International Journal of Intelligent Computing and Information Science

THE IMPACT OF CYBER CRIME ON E-COMMERCE

Houssam Saleh, Amira Rezk, Sherif Barakat

Department of Information System, Faculty of Computer and Information Sciences, Mansoura University, Egypt
Smile00972@yahoo.com, amira_rezk@mans.edu.eg , sheiib@mans.edu.eg

Abstract: *Although E-Commerce has increased during the last years around the world, many users, especially in developing countries, do not trust E-Commerce to complete their purchase. So, it is important to study the reasons that make the user does not trust E-Commerce and override any obstacles that may delay the expanding of E-Commerce and get its benefits. One of these obstacles is Cyber Crime. Cyber Crime has a serious effect on E-Commerce, not only because it causes big losses in E-Commerce, but also it is one of the important reasons that makes users do not trust E-Commerce. In this paper, we will study the impact of Cyber Crime on E-Commerce from the user's point of view. The opinions of sample users are collected by using a questionnaire. The analysis of the questionnaires illustrates that not only falling as a Cyber Crime victim has a bad impact on E-Commerce, but also the fear of Cyber Crime makes users distrust E-Commerce to complete their purchase.*

Keywords: *E-Commerce, Cyber Crime, Fear, Trust.*

1. Introduction

E-Commerce, also called Electronic Commerce, mostly consists of electronic business transactions related to the purchase and delivery of goods and services. E-Commerce uses the Internet to submit its deals, therefore we must know the things which threat or hamper the E-Commerce trust such as the Cyber Crime because the continuous growth of E-Commerce still attracts the Cybercriminals to develop new schemes to trick the traders and their customers [1].

Cyber Crime, e-crime, electronic crime, hi-tech crime and computer crime are terms included criminal activities; such as, denial of service, phishing and hacking, to attack the E-Commerce websites or the individuals to lose money, harm the victims, defamation of reputation or steal information by advanced computer networks [1]. The Cyber Crime has become a main concern all over the world due to the fact that a lot of companies lose billions of dollars yearly in lost business, stolen assets, and damaged reputations because of Cyber Crime. The E-Commerce stops when a company website goes down [2,3].

The Cyber Crime can be categorized according to its target and method into four major categories: Cyber Crime against individuals, Cyber Crime against property, Cyber Crime against society, and Cyber Crime against organization. Table **1** summarizes the most common Cyber Crime and their methods to attack the different targets.

Table 1: The Summary of Cyber Crime categories according its target

Target	Cyber Crime	Method
Against individual	Email spoofing	Email
	Spamming	Ads
	Phishing	Fake emails
	Botnet	Sends the instructions to another computers
	Netspionage	Hack into individual PCs
	Cyber defamation	Websites or sending emails
	Harassment and cyber stalking	Emails, posting messages on bulletin boards, chat rooms, user net groups
Against property	Credit Card Fraud (CCF)	Unlawful online getting of a credit card number
	Intellectual property crimes	Software hacking, illicit programs copying, distribute of copies of software illegally
	Copyright infringement	Reproduce right or the copyrighted perform work
	Trademarks Violations	Attaching to a trademark with unauthorized of the trademark owner or any licensees
Against society	Forgery	Forged by usage the high-quality scanners and printers and computers.
	Cyber Terrorism	Terrorists trigger virtual devastation in online computer systems.
	Web Jacking	Hacking
Against organization	E-bank theft	Hacks into the system of banking
	Unauthorized Accessing of Computer	Hacking
	Denial of Service (DoS)	Viruses, email barrages
	Computer Contamination	Virus attack and Worm attack
	Email Bombing	Emails
	Logic Bomb	Event dependent programs
	Trojan Horse	Unauthorized program and working from an inside authorized program
	Data diddling	Commands

