

Factors Affecting Identity Theft Anxiety Level in College Students

Dr. Sushma Sanga, Bosch Inc

Dr. Ali Eydgahi, Eastern Michigan University

Ali Eydgahi started his career in higher education as a faculty member at the Rensselaer Polytechnic Institute in 1985. Since then, he has been with the State University of New York, University of Maryland Eastern Shore, and Eastern Michigan University. During 2006-2010, he was Chair of the Department of Engineering and Aviation Sciences, Founder and Director of the Center for 3-D Visualization and Virtual Reality Applications, and Technical Director of the NASA funded MIST Space Vehicle Mission Planning Laboratory at the University of Maryland Eastern Shore. In 2010, he joined Eastern Michigan University as an Associate Dean in the College of Technology and currently is a Professor in the School of Engineering Technology. He has an extensive experience in curriculum and laboratory design and development. Dr. Eydgahi has served as a member of the Board of Directors for Tau Alpha Pi, as a member of Advisory and Editorial boards for many International Journals in Engineering and Technology, as a member of review panel for NASA and Department of Education, as a regional and chapter chairman of IEEE, SME, and ASEE, and as a session chair and as a member of scientific and international committees for many international conferences.

Factors Affecting Identity-Theft Anxiety Level in College Students

Abstract

Each year, millions of Americans are becoming the victims of identity-theft and this is one of a number of serious, growing and widespread issues. Examining the factors that affect anxiety levels of identity-theft victims and determining whether there is any significant relationship between these factors are an important issue.

In this paper, a research model is presented to determine whether electronic devices self-efficacy, electronic devices usage and information security awareness are the main and direct factors that affect identity-theft anxiety level in college students. This study performed several analyses on a developed questionnaire to ensure validity and reliability. After examining all proposed hypotheses, it was found that electronic devices self-efficacy and electronic devices usage have significant impact on identity-theft anxiety level of the students. The data also support a relationship between information security awareness of the students and their identity-theft anxiety level. This research also showed that gender, employment status, race, and age have moderating effects on all hypotheses. The outcome of this study indicated that more information should be provided to students regarding how to take proactive measures in using their electronic devices in order to avoid identity-theft.

Introduction

Identity-theft means stealing someone's personal information and using it without their permission. The list of consumer complaints received by the Federal Trade Commission in 2011 [1] indicates that for the 12th year in a row, identity-theft complaints are in the top of the list. Among 1.8 million complaints that were filed in 2011, 279,156 or 15% were identity-theft complaints. Nearly 25% of the identity-theft complaints were related to tax or wage-related fraud [1]. In December 2010, the United States Bureau of Justice Statistics announced that about 11.7 million people were the victims of identity theft, which constitutes five percent of people age 16 or older in the U.S. [2]. In 2007, identity-theft was on the list of the top ten consumer complaints to the Federal Trade Commission. According to Paganini [3] in the

FBI report of scams in 2011, identity-theft was in second place and had jumped from the top ten crimes in 2007 to the top two in 2011, which obviously must be considered as a serious issue. The Federal Trade Commission report [4] shows that identity-theft was the number one complaint category in the Consumer Sentinel Network for calendar year 2014 with thirteen percent of the overall complaints.

Government documents/benefits fraud (39%) was the most common form of reported identity-theft, followed by credit card fraud (17%), phone or utilities fraud (13%), and bank fraud (8%). Other significant categories of identity-theft reported by victims were employment-related fraud (5%) and loan fraud (4%). Thirty-two percent of identity-theft complainants reported they contacted law enforcement. Of those victims, eighty-eight percent indicated a report was taken. Florida is the state with the highest per capita rate of reported identity-theft complaints, followed by Washington and Oregon [4].

A six-factor computer anxiety model has been developed [5] that consists of computer literacy of basic computer skills, self-efficacy on learning how to use computers, physical awareness while using computers such as breathing or sweating, attitudes toward computers, positive belief regarding the benefits of computers to society, and negative beliefs on effects of computers.

While there is little information on the perceptions and awareness that college/university students have about identity theft, considerable research has been done with this group on a range of crime and justice-related topics.

A review of the literature shows a lack of studies on the perception held by college/university students about identity-theft [6] and there has been a void in research related to information security awareness and identity-theft anxiety levels among students [5]. Also, there has been a void in literature review related to electronic devices self-efficacy.

