

An Empirical Assessment of the Role of Password Compliance

Iqbal Amiri
ia195@nova.edu
Nova Southeastern University

Jared Briggs
jb2669@nova.edu
Nova Southeastern University

Keywords

New password, Password-protected storage, Computer self-efficacy, Password structure, Confirmatory Factor Analysis, Goodness-of-fit, Cronbach Alpha.

Abstract

Password and password protection systems are the most frequently attacked security systems. However, passwords are considered the first line of defense in computer-based systems, when it comes to user authentication. The purpose of this study was to measure user's behaviors and their adherence to password compliance when organizations change to a new password policy. This study also identified how users protected and stored their passwords. The instrument used for this study was a survey, which collected data from 60 participants. The survey collected data, how users created new passwords, and how users protected their passwords. Pre-screening was performed for Mahalanobis Distance and descriptive statistics prior to analysis. The data was analyzed for confirmatory factor analysis, and Cronbach Alpha if items would be deleted. End user computer skills and password-protected storage were found to influence password structure. Future research could include a larger sample size and include the entire population beyond information technology.

Introduction

According to Shay, Komanduri, Kelley, Leon, Mazurek, Bauer, Christin, and Cranor (2010), one of the fundamental problems in computer security is how to authenticate a user to a computer system conveniently and securely. Passwords are a defense mechanism that a user uses in an authentication system. Taneski, Henrico, and Brunmen (2014) described that 86% of the passwords used are weak, and that passwords are often created with an inadequate amount of characters that usually contain only lowercase letters, or numerical content, along with dictionary based password. Thus, making the passwords easy targets to security threats. Adeka, Shepherd, and Abd-Alhameed (2013) described that 50% of users wrote their passwords down. Gehringer (2012) suggested users to not write their password because it posed as a security risk, and the paper could be lost, or read by a bystander.

Research Questions and Hypotheses

RQ1: Does computer self-efficacy exert a significant positive influence on password structure?

RQ2: Does end user computer skills exert a significant positive influence on password structure?

RQ3: Does new password exert a significant positive influence on password structure?

RQ4: Does password protected-storage exert a significant positive influence on password structure?

RQ5: Does computer self-efficacy exert a significant positive influence on password protected-storage?

H1: Computer self-efficacy will exert a positive influence on password structure.

H2: End user computer skills will exert a positive influence on password structure.

H3: New password will exert a positive influence on password structure.

H4: Password protected-storage will exert a positive influence on password structure.

H5: Computer self-efficacy will exert a positive influence on password protected-storage.

