Password Security: What Users Know and What They Actually Do

By [Shannon Riley](#)

Summary: This study investigated the common password generation practices of online users. Three hundred and fifteen undergraduate and graduate students completed a survey querying (1) the types and number of different password protected accounts maintained; (2) actual practices used in generating, storing and using passwords; (3) practices believed they should use in generating and storing passwords; and (4) general demographic information. Results indicate that, in general, users do not vary the complexity of passwords depending on the nature of the site (bank account vs. instant messenger) or change their passwords on any regular basis if it is not required by the site. Users report using lower case letters, numbers or digits, personally meaningful numbers and personally meaningful words when creating passwords, despite the fact that they realize that these methods may not be the most secure.

INTRODUCTION

Password protected accounts are very common and widely used for a variety of online applications including instant messaging, personal and business e-mail, and online banking and retail purchasing accounts. Given the sensitivity of the information within these accounts and the potential for abuse and misuse of this information by others, one might suspect that users would create very secure passwords. This has not proven to be the case. In spite of the fact that online shoppers report that information security and protection are their primary concern (Luo, 2002, Lightner, 2003), many studies have shown that users' consistently use very simplistic, easily predictable practices when constructing and using passwords. This includes using meaningful words or personal dates that are easy to remember (Bishop & Klein, 1995), using a proper name or using a word commonly found in the dictionary, or relating the password to the type of account for which it is used (Vu, Bhargav & Proctor, 2003). Such predictable and systematic practices are easier for the user to remember but they sacrifice the security that passwords are intended to provide.

Purpose

The purpose of this study is to comprehensively assess what practices users employ in creating and storing passwords for online accounts.

METHOD

Participants

A total of 328 undergraduate and graduate level college students from Wichita State University volunteered to participate in the survey, and were regular users of the Internet with one or more password protected accounts. Ages of the participants ranged from 18 to 58 years (M = 25.34).

Thirteen cases were deleted due to missing data, resulting in 315 participants in the final data analysis.

Materials

Participants were administered the Password Practices Survey, a 101-item self-report questionnaire that requests information about four areas:
(1) Internet usage behaviors (frequency, duration and longevity of use);
(2) Types and number of different password protected accounts maintained;
(3) Actual practices used in generating, storing and using passwords;
(4) Practices believed they should use in generating and storing passwords;
(5) General demographic information.

The Password Practices Survey was developed to investigate and expand on information regarding a diverse range of specific user practices, the extent of knowledge users have and use in the construction and use of passwords and the potential influence of internet usage practices. Survey questions were developed through a series of pilot tests. Questions regarding frequency, duration and method of internet access as well as frequency and variety of internet activities were taken directly from Lida-Rogers (2004) dissertation on the Development of the Internet Experience Scale. The Password Practices Survey uses a variety of forced-choice, multiple-response, fill-in-the-blank and open-ended response items, and was administered both on paper and online. The online version of the Password Practices Survey was created using SPSS Data Entry Builder™ and was accessed via the web. Completion of the survey took between 15 – 25 minutes.

RESULTS

General password characteristics

Descriptive analysis of the data revealed that 35% (112) of respondents reported that they use a predetermined number of characters in their passwords. Of these participants, the average number of characters per password was found to be 6.84 (SD = 1.79).

Overall, 74.9% of respondents (236) reported that they have a set of predetermined passwords that they use frequently, of those 98.3% (232) reported an average of 3.1 (SD = 2.028) passwords. More than half (59.7%, 188) reported that they do not vary the complexity of their password depending on the nature of the site they are using, such as an online bank account compared to an online chat program. The average length of time users have maintained their primary personal use password was reported as 31.07 months (SD, 28.01), roughly two years and seven months. When asked "How frequently do you change your password on a regular basis when not required by the system?" 52.7% (166) responded "Never" (Table 1).

Table 1. Frequency of changing password if not required by the system

Frequency	Responses	Percentage
Never	166	52.70%
Yearly	53	16.83%
Every six months	44	13.97%
Every three months	38	12.06%
Monthly	12	3.81%
Weekly	1	0.32%
Unknown	1	0.32%
Total	315	100.00%

Password construction practices/strategies used

In regard to practices that respondents report using "Very Frequently" or "Always" when creating passwords, 85.7% (270) reported that they use lowercase letters and 56.5% (178) reported that they use numbers or digits in their passwords. In addition, 54.9% (173) indicated that they use personally meaningful words, such as names of children, pets or street names, while 49.8% (156) indicated that they use personally meaningful numbers, such as birthdates or telephone numbers (Table 2).

Table 2. Frequency of password generation practices. Numbers in bold indicate those practices used most often.

Password Generation Practices	Never	Very Rarely	Rarely	Occasionally	Very Frequently	Always
Upper case letters	120	101	35	32	21	5
Numbers or digits	17	23	26	71	107	71
Special characters (&,^,$,*)	222	36	23	22	6	6
Spaces	255	31	21	5	2	1
Personally meaningful words (pets, street addresses)	61	23	14	59	89	67
Names of friends, relatives, movie stars	144	30	23	50	46	22
Personally meaningful numbers(birthdates, phone numbers, etc)	48	11	17	66	109	64
Geographical locations	215	33	21	20	19	6
Simple sequences of characters(12345, qwerty, mmmmm)	211	36	23	28	11	4
Numbers and special characters in place of letters(w1Ch!T@)	255	27	13	15	5	0
Capitalized word with numbers	178	43	23	37	24	9
Same character three or more times	189	62	25	24	12	3
Relate password to site you are on	227	40	11	19	13	1

In using passwords, 54.6% of users (177) report using the same exact password for multiple accounts "Very Frequently" or "Always", while 33.0% (104) report using some variation of the same password for multiple accounts (Table 10). About 15% of the users also report that they write down their list of passwords in case they forget them, while 28.6% (90) report using the "remember my password" function (Table 3).