Today, the effect of organized Cyber Crime is felt worldwide through the E-Commerce and financial sectors. Wherein the personal accounts and the financial services are accessed by more people from PCs, the providers of services and their users have become the main aims for online fraud. Gartner (2015) exhibits that more than 50% of online attacks are targeted at E-Commerce and financial services users. It assures that people are still being the weakest link in the chain of security and expect that the criminal social engineering scams; such as, Phishing and Distributed Denial of Service (DDoS), have reached new levels of deviousness and prevalence. Because the industry of security fails to create efficacious solutions to these problems, more inventive and newer scams deceive people, every day to capture their personal and financial information [4]. Companies lose billions of dollars yearly in lost business, stolen assets, and damaged reputations as a result of Cyber Crime. Money is stolen with the push of a button, literally. The E-Commerce stops when a company website goes down. When a company becomes the Cyber Crime victim, the customers of company often take their business to another website, and this hurts the reputation of this company. Obvious vulnerability to Cyber Crime may cause customers to distrust the ability of company to safeguard customer information and process transactions of sales effectively. As a result, companies must combat to protect themselves from Cyber Crime [3].

The bad impact of Cyber Crime not only causes the companies lose money but also lose their customers. On the other hand, it destroys the trust of both of traders and customers on E-Commerce which considered intangible lose. In this paper, we will try to analyze the opinion of users of E-Commerce to get a complete view about how they think about E-Commerce and their requirement and considerations from E-Commerce, as well as, what affects their use of E-Commerce. So, this paper will be organized as following: section 2 will study the related work, section 3 will introduce the study model, section 4 will test the study model and discuss its results, and finally section 5 gives a conclusion and recommendations for future research.

2. Related Works

Many researches interest in studying the impact of Cyber Crime on E-Commerce from different points of view. In this section, the most related researches will be discussed.

Billy Henson [2011] analyzed the extent of fear of Cyber Crime victimization as well as examining the relationship between perceived risk of Cyber Crime victimization and Cyber Crime victimization. He made use of the data collected from a large number of undergraduate students of University of Cincinnati to get accurate results. The research results showed that a large number of people are worried about becoming victims of cyber-crimes. They, also, emphasized that type of offender, relationship status, gender and pursuit behaviors frequency have great effects on the fear levels of Cyber Crime victimization. This research is agreed with previous related works on the idea that perceived risk of Cyber Crime victimization and Cyber Crime victimization are main predictors of fear of Cyber Crime victimization too [5].

Ainur Rofiq [2012] developed a conceptual model by considering the perceptions of Cyber fraud and trust. He used the planned behavior theory which made up of perceived behavioral control, subjective norm and attitude towards behavior. He investigated the perspectives of customers toward the E-Commerce transactions, by performing an online questionnaire in Indonesia for 602 respondents then analyzed the data with applying the structural equation model. The study results showed that the perceptions of Cyber fraud have a negative impact on the customers' intention to use E-Commerce for buying goods; therefore, any information about Cyber fraud experience will curb E-Commerce transaction [6].

Rainer Bohme & Tyler Moore [2012] accomplished an analysis of collected data to study European Union citizens' fears and experiences arising from Cyber Crime. They put logistic regressions series which measure how exposure to Cyber Crime can prevent online shopping, online banking and other online activities. They found that falling as a Cyber Crime victim decreases the possibility of online banking and online shopping by 4-5 percentage point. Also, they found out that showing concern about Cyber Crime has nearly twice as much negative effect on online behavior as falling as a Cyber Crime victim. Persons that have not heard anything about Cyber Crime from colleagues or from news reports are most probably willing to use online banking than persons that have heard those reports [7].

Szde Yu [2014] mentioned three main predictors for fear of Cyber Crime: victimization experience, perceived risk of victimization and perceived Cyber Crime seriousness. This study tested these factors on Cyber Crime as well as analyzing their relationships with Cyber Crime's fear. It discussed concurrently four kinds of Cyber Crime and handled the relationship between Cyber Crime's fear and the three main predictors. Depending on the crime, the results referred to that Cyber Crime's fear does not usually share the same predictors, and the using of Internet plays an important role in Cyber Crime's fear too [8].

Wekundah Ruth Nangechey [2015] focused on the different Cyber-attacks that attack small and medium enterprises. The two quantitative and qualitative research methods are performed in this study to collect data from different small and medium enterprises regarding Cyber Crime attacks. The results showed that most small and medium enterprises do not focus or specify sufficient resources on Cyber Crime attack although they continuously fall as victims of Cyber Crime attacks. The small and medium enterprises do not have experience or minimal to confront Cyber Crime and depend dearly on the Internet or friends for information of Cyber-attack [9].