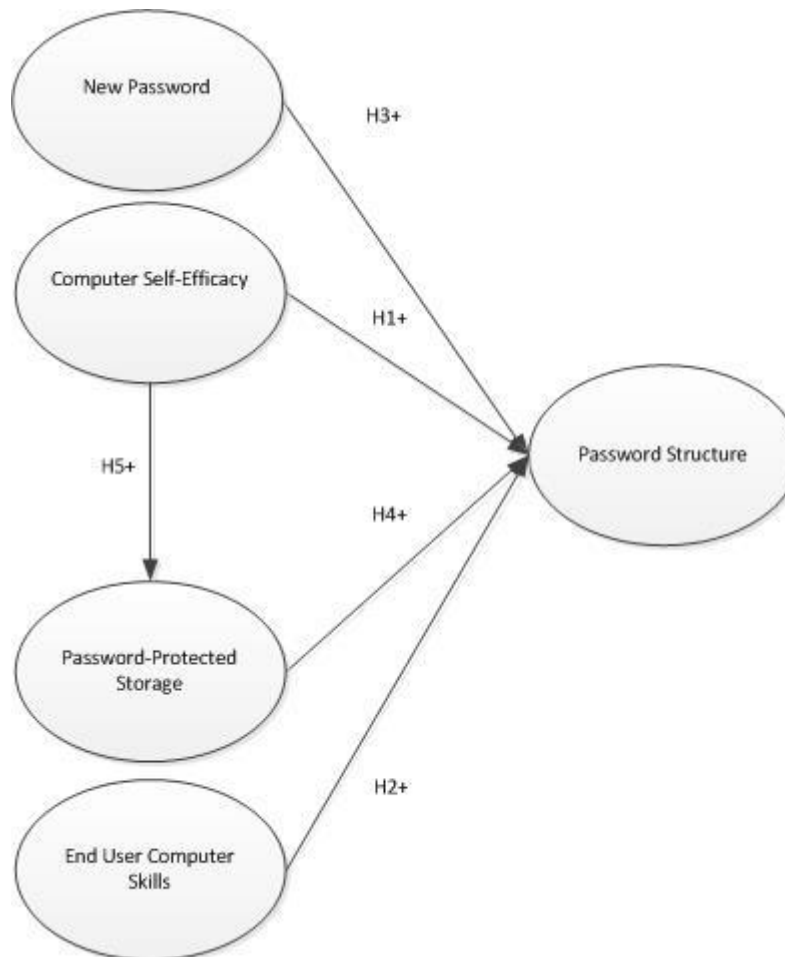


Figure 1. Conceptual Research Map

Methodology

An online survey instrument was developed and used to collect data for password storage, password compliance, and user sentiments about the new password requirements. The unit of analysis was individual, specifically – employees of an information technology (IT) organization. A 7-point Likert scale was chosen from a previous study conducted by Levy and Green (2009) to collect responses to questions, which was adapted by Gefen, Straub, and Boudreau (2000) where 7-Strongly Agree to 1-Strongly Disagree. This study was cross-sectional, as the survey and data were collected one time only, instead of longitudinal. Convenience sampling was used; participants were selected from coworkers and friends, which worked in IT organizations in getting the results for the survey. A pilot

study was conducted with 15 users to make sure the survey instrument was working correctly.

Results

This study concluded that there were five multivariate outliers present from raw data constructs of new password (NP), password-protected storage (PPS), computer self-efficacy, (CSE), end user computer skills (EUCS) and. The outliers exceeded the critical value of 50.998 of Chi-squared degrees of freedom, from cases 112, 113, 114, 115, and 125 (see Appendix B1 Mahalanobis Distance). Mahalanobis Distance was calculated from the critical value of chi-square at $p < .005$ with $df = 36$ is 50.998 (Mertler & Vannatta, 2013). Frequencies were run to ensure the constructs did not contain missing data. Confirmatory factor analysis (CFA) was conducted using structure equation modeling (SEM) with Amos statistical software package (Levy & Green, 2009). The five hypotheses were tested for model-fit with the following measures analyzed: goodness-of-fit (GFI), Chi-square/degrees of freedom (Chi-square/df), adjusted goodness-of-fit (AGFI), normalized fit index (NFI), comparative fit index (CFI), root mean square error approximation (RMSEA), and standardized root mean square residual (SRMSR) (see Appendix B4 Model Fit). The results from GFI were 0.554, which indicated a poor fit. The results of Chi-square/df were 3.19, which indicated an acceptable level because Chi-square/df was less than 5.0. AGFI resulted an unacceptable level for model fit with the value of 0.493 with a recommended value of $>.80$ (Levy & Green, 2009). NFI resulted an unacceptable level for model fit with the value of 0.577 with a recommended value of $>.90$ (Levy & Green, 2009). CFI resulted an unacceptable level for model fit with the value of 0.633 with a recommended value of $>.90$ (Levy & Green, 2009). RMSEA resulted unacceptable level for model fit with the value of 0.124 with a recommended value of $>.10$. SRMSR resulted an unacceptable level for model fit with the value of 0.555 with a recommended value of $>.10$ (Levy & Green, 2009). The significance was found to be a poor fit with the model with a value of $p < 0.001$ (see Appendix B4 P-Value). RMSEA analysis also provided a significance value (PCLOSE) of $p < 0.001$, which result in a poor fit (see Appendix B5 Significance PCLOSE). A path diagram was created with Amos to determine strengths of influence with covariance (see Appendix B6 Path Diagram). EUCS was determined to significantly influence password structure with value of 0.71. PPS was determined to significantly influence password structure with value of 0.11. CSE CSE, and NP did not have a significant influence on PS with values of -0.03, and -0.04. CSE did not have a significant influence on PPS with a value of -0.29. Cronbach alpha value for the component one EUCS was 0.966 (see Appendix B7 Cronbach Alpha). Cronbach alpha value for the component two PPS was 0.608. Cronbach alpha value for the component three PS was 0.799. Cronbach alpha value for the construct NP was 0.436. Cronbach alpha value for the construct CSE was 0.892.

Discussion

The data for the constructs of CSE, NP, PS, PPS and EUCS (end-user computer skills) contained one multivariate outlier above the 75th percentile (see Appendix B2 Mahalanobis Distance Figure). Mahalanobis Distance was calculated based on distance from the centroid (mean of all variables) (Mertler & Vannatta, 2013). “Analysis of instrument reliability indicated high Cronbach’s alpha for” three of the instrument constructs: end user computer skills, password structure, and computer self-efficacy (Levy & Green, 2009 p.16). The values of Cronbach’s alpha were greater than the recommended value, which indicated good reliability (Levy & Green, 2009). The overall results of the goodness-of-fit were found to be a poor fit for the model in this study. The results concluded, all of the tests except Chi-square/df to be unacceptable with very little significance. The hypotheses were found significant when PPS positively influenced PS,

and when EUCS positively influenced PS (see Appendix B8 SEM Figure). The remaining hypotheses of CSE positively influenced PS, CSE positively influenced PPS, and NP positively influenced PS were rejected with negative values (see Appendix B8 SEM Figure).

