Open Access License Notice

Identity Theft Education: FIT Report

Susan Helser
shelser@norwich.edu

Computer Science, Computer Security
and Information Assurance

Norwich University
Northfield, Vermont

Abstract - Identity theft losses are in the billions of dollars. The crime affects individuals and industry. It consumes valuable resources and results in higher costs across the board. Technical strategies to address the problem have had mixed effects. The focus of this work is to report outcomes from research that assessed two distinct educational methods that targeted identity theft at the college level. One mode of presentation is text-based while the other is game-based. Study data show that students exposed to information through the game-based approach scored better on the identity theft assessment than did their counterparts who experienced the same information through the text-based method. Also, game-based participants remained longer in the educational unit and reported greater satisfaction than their text-based counterparts. Digital educational game-based learning is in its infancy. FIT demonstrates the efficacy of this method in the field of cyber education.

Categories and Subject Descriptors

[Software organization and properties]: *Virtual Worlds Software – Interactive Games*

[Human and Societal Aspects of Security and Privacy]: *Social Aspects of Security and Privacy*

[Human Computer Interaction (HCI)]: *HCI Design and Evaluation Methods-User Studies*

[Education]: *Interactive Learning Environments*

[Professional Topics]: *Computer Crime – Identity Theft*

General Terms

Identity Theft, Identity Theft Education, Text- and Game-Based Learning, Interactive Learning, Cyber Security

Keywords

Con, Cyber Crime, Deceive, Deception, Education, Fraudster, Identity, Identity Theft, Identity Thieves, Malware, Phishing, Personally Identifiable Information (PII), Scam, Steal, Theft

1 INTRODUCTION

Identity theft continues to grow and evolve at an alarming rate. Millions of people's lives have been affected. Unknown and unwarranted legal trouble haunts the victim, often years after the person's *identity* is stolen. Losses totaling in the hundreds of billions of dollars impact the consumer, business and the economy as a whole. The cost of fraudulently acquired goods and services are passed on from industries such as retail and the medical community to the public through higher prices and premiums.

Malware is one of the tools successfully used by *identity thieves* to steal *PII*, aka personally identifiable information. Figures 1 through 4 reflect the severity of the problem. They indicate the extent to which *malware* is used. The creators of the infectious code work diligently to design it in such a way that it is able to pass unnoticed. Without regular and substantive checks, electronic systems are susceptible. In recent years large retailers' billing technology has been targeted. Corrupted systems continued to process financial transactions, but passed on sensitive information to the remote *fraudster*. In addition to the loss of *PII*, events had a substantial and detrimental effect on the businesses [18, 27, 29, 36, 39, 41,

42]. Data displayed in Figures 1 through 6 is available from the *Anti-Phishing Working Group* (APWG) [1, 2, 3, 4, 5, 6, 7, 8].

The APWG collects and disseminates information that concerns *phishing* related cyber activities. Statistics are computed from self-reported events from individuals and companies. Figures 1 and 2 show *Malware by Strain* in 2015 and 2016. *Trojans* continue to represent a major concern. From their inception they are designed to be unseen. Figures 3 and 4 show the percent of *Malware Infections by Type* for the same two-year period. Similarly, *Trojans* constitute a significant form of attack. Their detection presents a real challenge. Figures 5 and 6 report the *Most Targeted Industries* for 2015 and 2016. Vulnerabilities exist and are readily exploited by *identity thieves*. Some industries such as financials are targeted, but no sector is immune. In addition to harm to the individual, economic losses are catastrophic [15, 16, 17, 23, 34, 25, 28, 30, 31, 32, 33]. Consequences are sufficient to undermine the economy [43, 44, 45, 46, 47, 48, 49].

Methods to address the crime of *identity theft* have been varied with mixed results. Technical and non-technical strategies have been tried. Technical solutions have limited effect, in part, because the problem involves people and their behavior. Educational resources that consist of informational text materials provided by numerous government and non-government agencies are available on Internet websites and in pamphlets. The message has reached some people, but more must be done to combat *identity theft*. Another strategy is needed, one that moves in a new direction to inform citizens of the ongoing threats posed by the *crime*. An engaging method to deliver critical and relevant material is crucial. For this reason, *Fight Identify Theft* (FIT) was developed. FIT is an educational *identity theft* game.

To assess FIT's value as an instructional tool this study compares results from exclusively text-based learning to a game-based approach. Because college students are targeted by *identity thieves* due to their increasing earning potential over time, the focus of this research is centered on this group. Study results reflect greater improvement between *identity theft* pre- and post-surveys, time participants remained in the educational module, and benefit and enjoyment responses for

game-based learners than for their text-based counterparts. Results are reported in this paper.