3. The Study Model

This study model will analyze the impact of Cyber Crime on E-Commerce through testing a set of hypotheses by suitable statistical models to the sample data collection. This study model aims to:
1- Study the direct impact of the two Cyber Crime constructs: User's falling as a Cyber Crime victim and user's fear of Cyber Crime on the user's trust of E-Commerce and user's trust of the Internet (medium).
2- Study the direct impact of the two trust constructs: User's trust of E-Commerce and user's trust of the Internet (medium) on using E-Commerce.
3- Showing the indirect impact of Cyber Crime on Using E-Commerce with trust as a mediator between them.
To achieve these aims, the study model consists of three variables as shown in figure **1**. The first variable is Cyber Crime as an independent variable represented in two constructs (User's falling as a Cyber Crime victim and user's fear of Cyber Crime). The second variable is trust as a mediator variable represented in two constructs (User's trust of E-Commerce and User's trust of the Internet). The third variable is using E-Commerce as a dependent variable.

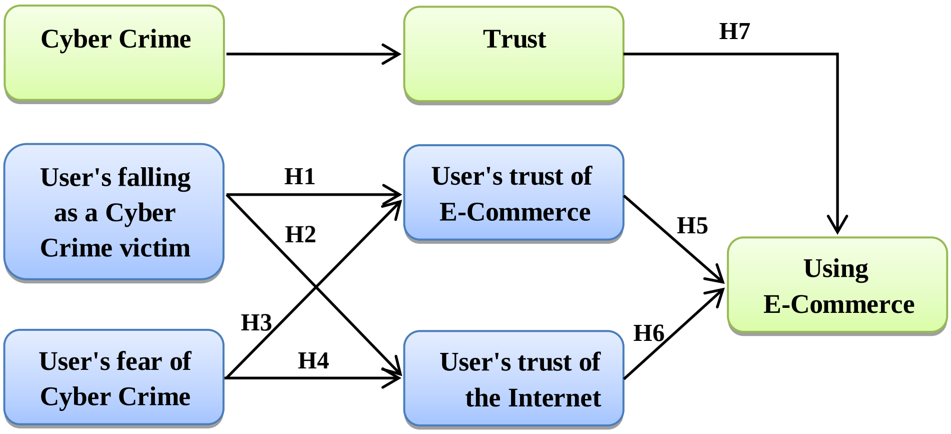
Cyber Crime
Trust
H7
User's falling as a Cyber Crime victim
H1
H2
User's trust of E-Commerce
H5
Using E-Commerce
H3
H4
H6
User's fear of Cyber Crime
User's trust of the Internet

Figure **1**: The Study Model Constructs

As Shown in Figure 1, the study model supposes the following hypotheses:
H1: User's falling as a Cyber Crime victim has a negative impact on User's trust of E-Commerce.
H2: User's falling as a Cyber Crime victim has a negative impact on User's trust of the Internet (medium).
H3: User's fear of Cyber Crime has a negative impact on User's trust of E-Commerce.
H4: User's fear of Cyber Crime has a negative impact on User's trust of the Internet (medium).
H5: User's trust of E-Commerce has a positive impact on Using E-Commerce.
H6: User's trust of the Internet (medium) has a positive impact on Using E-Commerce.
H7: Cyber Crime has a negative impact on Using E-Commerce with trust as a mediator.
The following subsections will try to test and verify these hypotheses.

3.1 Instrument

The researcher used a questionnaire as the main instrument for the data collections; 500 questionnaires are distributed but 377 are valid. The remains are eliminated because of answers duplicity. The study population includes the students, administrative and academic stuff at the Faculty of Computers and Information Sciences at Mansoura University.

3.2 Reliability and Validity Test

The reliability and validity test are accomplished before the data analysis to ensure that the collected data are credible, accurate and consistent to get reliable results. All the study variables are conducted using Cronbach's alpha to calculate the reliability values. The validity is determined by calculating the square root of Cronbach's alpha. The results are shown in Table **2**.

Table 2: Reliability and Validity Coefficients for the Study Variables

Variables	No. of Items	Cronbach's Alpha	Validity
Cyber Crime	7	0.808	0.898
Trust	12	0.818	0.904
Using E-Commerce	4	0.608	0.779

Table 2 shows that all the study variables are significant because all the values of reliability are greater than 0.6 (it must be greater than or equal to 0.6) [10, 11].

