CybercrimeAwareness among Students at a Teacher Training College

Moanes H. **Tibi**, Ph.D[*1], Kholod Hadeje B.Ed[*2], Bashier Watted M.Sc[*3]
Computer Science Department, Faculty of Education, Beitberl College, Israel

Abstract
Instances of cybercrimes have increased rapidlyover the past decade and have become part of the everyday lives of citizens. The purpose of this pilot study was to assess the level of cybercrime awareness among teaching students and to find out whether computer science students had heightened cybercrime awareness compared to students taking other majors at the same college. For this purpose, a sample of 73 Arab students from a teacher education college in the center of Israel was selected. A questionnaire survey was conducted to collect the data about students' awareness of cybercrime. The finding of the study revealed that the level of cybercrime awareness among the participants was inadequate and that the independent variables, such as year of study, major subject, and prior computer knowledge did not yield any statistically significant differences. In addition, no correlation was found between the students' prior computer knowledge and theirsusceptibility to being victims of cybercrimes. We conclude that higher education institutions should provide training courses on cyberspace security to all students in order to enable them to avoid becoming victims of cybercrimes.Finally, recommendations for future research are suggested.

Keywords - *Cybercrime, Cybercrime Awareness, College students,Student teachers*

I. INTRODUCTION

Cybercrimes are any criminal activities that are performed using networked computers or other networked devices as a medium. Reference [7] define Cybercrimes as"offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (networks including but not limited to chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)" (p. 1019).

Moreover, cybercrimes are not just increasing; they are also evolving. Their methods vary and can take the form of fake emails, link manipulation, fraudulent invoices, phone calls and phone messages. You might even receive a fraudulent email seemingly from your employer inviting you to attend a staff party,for which you need to register;thus you will be asked to input your private information on a fraudulent sign-in page. You might notnotice the difference between the sender's email address and your employer's email address, because only one letter or character is different. Moreover, thedifference between the sign-in page URL and the original sign in page for your organization might bebarely noticeable.

Hackers tend to use certain techniques to make a fraudulent website seem valid and to make the victim feel safe while luring him or her into the "crime scene," which makes it extremely difficult to recognize a fraudulent email or bank website, and makes it even harder to recognize that one is a victim of a cybercrime.It is difficult to identify a fraudulent website at first sight, but being aware of the features of such a website and of the types of cybercrimes decreases one's susceptibility to being a victim ofthe latter. Thus, users' understanding of the risks and how to protect themselves from cybercrime is a fundamental issue in modern life.

The main objective of the current study was to examine the awareness level of cybercrime among students at a teacher training college and to find out whether computer science studentshad ahigher awareness of cybercrimethan students who were majoring in other subjectsat the same college.

II. LITERATURE REVIEW

Reference [2] argues that criminals are taking advantage of the developed Internet infrastructure and convenience provided by the Internet to perform various types of criminal activities. In her paper, she insists that it becomes the duty of all Internet users to be aware of the different types of cybercrime and the cyber law in place to deal with them.

Several studies have been conducted in recent years to assess the level of cybercrime awareness among students. Reference [10] investigated students' awareness ofcyber security and the resulting risks. He found that college students were not particularly aware of how to protect their data. He also concluded that educational institutions

did not have an active approach to improving awareness among college students to protect themselves from potential cyberattacks.Reference [15] surveyed students at the college of Business and Economics at California State University. Based on the results of their research, they suggested that the major problem with cybercrime and security awarenesswas not a lack of knowledge about cybercrime and security, but rather the way, students applied that knowledge in real-world situations. They concluded that compliance with information and cyber security awareness was lower than their understanding of it.

In another study,[3] analyzed cybercrime and cyber security awareness among academic staff, researchers, undergraduate students, and employees in the education sector in the Middle East. The results revealed that the participants did not have the requisite knowledge of the importance of cyber security principles or an understanding of their practical application in day-to-day work.

