International Journal of Innovative Research in Management Studies (IJIRMS)
ISSN (Online): 2455-7188
Volume 1 | Issue 4 | May 2016

A STUDY ON ONLINE AND WEB-BASED PASSWORD MANAGERS

Dr.P.Vaijayanthi* **M.Thasbiha Amjeth****

**Professor, School of Management, SASTRA University, Thanjavur, South India*

***II Year MBA Student, School of Management, SASTRA University, Thanjavur, South India*

ABSTRACT

A Password Manager is a software application that helps users securely store and manage passwords. Password managers usually store passwords encrypted requiring the user to create a master password or pass-phrase with a combination of special characters, uppercase and lowercase, ideally very strong which grants the user access to their entire password database. And passwords are encrypted with strongest encryption standard, AES-256. Online password managers use various tools to secure password by setting stronger passwords, locating your passwords with ease, access passwords when offline, import passwords in bulk and export password. Password managers also configure an additional layer of security by establishing two factor authentication, track activities through audit trials, ensure periodic password changes through expiry alerts, transfer ownership when someone leaves and acquire secrets when someone leaves on bad terms, automatically log its users out of the session to avoid unauthorized access to secrets. The study on online password managers was done during the period of March to April 2016 in ZOHO Corp, Chennai. ZOHO Corp has a password manager application named ZOHO Vault. So this study helps ZOHO Corp in creating awareness about password managers among potential individuals and business firms. The primary purpose of the study is to assess the common password management practices, examine the acceptance of the concept of online password managers among potential individuals and to create awareness about hackers and therefore using strong, unique passwords, periodic changing and prevent password leaks and re-use. This study also identifies how business firms and individuals securely store, share and manage passwords and other sensitive data and are they satisfied with the common password management system. The sample for this study included 50 students and 100 employees working in big corporate firms including HCL, CTS, ZOHO, WIPRO AND IGATE. Percentage analysis, Chi square and correlation co-efficient were used to analyze the data obtained.

Key words: Password Managers, Hackers, Password Leak, Strong Encryption, Secure Storage

INTRODUCTION

A password manager is a software application that helps a user store and organize passwords. Password managers usually store passwords encrypted, requiring the user to create a master password; a single, ideally very strong password which grants the user access to their entire password database. Some password managers store passwords on the user's computer (called offline password managers), whereas others store data in the provider's cloud (often called online password managers).

Online password managers helps securely store and manage your passwords that is securely store all your passwords and organize them for easy access and management. Passwords are encrypted with the strongest encryption standard, AES-256. Safely share passwords with the members of your organization Share chambers with users / user groups that is after organizing your secrets into chambers, you can share the chambers with individual users or a group of users in bulk. When you add a new member to the marketing group, the user will automatically inherit all the shares and permissions already granted to that group. Similarly, when you add a new secret to the chamber, it will become automatically available to all the members with whom the chamber has been shared.

Password managers also configure an additional layer of security by establishing request-release access controls for passwords and assign roles for access controls. It also helps in transferring ownership when someone leaves; acquire secrets when someone leaves on bad terms. Online password managers uses various tools to secure passwords by setting stronger passwords, locating your passwords with ease, access passwords even when you are offline, import passwords in bulk and export password.

It provides various security aspects to users like: Strongest encryption, rock-solid security, Track activities through audit trails, Gain visibility on 'who' has access to 'what' passwords, Get instant notifications on password events, Ensure periodic password changes through expiry alerts, Centrally control usage of features by your users, Periodic data backup for disaster recovery, Protection against shoulder surfing, Automatically log its users out of the session after a set period of inactivity, to avoid unauthorized access to secrets.

2. REVIEW OF LITERATURE

Zhiwei Li, Warren He, DevdattaAkhawe, and Dawn Song, University of California, Berkeley conducted a security analysis of five popular web-based password managers. Unlike "local" password managers, web-based password managers run in the browser. **AmbarishKarole, NiteshSaxena, Nicolas Christin** proposed in response to the growing number of passwords users have to memorize, password managers allow to store one's credentials, either on a third-party server (online password manager), or on a portable device (portable password manager) such as a mobile phone or a USB key. **David Silver, Suman Jana, and Dan Boneh, Stanford University; Eric Chen and Collin Jackson, Carnegie Mellon University** studied the security of popular password managers and their policies on automatically filling in Web passwords. **Rui Zhao, Chuan Yue, Kun Sun said that** Web users are confronted with the daunting challenges of managing more and more password to protect their valuable assets on different online services. Password manager is one of the most popular solutions designed to address such challenges by saving users' passwords and later auto-filling the login forms on behalf of users. **Daniel McCarney said that** Passwords continue to prevail on the web as the primary method for user authentication, despite well-known security and usability drawbacks. Password managers are known to o↵er some improvement without the deployment barrier of server-side changes. **Daryl Cromer, Richard Cheston, Steven Goodman, Howard Locker, Randall Springfield said that** Systems and methods to access password-protected stored data when a corresponding data password has been lost, forgotten, or is otherwise unavailable, and to recover the data password to facilitate access to the password-protected data from a digital memory device such as a hard disk drive associated with a user computer.