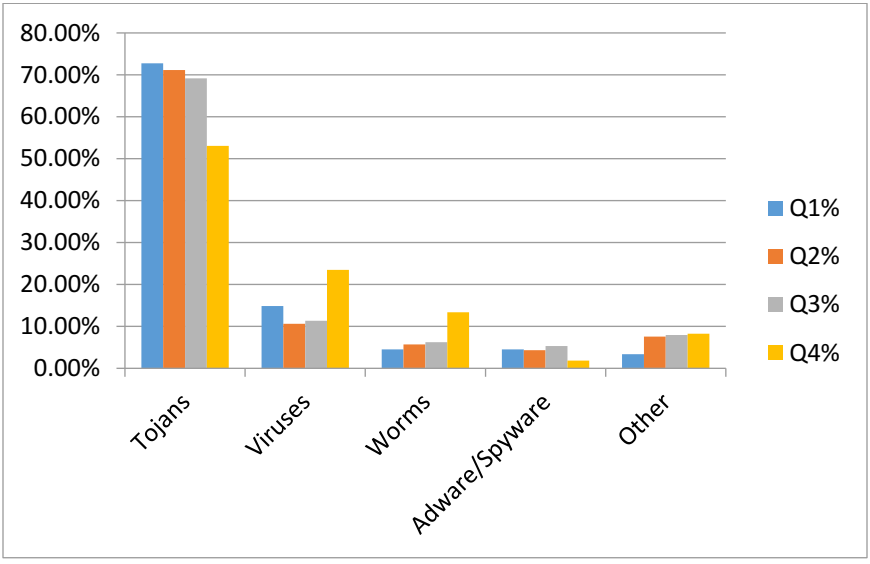

Figure 1: 2015 % Malware by Strain

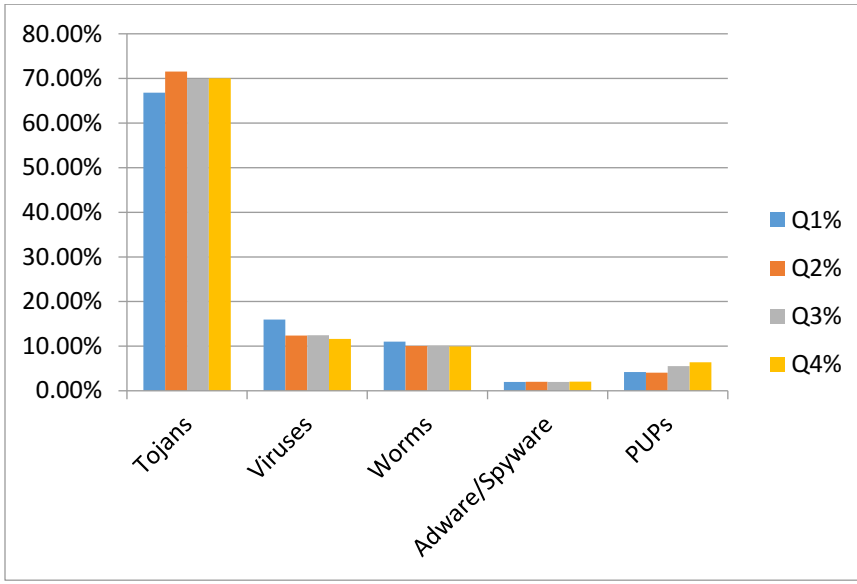

Figure 2: 2016 % Malware by Strain

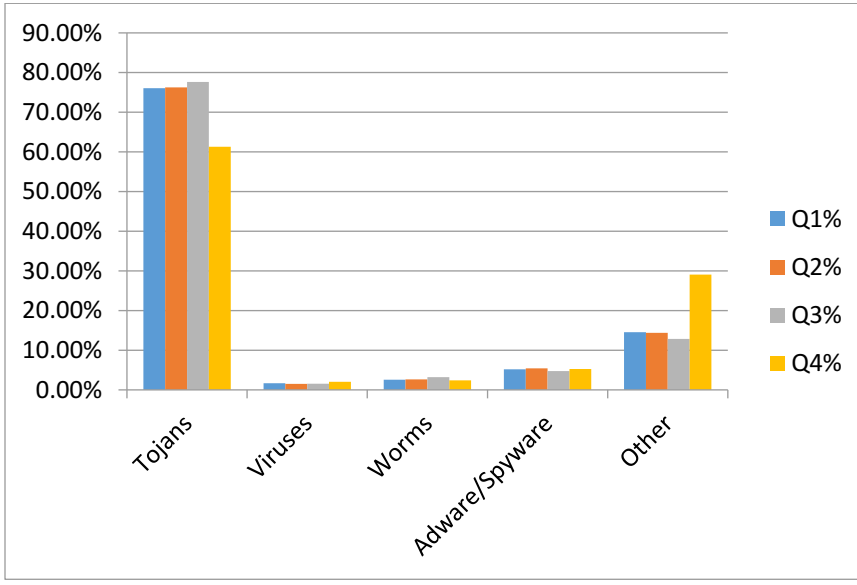

Figure 3: 2015 % New Malware Infections by Type

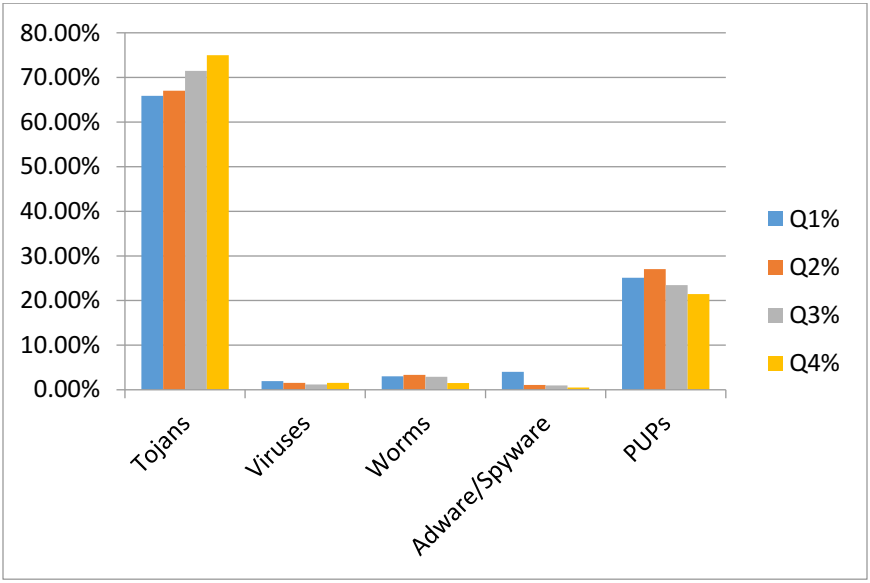

Figure 4: 2016 % Malware Infections by Type

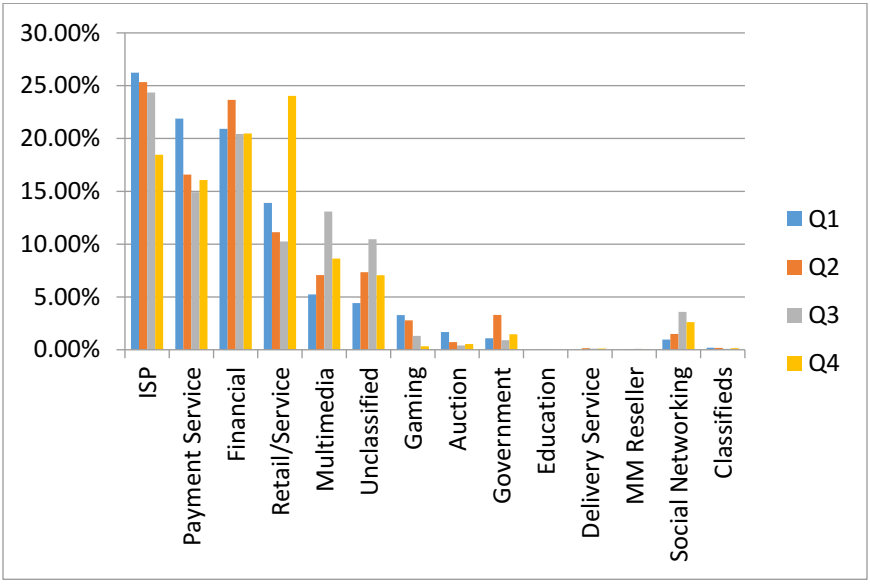

Figure 5: 2015 Most Targeted Industries

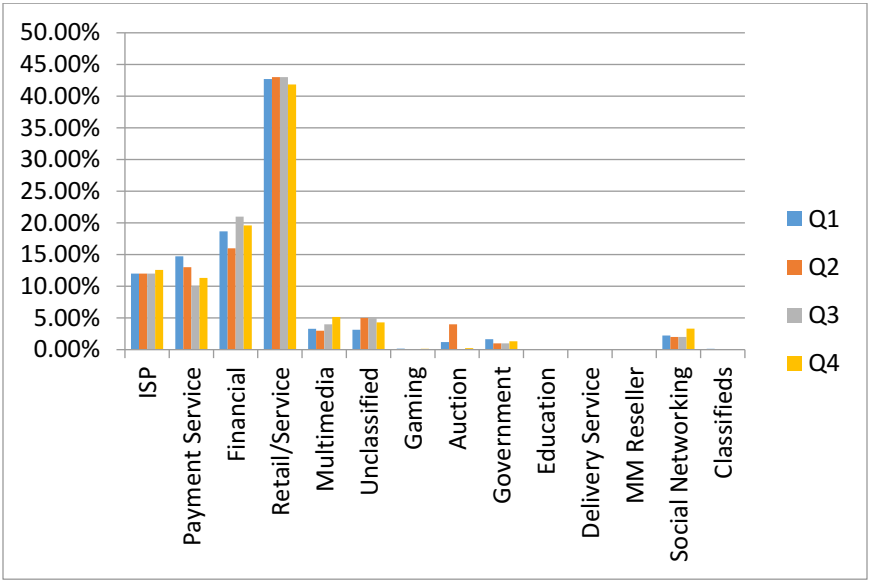

Figure 6: 2016 Most Targeted Industries

2 OBJECTIVE

The objective of this research is to assess the efficacy of game-based learning about *identity theft* in relation to a traditional text-based format that presents the same material to college students. Participants in the study are at least 18 years of age. *Fraudsters* exploit the population regardless of demographic information, because individuals' *identities* have value. Given the appropriate documentation, people are able to gain credit which, in turn, can be used by the actual person or by anyone who appears to be that individual. In the case of college students, the worth of their *identities* tends to grow with time as they proceed through their educational goals and careers. It is possible that an *identity thief* will retain a student's *identity* information for a number of years before reaping any benefit. The assumption is that upon completion of a college degree that the former student, now entering the workforce, will be able to access a significantly greater amount of credit. Given this scenario, it makes sense for a *fraudster* to be patient and to wait before using or selling the *identity*.