Reference [5] investigated cybercrime awareness among B.Ed. teacher trainees. The results showed that awareness of cybercrime was not significantly affected by gender, but that it was affected by stream, that is, whether the students were taking science or art courses.Reference [4] investigated the level of knowledge about cybercrimes of 130 students from two universities located in the capital city of the United Arab Emirates. She found that only 32% of the participants had a high or adequate level of knowledge about cybercrime, while the rest had low to medium levels of knowledge of the topic, and that students specializing in Computer and Information Technology subjects had the highest levels of knowledge about cybercrimes, compared to all other students who were majoring in other subjects.Reference [1]examined computer ethics and security awareness behavior at two tertiary institutions in the south-western part of Nigeria. The results indicated that the level of computer security awareness among males and females was almost the same. Similarly, the results of the study conducted by [9] showed that there was a significant independent effect of the variables gender and locality on the level of cybercrime awareness among student teachers. In contrast, [14]found that cybercrime awareness among college students in Tamil Nadu (a city in India)could be measured at 69.45%, in which the males scored 38.6% and females 30.85%.

Reference [11]surveyed 100 young Internet users about the awareness of cybercrimes. The results were as follows: 11% were not familiar with the term "cybercrime;" only 15% understood the technical meaning of cybercrime,that is, "cybercrime is a criminal activity or a crime that involves the Internet, a computer system or a computer technology;" 32% felt that any individual could be victim of cybercrime; 45% felt they would be safe if they updatedtheir anti-virus software from time to time; 9% agreed that their identities had been stolen; 48% had shared their personal details with other persons, even when they did not know them closely; 42% agreed that sharing photographs on social networking siteswas not a risky activity; 67% agreed that they often received phishing emails asking for their sensitive information, such as mobile phone numbers, bank account numbers, addresses, etc.; 13% felt that they were not well protected; and 35% were not sure if they were protected from cybercrimes.

In short, research on cybercrime awareness among students has been established by previous studies ([3],[5], [9],[10], [15]). However, cybercrime awareness among Israeli Arab teacher students has not yet been researched and therefore there is an urgent need to do so in order to fill this gap in research.

A. Purpose of the Study

The purpose of the current study was to examine the level of awareness of cybercrime among Arab undergraduate students at a teacher training college and to determine how the field of study, year of study and the prior computer knowledge of the students could affect their levels of cybercrime awareness.

B. Importance of the Study

The amount of research on the awareness of cybercrimes has recently increased, since this growing problem is becoming an important issue. Furthermore, as the number of Internet users increases, so does the occurrence of cybercrimes. Academic students can be victims of cybercrimes, just like all other users of the Internet. On the other hand, academic students, and especially computer science students, should,theoretically,be more aware of cybercrimes than other users in their age group. Since no research has been done on Arab student teachers in Israel on the topic of the awareness of cybercrimes, the aim of this study is to fill this gap in the knowledge. The study expands our understanding of cybercrime awareness among students who are majoring in differing subjects and their attempts to be more protected from cybercrime. In addition, developing an awareness of cybercrime among student teachers is also vital, because teachers will be the ones to deliver the online safety message to pupils at schools. The study's findings are likely to contribute to educators, policymakers, and other researchers' understanding of the behavior of Arab student teachers in the digitalworld and how their behavior affects them. It could alsohelp this slice of society to understand how to use the Internet wisely and safely.

III. RESEARCH OBJECTIVES AND HYPOTHESES

The study's main objective was to assess the level of awareness about cybercrime among students at a teacher training collegeand to find out if computer science students have increased cybercrime awareness compared to students from other majors.

A.Research Questions

The research questions were:

1. To what extent is the level of cybercrime awareness of the students affected by the following variables: (1) *major – field of study*, (2) *study year*, and (3) *prior computer knowledge*?
2. Are students (majoring in all subjects) with higher prior computer knowledge less likely to be victims of cybercrime?

Specifically, the research objectives were:

1. To find out whether students involved indifferent fields of study had differing levels of awareness regarding cybercrime.

   Independent variable: ***field of study***. This variable had the following values: computer science, sciences (biology/chemistry/physics) and languages (Arabic/Hebrew/English).

2. To find out whether the level of cybercrime awareness among students increasedover the years of their academic learning.

   Independent variable: ***study year***. This variable had the following two values: first year of study and fourth year of study.