Conclusion

As mentioned by Levy and Ellis (2006) that the main definitional components of research is the ability to add to the current body of knowledge, thus it is believed that this research will contribute to the body of knowledge on password security and policy compliance. Resistance to password change was affected by computer self-efficacy and password-protected storage. Confirmatory factor analysis was performed using structured equation modeling using Amos software. Goodness-of-fit analysis tests found the model to be a poor or unacceptable fit. Cronbach Alpha was conducted as a secondary test, which found components one, three, and five to be reliable, components two and four were not. Computer self-efficacy, and new password hypotheses in relation to construct password structure were rejected due to negative significance. End user computer skills and password-protected storage were found to positively significantly influence password structure, which validated the hypotheses.

References

- Adeka, M., Shepherd, S., & Abd-alhameed, R. (2013, January). Resolving the password security purgatory in the contexts of technology, security and human factors. *2013 International Conference on Computer Applications Technology (ICCAT)*, 1-7.
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.
- Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, 4(1), 7.
- Gehringer, E.F. (2012). Choosing passwords: Security and human factors. *2012 International Symposium on Technology and Society (ISTAS'12)*, 369-373.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, 51(4), 1664-1675.
- Levy Y., & Ellis T. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*. 9, 181-208.
- Levy, Y., & Green, B. D. (2009). An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of a U.S. navy combat information system. *Journal of Organizational and End User Computing*, 21(3), 11-13.
- Mertler, C., & Vannatta, R. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (Fifth ed.). Glendale, CA: Pyrczak Publishing.
- Raschke, R. L., Krishen, A. S., Kachroo, P., & Maheshwari, P. (2013). A combinatorial optimization based sample identification method for group comparisons. *Journal of Business Research*, 66(9), 1267-1269.

- Reid, M., & Levy, Y. (2008). Integrating trust and computer self-efficacy with TAM: An empirical assessment of customers' acceptance of banking information systems (BIS) in Jamaica. *Journal of Internet Banking and Commerce, 12*(3), 2008-12.
- Sekaran, U. & Bougie, R. (2013). Research methods for business: A skill building approach (6th ed.). West Sussex, UK: John Wiley & Sons
- Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., & Cranor, L. F. (2010, July). Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2, 1- 20.
doi:dx.doi.org/10.1145/1837110.1837113
- Taneski, V., Hericko, M., & Brumen, B. (2014, May). Password security - No change in 35 years? *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1360-136

Appendix A: Password Security Assessment Survey

Link to the survey:

https://docs.google.com/forms/d/1gT8M-YPfeh-4d5jeUE97kkePkRT0UH-DiGrGD5Fi_-Y/edit#

Appendix A.1: Password Security Assessment Survey

Password Security Assessment Survey

Dear Participant,

We, Iqbal Amiri and Jared Briggs are doctoral students from Nova Southeastern University pursuing PhD in Information Systems and for one of our courses we are seeking some anonymous input to some survey questions based on passwords and password compliance issues/motivations. The survey relates to understanding the factors that lead users to comply with password guidelines. Responses to the survey are completely anonymous, thus we will be neither collecting nor storing any personal identifiable information.

It will be really helpful if you could spare some time in completing this short survey on password compliance.

If you have any questions, you can reach us at iamiri@gmail.com - Iqbal Amiri or briggs.jared@gmail.com - Jared Briggs.

Thank you in advance for your participation in this survey.

Please rate the following questions using the following scale:

- 1 – Strongly disagree
- 2 – Disagree
- 3 – Somewhat disagree
- 4 – Neither agree or disagree
- 5 – Somewhat agree
- 6 – Agree
- 7 – Strongly agree

Thanks and Regards,
Jared and Iqbal

* Required

Computer Self-Efficacy

Please use the scale from (1) Strongly Disagree to (7) Strongly Agree

*

	1.Strongly Disagree	2.Disagree	3.Somewhat Disagree	4.Neither Agree or Disagree	5.Somewhat Agree	6.Agree	7.Strongly Agree
CSE1. I am able to work with computers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CSE2. If I am given some training, I can learn to use most computer programs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CSE3. I can learn to use most computer programs just by reading the manuals and help	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Appendix A.2: Password Security Assessment Survey