4. The Study Model Test

The study tests the direct and indirect relationships between the study variables by using regression analysis. This procedure aims to examine if there are any effects between the variables or not. Also, the correlation coefficient is used to know the nature of these relationships (if they are positive or negative). To test the indirect relationship between the study variables as well as drawing better supported models by statistical tools, the path coefficients between the study variables are estimated. Then, The Goodness of Fit Index (GFI) and The Root Mean Square Residual (RMSR) of the default model are found to identify if the whole study model is significant or not. If GFI of default model = 1 and RMSR of default model = 0, then this study model is significant [12, 13].

4.1 The Path Coefficient

The path coefficients are estimated between the study variables. The first variable, Cyber Crime as an independent variable, is represented in two constructs: User's falling as a Cyber Crime victim and User's fear of Cyber Crime. The second variable, Trust as a mediator variable, is represented in two constructs: User's trust of E-Commerce and User's trust of the Internet. The third variable is using E-Commerce as a dependent variable. After that, the mean of the Cyber Crime represented in (User's falling as a Cyber Crime victim) and (User's fear of Cyber Crime) and the mean of trust represented in (User's trust of E-Commerce) and (User's trust of the Internet) are found to estimate the path coefficients between The Cyber Crime mean and using of E-Commerce with the trust mean as a mediator. Then, The Goodness of Fit Index (GFI) is found to identify whether the whole study model is significant or not.

Figure **2** illustrates the path coefficients between the variables and Table **3** states the path coefficients estimation between the Figure **2** variables; where x is User's falling as a Cyber Crime victim, xx is User's fear of Cyber Crime, m is User's trust of E-Commerce, mm is the User's trust of the Internet, and y is Using E-Commerce. The results of Figure **2** and Table **3** will be discussed in section **4.3**.

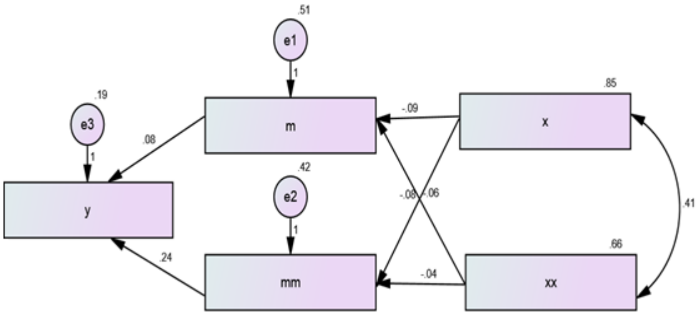

Figure **2.** The Path Coefficients between the variables

Table3: The Path Coefficients estimation on Figure2

Paths			Estimate
x	→	mm	**-0.090**
x	→	mm	**-0.079**
xx	→	m	**-0.055**
xx	→	mm	**-0.043**
m	→	y	**0.080**
mm	→	y	**0.236**

Figure **3** illustrates the path coefficients between the Cyber Crime mean and using of E-Commerce with trust mean as a mediator and Table **4** shows the path coefficients estimation between them; where BBB is the Cyber Crime mean, NNN is the trust mean, and Y is using E-Commerce. The results of Figure **3** and Table **4** will be discussed in subsection **4.3**.

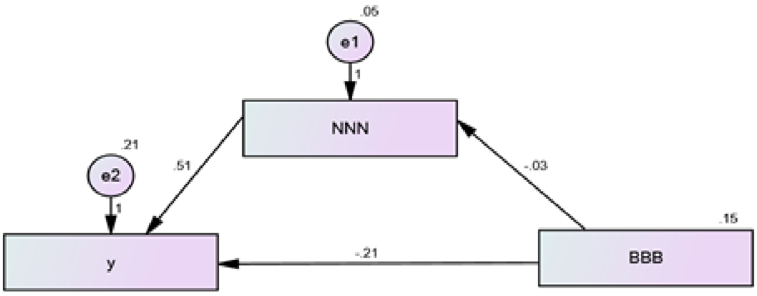

Figure **3**. The Path Coefficients between the Cyber Crime Mean and Using of E-Commerce with the Trust Mean as a mediator.