Currently, numerous printed resources that address *identity theft* are available [11, 20, 21, 34, 37,40]. Materials are useful and informative, but more needs to be done to reach a greater number of individuals. One possibility that is considered in this research is game-based learning [9, 10, 12, 13, 14, 19, 22, 26, 35, 38]. Because of the format, this method affords the opportunity to address different learning modalities. For example, rather than presenting information exclusively as text, audio and video components can be incorporated. Engaging digital resources can be created and then adapted to suit the respective educational requirements of a discipline. Data gathered from the assessment of the learning tool regarding what is effective can be used to make improvements and enhancements.

3 METHODOLOGY

To help educate college students about the *crime* of *identity theft* FIT was developed. It is a software application that incorporates game-based learning. To assess FIT's efficacy, two independent educational modules are used to present identical content, but through different means. One is a traditional text-based delivery system similar to what can be found on the Internet, in pamphlets or in periodicals. The other is a new game-based approach complete with scoring, colorful graphics, audio, video and puzzles. In addition, FIT includes the collection of demographic data, the administration of pre- and post- surveys used to assess participants' knowledge of *identity theft*, and three areas for users to supply feedback about their experience by way of enjoyment level, benefit level and open response. Time is recorded as well. Figure 7 shows FIT flow.

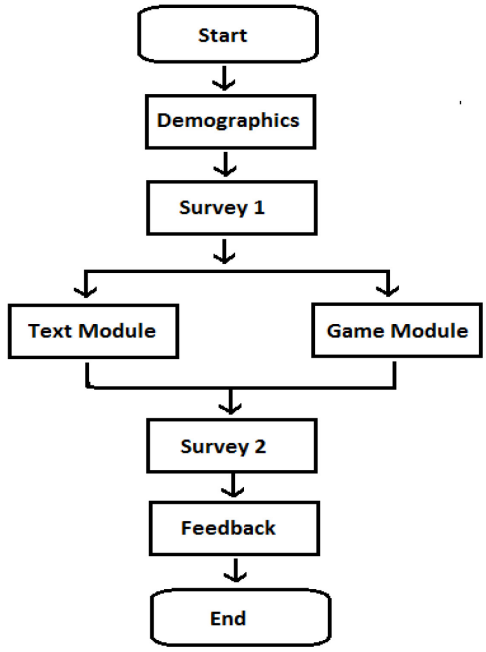

Figure 7: FIT Flowchart

After an individual agrees to participate and enters the requested demographic information he or she receives Survey 1, the first of a set of two identical survey questions that include the following:

1. Identity theft can lead to credit problems.
2. Medical insurance can be denied, because of identity theft.
3. It is smart to buy from the cheapest online vendor.
4. Phishing can occur at work.
5. Social engineering is a form of social media.
6. It's okay to stay logged on to a computer when you leave it for a few minutes.

7. Purchases that you don't make don't impact your credit.
8. Social media sites are good places to share your information.
9. Cell apps are reliable.

Once Survey 1 has been completed FIT randomly selects one of the two educational modules. The individual then has the opportunity to explore resources that are available in that particular unit. Topics include *finance*, *health*, *entertainment*, *work*, *home*, *education*, *shopping*, *home*, *and mobile communication*. In the case of the text-based track nine topic specific panels that include six paragraphs of material about different areas where PII is at risk can be viewed in any order. A participant is free to remain on a given panel, can leave the panel to select another topic area to investigate, or return to a previously viewed panel. Figures 8 – 10 show the selection screen for the text-based module and a sample of two text-based informational panels.

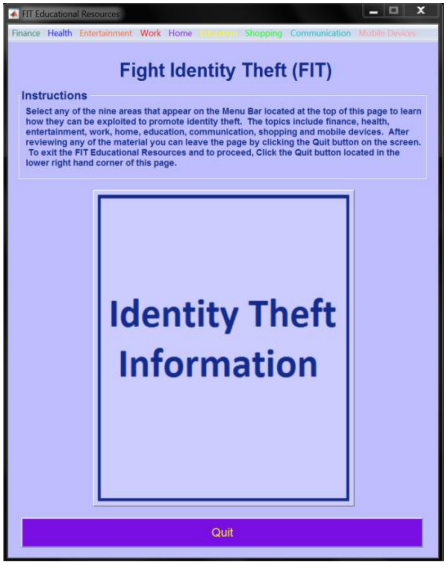

Figure 8: Text Screen

Figure 9: Education Text Panel

Figure 10: Finance Text Panel

The same material is presented in the game-based module, but through variety of formats. Nine colorful buttons used to select topics replace text-based panels. Similarly, sets of six game-panels with "clues" that address each of the nine topic areas are used. "Clues" correspond to paragraphs in the text-based unit. Three game panels are presented in a Q & A format. Content on these panels is identical to text that appears in the text-based module. Two of the three remaining game-based panels have "clues" in the form of messages that are either of audio of video format. Information is the same as what is displayed on the text-based panels, but delivered differently. Participants can access the audio or video resources repeatedly, so long as they remain on a particular game panel. The last of the six game panels includes a word search puzzle with terms that are related to the text "clue" on the screen. Figures 11 - 17 show the user selection screen and a sample of the game play panels.