3. OBJECTIVE OF THE STUDY

- To determine the acceptance of the concept of online password managers among potential consumers.
- To create awareness about password managers among individuals and business firms.
- To create awareness about hackers and therefore safely secure passwords and prevent password leaks and re-use.
- To confirm that businesses securely store, share and manage passwords and other sensitive data, online credentials in a centralized repository and access control.

- To determine the elements of this application in various consumer options

4. NEED FOR THE STUDY

Comparative study on various online and web-based password managers. There are various software applications available to manage passwords like ZOHO Vault, RoboForm, Dashlane, KeePass, Last Pass etc. Determination of how these password managers help individuals and business firms to safely secure their passwords and comparative study of various password managers along with ZOHO Vault so that it helps ZOHO Corp to improve its vault service

5. ANALYSIS AND DISCUSSIONS:

Primary data were collected through questionnaire and the same were analysed using the Statistical tools like Chi-square, Correlation, which were interpreted in the following tables

Table 1

Percentage analysis

Age (in years)	Number of respondents	Percentage to total	Nature of the job	Number of respondents	Percentage to total
12-18	27	18.0	TECHNICAL USER IN NON INFORMATION SECURITY	36	24.0
18-25	51	34.0	TECHNICAL USER IN INFORMATION SECURITY	50	33.3
26-35	23	15.3	NON TECHNICAL IT USER	21	14.0
36-45	23	15.3	NON TECHNICAL IT HOME USER	22	14.7
45+	26	17.3	STUDENT	21	14.0
Total	150	100.0	Total	150	100.0

No. of passwords of the respondents	Number of respondents	Percentage to total	Minimum length of password	Number of respondents	Percentage to total
1-5	74	49.3	atleast 5	6	4.0
6-10	62	41.3	atleast6	21	14.0
11-20	9	6.0	atleast 7	17	11.3
ABOVE 20	5	3.3	atleast 8	96	64.0
			atleast 9	9	6.0
Total	150	100.0	Total	150	100.0
Strong and secure password	**Number of respondents**	**Percentage to total**	**Passwords used by respondents**	**Number of respondents**	**Percentage to total**
SPECIAL CHARACTERS	16	10.7	movie or book character	8	5.3
NUMERIC	7	4.7	birthdate	34	22.7
CAPITAL AND SMALL LETTERS	7	4.7	telephone or mobile number	9	6.0
SPECIAL CHARACTERS, NUMERIC, CAPITAL AND SMALL LETTERS	96	64.0	social security or ID number	5	3.3
DATE	6	4.0	kids names	10	6.7
NUMERIC AND CAPITAL & SMALL LETTERS	18	12.0	spouse name	8	5.3
Total	150	100.0	company name	6	4.0
Methods used to keep track of passwords	**No of respondents**	**Percentage to total**	pet name	10	6.7
WRITE THEM DOWN	14	9.3	vehicle lisence number	2	1.3
SAVE THEM IN A DOCUMENT	28	18.7	town, city or country	13	8.7

ALWAYS USE SAME PASSWORD	18	12.0	oldboyfriend/girl friend name	26	17.3
USE PERSONAL INFORMATION	29	19.3	others	19	12.7
ENTER AS NUMBER ON MOBILE DEVICES	6	4.0	Total	150	100.0
USE PASSWORD MANAGERS	23	15.3	**Password Managers**	**No of respondents**	**Percentage to total**
OTHERS	32	21.3	1PASSWORD	1	.7
Total	150	100.0	KEEPASS	3	2.0
Overall satisfaction	**No of respondents**	**Percentage**	LASTPASS	1	.7
strongly disagree	1	.7	ZOHOVAULT	16	10.7
Disagree	90	60.0	I DONT USE ONE	127	84.7
Neutral	43	28.7	OTHERS	2	1.3
Agree	11	7.3	Total	150	100.0
strongly agree	5	3.3			
Total	150	100.0			

Majority of respondents are in the age group of 18-25, out of which 24% of respondents are technical user in non information security, 33% of respondents are technical user in information security.Majority of respondents (49%) have to remember 1-5 passwords in their daily routine. 64% of respondents say that a password with special characters, numeric and capital and small letters makes a strong and secure password. (64%) of respondents say that the minimum length of Passwords should be at least 8 characters. Majority of respondents 23% use their birthdate as password or part of the password. It is interpreted that 10% of respondents write their passwords to keep track of their passwords, 19% of respondents save them in a document, 12% of respondents always use same password, 19% of respondents use personal information, 4% of respondents enter as number on mobile devices, 15% of respondents use password managers, and 21% of

respondents use other methods to keep track of their passwords. Majority of respondents do not use a password manager. Among the password manager users ZOHO Vault is mostly used (11%)

Majority of respondents 61% are dissatisfied with the password management system they use, this indicates the scope for the usage of Password Managers.