Table 4: The Path Coefficients Estimation on Figure 3

Paths			**Estimate**
BBB	→	NNN	-0.025
NNN	→	y	0.512
BBB	→	y	-0.212

Table **5** shows The Goodness of Fit Index (GFI) and The Root Mean Square Residual (RMR); where the default model is the researcher's study model, the saturated model is a model that has many parameter estimates, and the independence model is a model that indicates the correlations among the variables.

Table **5** yields the following:
1- The Goodness of Fit Index (GFI) of the default model = 1.
2- The Root Mean Square Residual (RMR) of the default model= 0.
Then, the study model is significant because both (GFI) of the default model = 1 and (RMR) of the default model = 0, which indicates Perfect Fit [12, 13].

Table 5: RMR, GFI

Model	**RMR**	**GFI**
Default model	**0.000**	**1.000**
Saturated model	0.000	1.000
Independence model	0.018	0.940

4.2 Regression Analysis

Regression analysis is used to test the direct and indirect effect between the study variables. Also, the correlation coefficients are used to know the nature of this relationship as well as estimating the path coefficients between the study variables [14, 15].
The regression equation between the independent and dependent variable is: **Y= a + βX+ e**; where "Y" is the dependent variable, "a" is the intercept, "β" is the slope, "X" is the independent variable and "e" is the standard error [16].

4.3 Hypotheses Test

In this Subsection, the study model hypotheses are tested to get the final results. Table **6** summarizes hypotheses variables relationships according to the regression model, correlation coefficients and path coefficients among them.

Table 6: Summary of hypotheses variables relationships according to Regression Model, Correlation Coefficients and Path Coefficients among them

Hs.	Variables			F	R^2	a	β	e	Regression Equation	r	Path Coefficient
H1	User's falling as a Cyber Crime victim	→	User's trust of E-Commerce	8.146	0.021	2.740	-0.103	0.036	$Y= 2.740-0.103X_1+ 0.036$	-0.146	-0.090
H2	User's falling as a Cyber Crime victim	→	User's trust of the Internet (medium)	7.534	0.0196	2.725	-0.100	0.036	$Y= 2.740-0.103X_2+ 0.036$	-0.140	-0.079
H3	User's fear of Cyber Crime	→	User's trust of E-Commerce	5.595	0.015	2.735	-0.097	0.041	$Y= 2.735-0.097X_3+ 0.041$	-0.121	-0.050
H4	User's fear of Cyber Crime	→	User's trust of the Internet (medium)	4.936	0.013	2.715	-0.092	0.041	$Y= 2.715-0.092X_4+ 0.041$	-0.114	-0.043
H5	User's trust of E-Commerce	→	Using E-Commerce	91.211	0.196	1.861	0.329	0.034	$Y= 1.861+ 0.329X_5+ 0.034$	0.442	0.080
H6	User's trust of the Internet (medium)	→	Using E-Commerce	89.088	0.192	1.876	0.324	0.034	$Y= 1.876+ 0.324X_6+ 0.034$	0.438	0.236
H7	**Cyber Crime**	$\xrightarrow{\text{Trust}}$	**Using E-Commerce**								**-0.212**

Here, "F" is the F statistic value in the regression model, "R^2" is the coefficient of determination "R-Squared", "a" is the intercept, "β" is the slope, "e" is the standard error and "r" is the correlation coefficient.

According to the tables 3, 4 and 6 the hypotheses test yields the following:

H1: User's falling as a Cyber Crime victim has a negative impact on User's trust of E-Commerce.

Through this hypothesis, there are two variables: User's falling as a Cyber Crime victim as an independent variable and User's trust of E-Commerce as a dependent variable. The analysis results are:
1- The regression model is significant for effect of the independent variable on the dependent, with (F=8.146).
2- There is a negative relationship between the independent and dependent variable, where the correlation coefficient (r = -0.146); therefore, the percentage of this inverse relationship is 14.6%.
3- The independent variable (User's falling as a Cyber Crime victim) determines the changes of the dependent variable (User's trust of E-Commerce) with percentage = 2%, where the coefficient of determination "R-Squared" between these variables is (R^2 = 0.021).
4- There is a negative effect between the independent and dependent variable because of the inverse relationship between them, and due to the path coefficient between them is -0.090.