End-User Computer Skills

★

	1.No skill or ability	2.I'm now learning this skill	3.I can do this skill with some help from a supervisor	4. I am a competent performer in this area	5.I am an outstanding performer in this area	6.I am an exceptional performer in this area	7.I am an expert and/or leader in this area
EUCS1. I am able to design output format for password compliance systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS2. I am able to asses system needs or evaluate system features for password compliance systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS3. I am able to design input forms/screens for password compliance systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS4. I am able to define my own information requirements for password systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS5. I am able to provide the system designer(s) with information/knowledge required to develop a password compliance system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS6. I am able to use advanced programming languages	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS7. I am able to create my own application for password compliance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS8. I have knowledge of am able to use databases	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS9. I have knowledge of am able to use operating systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS10. I have knowledge of am able to use hardware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS11. I have knowledge of am able to use packages application software	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
EUCS12. I have knowledge of am able to use mainframes and its operating system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Appendix A.3: Password Security Assessment Survey

New Password

Please use the scale from (1) Strongly Disagree to (7) Strongly Agree

★

	1.Strongly Disagree	2.Disagree	3.Somewhat Disagree	4.Neither Agree or Disagree	5.Somewhat Agree	6.Agree	7
NP1. Creating a password that meets the new requirements was annoying	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
NP2. Creating a password that meets the new requirements was fun	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
NP3. Creating a password that meets the new requirements was difficult.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
NP.4 With the new password requirements, my account is more secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
NP5. Any added protection provided by the new password is worth the added effort of creating/remembering/using it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Appendix A.4: Password Security Assessment Survey

Password Structure

Please use the scale from (1) Strongly Disagree to (7) Strongly Agree

*

	1.Strongly Disagree	2.Disagree	3.Somewhat Disagree	4.Neither Agree or Disagree	5.Somewhat Agree	6.Agree	7.Strongly Agree
PS1. My passwords are based on the first letter of each word in a phrase	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS2. My passwords are based on the name of someone or something	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS3. My passwords are based on a word or name with numbers / symbols added to beginning or end	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS4. My passwords are based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS5. My passwords are based on a word or name with letters missing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS6. My passwords are based on a word in a language other than English	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS7. My passwords are based on a phone number	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS8. My passwords are based on an address.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PS9. My passwords are as on a birthday's	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Appendix A.5: Password Security Assessment Survey

Password Protected Storage

Please use the scale from (1) Strongly Disagree to (7) Strongly Agree

★

	1.Strongly Disagree	2.Disagree	3.Somewhat Disagree	4.Neither Agree or Disagree	5.Somewhat Agree	6.Agree	7.Strongly Agree
PPS1. I always write down my current password	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPS2. I always write down my old password.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPS3. I store my password on a computer or device protected with another password.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPS4. I store my password in an encrypted file or application	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPS5. I store my password on a paper.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPS6. I always keep my password with me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPS7. I always protect my password.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PPU8. I always hide my password.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Appendix A.6: Password Security Assessment Survey

Demographics Information

What is your gender *

- ☐ Male
- ☐ Female

What is your age *

- ☐ 1) 18 or under
- ☐ 2) 19-24
- ☐ 3) 25-34
- ☐ 4) 35-44
- ☐ 5) 45-54
- ☐ 6) 55-64
- ☐ 8) 65 or older

Highest academic level achieved *

- ☐ 1) Highschool
- ☐ 2) AA/AS
- ☐ 3) BS/BA
- ☐ 4) MA/MS
- ☐ 5) Post graduate
- ☐ 6) Ph.D./MD/JD
- ☐ 7) Other