Table 2

ATTITUDE TOWARDS SECURITY MEASURES

Frequently resetting password	**Number of respondents**	**Percentage to total**	**Change passwords every month**	**Number of respondents**	**Percentage to total**
strongly disagree	80	53.3	strongly disagree	79	52.7
Disagree	42	28.0	Disagree	39	26.0
Neutral	9	6.0	Neutral	8	5.3
Agree	19	12.7	Agree	24	16.0
Total	150	100.0	Total	150	100.0
Browser to remember passwords	**Number of respondents**	**Percentage to total**	**Share passwords**	**No of respondents**	**Percentage**
strongly disagree	3	2.0	strongly disagree	1	.7
Disagree	48	32.0	Disagree	39	26.0
Neutral	77	51.3	Neutral	85	56.7
Agree	14	9.3	Agree	19	12.7
strongly agree	8	5.3	strongly agree	6	4.0
Total	150	100.0	Total	150	100.0
Logout of websites	**No of respondents**	**Percentage**	**Check for SSL**	**No of respondents**	**Percentage to total**
strongly disagree	81	54.0	strongly disagree	1	.7
Disagree	43	28.7	Disagree	38	25.3
Neutral	8	5.3	Neutral	85	56.7

Agree	18	12.0	Agree	20	13.3
Total	150	100.0	strongly agree	6	4.0
			Total	150	100.0

Majority of respondents (82%) do not forget their passwords and need to reset them if they use a very strong and secure password. 57% of respondents are neutral that is they neither agree that they share the passwords nor do they disagree. 17% of respondents agree that they share their passwords with their friends or relatives. Since there is considerable no. of respondents who share their passwords with friend's usage of password managers should be provoked. Nearly 34% of respondents were found to be confident about their passwords and did not use browser extensions for support, 51% of respondents neither agree nor disagree the same, this indicates that they were not aware of the option of browser extension for remembering passwords.

Nearly (79%) of respondents were not in the habit of changing passwords every month. Since awareness about the safety of passwords is very low, broad promotional strategies to sensitize the target population of both individuals and organizations should be taken up by the providers of Password Managers. Majority of respondents (83%) were found to be careless and do not logout of websites during their day to day browsing. Nearly 60% of the respondents were not aware of the precautionary steps of checking for SSL, this indicates majority of the internet users are ignorant of this precautionary step in browsing.

Table 3

Password Manager used by the respondents and the methods used by the respondents to keep track of their passwords - Chi-Square

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	126.197(a)	30	.000
Likelihood Ratio	104.948	30	.000
Linear-by-Linear Association	7.499	1	.006
N of Valid Cases	150		

Source: Primary data (at 5% level of significance)

From the above table it is inferred that that there is some that the Pearson Chi square is less than 0.05; this indicates that there is some relationship between password managers used by the respondents and the methods used by the respondents to keep track of their passwords. Hence reject the null hypothesis and accept the alternate hypothesis.

Table 4

Password Managers used by the respondents and the no of passwords the password manager remembers for the respondents – Chi square

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	170.150(a)	25	.000
Likelihood Ratio	89.452	25	.000
Linear-by-Linear Association	16.936	1	.000
N of Valid Cases	150		

Source: Primary data (at 5% level of significance)

From the above table, it is inferred there is some that the Pearson Chi square is less than 0.05; this indicates that there is some relationship between password managers the respondents use and the no. of passwords the password manager remembers for the respondents. Hence reject the null hypothesis and accept the alternate hypothesis.

Table 5

Age and passwords of the respondents – Chi Square

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	63.383(a)	44	.029
Likelihood Ratio	73.995	44	.003
Linear-by-Linear Association	2.229	1	.135
N of Valid Cases	150		

Source: Primary data(at 5% level of significance)

From the above table, it is inferred that there is some that the Pearson Chi square is less than 0.05; this indicates that there is some relationship between age and passwords of the respondents. Hence reject the null hypothesis and accept the alternate hypothesis

Table 6

Correlation between nature of the job of respondents and the attitude towards password security measures

		NATURE OF THE JOB OF THE RESPONDENT	ATTITUDE TOWARDS SECURITY MEASURES
NATURE OF THE JOB OF THE RESPONDENT	Pearson Correlation	1	.052
	Sig. (2-tailed)		.525
	N	150	150
Attitude towards security measures	Pearson Correlation	.052	1
	Sig. (2-tailed)	.525	
	N	150	150

Source: Primary data (at 5% level of significance)

From the above table, it is inferred that there is a significant correlation between nature of the job of respondents and the attitude towards security measures. It shows positive relationship between nature of the job of respondents and the password manager and its storage limits.