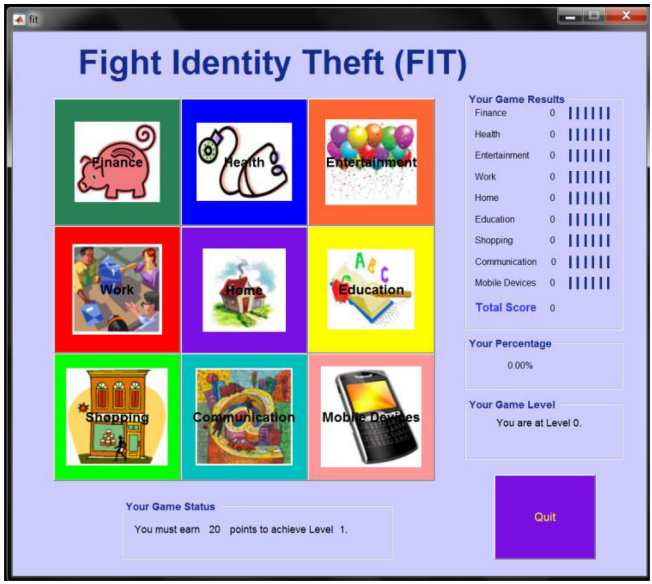

Figure 11: Game Screen

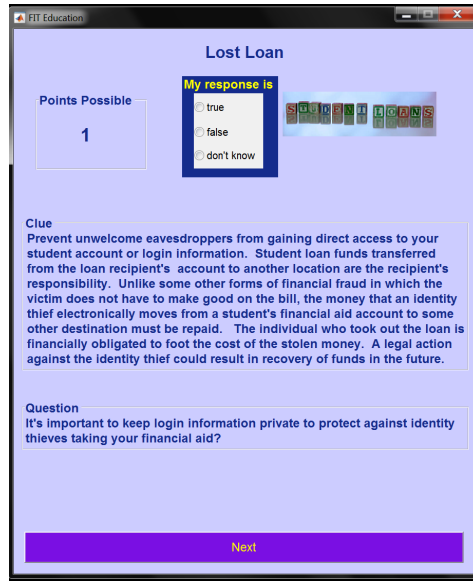

Figure 12: Lost Loan Game Panel

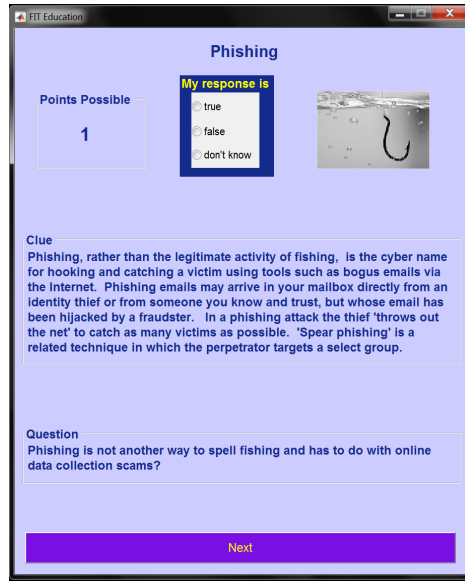

Figure 13: Phishing Game Panel

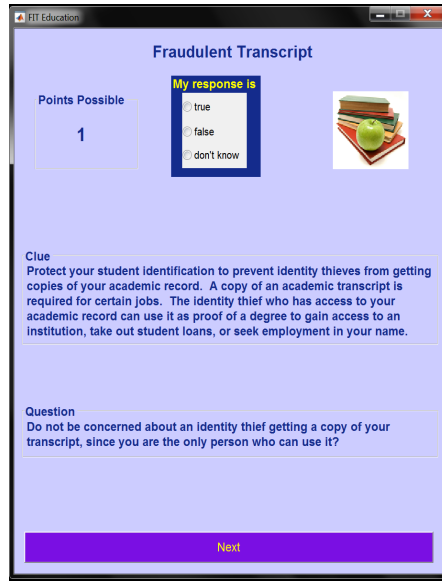

Figure 14: Fraudulent Transcript Game Panel

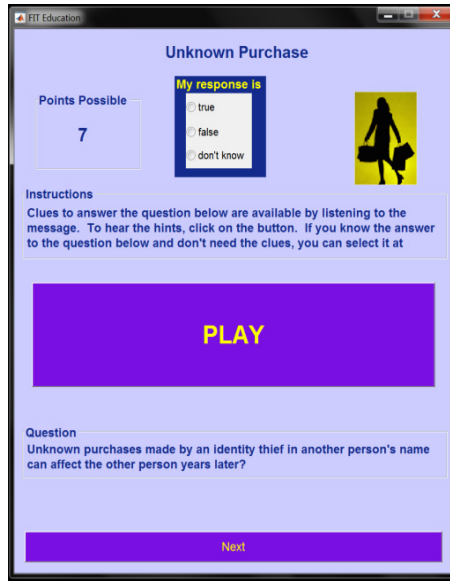

Figure 15: Unknown Purchase Game Panel

Figure 16: Bogus Email Game Panel

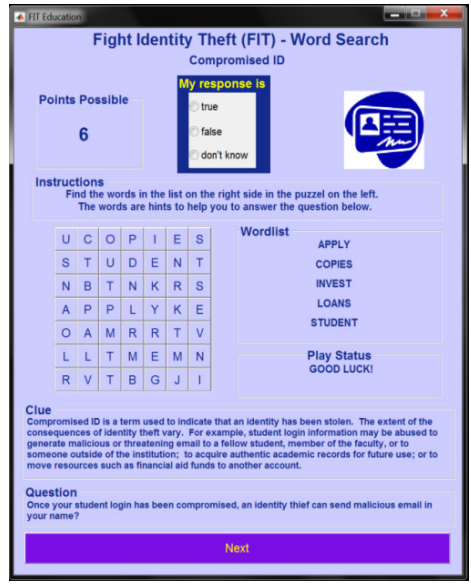

Figure 17: Word Search Game Panel

In the case of the game modules, points are awarded for correct responses. Questions are weighted differently so points earned vary. This is indicated in the Points Possible box that is displayed on each game panel screen. Users can view their status in the game anytime they return to the main screen. Statistics include the participant's score, relative percentage in the game, number of points needed to reach the next level, current level, and how many questions remain to be answered in a given topic area. Participants can exit the game module at any time.

After a participant quits either of the learning modules he or she receives Survey 2, second of the set of two identical surveys. Data collected in pre - and post - surveys for both groups is used to assess movement in the participant's responses to the survey questions. Three responses are possible that include *true*, *false* and *don't know*. Scoring for nine combinations of possibilities is listed in Table 1. The terms *incorrect*, *don't know*, and *correct* reflect whether a participant answered the question correctly. For example, suppose a participant indicates the *incorrect* response on Survey 1 and answers in the same way on Survey 2, then no points are awarded, since no change occurred. On the other hand, if the participant answered *don't know* on Survey 1, but responded the *correct* answer on Survey 2, then 1 point is awarded that reflects positive movement following the exposure to the educational module.