5- The hypothesis 1 states "User's falling as a Cyber Crime victim has a negative impact on User's trust of E-Commerce" is supported.
6- Then: $Y= 2.740-0.103X_1+ 0.036$

H2: User's falling as a Cyber Crime victim has a negative impact on User's trust of the Internet (medium).

Through this hypothesis, there are two variables: User's falling as a Cyber Crime victim as an independent variable and User's trust of the Internet (medium) as a dependent variable. The analysis results are:
1- The regression model is significant for effect of the independent variable on the dependent, with (F=7.534).
2- There is a negative relationship between the independent and dependent variable, where the correlation coefficient (r = -0.140); therefore, the percentage of this inverse relationship is 14%.
3- The independent variable (User's falling as a Cyber Crime victim) determines the changes of the dependent variable (User's trust of the Internet) with percentage = 1.96%, where the coefficient of determination "R-Squared" between these variables is (R^2 = 0.0196).
4- There is a negative effect between the independent and dependent variable because of the inverse relationship between them, and due to the path coefficient between them is -0.079.
5- The hypothesis 2 that "User's falling as a Cyber Crime victim has a negative impact on User's trust of the Internet" is supported.
6- The regression equation $Y= 2.725-0.100X_2+ 0.036$

H3: User's fear of Cyber Crime has a negative impact on User's trust of E-Commerce.

Through this hypothesis, there are two variables: User's fear of Cyber Crime as an independent variable and User's trust of E-Commerce as a dependent variable. The analysis results are:
1- The regression model is significant for effect of the independent variable on the dependent, with (F=5.595).
2- There is a negative relationship between the independent and dependent variable, where the correlation coefficient (r = -0.121); therefore, the percentage of this inverse relationship is 12.1%.
3- The independent variable (User's fear of Cyber Crime) determines the changes of the dependent variable (User's trust of E-Commerce) with percentage = 1.5%, where the coefficient of determination "R-Squared" between these variables is (R^2 = 0.015).
4- There is a negative effect between the independent and dependent variable because of the inverse relationship between them, and due to the path coefficient between them is -0.050.
5- The hypothesis 3 that "User's fear of Cyber Crime has a negative impact on User's trust of E-Commerce" is supported.
6- The regression equation $Y= 2.735-0.097X_3+ 0.041$

H4: User's fear of Cyber Crime has a negative impact on User's trust of the Internet (medium).

Through this hypothesis, there are two variables: User's fear of Cyber Crime as an independent variable and User's trust of the Internet (medium) as a dependent variable. The analysis results are:
1- The regression model is significant for effect of the independent variable on the dependent, with (F=4.936).

2- There is a negative relationship between the independent and dependent variable, where the correlation coefficient (r = -0.114), therefore the percentage of this inverse relationship is 11.4%.
3- The independent variable (User's fear of Cyber Crime) determines the changes of the dependent variable (User's trust of the Internet) with percentage = 1.3%, where the coefficient of determination "R-Squared" between these variables is (R^2 = 0.013).
4- There is a negative effect between the independent and dependent variable because of the inverse relationship between them, and due to the path coefficient between them is -0.043.
5- The hypothesis 4 that "User's fear of Cyber Crime has a negative impact on User's trust of the Internet" is supported.
6- The regression equation $Y= 2.715-0.092X_4+ 0.041$

H5: User's trust of E-Commerce has a positive impact on Using E-Commerce.

Through this hypothesis, there are two variables: User's trust of E-Commerce as an independent variable and Using E-Commerce as a dependent variable. The analysis results are:
1- The regression model is significant for effect of the independent variable on the dependent, with (F=91.211).
2- There is a positive relationship between the independent and dependent variable, where the correlation coefficient (r = 0.442); therefore, the percentage of this positive relationship is 44.2%.
3- The independent variable (User's trust of E-Commerce) determines the changes of the dependent variable (Using E-Commerce) with percentage = 19.6%, where the coefficient of determination "R-Squared" between these variables is (R^2 = 0.196).
4- There is a positive effect between the independent and dependent variable because of the positive relationship between them, and due to the path coefficient between them is 0.080.
5- The hypothesis 5 that "User's trust of E-Commerce has a positive impact on Using E-Commerce" is supported.
6- The regression equation $Y= 1.861+0.329X_5+ 0.034$

H6: User's trust of the Internet (medium) has a positive impact on Using E-Commerce.