3. To examine whether the level of students'prior computer knowledge affected their level of cybercrime awareness:

   Independent variable: ***prior computer knowledge***. This variable refers to basic understanding about computers and how to use them; for example, the ability to use basic computer applications and conduct a basic search on the web, the ability to store and manage files, and the ability to convert files from type to type. This variable had the following values: low, moderate, or high.

B.Research Hypotheses

H1: Students in their fourth year of study (in all specializations) have a higher level of awareness regarding cybercrime than first-year students.

We hypothesized that as students' learning advanced over the years, they wouldbecome more knowledgeable and more aware of cybercrime, and could thus be considered to be more protected from cybercrime attacks due to the experience they had gained through the years.

H2: Computer science studentshave more awareness of cybercrimes than students who study sciences or languages.

We hypothesized that computer science students would have a higher level of cybercrime awareness than students majoring in other subjects because they would take more computer science courses than other students,and were therefore usually more knowledgeable than others in this domain.

H3: Students (taking all majors) with higher *prior computer knowledge* have increased cybercrime awareness compared to those with lower *prior computer knowledge*.

We hypothesized that students with higher prior computer knowledge would have the opportunity to develop more skills that could contribute to understanding cyberspace and its risks more than the students with lower *prior computer knowledge*.

H4: Students (taking all majors) with a higher degree of*prior computer knowledge* are less likely to be victims of cybercrime than the students with a lower degree of prior computer knowledge.

We hypothesized that students with more knowledge about computers, without regard to their field of study, wouldalso be more informed about the risks of cybercrime and would thus bemore aware of them, and wouldthus be less likely to be victims of cybercrime.

IV. METHODOLOGY

A. Research Instrument and Data Collection

A questionnaire, which was developed with Google Forms, was usedas the data collection instrument to collect the data from the respondents for this study. It comprised a total of 27 questions and was divided into two parts (see appendix A). The first part consisted of four demographic and background questions, and the second part consisted of 23 closed-ended statement about students'cybercrime awareness, which were rated on a five-point Likert scale, with one indicating "strongly disagree" and five indicating "strongly agree." The statements covered the following two areas: (1) *cybercrime awareness*, which included statements dealing with knowledge about cybercrime and whether the participants were trying to protect themselves from it; and (2) *being a victim of a cybercrime*, which examined whether the participants had been a victim of a cybercrime. This questionnaire was based on previous versions ([6],[13],[8],[10], [15]) that were used for the same purpose. The questionnaire underwent various changes until the final version was ready. Some statements were totally changed and some were added, or even deleted.

B.Validity and Reliability

To deal with the validity of the questionnaire, two computer science lecturers (who are teaching at the college) examined the questionnaire for face validity. After incorporating the comments of the reviewers, the questionnaire was given to three fourth-year computer science students in order to identify any ambiguities and to ensure an accurate interpretation of the instructions and the statements. Two statements were found to be unclear and they were rewritten in accordance with the notes received from the students.

The questionnaire also passed a reliability test in the SPSS program. The result of the Alpha Cronbach test of reliability for the whole questionnaire was 0.716. To increase the reliability,one question thatwas specified in the reliability report testwas deleted. The reliability of the questionnaire after deleting the recommended question was 0.739. The elimination of the statement did not affect or weaken the variable.

C. Research Participants

The sample for this pilot study was 90 Arab undergraduate student teachers at a teacher training college in the center of Israel. The participants were asked to anonymously complete the online survey by clicking on the link sent to them via email. They were given three weeks to respond and a reminder email was sent to them after 10 days.Of the 90 students, 73 (81%) completed the survey.Of these, 33 (45%) of them were in their first academic year and rest 40 (55%) were in their fourth academic year. A total of 69 (94%) students who completed the survey were female and the remaining four (6%) were male. This was in accord with the gender ratio at the college, because the majority (95%) of students at this teacher training college is female. Table 1 contains descriptive statistics about the research participants and their distribution according to the independent variables *study year*, *field of study* and level of *previous computer knowledge*.

D.Limitations of the Study

One limitation of the current pilot study was the low number of male respondents to the questionnaire, which was mainly due to the small number of male students at the education college. This meant we could not examine the effect of gender as a variable on cybercrime awareness among students.Another limitation was the small size of the sample. Therefore, it is recommended that this study be conducted in several colleges of education in order to ensure a more representative sample.