S1 vs. S2	incorrect	don't know	correct
incorrect	0	1	2
don't know	-1	0	1
correct	-2	-1	0

Table 1: Fit Score Scheme

Scores for each of the nine questions were determined in this way then added together for each participant. Figure 18 displays the results. Text-based results are displayed in blue while game-based results appear in red. The distribution of game-based data (red) is to the right of text-based data (blue). This reflects better performance on for game-based learners on the assessment.

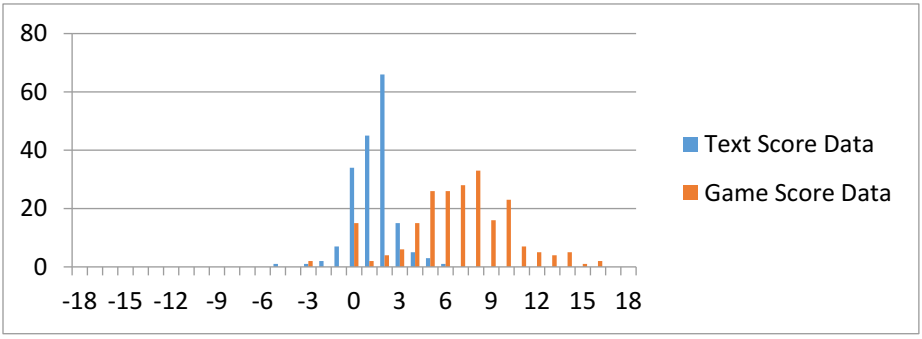

Figure 18: Game and Text Score Data

The total length of time an individual remains in the software is recorded. This in relation to the score received as described above is reported in Table 2. In addition, participants have the opportunity to supply feedback about their experience with FIT by way of benefit, enjoyment and in an open response area. Data for benefit and enjoyment are reported in Table 3.

	Text		Game	
	Score	Time	Score	Time
Average	1.36	527	6.85	1002
Std. Dev.	1.4	237	3.46	548
Minimum	-5	36	-3	40

Maximum	6	2373	16	4368
Correlation	0.24		-0.12	

Table 2: FIT Scores and Time

	Text		Game	
	Benefit	**Enjoy**	**Benefit**	**Enjoy**
Average	1.69	2.37	4.18	4.12
Std. Dev.	0.81	1.03	1.22	1.2
Minimum	1	1	1	1
Maximum	4	5	5	5

Table 3: Benefit and Enjoyment

4 SOFTWARE AND TECHNOLOGY

The Mathwork's software MATLAB was used to write FIT. The program was written on a PC platform using the MATLAB graphical user interface GUIDE. Microsoft images were used for the graphics on the numerous panels. Audio sound effects were selected from *6000 Sound Effects* from COSMI. CyberLink YouCam was used to produce the videos. Microsoft code was embedded in the MATLAB application to play the videos. The entire coding project required approximately one year.