Table 3. Frequency of password storage and usage practices

Password	Never	Very	Rarely	Occasionally	Very	Always

Storage/Usage Practices	Rarely				Frequently	
Write a list of passwords	130	66	27	44	20	27
Same exact password for multiple accounts	26	18	20	74	134	43
Some variation of same password	69	25	36	81	85	19
"remember my password" function	94	33	31	67	60	30
"wallet" to store passwords	294	8	3	6	3	1

User perceptions of password construction practices that should be used

When asked what practices should be used in the creation and usage of passwords, the majority of respondents, 50.8% (160), were able to identify most of the password practices that are recommended for creating secure passwords (Tufts University, 2005), although 62.9% (198) failed to identify a practice that would result in the most secure password; using numbers and special characters in place of letters.

Differences between password practices users reported and the passwords practices they believe they should use included:
· 73% (230) of respondents reported that they should change their passwords for accounts every three to six months, but 52.7% (166) responded that they "Never" change their password when not required.

· 50.8% (160) of respondents reported that they should use special characters in their passwords, but only 4.8% (12) reported doing so.

· 63.5% (200) of respondents reported that they should use seven or more characters in their passwords, but only 35.5% (112) indicated that they use this number of characters with any regularity.

· 70.5% (222) of respondents indicated that personally meaningful words should not be used, but 49.8% (156) reported that they use this practice.

· 68.3% (215) of respondents report that personally meaningful numbers should not be used in passwords, but 54.9% (173) reported using this practice.

DISCUSSION

The majority of participants in the current study most commonly reported password generation practices that are simplistic and hence very insecure. Particular practices reported include using lowercase letters, numbers or digits, personally meaningful words and numbers (e.g., dates). It is widely known that users typically use birthdates, anniversary dates, telephone numbers, license plate numbers, social security numbers, street addresses, apartment numbers, etc. Likewise, personally meaningful words are typically derived from predictable areas and interests in the person's life and

could be guessed through basic knowledge of his or her interests.

The finding that participants in the current study use such simplistic practices to develop passwords is supported by similar research by Bishop and Klein (1995) and Vu, Bhargav & Proctor (2003) who found that even with the application of password guidelines, users would tend to revert to the simplest possible strategies (Proctor et al., 2002). In the current study, nearly 60% of the respondents reported that they do not vary the complexity of their passwords depending on the nature of the site and 53% indicated that they never change their password if they are not required to do so. These practices are most likely encouraged by the fact that users maintain multiple accounts (average = 8.5) and have difficulty recalling too many unique passwords.

It would seem to be a logical assumption that the practices and behaviors users engage in would be related to what they think they should do in order to create secure passwords. This does not seem to be the case as participants in the current study were able to identify many of the recommended practices, despite the fact that they did not use the practices themselves. These findings contradict the ideas put forth in Adams & Sasse (1999) and Gheringer (2002) who state that users are largely unaware of the methods and practices that are effective for creating strong passwords. Davis and Ganesan (1993) point out that the majority of users are not aware of the vulnerability of password protected systems, the prevalence of password cracking, the ease with which it can be accomplished, or the damage that can be caused by it. While the majority of this sample of password users demonstrated technical knowledge of password practices, further education regarding the vulnerability of password protected systems would help users form a more accurate mental model of computer security.

REFERENCES

Adams, A. & Sasse, M. A. (1999). Users are not the enemy; Why users compromise computer security and how to take remedial measures. Communications of the ACM, vol. 42, 12, (pp. 40-46).

Bishop, M., & Klein, D.V. (1995). Improving system security via proactive password checking. Computers & Security, 14, 233 – 249.

Davis, C., & Ganesan, R. (1993). BApasswrd: A new proactive password checker. Proceedings of the National Computer Security Conference '93, the 16th NIST/NSA conference (pp. 1 – 15).

Gheringer, E. F. (2002). Choosing passwords: security and human factors. Proceedings of IEEE 2002 (pp. 369-373).

Lida-Rogers, B., (2004). Development of the internet experience scale: Investigating the relationships between cognitive, affective, and conative components of internet experience. Unpublished doctoral dissertation, Wichita State University, Kansas.

Lightner, J. (2003). What users want in e-commerce design: effects of age, education and income. Ergonomics, 46, 153-168.

Luo, X. (2002). Trust production and privacy concerns on the internet: a framework based on relationship marketing and social exchange theory. Industrial Marketing Management, 31, 111-118.

Proctor, R.W., Lien, M.C., Vu, K.-P. L., Schultz, E. E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. Behavior Research Methods, Instruments & Computers, 34, 163–169.

Tufts University Computing and Communications Services. (2005). Creating strong passwords, Retrieved March 28, 2005 from http://www.tufts.edu/tccs/r-strongpass.html

Vu, K. P. L., Bhargav, A., & Proctor, R.W. (2003). Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords. Proceedings of the 47th annual meeting of the Human Factors and Ergonomics Society (pp. 1331 – 1335). Santa Monica, CA: HFES.