Thus, with increasing identity-theft complaints and with very little research in this area on higher education students, this study investigated the effect of electronic devices usage, electronic devices self-efficacy and information security awareness on identity-theft anxiety

level among college students in southeast Michigan. Also, grade level, gender, age and race of the students were examined to determine whether they have any influence on these relationships. The impact of these factors on identity-theft anxiety level has not been tested in prior research using descriptive methodology.

Methodology

In this research, quantitative methodology was used by utilizing an electronically distributed survey, as presented in the appendix, to measure each construct of the research model utilizing the six-factor computer anxiety model that was developed in [5]. The six factors in computer anxiety model are computer literacy of basic computer skills, self-efficacy on learning how to use computers, physical awareness while using computers such as breathing or sweating, attitudes toward computers, positive belief regarding the benefits of computers to society, and negative beliefs on effects of computers.

A sample of 187 students from a university located in southeast of Michigan was considered and a purposive sampling method was used. Cross-sectional or correlation analysis was utilized to examine the research questions. The followings are the hypotheses examined in this study:

- H1. There is a positive effect of electronic devices self-efficacy on identity-theft anxiety level among students in southeast of Michigan.
- H2. There is a positive effect of electronic devices usage on identity-theft anxiety level among students in southeast of Michigan.
- H3. There is a positive effect of information security awareness on identity-theft anxiety level among students in southeast of Michigan.
- H4. Educational level of students and electronic devices self-efficacy are in a positive relationships with identity-theft anxiety level among students in southeast of Michigan.
- H5. Educational level of students and information security awareness are in a positive relationship with identity-theft anxiety level among students in southeast of Michigan.
- H6. Educational level of students and electronic devices usage are in a positive relationship with identity-theft anxiety level among students in southeast of Michigan.

Instrument

This study consisted of three independent variables and one dependent variable. The dependent variable was anxiety level caused by fear of identity-theft. The independent variables were electronic devices self-efficacy, electronic devices usage and information security awareness. Age, gender, race, and educational level were used as demographical variables, which could be considered as covariates. The survey used a 7-point Likert scale with the ratings of strongly agree, agree, slightly agree, neither agree nor disagree, slightly disagree, disagree, and strongly disagree for anxiety, electronic devices self-efficacy and information security awareness variables.

Demographic Characteristics of the Sample

The demographics analysis of the participants are presented in Tables 1 – 5 that include gender, age, educational level, race, and device ownership.

Table 1: Gender of the Participants

Gender	Male (82) 43.9%	Female (105) 56.1%
---------------	--------------------	-----------------------

Table 2: Age of the Participants

Age	Frequency	Percent	Cumulative Percent
< 19	7	3.7%	7%
20 - 29	110	58.8%	110%
30 - 39	37	19.8%	37%
40 - 49	18	9.6%	18%
50 - 59	12	6.4%	12%
> 60	3	1.6%	3%
Total	187	100.0%	

Table 3: Educational Level of the Participants

Educational level	Frequency	Percent	Cumulative Percent
Undergraduate	92	49.2%	49.2%
Graduate	75	40.1%	89.3%
Doctoral	20	10.7%	100.0%
Total	187	100.0%	

Table 4: Race of the Participants

Race	Frequency	Percent	Cumulative Percent
American Indian/Native American	2	1.1%	1.1%
African American	10	5.3%	6.4%
Asian	25	13.4%	19.8%
Hispanic/Latino	13	7.0%	26.7%
White/Caucasian	126	67.4%	94.1%
Other	11	5.9%	100.0%
Total	187	100.0%	

Table 5: Device Ownership of the Participants

Device Ownership	Frequency	Percent
Netbook	11	5.9%
Desktop	58	31%
Laptop	170	90.9%
Mobile phone	125	66.8%
Internet enabled mobile device (Smartphone, tablet, etc.)	144	77%
Dedicated e-book device (Kindle, Nook, Sony Reader, etc.)	43	23%
None of the above	8	4.3%
All the above	2	1.1%

For electronic devices usage, the survey provided multiple checkbox options as Likert scaling is designed to measure people's attitudes and awareness [7]. The analysis of device

usage are shown in Table 6.