5 RESULTS

F-table for $\alpha = 0.05$

(http://www.socr.ucla.edu/Applets.dir/F_Table.html)

H_0: $\delta_1^2 = \delta_2^2$ H_1: $\delta_1^2 \neq \delta_2^2$

	Game (1)	Text (2)	F Score
n	220	180	
Degrees freedom	219	179	
Time (variance)	300772.44	56338.63	4.37
Score (variance)	11.96	1.97	4.96
Benefit (variance)	1.49	0.65	1.87
Enjoyment (variance)	1.45	1.06	1.12

Table 1: F-Test Results

t-table for $\alpha = 0.05$

(http://www.socr.ucla.edu/applets.dir/t-table.html)

H_0: $\mu_1 = \mu_2$ H_1: $\mu_1 > \mu_2$

n1 = 220, n2 = 180 degrees freedom, n1 + n2 - 2 = 398	t	Critical Value
Time	11.58	1.645
Score	21.51	1.645

Benefit	24.42	1.645
Enjoyment	15.72	1.645

Table 2: t test

6 CONCLUSION

F- and t-test study results indicate the effectiveness of game-based learning to address *identity theft* education in college students. FIT scores and time spent learning about *identity theft* were greater for game-based participants. Feedback provided by the game-based learners was better for benefit and enjoyment levels. Open responses revealed greater satisfaction as well. Participants supplied a variety of suggestions to improve FIT. For example, participants recommended enhancing FIT to provide *resume* functionality so that a *player* could exit the game, return, and continue at a later time. Game-based players offered other ideas too, such as allowing *players* to revisit a question, even if it meant points earned would be reduced. Another suggestion was that participants be allowed to select questions to answer. Older students and those with young children asked that versions of FIT be written to educate the elderly and teens. A longitudinal study is another possibility. Additional work needs to be done.

REFERENCES

[1] Anti-Phishing Working Group, P*hishing Activity Trends Report 4th Quarter 2016*, http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

[2] Anti-Phishing Working Group, *Phishing Activity Trends Report 3rd Quarter 2016*, http://docs.apwg.org/reports/apwg_trends_report_q3_2016.pdf

[3] Anti-Phishing Working Group, *Phishing Activity Trends Report 2nd Quarter 2016*, http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

[4] Anti-Phishing Working Group, *Phishing Activity Trends Report 1st Quarter 2016*, http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[5] Anti-Phishing Working Group, *Phishing Activity Trends Report 4th Quarter 2015*, http://docs.apwg.org/reports/apwg_trends_report_q4_2015.pdf

[6] Anti-Phishing Working Group, *Phishing Activity Trends Report 3rd Quarter 2015*, http://docs.apwg.org/reports/apwg_trends_report_q3_2015.pdf

[7] Anti-Phishing Working Group, *Phishing Activity Trends Report 2nd Quarter 2015*, http://docs.apwg.org/reports/apwg_trends_report_q2_2015.pdf

[8] Anti-Phishing Working Group, *Phishing Activity Trends Report 1st Quarter 2015*, http://docs.apwg.org/reports/apwg_trends_report_q1_2015.pdf

[9] S. A. Barab, M. Gresalfi, and A. Arici, *Why Educators Should Care About Games*, Educational Leadership, September 2009, Vol. 67, No. 1 pp 76 – 80.

[10] F. Bellotti, B. Kapralos, K. Lee, P. Moreno-Ger, and R. Berta, *Assessment in and of Serious Games: An Overview*, Hindawi Publishing Corporation, Advances in Human Computer Interaction, Vol. 2013, Article ID 136864, pp 1 – 11

[11] F. Cassim, *Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thieves?*, ISSN 1727-3781, PER: Potchefstroomse Elektroniese Regsblad, 18(2):pp 69 – 110, http://dx.doi.org/10.4314/pelj.v18i2.02, Retrieved March 14, 2017

[12] M-T Cheng, H-C She, and L.A. Annetta, *Game Immersion Experience: Its Hierarchical Structure and Impact on Game-based Science Learning*, Journal of Computer Assisted Learning, June 2015, Vol. 31 Issue 3, pp 232 – 253

[13] M. Csikszentmilhalyi, Applications of Flow in Human Development and Education, *Chapter 8: Intrinsic Motivation and Effective Teaching*, 2014 Springer Science & Business Media Dordrecht, DOI: 10.1007/978-94-017-9094-9_8, pp 173 – 187

[14] M. Csikszentmihalyi, *The Psychology of Optimal Experience*, Harper & Row; 1st Ed., March 1990, ASIN: B010EV0KHW

[15] *Deter, Detect, Defend, Avoid Theft*, https://www.in.gov/isp/files/Avoid_ID_Theft_Deter_Detect_Defend.pdf, Retrieved March 14, 2017

[16] *Expanding Service to Reach Victims of Identity Theft and Financial Fraud*, October 2010, http://www.ovc.gov/pubs/ID_theft/idtheftlaws.html, retrieved March 8, 2017

[17] Federal Trade Commission, August 27, 2014, *Can you spot a government imposter?*, Amy Hebert, https://www.consumerftc.gov/blog/whos-calling-not-government, retrieved February 18, 2017

[18] Federal Trade Commission, IdentityTheft.gov, https://identitytheft.gov/, retrieved February 16, 2017

[19] M. Gaydos, *Seriously Considering Design in Educational Games*, 2015, Educational Researcher, Vol. 44, No. 9, pp 478 – 483, DOI: 10.3102/0013189X15621307

[20] K. Higgins, *Price Tag Rises for Stolen Identities Sold in the Underground*, December 15, 2014, http://www.darkreading.com/attacks-breaches/price-tag-rises-for-stolen-identities-sold-in-the-underground/, retrieved February 27, 2017

[21] J. Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, New York Times, July 9, 2015, http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html, retrieved February 27, 2017

[22] M. A. Honey and M. Hilton, Editors, Learning Science Through Computer Games and Simulation, *Chapter 3: Simulation and Games in the Classroom*, pp 57 - 62, Chapter 7: Research Agenda for Simulation and Games, pp 119 – 128, National Academy of Science, ISB 978-0-309-38664-7, DOI: 10.17226/13078