V. RESULTS AND DISCUSSION

Table I below shows the descriptive statistics of the research participants, organized according to the following three independent variables:*study year*, *field of study* and *prior computer knowledge*.

TABLEI: Descriptive Statistics of the Research Participants According to the Independent Variables

Variable		N (%)
Study year	First	33 (45%)
	Fourth	40 (55%)
Field of study	Computer Science	21 (29%)
	Science	30 (41%)
	Languages	22 (30%)
Prior computer knowledge	High	28 (38%)
	Moderate	40 (55%)
	Low	3 (7%)

The following paragraphs are an outline of the responses of the 73 students in relation to each of the hypotheses.

H1*: Students in their fourth year of study (in all specializations) have a higher level of awareness regarding cybercrimes than first-year students.*

TABLE II: Cybercrime Awareness among Students According to their Year of Study

Variable		N	Mean	S.D.
Study year	First Year	33	2.94	0.64
	Fourth Year	40	3.09	0.63

Table II shows that the group of first-year students had a numerically smaller mean level of cybercrime awareness (*M*=2.94, SD=.64) compared to the group of fourth-year students (*M*=3.09, SD=.63). In order to test the hypothesis that fourth-year students have more cybercrime awareness than first year students, a t-test for independent sample means was conducted. The result (t(71)=1.005, p=0.318) showed that there was no significant difference in the means of cybercrime awareness between students who were in their first year of study and those who were in their fourth year of study. According to this result, it can be concluded that student teacherswith advanced study years are not necessarily developing more awareness of cybercrime than students in previous years of study.Thus the first hypothesis of this study was rejected.

H2*: Computer science students have more awareness of cybercrimes than students who study sciences or languages.*

Figure 1 shows the means of cybercrime awareness among students in the three fields of study. Surprisingly, the students who the majoredin the sciences showed the highest numerically mean level of cybercrime awareness (*M*=3.19, SD=.47), compared to the mean level of cybercrime awareness

among computer science students (*M*=2.94, SD=.56) and students who major in languages (*M*=2.71, SD=.52). In order to find out if these results were statistically significant, a between-groups ANOVA was performed. The independent between-groups ANOVA yielded a statistically no significant effect (F(2,71)=0.4, p=0.678, NS) and thus the null hypothesis of differences between the means was rejected. This result is dissimilar to the result obtained in the research conducted by [4], which indicated that students specializing in computer information technology had the highest level of knowledge and awareness of cybercrimes.

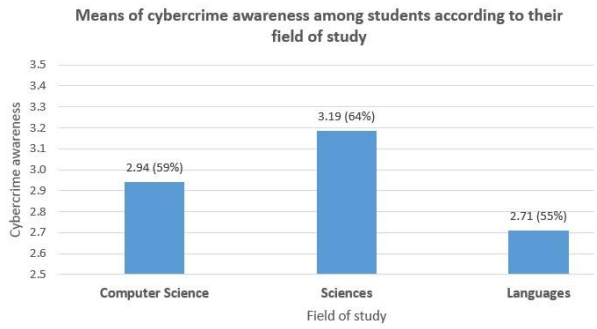

Fig. 1 Means of cybercrime awareness among students in the three majors

H3*: Students (taking all majors) with a higher degree of prior computer knowledge have higher cybercrime awareness than those with a lower degree of prior computer knowledge.*

Figure 2 shows the means of cybercrime awareness among students in relation to their level of prior computer knowledge. As expected, the students with more prior computer knowledge showed more cybercrime awareness (*M*=3.18, SD=.48) than those whohad moderate (*M*=2.86, SD=.60) or low (*M*=2.32, SD=.81) prior computer knowledge. In order to find out if these numerical means were statistically significant, a between-groups ANOVA was performed. This yielded a statistically no significant effect (F(2,71)=1.411, p=0.281, NS) and thus the null hypothesis of differences between the means was rejected. Although this result was not statistically significant, it could be in alignment with the results obtained by [12], which revealed that as students gained more knowledge of computer applications, their cybercrime awareness increased.

