

**Customer Awareness On Cyber Security Issues With Special Reference To
Online Shopping: A Study Among Generation Y**

By NazreenParveen Ali (Junior Research fellow, Deptt of Commerce, Dibrugarh University)
&

& Rina Adak (M.Phil Research Scholar, Deptt of Commerce, Dibrugarh University)

Abstract

Online shopping is the latest developmental trend among generation Y. With the emergence of latest online shopping apps every day, there has also been an expansion on the cliental base. The reach to global and imported products along with domestic ones delivered at the very doorstep at a relatively economic manner has drawn the fascination of almost every human and most particularly the younger generation. Despite of increasing cyber crimes and risk of hackers, phishing scams, and ransom ware attacks etc., customers rushing for the best deals online are not really caring about such serious threats to their personal and financial possessions. At the same time, it is still a great challenge to cyber security due to threats from insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge to combat the attacks. As the younger generation is responsible for carrying the rich legacy of leading the genets towards a brighter digital world, the present study seeks to understand the generation Y's awareness on cyber security related to online shopping practices and find a solution to educate them on same for a secure and hassle free online shopping experience.

Keywords: Cyber security, Generation Y, online shopping, phishing, ransom ware

1. Introduction:

Online shopping is the latest technology of the 21st century the craze of which has gripped the fascination of the youth in a very less span of time. Currently almost all the youngsters are aware of this development and have been availing the benefits without having to step out of their home to meet their materialistic needs. Traditional shopping has lost its charm in the digital world. Online shopping offers a wider variety of world class facilities to buyers such as reach for global as well as imported products, economy in meeting rare and customised demands, fooding, clothing and almost anything delivered at your doorstep, easy price, etc. But such benefits may override the cost if proper security measures are not taken by the beneficiaries. One such major threat is cyber security issues where third parties or hackers get involved and threaten consumer's privacy and monetary information leading to online theft of personal information and financial losses. Such threats bother consumers who may hesitate to share credit card and debit card details over the online shopping apps and thereby prefer not to continue with the purchase. Even though they continue with the purchase, a level of mental stress sometimes grips their mind regarding

the potential threats. Thus “Customer Trust” plays a key role towards his/her decision making process. A protected infrastructure installed in devices may sometimes prove to be a fruitful solution but this itself not sufficient for building the level of trust of consumers in electronic shopping. Only a consumer well aware and well educated of the cyber threats and safety measures will be confidently able continue smoothly with “happy purchases” online. So for secured and hassle free transactions online, it is very much needed to understand the awareness needs and educate the online buyers on the potential threats and associated security measures on cyber security.

Since online shopping practices are most popular among the younger generation, the study makes a sincere attempt to understand and find solutions to improve their knowledge on cyber security threats associated with online shopping.

2. Review of Literature

Azadava et al (2011) attempted to examine the factors influencing perception of consumer on online shopping to draw a link as how it affects their online-shopping behaviour. They developed a model which reflected direct influence of “perception”-related factors on behaviour or their indirect influence through consumers’” attitudes” on online buying behaviour. **Goutam** (2015) studied the nature of cyberspace and observed that internet is not at all secure to transmit the confidential and financial information. He further emphasized on hacking as common and harmful for global economy and security and the growing worldwide incidences over the years. **Maurya and Bharati** (2016) studied the level of cyber security in e commerce so as to provide better solutions to the threats and improve customer,s confidence in online transactions. They identified prevention against unauthorised data modification, authenticity, Confidentiality, privacy and repudiation of agreements as the dimensions for e commerce safety. **Niranjanamurthy & Chahar** (2013) discussed E-commerce security issues, security measures, digital e-commerce cycle/online shopping, security threats and guidelines for safe and secure online shopping through shopping web sites. They suggested not revealing to much information and antivirus measures to combat against e commerce frauds. **Hamza**(2017) conducted a study on Cyber Crimes which cause our sensitive data to be used without our permission. Governments are aware of this matter doing everything they can to secure our networks but many say security is just an illusion. In this whole report he analyzed the strength of the people who are trying to spoil the Cyber Ecosystem. **DamboItari et al** (2017) conducted a study on a series of organized crime attacking cyberspace and cyber security. Cyber security is at a threat clicking into unfamiliar links connecting to unfamiliar Wi-Fi, downloading software and files from unsafe sites, power consumption, electromagnetic radiation waves, and many more. By having strong internal interactions of properties, software complexity can prevent software crash and security failure.