Table 7

Correlation between nature of the job of respondents and number of passwords used by respondents in their daily routine

		NATURE OF THE JOB OF THE RESPONDENT	NO. OF PASSWORDS THE RESPONDENTS REMEMBER
NATURE OF THE JOB OF THE RESPONDENT	Pearson Correlation	1	.071
	Sig. (2-tailed)		.389
	N	150	150
NO. OF PASSWORDS THE RESPONDENTS REMEMBER	Pearson Correlation	.071	1
	Sig. (2-tailed)	.389	
	N	150	150

From the above table it is interpreted that there is significant correlation between nature of the job of respondents and number of passwords used by respondents in their daily routine**.**It shows positive relationship between nature of the job of respondents and number of passwords used by respondents in their daily routine

Table 8

Correlation between nature of the job of respondents and methods used to keep track of their passwords

		NATURE OF THE JOB OF THE RESPONDENT	METHODS USED BY RESPONDENT TO KEEP TRACK OF PASSWORDS
NATURE OF THE JOB OF THE RESPONDENT	Pearson Correlation	1	-.080
	Sig. (2-tailed)		.330
	N	150	150

METHODS USED BY RESPONDENT TO KEEP TRACK OF PASSWORDS	Pearson Correlation	-.080	1
	Sig. (2-tailed)	.330	
	N	150	150

From the above table it is interpreted that there is significant correlation between nature of the job of respondents and the methods used to keep track of their passwords. It shows inverse relationship between nature of the job of respondents and the methods used to keep track of their passwords

Table 9

Correlation between password managers used by the respondents and the no. of password the password managers remembers for the respondents

		NO.OF PASSWORDS THE PASSWORD MANAGER REMEMBER FOR THE RESPONDENT	PASSWORD MANAGER THE RESPONDENT USE
NO.OF PASSWORDS THE PASSWORD MANAGER REMEMBER FOR THE RESPONDENT	Pearson Correlation	1	.337(**)
	Sig. (2-tailed)		.000
	N	150	150
PASSWORD MANAGER THE RESPONDENT USE	Pearson Correlation	.337(**)	1
	Sig. (2-tailed)	.000	
	N	150	150

From the above table it is interpreted that there is significant correlation between password managers used by the respondents and the no. of password the password managers remembers for the respondents.It shows positive relationship between password managers used by the respondents and the no. of password the password managers remembers for the respondents

6. RECOMMENDATIONS

Students should be sensitized with the benefit of password managers since considerable number of respondents especially students were confirmed to share password with their friends. Broad promotion strategies to sensitize the target population of both individual and organizations should be taken up by the providers of password managers since the awareness about the safety of password is very low. Majority of respondents are careless and ignorant of the precautionary steps like checking for SSL before entering password in a website, loging out of websites after use, setting strong and secure passwords and changing password every month. So they must be sensitized on having secure password managing practices.

7. CONCLUSION

The study done on behalf of ZOHO vault, Password Manager service provider, confirms a huge scope for promoting usage of passwords manager. This is mainly due to practices among the internet users that confirm a huge level of ignorance towards securing password manager system. Hence this study concludes that password manager providers need to sensitize the heavy internet browsers through appropriate awareness programs to reap on a huge market share.

REFERENCES:

1. Z. L., W. H., D. A., & D. S. (2014). The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. Retrieved August 22, 2014, from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/li_zhiwei
2. Karole, A., Saxena, N., & Christin, N. (2011). A Comparative Usability Evaluation of Traditional Password Managers. Information Security and Cryptology - ICISC 2010 Lecture Notes in Computer Science, 233-251
3. D. S., S. J., D. B., E. C., & C. J. (2014). Password Managers: Attacks and Defenses. Retrieved August 22, 2014, from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/silver
4. Zhao, R., Yue, C., & Sun, K. (2013). A Security Analysis of Two Commercial Browser and Cloud Based Password Managers. 2013 International Conference on Social Computing. http://inside.mines.edu/~chuanyue/papers/ASEScience13.pdf

5. D. M. (2013). password managers: comparative evaluation, design, implementation and empirical analysis (unpublished master's thesis). carleton university ottawa, ontario, canada.
6. D. C., R. C., S. G., H. L., & R. S. (2006). Systems and methods for recovering passwords and password-protected data
7. Stajano, F., Spencer, M., Jenkinson, G., & Stafford-Fraser, Q. (2015). Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers. Technology and Practice of Passwords Lecture Notes in Computer Science, 61-73.

*****