Through this hypothesis, there are two variables: User's trust of the Internet (medium) as an independent variable and Using E-Commerce as a dependent variable. The analysis results are:
1- The regression model is significant for effect of the independent variable on the dependent, with (F=89.088).
2- There is a positive relationship between the independent and dependent variable, where the correlation coefficient (r = 0.438); therefore, the percentage of this positive relationship is 43.8%.
3- The independent variable (User's trust of the Internet) determines the changes of the dependent variable (Using E-Commerce) with percentage = 19.2%, where the coefficient of determination "R-Squared" between these variables is (R^2 = 0.192).
4- There is a positive effect between the independent and dependent variable because of the positive relationship between them, and due to the path coefficient between them is 0.236.
5- The hypothesis 6 that "User's trust of the Internet has a positive impact on Using E-Commerce" is supported.
6- The regression equation $Y= 1.876+0.324X_6+ 0.034$

H7: Cyber Crime has a negative impact on Using E-Commerce with Trust as a mediator.

Through this hypothesis, there are three variables: Mean of the Cyber Crime as an independent variable, represented in (User's falling as a Cyber Crime victim) and (User's fear of Cyber Crime), Mean of Trust as a mediator variable, represented in (User's trust of E-Commerce) and (User's trust of the Internet) and Using E-Commerce as a dependent variable; where the relationship between the Cyber Crime and Using E-Commerce is indirect, due to trust is a mediator variable. The analysis results are:
1- There is a negative effect between the independent and dependent variable with trust as a mediator due to the path coefficient between them is -0.212.
2- The hypothesis 7 that "Cyber Crime has a negative impact on Using E-Commerce with the Trust as a mediator" is supported.
3- According to the path coefficients between the whole study variables, the study model will be as shown in figure **4**.

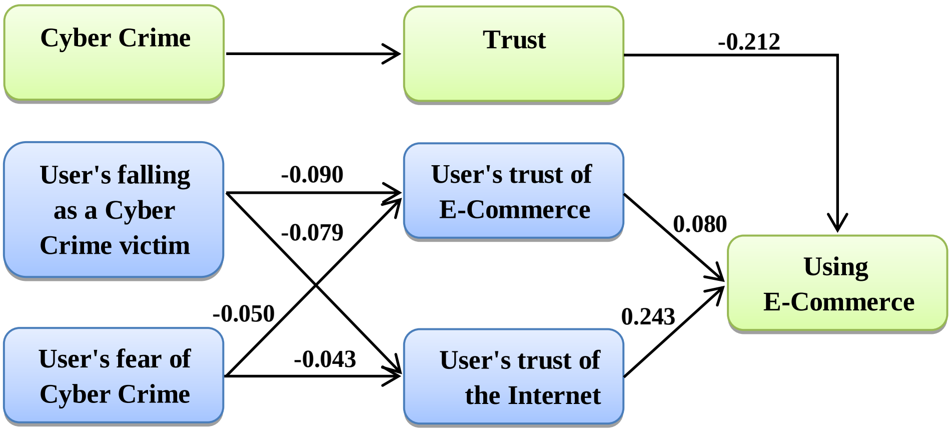
Cyber Crime
Trust
-0.212
User's falling as a Cyber Crime victim
-0.090
User's trust of E-Commerce
-0.079
0.080
Using E-Commerce
-0.050
0.243
User's fear of Cyber Crime
-0.043
User's trust of the Internet

Figure 4: The Study Model according to The Path Coefficients between the whole variables study