How many years have you been in your current organization? *

- ☐ 1) Less than 5
- ☐ 2) 5-9
- ☐ 3) 10-14
- ☐ 4) 15-19
- ☐ 5) 20 or more years

How many years have you been using computers? *

- ☐ 1) Less than 5
- ☐ 2) 5-9
- ☐ 3) 10-14
- ☐ 4) 15-19
- ☐ 5) 20 or more years

Submit

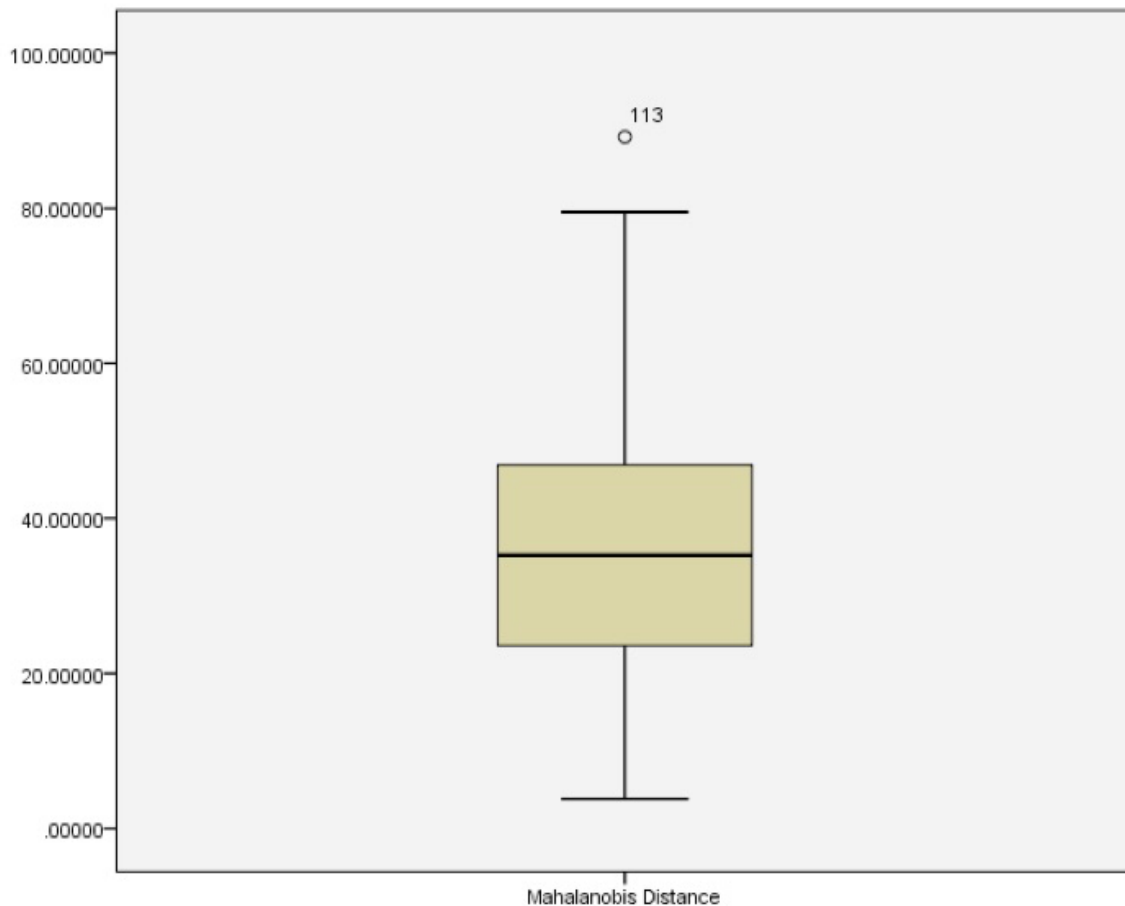

100%: You made it.

Appendix B: Figures

B1. Mahalanobis Distance

Extreme Values					
		Case Number	Value		
Mahalanobis Distance	Highest	1	113	89.20494	
		2	112	79.51344	
		3	125	78.70815	
		4	114	76.61729	
		5	115	75.48996	

B2. Mahalanobis Distance Figure



B3. Model Fit

A	B	C	D
Goodness-of-Fit Measure (n=141)	Recommended Value*	Values from this study	Levy & Green (2009)
Chi-Square (χ^2)		1942.744	112.2
Degrees of freedom		619	70
Chi-square/df	<3.0	3.139	1.161
Goodness-of-Fit Index (GFI)	>.90	0.554	0.94
Adjusted Goodness-of-Fit (AGFI)	>.80	0.493	0.9
Normalized Fit Index (NFI)	>.90	0.577	0.94
Comparative Fit Index (CFI)	>.90	0.663	0.98
Root Mean Square Error Approximation (RMSEA)	<.10	0.124	0.05
Standardized Root Mean Square Residual (SRMSR)	<.10	0.555	Not Reported

B4. Significance P-Value

Model Fit Summary

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	84	1942.744	619	.000	3.139
Saturated model	703	.000	0		
Independence model	37	4598.062	666	.000	6.904

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.555	.554	.493	.487
Saturated model	.000	1.000		
Independence model	1.284	.217	.174	.206

Baseline Comparisons

Model	NFI	RFI	IFI	TLI	CFI
	Delta1	rho1	Delta2	rho2	
Default model	.577	.545	.667	.638	.663
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