Table 6: Device Usage of the Participants

Device Usage	Options Frequency				
	Always	Frequently	Occasionally	Rarely	Never
Social Networking	91	55	20	13	8
Reading content (e-books, articles, etc.)	49	72	48	15	3
Accessing email	148	38	1	0	0
Text messaging	130	43	6	5	3
Searching for Information	133	51	3	0	0
Getting directions	97	63	20	7	0
Playing content	63	47	41	25	11
Listening to music/Watching videos	80	57	34	14	2
Banking	68	62	38	14	5
Filing Taxes	34	25	30	26	72
Shopping	32	64	56	26	9
Utility billing	58	43	32	15	39
News	64	73	32	12	6
Weather	87	66	21	7	6
Research	81	66	25	9	6
School Work	105	55	15	7	5
Company Work	68	35	18	27	39
Medical Bill	27	25	31	37	67

Analysis

A survey questionnaire was designed to measure each construct of the research model. Out of 251 students who participated in the survey, only 187 completed the entire survey. Thus, only complete responses were used for data analysis and all incomplete responses were excluded. Survey Monkey was used to collect the information and SPSS, Minitab, Statgraphics Centurion

software were used to analyze the collected data. The statistical analysis of the surveyed data using different techniques included reliability analysis, normality testing, distribution fitting, factor analysis, validity, and hypothesis testing.

The Cronbach's alpha coefficient was used to estimate the reliability and internal consistency. As shown in Table 7, all Cronbach's alpha values for the variables were over 0.7, which indicate that all of the items had good reliability and internal consistency.

Table 7: Reliability Analysis

Variable	Valid	Number of items	Cronbach's alpha
Anxiety level	187	15	0.836
Electronic device self-efficacy	187	8	0.885
Information security awareness	187	16	0.843
Electronic device usage	187	18	0.931

Since Likert scale data is ordinal and is not normally distributed, for non-normal distributions of location and scale, Minitab software was used to compute the descriptive statistics of each construct. Data normality was tested using best-fit distribution tests to determine whether the data was normally-distributed. Generalized Linear Model analysis was used to test the hypotheses and was utilized to analyze the relationships between dependent variable and the independent variables.

The best-fit distributions of scale and location values for the 15-level ITAL response (ITAL1-ITAL15), 8-level EDSE response (EDSE1-EDSE8), 16-level ISA response (ISA1-ISA16) and 18-level EDU response (EDU1-EDU18) were the intrinsic distribution parameters for non-normal distributions. They served the same purpose as the mean and standard deviation for normally-distributed data.

Likert scale numerical values could not be created for ISA1, ISA2, ISA3, ISA4, ISA5, ISA6, ISA7 and ISA8 as they are attributes, not ordinal. They were used as independent variables

in Generalized Linear Model analyses. According to the comparison of alternative distributions log likelihood statistics for anxiety level, electronic devices self-efficacy, electronic devices usage and information security awareness, the best fitting distribution is the smallest extreme value distribution.

As the data clearly seemed not to be normal, the Box-Cox transformation procedure was used to transform and normalize the data. The procedure is termed a variance stabilizing transform as it causes data to be more normally distributed. The Box-Cox λ normalized values are presented in Table 8. It should be noted that the normal distribution now fits best. According to the comparison of alternative distribution log likelihood statistic, the best fitting distribution is the normal distribution.

Table 8: Box-Cox Transformation

Construct	Factor	λ
Electronic device usage	EDU1	3.0
	EDU2	2.0
	EDU3	5.0
	EDU4	5.0
	EDU5	5.0
	EDU6	4.0
	EDU7	2.0
	EDU8	3.0
	EDU9	2.0
	EDU10	0
	EDU11	1.32
	EDU12	1
	EDU13	2.0
	EDU14	3.0
	EDU15	3.0
	EDU16	4.0
	EDU17	1.0
	EDU18	0

Information security awareness	ISA9	1
	ISA10	3.0
	ISA11	3.0
	ISA12	1.0
	ISA13	2.0
	ISA14	1.46
	ISA15	3.0
	ISA16	-0.5
Electronic device self-efficacy	EDSE1	0.5
	EDSE2	1
	EDSE3	1
	EDSE4	1
	EDSE5	1
	EDSE6	0
	EDSE7	1
	EDSE8	1
Anxiety level	ITAL1	2
	ITAL2	2
	ITAL3	1
	ITAL4	1
	ITAL5	1.3
	ITAL6	1
	ITAL7	1.42
	ITAL8	1.51
	ITAL9	1.57
	ITAL10	1
	ITAL11	1.57
	ITAL12	1
	ITAL13	0.5
	ITAL14	0.5
	ITAL15	0.5

As part of assessing the measures, confirmatory factor analysis was used to examine the

construct validity of the research instrument as shown in Table 9.