[23] *Identity Protection: Prevention, Detection and Victim Assistance*, IRS, https://www.irs.gov/individuals/identity-protection, retrieved March 8, 2017

[24] *Identity Theft: Prevalence and Cost Appear to be Growing*, United States General Accounting Office, http://www.gao.gov/assets/240/233900.pdf, retrieved March 8, 2017

[25] Identity Theft Resource Center, June 24, 2013, http://www.idtheftcenter.org/Identity-Theft/how-much-is-your-identity-worth-on-the-black-market.html, retrieved March 18, 2017

[26] A. Iliya, A. Jabbar, and P. Felicia, *Gameplay Engagement and Learning Game-Based Learning: A Systematic Review*, Review of Educational Research, December 2015, Vol. 85, No. 4, pp 740 – 779, DOI: 10.3102/0034654315577210

[27] T. Judson MPH, M. Haas MBA, T Lagu MD MPH, *Medical Identity Theft: Prevention and Reconciliation Initiatives at Massachusetts General Hospital*, Joint Commission Journal on Quality & Patient Safety, July 2014, ; 40(7): pp 291 – 295

[28] D. Kirk, *Identifying Identity Theft*, The Journal of Criminal Law, 2014, DOI: 10.1177/0022018314557418, Vol. 78(6) pp 448 – 450

[29] Medicare.gov, *Help fight Medicare fraud*, https://www.medicare.gov/forms-help-and-resources/report-fraud-and-abuse/fraud-and-abuse.html, retrieved February 1, 2017

[30] A. C. Moise, *Identity Theft Committed Through the Internet*, Juridical Current, 2015, Vol. 18 Issue 2, pp 118 - 125

[31] T. Nagunwa, *Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors*, International Journal of Cyber-Security and Digital Forensics. 3.1 (Jan. 2014): p72.

[32] *Phishing*, https://www.consumer.ftc.gov/articles/0003-phishing, retrieved February 1, 2017

[33] *Phone Scams*, August 6, 2016, https://www.consumer.ftc.gov/articles/0076-phone-scams, retrieved February 8, 2017

[34] Po-Ching Lin and Pei-Ying Lin, *Unintentional and involuntary personal information leakage on Facebook from user interactions*, KSII Transactions on Internet and Information Systems, July 2016, Vol. 10 Issue 7, pp 3301 – 3019

[35] L.P. Reiber, *Seriously Considering Play: Designing Interactive Learning Environments Based on the Blending of Microworlds, Simulations and Games*, 1996, ETR&D, Vol. 44, No. 2, pp 43 – 58, ISSN 1042-1629

[36] M. Riley, B. Elgin, D. Lawrence, C. Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg News, March 17, 2015, http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data, retrieved February 6, 2017

[37] J. Showronski, *What Your Information is Worth on the Black Market*, http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx, retrieved March 8, 2017

[38] V. J. Shute and F. Ke, Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives, *Chapter 4 Games, Learning, and Assessment*, 2012

Springer Science & Business Media Dordrecht, pp 43 - 58, DOI: 10.1007/978-1-4614-3546-4_4

[39] *6 More Stores Attacked By Same Hack As Target: Firm*, Jim Finkle, January 25, 2014, http://www.huffingtonpost.com/2014/01/17/six-other-stores-are-bein_n_4618414.html, retrieved March 27, 2017

[40] L. Sweeney, *Data Privacy Lab SOS Social Security Number Watch*, IQSS Harvard University, http://dataprivacylab.org/projects/ssnwatch/index.html

[41] *Target: 40 Million Credit Card Compromised*, December 19, 2013, http://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html, retrieved March 27, 2017

[42] *Target Missed Signs of a Data Breach*, Elizabeth Harris and Nicole Perlroth, March 13, 2014, http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html?_r=0, retrieved March 27, 2017

[43] *The Challenge of Health Care Fraud*, National Health Care Anti-Fraud Association, https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx, retrieved April 2, 2017

[44] United States General Accountability Office, August 20, 2014, *Identity Theft Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, http://www.gao.gov/assets/670/665368.pdf, retrieved April 2, 2017

[45] United States General Accountability Office, May 24, 2016, *Identity Theft and Tax Fraud IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, http://www.gao.gov/assets/680/677406.pdf, retrieved April 8, 2017

[46] United States General Accountability Office, June 23, 2016, *Identity Theft Tax Refund Fraud*, http://www.gao.gov/multimedia/podcasts/677925, retrieved April 8, 2017

[47] United States General Accountability Office, November 29, 2012, *Identity Theft Total Extent of Refund Fraud Using Stolen Identities is Unknown*, http://www.gao.gov/assets/660/650365.pdf, retrieved April 18, 2017

[48] United States General Accountability Office, April 12, 2016, *Information Security IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud*, http://www.gao.gov/assets/680/676493.pdf, retrieved April 2, 2017

[49] United States General Accountability Office, April 19, 2016, *Tax Filing: IRS Needs a Comprehensive Customer Service Strategy and Needs to Better Combat Identity Theft Refund*

Fraud and Protect Taxpayer Data, http://www.gao.gov/assets/680/676675.pdf, retrieved March 7, 2017