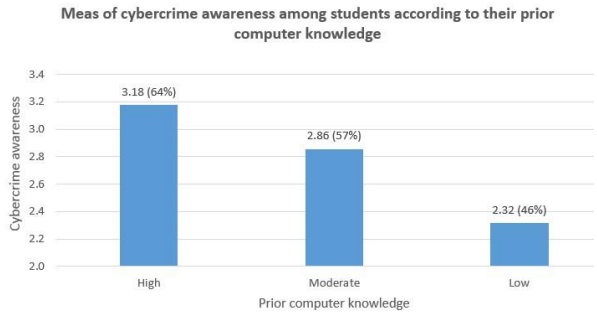

Fig. 2 Means of cybercrime awareness among students according to their prior computer knowledge

H4*: Students (taking all majors) with higher prior computer knowledge are less likely to be victims of cybercrimes than the students with lower prior computer knowledge.*

TABLEIII: Being a victim of a cybercrime

Variable		N	Mean	S.D.
Prior computer knowledge	High	28	2.43	.50
	Moderate	40	2.33	.49
	Low	5	2.33	.94

Table III shows the data from the respondents regarding being a victim of cybercrime. Surprisingly, it shows that students who claimed to had a high level of prior computer knowledge were found to be victims of cybercrimes (*M*=2.43 SD=.50) more than those who claimed to have a low (*M*=2.33 SD=.94) or moderate degree of (*M*=2.33 SD=.49) prior computer knowledge. We conducted an independent between-groups ANOVA to determine whether the numerical means were statistically significant. Ityielded a statistically no significant effect (F(2,71)=0.074, p=0.929, NS) and thus the null hypothesis of differences between the means for this hypothesis was rejected. One interpretation for this result is that even if students demonstrate more skills in their work with computers and have a higher level of cybercrime awareness, it still does not mean that they act carefully in cyberspace and thus are less susceptible to being victims of cybercrimes. Several scholars who have conducted research on students' cybercrime awareness concluded that students do not always know how to protect themselves from cyberattacks or what actions they should take in order to reduce the risks of cybercrimes, even if they show a high level of awareness of cybercrime ([8],[10],[15]).

VI. CONCLUSION AND RECOMMENDATIONS

The overall findings of this pilot study indicatedan unsatisfactory awareness of cybercrimes among student teachers independently of their specializations, especially among those majoring in computer science. The results also did not show a significant correlation between students' prior computer knowledge and their awareness of cybercrime, or between the students' prior computer knowledge and their ability to protect themselves in cyberspace. Therefore, it is concluded that the hypotheses were not proved to be valid; i.e., student teachers are not aware of cybercrime.Based on these

findings, we conclude that although information technology is widely used at higher educational institutions, cyberspace security topics need to be taught to all students across the board in order to increase their cybercrime awareness and to prevent them from becoming victims of cybercrime. It is vital that students in higher education develop a deeper understanding of cyber risks and a set of skills to mitigate these.This is especially true of student teachers, since tomorrow'sschool teachers are the ones who will deliver the online safety message to pupils.

It also seems to be the case that learning how to work with computer applications or even learning courses in algorithms and programmingdo not necessarily affect the level of cybercrime awareness among students, or help them to know howthey should act in cyberspace in order to protect themselves. Therefore, we recommend that higher educational institutions should adopt an active approach to improvingcybercrime awareness among all college students in order to increase their knowledge of cybercrimes and about how to protect themselves from potential cyberattacks.

VII. FUTURE RESEARCH

It would be of value to conduct research into cybercrime awareness among a larger sample of student teachers from different teacher training colleges. Future researchers could also focus on developing strategies to increase the level of cybercrime awareness and to alert students to the risks of being victims of cybercrimes.

REFERENCES

[1] Abolarinwa, O., Tiamiyu, M., & Eluwa, S. (2015). Computer Ethics and Security Awareness Behavior of Tertiary Institution Students In South-Western, Nigeria. *Engineering Science and Technology: an international journal*, 5, 260-265.

[2] Aggarwal, G. (2015). General Awareness on Cyber Crime. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(8), 204-206.

[3] Al-Janabi, S. & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management 15*(1), 1-30.