2. 1 Research Gap:

The above literature review reveals that though studies are conducted in large scale on cyber security threats in various areas, comparatively very few studies have dealt with awareness on cyber threats and safety measures associated with online shopping.

2.2 Statement of the problem:

With the advent of technology and everything transforming into digital in the busy modern society, the fascination and frequency of online shopping is increasing due to its time saving and economic nature where we get everything (clothing, furnishings, food, movie tickets etc) we need right at click of a mouse. However these facilities are bringing with them some unwanted threats which pose great danger to one's financial and sometimes possessions. Insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge to combat the attacks place in an insecure environment. As the younger generation is responsible for carrying the rich legacy of leading the genext towards a brighter digital world, there is a need to have an understanding the generation Y's awareness on cyber security threats and safety measures related to online shopping practices and identify feasible modes to educate them on same for a secure and hassle free online shopping experience.

3. Objectives of the study:

- (a) To know the extent of cyber crime threats in online shopping practices
- (b) To understand the awareness level of youth on cyber crime practices associated with online shopping with respect to demographic features.
- (c) To offer valuable suggestions for cyber crime education based on needs of youth

4. Hypothesis of the study:

Ho1: There is no significant relationship between frequency of online shopping and cyber crime incidences

Ho2: There is no association between the trust score of respondents on cyber security and the frequency of online shopping by them

Ho3: There is no significant relationship between awareness score and demographic profiles(age, gender, educational qualification)

Ho4: There is no significant relationship between time spent online and education on cyber threats

5. Limitations of the study:

- a) There is some scope for biasness in responses from respondents since the study include some psychological questions to gauge awareness score of respondents
- b) The sample of study being small, the scatteredness around a large region offer some scope of error.

4. Methodology

The study is based on primary data collected through questionnaires designed over google forms which were mailed to over 100 respondents. Secondary data used for the purpose of the study was collected from various books and e- journals.

Sampling technique

The sample consists of only young people within Northeast. To distinguish this better we have collected data from people having their birth days in the 1880 and 2003 (beyond age of 18 but below 40). Convenience sampling technique is used for selecting the respondents. 100 questionnaires were mailed out of which 84 responses were received. 4 questionnaires were discarded due to incomplete responses leaving us with only 80 responses to be evaluated to fulfil our purpose.

Structure of the questionnaire

The questionnaire is designed by incorporating questions starting with demographic profile of the respondents, their buying behaviour and experiences over online shopping sites, their attitude and habits for safety measures against cyber threats and their opinion on need and modes of cyber security education.

Tools and Techniques for analysis

Cross tables and chi square test are applied to test the stated hypothesis. Cross table are compiled and the test for chi square is conducted using SPSS 21.0 version.

5. Analysis and Discussions

Ho1: There is no significant relationship between frequency of online shopping and cyber crime incidences

Table 1.1: Table showing relationship between frequency of online shopping and incidences of cyber crime encountered by respondents

		No . of times encountered cyber threat				Total
		Never	1time	2 times	3 times and more	
Frequency of online purchase	Rarely	7	0	0	0	7
	Ocasionally	20	1	0	0	21
	Often	28	8	2	0	38
	Regularly	4	7	4	1	16
Total		59	16	6	1	82

Source: Compiled by Primary Data

Table1.2.: Table showing results of chi square test for relationship between frequency of online shopping and incidences of cyber crime encountered by respondents

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	29.067 ^a	9	.001
Likelihood Ratio	30.179	9	.000
Linear-by-Linear Association	20.968	1	.000
N of Valid Cases	82		

a. 11 cells (68.8%) have expected count less than 5. The minimum expected count is .09.

Source: Results from SPSS version 21.0

Observation: From table 1.1, it can be observed that online shopping is a popular practice among all the respondents. Only 8.53% respondent purchase things online very rarely and 25.61% respondents answered that they purchase online products occasionally. Whereas it can be seen that majority of the respondents engage in online purchases either more often (46.3%) or regularly (19.51%). Looking towards the cyber crime incidences, only 28.05% respondents have been the victims of this unfortunate event.

Interpretation: Again from table .1.2, it can be observed that, the p value of chi square test is 0.001 which is less than 0.05. Therefore we reject the null hypothesis and interpret that there is a significant relationship between frequency of online shopping and cyber crime incidences encountered by the respondents.

