October 2008*. Retrieved January 5, 2010 from U.S. Census Bureau Web site: http://www.census.gov/population/www/socdemo/school/cps2008.html (Accessed 1/5/2010).
25. Young, J. R. (2009). Top 10 Threats to Computer Systems Include Professors and Students. *Education Digest*, May2009, Vol. 74 Issue 9, p24-27, 4p.

Table 8. Password Components (Requirements)

	Exceptional		**Sufficient**		**Warning**		**Failure**	
Additions								
Numbers of Characters	310	51%	195	32%	0	0%	108	18%
Uppercase Letters	150	24%	127	21%	0	0%	336	55%
Lowercase Letters	458	75%	74	12%	0	0%	81	13%
Numbers	389	63%	111	18%	0	0%	112	18%
Symbols	102	17%	95	15%	0	0%	416	68%
Middle Numbers or Symbols	320	52%	143	23%	0	0%	150	24%
Deductions								
Letters Only	97	16%	418	68%	62	10%	36	6%
Numbers Only	97	16%	460	75%	16	3%	40	7%
Repeat Characters	102	17%	147	24%	327	53%	37	6%
Consecutive Uppercase Letters	97	16%	440	72%	36	6%	40	7%
Consecutive Lowercase Letters	97	16%	125	20%	355	58%	36	6%
Consecutive Numbers	106	17%	184	30%	284	46%	39	6%
Sequential Letters	97	16%	476	78%	5	1%	35	6%
Sequential Numbers	98	16%	470	77%	9	1%	36	6%