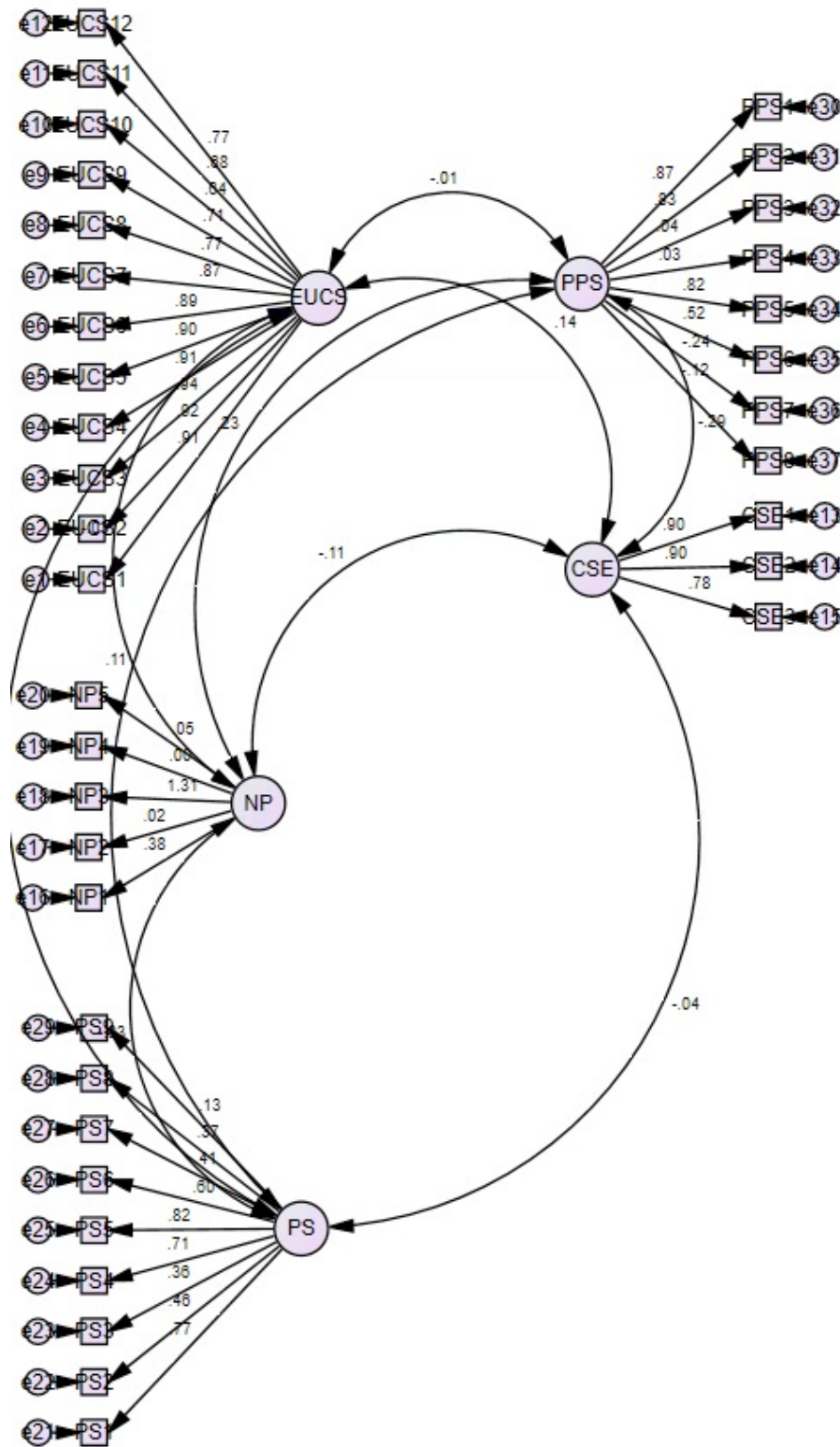
B5. Significance PCLOSE

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.124	.117	.130	.000
Independence model	.205	.200	.211	.000