6. Conclusion and Future Works

The main study question of this study is: To what extent does the Cyber Crime affect using E-Commerce? This study proposes a model to answer this question by including the concepts of Cyber Crime and trust. The Cyber Crime is represented in user's falling as a Cyber Crime victim and user's fear of Cyber Crime, while trust is represented in user's trust of E-Commerce and user's trust of the Internet (medium). The data is gathered from a sample of respondents, by conducting a questionnaire. The researcher proved that there is a negative impact of user's falling as a Cyber Crime victim and user's fear of Cyber Crime on the trust of E-Commerce and user's trust of the Internet (medium). Also, he proved that there is a positive impact of user's trust of E-Commerce and user's trust of the Internet (medium) on using E-Commerce. Finally, there is a negative impact of the Cyber Crime on E-Commerce with trust as a mediator. The future works should consider the Cyber Crime impact on E-Commerce via examination of the Cyber Crime falling and Cyber Crime fear on E-Commerce with the existence of trust, by using various samples from various populations. It would be much better to generalize our results than restricting to the faculty samples. The future researchers should combat the Cyber Crime via obtaining more information about experiences, fears and perceptions of E-Commerce users with Cyber Crime to solve this phenomenon and enhance the E-Commerce trust to avoid any risk may threat the E-Commerce users.

References

1. Mayur Patel, Neha Patel, Amit Ganatra and Yogesh Kosta. "E-Commerce and Attached E-Risk with Cybercrime," in *International Conference ISCET*. RIMT University, Punjab, India, 2010.
2. Katherine Taken Smith, "An Analysis of E-Commerce: E-Risk, Global Trade, and Cybercrime", SSRN Electronic Journal, December 2008DOI: 10.2139/ssrn.1315423
3. Stan Kratchman, Jacob Lawrence Smith and Murphy Smith, "Perpetration and Prevention of Cyber Crimes", *Internal Auditing*, Vol. 23, No. 2, 2008, pp. 3-12.
4. Webroot Inc, "Combatting Today's Financial and E-Commerce Threats", Available at:https://www.webroot.com/shared/pdf/wsab-mp-ds-finance-ecommerce-threats.pdf, Visited: 20/12/2016
5. Billy Henson, "Fear of Crime Online: Examining the Effects of Online Victimization and Perceived Risk on Fear of Cyberstalking Victimization", PhD Thesis, School of Criminal Justice of the University of Cincinnati, 2011.
6. Ainur Rofiq, "Impact of Cyber fraud and Trust of E-Commerce System on purchasing intentions: Analyzing Planned Behaviour in Indonesian Business", PhD thesis, Faculty of Business and Law of the University of Southern Queensland, 2012.
7. Rainer Bohme and Tyler Moore, "How Do Consumers React to Cybercrime?", The 7th APWG e-Crime Researchers, Las Croabas, Puerto Rico, 2012.
8. Szde Yu, "Fear of Cyber Crime among College Students in the United States: An Exploratory Study", *International Journal of Cyber Criminology* (IJCC), Vol. 8, No. 1, 2014, pp. 36–46.
9. Wekundah Ruth Nangeche, "The Effects of Cyber-crime on E-Commerce; a model for SMEs in Kenya", Master's thesis, School of Computing and Informatics of the University of Nairobi, 2015.
10. Ganesh Thanasegaran, "Reliability and Validity Issues in Research", Available at: http://aupc.info/wp-content/uploads/35-40-ganesh.pdf, Visited: 09/01/2017.
11. Mohsen Tavakol and Reg Dennick, "Making sense of Cronbach's alpha", International Journal of Medical Education, Vol. 2, No. 53, 2011, pp. 53-55.
12. Dr. V Ramadevi, Dr. M Meenakshi Saratha and Dr. K Vanaja, "Structural equation modelling on shoppers purchasing outcomes in shopping malls, Coimbatore City", International Journal of Multidisciplinary Research and Development, Vol. 3, No.11, 2016, pp. 94-98.
13. James L. Arbuckle, "IBM SPSS Amos 21 User's Guide", 2012 edition, IBM Corp, 2012.
14. Dan Campbell and Sherlock Campbell, "Statlab Workshop Introduction to Regression and Data Analysis", Available at: http://statlab.stat.yale.edu/workshops/IntroRegression/StatLab-IntroRegressionFa08.pdf, Visited: 09/01/2017.
15. John O. Rawlings, Sastry G. Pantula and David A. Dickey, "Applied Regression Analysis: A Research Tool", Second Edition, Springer, 1998.
16. Saint Germain, "Research Methods: Application of relevant research techniques to problems in public policy and administration", PPA 696, Available at: http://web.csulb.edu/~msaintg/ppa696/696regs.htm, Visited: 09/01/2017.