Ho2: There is no association between the trust score of respondents on cyber security and the frequency of online shopping by them,

Table 2.1.: Cross table showing relationship between frequency of online purchases and trust level of respondents in cyber security in online shopping

	Frequency of online purchase				Total
	Rarely	Ocasionally	Often	Regularly	
6.00	0	0	1	0	1
8.00	0	1	2	0	3
9.00	0	1	5	0	6
10.00	2	3	5	5	15
11.00	1	3	7	1	12
12.00	2	6	7	3	18
13.00	1	4	5	1	11
14.00	1	3	2	5	11
15.00	0	0	3	1	4
17.00	0	0	1	0	1
Total	7	21	38	16	82

Source: Compiled by Primary Data

Table2.2. : Chi square test for frequency of online purchases and trust level of respondents in cyber security in online shopping

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.678 ^a	27	.801
Likelihood Ratio	24.384	27	.609
Linear-by-Linear Association	.179	1	.672
N of Valid Cases	82		

a. 35 cells (87.5%) have expected count less than 5. The minimum expected count is .09.

Source: Results from SPSS version 21.0

Interpretation: Table 2.1. shows the trust score of the respondents in online shopping based on certain questions on trust issues being asked to them. It can be observed that trust score of 54.88% respondents are higher than the mean trust score (of 11.66)

Further table 2.2. shows that the p value for chi square test is .801. Hence we are unable to reject the null hypothesis and conclude that no association was found between the trust score of respondents and the frequency of online shopping by them,

Ho3: There is no significant relationship between awareness score and demographic profiles(age, gender, educational qualification)

Table3.1.: Table showing relationship of awareness scores of online buyers on cyber crime threats and associated security measures with demographic characteristics

gender of respondent * awareness score Cross tabulation

		awareness score																	Total
		20	26	27	28	29	30	31	32	33	34	35	36	37	38	39	41	42	
gender of respondent	male	0	1	1	1	4	3	0	5	5	3	1	0	1	0	1	1	1	28
	female	1	2	1	6	7	6	5	5	10	3	3	1	1	2	1	0	0	54
Total		1	3	2	7	11	9	5	10	15	6	4	1	2	2	2	1	1	82

age of respondent * awareness score Cross tabulation

age of respondent	18-25 years	0	1	1	2	2	3	0	5	3	3	1	0	0	0	0	0	21
	26-30 years	0	1	0	3	2	1	0	2	7	1	0	0	0	1	2	0	21
	31-35 years	0	1	1	1	6	4	4	2	4	0	2	1	1	0	0	1	28
	36-40 years	1	0	0	1	1	1	1	1	1	2	1	0	1	1	0	0	12
Total		1	3	2	7	11	9	5	10	15	6	4	1	2	2	2	1	82

educational qualification of respondent * awareness score Crosstabulation

educational qualification of respondent	Below HS	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	3
	HS	1	1	1	1	4	2	2	3	3	0	0	0	0	1	1	0	20
	graduation	0	2	0	5	5	7	1	5	7	4	2	1	0	1	1	0	41
	post graduate and above	0	0	1	0	2	0	2	2	5	1	1	0	2	1	0	0	18
Total		1	3	2	7	11	9	5	10	15	6	4	1	2	2	2	1	82

Source: Compiled by Primary Data

Observation: The above cross table 3.1. shows the relationship of awareness scores of online buyers on cyber crime threats and associated security measures with demographic characteristics of the respondents (namely gender, age and educational qualification). It was observed that maximum respondents (15) attained the median awareness score of 33 and most of the respondents are scattered around this median score which indicates moderate level of awareness among youngsters on cyber crime and associated security measures

Table 3.2. : Chi-Square Test on awareness scores of online buyers on cyber crime threats and associated security measures with gender

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.391 ^a	16	.717
Likelihood Ratio	15.757	16	.470
Linear-by-Linear Association	1.845	1	.174
N of Valid Cases	82		

a. 29 cells (85.3%) have expected count less than 5. The minimum expected count is .34.

Source: Results from SPSS version 21.0

Interpretation:

Table 3.2. shows that the p value for chi square test is .717. Hence we are unable to reject the null hypothesis and conclude that no association was found between the gender of the respondents and awareness level on cyber security threats and associated safety measures.

Table 3.3. : Chi-Square Test relationship of awareness scores of online buyers on cyber crime threats and associated security measures age

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	50.918 ^a	48	.360
Likelihood Ratio	54.170	48	.251
Linear-by-Linear Association	.031	1	.860
N of Valid Cases	82		

a. 67 cells (98.5%) have expected count less than 5. The minimum expected count is .15.