AIC

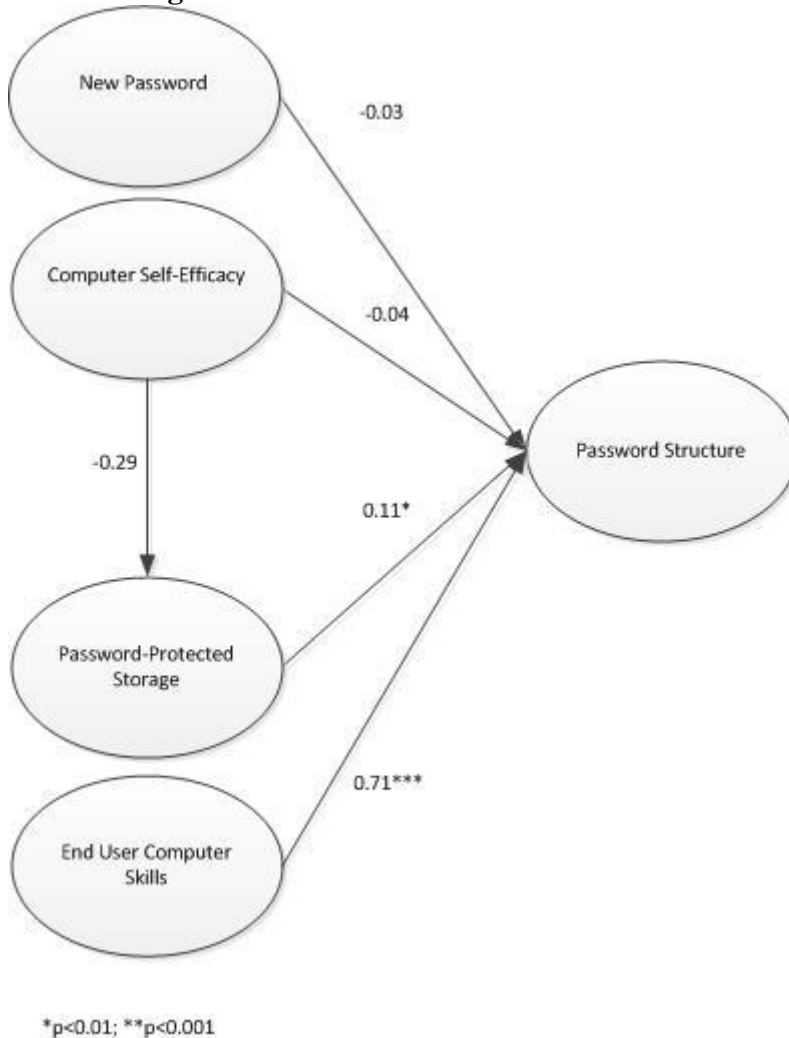
B6. Path Diagram



B7. Cronbach Alpha

	A	B	C	D	E	F	G	H
1								
2			Rotated Component Matrixa					
3	Component Name		Components					
4			1	2	3	4	5	Chronbach Item if deleted
5	EUCS	EUCS6	0.886	0.019	0.169	0.019	0.064	0.961
6		EUCS3	0.877	0.037	0.252	-0.056	0.001	0.961
7		EUCS5	0.871	0.038	0.151	-0.024	-0.009	0.962
8		EUCS2	0.869	0.056	0.235	-0.051	-0.048	0.961
9		EUCS4	0.866	0	0.193	-0.073	0.047	0.962
10		EUCS1	0.865	0.086	0.157	-0.158	0.096	0.962
11		EUCS8	0.838	-0.023	0.002	0.131	0.072	0.963
12		EUCS7	0.828	0.113	0.282	-0.042	-0.009	0.962
13		EUCS12	0.821	0.111	0.055	-0.071	0.038	0.963
14		EUCS9	0.808	-0.105	-0.049	0.182	0.145	0.964
15		EUCS11	0.79	-0.126	-0.129	0.155	0.131	0.965
16		EUCS10	0.751	-0.18	-0.122	0.249	0.205	0.966
17		PPS4	0.48	-0.088	0.349	0.27	-0.36	0.587
18	PPSPSNP	PPS1	-0.095	0.774	-0.136	0.136	-0.12	0.533
19		PPS2	0.078	0.772	-0.065	0.007	-0.199	0.54
20		PPS5	0.055	0.724	-0.086	0.022	-0.103	0.547
21		PS9	-0.128	0.698	0.197	-0.1	0.025	
22		PS7	0.197	0.698	0.234	-0.236	-0.207	0.795
23		PS8	0.139	0.688	0.266	-0.229	-0.004	0.795
24		PPS6	0.032	0.551	-0.026	0.028	-0.287	0.567
25		NP3	-0.013	0.496	-0.212	0.023	0.034	0.352
26		NP2	-0.122	0.333	0.139	-0.089	0.014	0.517
27		PS4	0.392	-0.106	0.696	0.091	-0.029	0.757
28	PS	PS6	0.289	0.04	0.62	-0.07	-0.11	0.768
29		PS2	0.066	0.188	0.59	0.068	0.194	0.784
30		PS3	0.035	-0.066	0.584	0.237	0.136	0.797
31		PS5	0.552	0.121	0.576	-0.047	-0.05	0.746
32		PS1	0.552	0.039	0.569	-0.015	-0.174	0.758
33		NP1	0.105	0.247	-0.26	0.058	0.113	0.443
34	PPSPNP	PPS7	0.078	-0.253	-0.046	0.732	0.117	0.629
35		PPS8	0.069	-0.148	-0.082	0.728	0.019	0.617
36		NP5	-0.039	0.107	0.131	0.71	0.123	0.299
37		NP4	-0.108	0.106	0.132	0.664	0.166	0.257
38		PPS3	0.377	-0.05	0.254	0.422	-0.172	0.57
39	CSE	CSE2	0.088	-0.179	0.047	0.178	0.843	0.817
40		CSE1	0.09	-0.218	-0.038	0.122	0.841	0.828
41		CSE3	0.247	-0.178	0.055	0.125	0.787	0.899
42	Cumulative Variance		29.18%	43.18%	49.98%	56.30%	61.41%	
43	Chronbach's Alpha		0.966	0.608	0.799	0.436	0.892	
44								
45								
46	Extraction Method: Principal Component Analysis.							
47	Rotation Method: Varimax with Kaiser Normalization.							
48	a Rotation converged in 8 iterations.							