Table 9: Factor Analysis

Construct	Factor	Factor Loading
Electronic device usage	EDU1	0.514
	EDU2	0.631
	EDU3	0.579
	EDU4	0.619
	EDU5	0.608
	EDU6	0.534
	EDU7	0.650
	EDU8	0.763
	EDU9	0.781
	EDU10	0.629
	EDU11	0.565
	EDU12	0.715
	EDU13	0.729
	EDU14	0.788
	EDU15	0.830
	EDU16	0.788
	EDU17	0.782
	EDU18	0.720
Information security awareness	ISA9	0.695
	ISA10	0.625
	ISA11	0.626
	ISA12	0.744
	ISA13	0.573
	ISA14	0.729
	ISA15	0.634
	ISA16	0.615

Electronic device self-efficacy	EDSE1	0.596
	EDSE2	0.781
	EDSE3	0.730
	EDSE4	0.785
	EDSE5	0.654
	EDSE6	0.612
	EDSE7	0.677
	EDSE8	0.698

Factor analysis related values that are < 0.30 are considered insignificant, those between 0.3 and 0.4 are important, and values > 0.5 are significant and are considered acceptable. In confirmatory factor analysis, factor loadings greater than 0.7 are considered very significant. According to [8], although factor loadings greater than 0.5 are significant and acceptable, in confirmatory factor analysis, factor loadings greater than 0.7 are considered very significant. ISA1, ISA2, ISA4, ISA5, ISA7 and ISA8 had factor loadings lower than 0.5. This showed that these factors were not related to the main construct. For this reason, these factors were eliminated from future analysis.

The General Linear Model analysis was used to test the hypotheses. Hypotheses H2 and H6 were rejected. Whereas, hypotheses H1, H3, H4, H5, and H6 were accepted.

Conclusions

The issue of rising identity-theft and how anxiety levels associated with it is related to electronic device usage and electronic device self-efficacy has been presented. The research showed that students exhibit either more or less anxiety levels depending on which electronic device self-efficacy was involved. Therefore, electronic device self-efficacy proved to be important in measuring the anxiety levels of the students.

One of the main considerations of this study involved electronic devices usage. Based on this study, a significant positive relationship exists between electronic devices usage and identity-theft anxiety level. This implies that with less electronic devices usage, the anxiety levels decrease

and with more electronic devices usage, the anxiety levels increase. Electronic devices self-efficacy and identity-theft anxiety showed negative relationship. This implies that with less self-efficacy, the anxiety level increase and with more self-efficacy, the anxiety levels decrease. Also, a significant positive relationship existed between information security awareness and identity-theft anxiety level. This emphasizes that more information regarding awareness of taking proactive measures about identity-theft and electronic devices usage among students are needed.

References

- [1] Federal Trade Commission. (2012, February 28). FTC Releases Top Complaint Categories for 2011 [News Release]. Retrieved from on complex decision making. *Journal of Personality and Social Psychology*, 60(6).
<http://www.ftc.gov/opa/2012/02/2011complaints.shtm>
- [2] Federal Bureau of Investigation. (2012, May 10). "More Than 300,000 Complaints of Online Criminal Activity Reported in 2011" Retrieved from
<http://www.fbi.gov/news/pressrel/press-releases/ic3-2011-internet-crime-report-released>
- [3] Paganini, P. (2012). 2011 IC3 Internet Crime Report. Retrieved November, 2012 from
<http://securityaffairs.co/wordpress/5297/cyber-crime/2011-ic3-internet-crime-report.html>
- [4] Federal Trade Commission. (2014, February 27). FTC Releases Top Complaint Categories for 2014 [News Release]. Retrieved from on complex decision making, *Journal of Personality and Social psychology*, 60(6). <https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014>
- [5] Beckers, J. J. & Schmidt, H. G. (2001). The structure of computer anxiety: A six-factor model. *Computers in Human Behavior*, 17(1), 35-49.
- [6] John Winterdyk. & Nikki Thompson. (2008). Student and Non-Student Perceptions and Awareness of Identity Theft. *Canadian Journal of Criminology and Criminal Justice* 50(2), 153-186. *Project MUSE*. Web. 5 Apr. 2013. <http://muse.jhu.edu>

- [7] Nachmias, D. & Nachmias, C. (1987). *Research methods in the Social Sciences*. New York: St. Martins Press.
- [8] Costello, A. B., & Osborne, J. W. (2005). Exploratory Factor Analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research, and Evaluation*, 10(7), 1-9.