Source: Results from SPSS version 21.0

Interpretation:

Table 3.3. shows that the p value for chi square test is .360. Hence we are unable to reject the null hypothesis and conclude that no association was found between the age of the respondents and awareness level on cyber security threats and associated safety measures

Table 3.4.: Chi-Square Tests relationship of awareness scores of online buyers on cyber crime threats and associated security measures with educational qualification

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	48.109 ^a	48	.468
Likelihood Ratio	50.915	48	.360
Linear-by-Linear Association	3.135	1	.077
N of Valid Cases	82		

a. 65 cells (95.6%) have expected count less than 5. The minimum expected count is .04.

Source: Results from SPSS version 21.0

Interpretation:

Table 3.4.shows that the p value for chi square test is .468. Hence we are again unable to reject the null hypothesis and conclude that no association was found between the gender of the respondents and awareness level on cyber security threats and associated safety measures.

Overall, we reach a conclusion that there is no significant association between demographic characteristics of respondents and their awareness on cyber security threats and associated safety measures.

Ho4: There is no significant association between time spent online and education on cyber threats

Table 4.1. Cross table on awareness score on cyber threats and time spent online

		Time spent online					Total
		less than 1 hr	1-2 hr	3-4 hr	4-5hr	more than 5 hrs	
Awareness	20.00	0	0	0	1	0	1
	26.00	1	0	1	1	0	3
	27.00	0	0	1	1	0	2
	28.00	0	0	1	2	4	7
	29.00	1	0	4	2	4	11
	30.00	0	1	0	4	4	9
	31.00	0	3	1	1	0	5
	32.00	0	1	0	5	4	10
	33.00	0	2	4	7	2	15
	34.00	0	2	1	3	0	6
	35.00	1	0	1	2	0	4
	36.00	0	0	1	0	0	1
	37.00	0	2	0	0	0	2
	38.00	0	1	0	1	0	2
	39.00	0	1	0	1	0	2
	41.00	0	0	1	0	0	1
	42.00	0	0	1	0	0	1
Total		3	13	17	31	18	82

Source: Compiled by Primary Data

Table 4.2. Chi-Square Tests on awareness score on cyber threats and time spent online

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	78.948 ^a	64	.099
Likelihood Ratio	76.485	64	.136
Linear-by-Linear Association	4.849	1	.028
N of Valid Cases	82		

a. 84 cells (98.8%) have expected count less than 5. The minimum expected count is .04.

Source: Results from SPSS version 21.0

Observation: The above cross table 4.1 was compiled to observe the relationship between the times spent by generation Y over internet and the level of awareness on cyber threats and associated safety measures. It was observed that respondents who spend 4-5 hrs. (37.8%) on internet are having maximum awareness on cyber threat issues and protection measures for them. But again those spending more than 5 hrs (21.9%) are showing a low level of awareness.

Interpretation: Further in table 4.2 it is seen that the p value for chi square test to check the association between these two variables is .099 which leaves us no option but to the null hypothesis that. There is no significant association between time spent online and education on cyber threats

Need for Cyber Education

Table 5.1. : Table showing views and need of respondents for cyber education

	Yes	%	No	%
People ought to be receive education on cyber security in their respective workplaces/institutes	74	90.25	8	9.75
Cyber Security should form a part of computer education in schools	63	76.83	19	23.17
Government should organize workshops on cyber security issues manually or online	49	59.76	33	40.24
Individuals themselves ought to educated themselves on cyber security issues	56	68.29	26	31.71

Source: Self Compiled from Primary Data

Table 5.1. shows that a vast majority (90.25%) of respondents want cyber education to be imparted in workplaces or institutes. &6.83% respondents agree cyber education to be an important part of computer education of students in the digital world. Further 68.29% believes people themselves should take initiative in educating themselves on cyber security. Some respondents(59.76%) also want government to address this issue since with turning the country into a digital global village, cyber education should form an inseparable part of government responsibility since some threats also come with the benefits of this simplified.

6. Findings:

1. It was observed that all the respondents are acquainted with the idea of online shopping and are engaged with the practice of buying thing online. This indicates how generation Y has adapted themselves to the digital changes around.
2. Only 28.05% of the responds have been victims of cyber crime. However multiple encounters with such unfortunate incident is very much less (8.54%). This indicate once the people are victimise by cyber crimes either they become more careful or take active interest in improving their awareness on safety against such crimes.