B8. SEM Figure



Appendix C: SPSS Syntax

C1. Mahalanobis Distance

DATASET NAME DataSet1 WINDOW=FRONT.

REGRESSION

/MISSING LISTWISE

/STATISTICS COEFF OUTS R ANOVA

/CRITERIA=PIN(.05) POUT(.10)

/NOORIGIN

/DEPENDENT ID

/METHOD=ENTER CSE1 CSE2 CSE3 EUCS1 EUCS2 EUCS3 EUCS4 EUCS5 EUCS6 EUCS7
EUCS8 EUCS9 EUCS10 EUCS11

EUCS12 NP1 NP2 NP3 NP4 NP5 PS1 PS2 PS3 PS4 PS5 PS6 PS7 PS8 PS9 PPS1 PPS2 PPS3
PPS4 PPS5 PPS6 PPS7

PPS8

/SAVE MAHAL.

C2. Mahalanobis Distance Extremes

EXAMINE VARIABLES=MAH_1

/PLOT BOXPLOT STEMLEAF

/COMPARE GROUPS

/STATISTICS DESCRIPTIVES EXTREME

/CINTERVAL 95

/MISSING LISTWISE

/NOTOTAL

C3. PCA

FACTOR

/VARIABLES CSE1 CSE2 CSE3 NP1 NP2 NP3 NP4 NP5 PS1 PS2 PS3 PS4 PS5 PS6 PS7 PS8 PS9
PPS1 PPS2 PPS3

PPS4 PPS5 PPS6 PPS7 PPS8 EUCS1 EUCS2 EUCS3 EUCS4 EUCS5 EUCS6 EUCS7 EUCS8
EUCS9 EUCS10 EUCS11 EUCS12

/MISSING LISTWISE

/ANALYSIS CSE1 CSE2 CSE3 NP1 NP2 NP3 NP4 NP5 PS1 PS2 PS3 PS4 PS5 PS6 PS7 PS8 PS9
PPS1 PPS2 PPS3

PPS4 PPS5 PPS6 PPS7 PPS8 EUCS1 EUCS2 EUCS3 EUCS4 EUCS5 EUCS6 EUCS7 EUCS8
EUCS9 EUCS10 EUCS11 EUCS12

/PRINT INITIAL EXTRACTION ROTATION

/FORMAT SORT

/PLOT EIGEN

/CRITERIA FACTORS(5) ITERATE(25)

/EXTRACTION PC

/CRITERIA ITERATE(25)

/ROTATION VARIMAX

/METHOD=CORRELATION.

C6. Cronbach Alpha CSE

RELIABILITY

/VARIABLES=CSE1 CSE2 CSE3

/SCALE('ALL VARIABLES') ALL

/MODEL=ALPHA

```
/STATISTICS=DESCRIPTIVE SCALE  
/SUMMARY=TOTAL.
```

C7. Cronbach Alpha EUCS

RELIABILITY

```
/VARIABLES=EUCS1 EUCS2 EUCS3 EUCS4 EUCS5 EUCS6 EUCS7 EUCS8 EUCS9 EUCS10  
EUCS11 EUCS12  
/SCALE('ALL VARIABLES') ALL  
/MODEL=ALPHA  
/STATISTICS=DESCRIPTIVE SCALE  
/SUMMARY=TOTAL.
```

C8. Cronbach Alpha NP

RELIABILITY

```
/VARIABLES=NP1 NP2 NP3 NP4 NP5  
/SCALE('ALL VARIABLES') ALL  
/MODEL=ALPHA  
/STATISTICS=DESCRIPTIVE SCALE  
/SUMMARY=TOTAL
```

C9. Cronbach Alpha PS

RELIABILITY

```
/VARIABLES=PS1 PS2 PS3 PS4 PS5 PS6 PS7 PS8 PS9  
/SCALE('ALL VARIABLES') ALL  
/MODEL=ALPHA  
/STATISTICS=DESCRIPTIVE SCALE  
/SUMMARY=TOTAL.
```

C10. Cronbach Alpha PPS

RELIABILITY

```
/VARIABLES=PPS1 PPS2 PPS3 PPS4 PPS5 PPS6 PPS7 PPS8  
/SCALE('ALL VARIABLES') ALL  
/MODEL=ALPHA  
/STATISTICS=DESCRIPTIVE SCALE  
/SUMMARY=TOTAL.
```