[4] Bamatraf, S. (2014). Assessing the Level of Knowledge about Cybercrimes Among Young Adults Within the United Arab Emirates. *Proceedings of The National Conference on Undergraduate Research*, 880-885.

[5] Goel, U. (2014). Awareness Among B.Ed. Teacher Toward Cybercrime- A Study. *Learning Community*, 5, 107-117.

[6] Ismailova, R., & Muhametjanova, G. (2016). Cybercrime risk awareness in Kyrgyz Republic. *Information Security Journal: A Global Perspective*, *25*(1-3), 32-38.

[7] Jaishankar, K., & Halder, D. (2011). *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations.* Chicago: IGI Global.

[8] Kim, E. B. (2013). Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective*, *22*(4), 171-179.

[9] Malhotra, T., & Malhotra, M. (2017). Cybercrime Awareness Among Teacher Trainees. *Scholarly Research Journal for Interdisciplinary Studies*, 4/31, 5249-5259.

[10] Moallem, A. (2018, July). Cyber Security Awareness Among College Students. In *International Conference on Applied Human Factors and Ergonomics* (pp. 79-87). Springer, Cham.

[11] Narahari, A., & Shah, V. (2016). Cyber Crime and Security- A study on Awareness Among Young Netizens of Anand. *IJARIIE*, 2, 1164-1172.

[12] Nwosu, J.. C., Adebawojo B., & Ifeoma, H. A. (2017). Cybercrime and Computer Science Undergraduate Students in Private Universities in Nigeria: An Empirical Investigation. *International Journal of Computer Trends and Technology (IJCTT) V51*(1):34-37

[13] Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

[14] Senthilkumar, K., & Sathishkumar, E. (2017). A Survey on Cyber Security Awareness Among College Students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, 263, 1-10.

[15] Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26.

APPENDIX A:

Questionnaire about cybercrime awareness

Dear Students,

In front of you is a questionnaire that is intended to measure your awareness of cybercrime. All the data you provide in this questionnaire will be used for research purposes only and will be kept confidential.

Clarification: Cybercrime refers to the use of computers and mobile phones to commit a crime. As a criminal activity, it began when hackers started illegally accessing high-level and modern computer networks. Some examples of cybercrime include credit card and identity theft, network intrusions and software piracy.

Thank you for participating.

Part I: Background

Please answer the following questions by circling\selecting the correct answer.

1. **Gender**: 1. Male 2. Female

2. **Yearof study**:1. First 2. Fourth
3. **Major**: 1. Computer Science 2. Science 3. Languages
4. **Computer knowledge level**: 1. Low 2. Moderate 3. High

Part II: This part includes statements related to cybercrimes. There are no right or wrong answers to each question because of different points of view among the students. Please state your opinion about each of the following statements by circling\clickingon the best choice, which describes your agreement or disagreement with each sentence. To answer the questions below please use the following rating scale.

1= strongly disagree, **2**= somewhat disagree, **3**=neutral, **4**= somewhat agree, **5**= strongly agree.

Statement	Strongly Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Strongly Agree
I know what a cybercrime is.					
I have heard about phishing.					
I think that a cybercrime is only a virtual crime.					
I would click any link that I receive via email/SMS.					
I think that a fraudulent email/website/link is easy to identify.					
I know some of the cyber laws.					
I trust any website that asks me to enter my bank account detail.					
I use other methods other than antivirus software to protect myself from cybercrimes.					
I am aware of some features of a fraudulent email.					
I think that antiviruses are enough to protect me from a cybercrime					
I think that downloading any file from any website is always safe.					
I believe that big companies are the only victims of cybercrime.					
I have experienced being a victim of a cybercrime.					
When I am online, I consider my permissible space and the forbidden space of others.					
I think that I am able to identify a fraudulent email /website.					
I think that I am protected from cybercrime.					
I protect myself from cybercrime.					
I think that it is difficult to identify a fraudulent website.					
I care about purchasing the best antivirus software.					
In general, I do not trust the websites that ask me to enter some details about my bankcard.					
I know what the details are about my card that I should not enter on any website when shopping online.					
I have been threatened online to pay money for someone who had stolen my personal photograph.					
I would report being a victim of a cybercrime if I had been a victim.					