3.It was also observed that the number of incidences of cyber crime reported to the closely associated with the frequency of online shopping.

4. The level of trust of the respondents on cyber safety has nothing to do with the frequency of online purchases. Thus online purchases are made irrespective of the trust of the respondents on cyber safety.

5. The awareness level of the respondents on cyber safety are irrespective of their gender, age, and educational qualification.

6. The awareness level of the respondents on safety measures against cyber crime has no association with the amount of time spent online.

7. Majority of the respondents want knowledge on cyber security measures to be a part of computer education since high school. The youth is also of the opinion that self education on cyber security shall be preferred over initiative of government to impart education on cyber security. But this might not always be possible because in the digital world when government is compelling every process digitally, it ought to be a responsibility of the government to impart cyber education correspondingly.

7. Conclusion:

Online shopping is the most popular and convenient trend among the youth in recent times. But the added benefits also bring with them dangerous threat which may hamper ones financial and identity. Although the young generation is engaged with digital technology most of the time still they are not fully aware of the associated threats. It's high time to fully the youth on security against cyber crime to protect themselves in a world which is rapidly moving towards a digital transformation. A lot of safety measures to protect themselves against the heinous crime are available. The only need is to cultivate these safety measures in the day to day practice of conducting online transactions. The same is possible through a proper awareness on the safety measures which can be imparted to the youth as apart of computer education during their school days. Also efforts can be made to make the youth aware of the need to self educate them on cyber crime safety measures over internet itself by spending a small portion of time spent online for the needful. A small loophole in this respect will add more cost over the benefits from such emerging technologies.

References:

1. Azadavar, R *et al* (2011), "The Role of Security as a Customer Perception on Customers' Online Purchasing Behavior", International Conference on Software and Computer Applications, IPCSIT vol.9, Pp.174-181
2. Goutam, R. K. (2011), "Importance of Cyber Security", International Journal of Computer Applications , Volume 111 – No 7, Pp. 14-17

3. Maurya, S.K., Bharati, N. P.(2016), "Cyber Security; Issue and Challenges in E-Commerce", *PARIPEX - INDIAN JOURNAL OF RESEARCH*, Volume : 5, Issue : 1, Pp. 191-193
4. Niranjana Murthy M 1 & Chahar, D (2011), "The study of E-Commerce Security Issues and Solutions", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 2, Issue 7, Pp. 1-12
5. Muhammad Hamza (2017) "Cyber Crime and Security" Research Gate
6. Buch, R *et al* (2018) "World Of Cyber Security And Cybercrime" ResearchGate
7. Damboitari, E *et al* (2017) "Mercy Cyber Space Technology: Cybercrime, Cyber Security And Models Of Cyber Solution, A Case Study Of NIGERIA" *IJCSMC*, Vol. 6, Issue. 11, , Pp.. 94-113

APPENDIX

I. 5 point Likert Scale questions for compilation of trust score

1. Personal data cannot be stolen over the online shopping apps to make money?
2. I believe anti virus as a preventive measure for cyber security
3. I m not annoyed from online shopping sites
4. I don't see any problem with web browsing histories being monitored as a security measure?
5. I have my debit/credit cards stored with online shopping apps
6. I trust in OTPs as a secure form for making payments
7. I trust online shopping as secure

II. 5 point Likert Scale for calculation of awareness score

1. I establish a strong password for each online shopping account
2. I check out as a guest to avoid saving payment information online.
3. I use different passwords on each of my online accounts
4. I use one credit card online or pay through a secure online mechanism.
5. I choose well-known online retailers that have an established reputation for cybersecurity.
6. I look for the lock symbol at the top of my browser or "https" in your URL bar.
7. I never shop or log in to personal accounts when on public Wi-Fi or a public device
8. I do not leave my browser open on a shopping site for long periods of time.
9. I keep my devices up-to-date apply all the available fixes for known problems and vulnerabilities
10. I am careful which links I click on in emails.
11. I do not use my work email address for retail accounts

3. Likert scale for education need for cyber security

1. People ought to be receive education on cyber security in their respective workplaces/institutes
2. Cyber Security should form a part of computer education in schools
3. Government should organize workshops on cyber security issues manually or online
4. Individuals themselves ought to educated themselves on cyber security issues
5. Cyber security education can be ruled out if security software is used
6. Education on cyber security is not particularly necessary