Appendix

Survey Questionnaire

The following survey was designed to measure each construct of the research model:

1. Electronic devices self-efficacy (EDSE)

EDSE1: I am confident that I am not a victim of identity-theft.

EDSE2: I feel confident that I have enough knowledge/ awareness about identity-theft.

EDSE3: I feel confident that I am taking necessary measures/ precautions to prevent myself from identity-theft.

EDSE4: I feel confident that I can understand different types/methods/schemes of identity-theft.

EDSE5: I feel confident sharing my personal information.

EDSE6: I feel confident that I am using screen password to lock my laptop, mobile phone, etc.

EDSE7: I feel confident in storing sensitive information on my laptop, mobile phone, etc.

EDSE8: I feel confident in performing online transactions over the internet.

2. Identity-theft anxiety level (ITAL)

ITAL1: I am concerned about becoming a victim of identity-theft as it is related to unauthorized access, or misuse of personal information.

ITAL2: I am concerned that I might be a victim of identity-theft in future.

ITAL3: I am concerned about becoming a victim of identity-theft even after monitoring my credit reports regularly.

ITAL4: I am concerned about becoming a victim of identity-theft even after taking necessary protection to safeguard my information.

ITAL5: I am concerned about becoming a victim of identity-theft even after reviewing the ongoing fraudulent activities of identity-theft.

ITAL6: I am concerned about becoming a victim of identity-theft even after shredding my personal documents regularly.

ITAL7: I feel concerned about my knowledge and awareness on identity-theft.

ITAL8: I feel concerned about my knowledge and awareness on identity-theft protection measures.

ITAL9: I feel concerned about my knowledge and awareness on identity-theft reporting agency.

ITAL10: I feel dreadful when I have to share my personal information in person.

ITAL11: I feel dreadful when I have to share my personal information in electronic methods.

ITAL12: I feel dreadful when I have to share my personal information in non- electronic methods.

ITAL13: My palms feel clammy when I have to share my personal information in person.

ITAL14: My palms feel clammy when I have to share my personal information in electronic methods.

ITAL15: My palms feel clammy when I have to share my personal information in non-electronic methods.

3. Information security awareness (ISA)

ISA1: Do you use any form of wireless encryption feature in your wireless connection?

ISA2: Do you use a pop-up window blocking function/tool on your computer?

ISA3: How often do you check and apply security updates/patches to the operating system and critical applications on your computer?

ISA4: Do you currently use firewall on your computer or in your home network?

ISA5: Do you currently use a spam-filtering function in the email software on your computer?

ISA6: If you have anti-virus software on your computer, how often do you update the virus database?

ISA7: Do you currently have anti-virus software on your computer?

ISA8: Do you currently have anti-spyware software on your computer?

ISA9: I check my credit reports regularly.

ISA10: I monitor my electronic accounts online for banking, medical records, etc.

ISA11: I do not share my personal information with relatives/ colleagues/ neighbors/friends.

ISA12: I shred confidential and sensitive documents regularly.

ISA13: I implement security (two factor authentication, firewall, anti-virus, and encryption) to protect my credentials and information.

ISA14: I avoid internet transactions which may involve sharing confidential information.

ISA15: I shield my bank account and pin numbers from the view of nearby patrons.

ISA16: I use a RFID (Radio-frequency identification) protection wallet.

4. Electronic devices usage (EDU)

EDU1: Social networking

EDU2: Reading content (e.g., e-books, articles, etc.)

EDU3: Accessing email

EDU4: Text messaging

EDU5: Searching for information

EDU6: Getting directions

EDU7: Playing content

EDU8: Listening to music or watching videos

EDU9: Banking

EDU10: Filing Taxes

EDU11: Shopping

EDU12: Utility billing

EDU13: News

EDU14: Weather

EDU15: Research

EDU16: School Work

EDU17: Company work

EDU18: Medical bill