

**Requirements of the social work institutions and faculties in  
confronting electronic crime  
from the view point of a sample of faculty members**

**BY**

**Dr. Mayada Mansour Omar**

Assistant Professor at Department of Community Organization  
The Higher Institute of Social work in Cairo

**Dr. Mervat Gamal El Dein Ali**

Assistant Professor at Department of Community Organization  
Faculty of Social Work, Helwan University



### Abstract

The study problem can be identified in determining the requirements of the social work institutions and faculties in confronting electronic crimes from the view point of faculty members in some institutions and faculties of social work.

The study aimed to identify the reality of the requirements of the social work institutions and faculties in confronting electronic crimes. The sub-aims of the study were as follows:

- 1- Determining the preventive requirements electronically for the social work institutions and faculties in confronting electronic crimes.
- 2- Determining the communication and informatics requirements electronically for the social work institutions and faculties in confronting electronic crimes.
- 3- Determining the educational requirements electronically for the social work institutions and faculties in confronting electronic crimes.
- 4- Determining the requirements for building the strategic planning capacity of the social work institutions and faculties in confronting electronic crimes.
- 5- Monitoring some of the obstacles that face the social work institutions and faculties in confronting electronic crimes.
- 6- Presenting some recommendations and suggestions that could contribute to confront electronic crimes within the social work institutions and faculties.

The current study was a field and descriptive / analytical type, the social survey method was used for a non-random sample of faculty members in some institutions and faculties of social work, its size was 50 faculty members.

An electronic questionnaire was sent to them in order to collect the required data regarding the subject of study (the electronic crimes).

The main question was: what is the reality of the requirements of social work institutions and faculties in facing cybercrime? In its most important results, it reached the necessity for concerted efforts with social work institutions and faculties and the external community to address the kind of crimes that threaten the achievement of development goals and affect the future of our university youth.

### Key words:

Electronic crime, requirements.

### ملخص الدراسة

تمثلت مشكلة الدراسة الحالية في تحديد متطلبات كليات ومعاهد الخدمة الاجتماعية في مواجهة الجرائم الإلكترونية من وجهة نظر عينة عمدية من أعضاء هيئة التدريس ببعض كليات ومعاهد الخدمة الاجتماعية.

وهدفت الدراسة إلى التعرف على واقع متطلبات كليات ومعاهد الخدمة الاجتماعية في مواجهة الجرائم الإلكترونية. وكانت الأهداف الفرعية للدراسة كالتالي:

- ١- تحديد المتطلبات الوقائية الكترونيا لكليات ومعاهد الخدمة الاجتماعية في مواجهه الجرائم الإلكترونية.
- ٢- تحديد المتطلبات الاتصالية والمعلوماتية الكترونيا لكليات ومعاهد الخدمة الاجتماعية في مواجهه الجرائم الإلكترونية.
- ٣- تحديد المتطلبات التوعوية الكترونيا لكليات ومعاهد الخدمة الاجتماعية في مواجهه الجرائم الإلكترونية.
- ٤- تحديد متطلبات بناء القدرة التخطيطية الاستراتيجية لكليات ومعاهد الخدمة الاجتماعية في مواجهه الجرائم الإلكترونية.
- ٥- رصد بعض المعوقات التي تواجه كليات ومعاهد الخدمة الاجتماعية في مواجهه الجرائم الإلكترونية.
- ٦- تقديم بعض التوصيات والمقترحات التي يمكن أن تساهم في مواجهة الجرائم الإلكترونية داخل كليات ومعاهد الخدمة الاجتماعية .

والدراسة الحالية من نمط البحوث الميدانية الوصفية/التحليلية، وتم استخدام منهج المسح الاجتماعي بالعينة العمدية من أعضاء هيئة التدريس بكليات ومعاهد الخدمة الاجتماعية ، حجمها ٥٠ عضو هيئة تدريس، تم ارسال استبيان الكتروني لهم بهدف جمع البيانات المطلوبة منهم.

الكلمات المفتاحية :  
الجرائم الإلكترونية - متطلبات .

### **The study Problem:**

This age is characterized as the information age, as the information industry (storage and retrieval) has become a stand-alone industry. We find that it is one of the priorities of preparing society for the information age to absorb and interact with information technology, and it undoubtedly needs effective participation from educational institutions to implement it in the faculty community. In the light of the scientific and technological changes and developments, many of those in charge of the educational system see the necessity of providing learning resource centers to keep pace with these developments and upgrading and improving the teaching and learning process in order to find a staff member capable of facing various situations and problems and finding a staff member capable of facing various situations and problems and finding appropriate solutions to them in scientific ways and correct relies on new and multiple sources of information to serve the educational process.

This is what was confirmed by the study of (Suad Aghanim :2019,p .175), which focused on judicial administration, the challenges of digital transformation, the widespread dissemination of mobile technology, the revolution of artificial intelligence, the development of its mechanisms, and the abandonment of its traditional methods, and it reached to obtain accurate statistics and indicators about scientific and technological developments. It recommended that learning centers be provided to keep pace with these developments.

Therefore, the information revolution is considered a social revolution whose changes affected all social systems and transformed them into new structures in politics, trade and social control, and therefore the effects of the information revolution were not limited to communication and transportation systems, but rather it went beyond human relations systems and transformed them from realistic and actual interactions to imaginary interactions in which it is sometimes difficult , separate reality from fiction. Electronic crime is one of the most dangerous criminal phenomena produced by organized crime at the world level, because it has a great danger to the security of societies, whether local, regional or at the international level. Therefore, all civil, governmental and private efforts must be combined to confront this imminent threat to social security, It must also participate in all scientific professions and disciplines to face the seriousness of these crimes, and the community organization method as one of the social work methods possesses scientific foundations and rules that can participate in confronting this danger.

This was confirmed by the study of (Al-Malt: 2005,p.33) where the study aimed to identify the different aspects of the uses of information systems. The study concluded that despite the bright aspects of information systems, it is offset by negative aspects that make the door wide open to the types of socially deviant behavior that were not It is possible to imagine its occurrence in the past, which made it not forbidden in many countries of the world. Information systems provide some opportunities for new forms of crimes that did not exist in the past, and they also provide some opportunities for committing traditional crimes in modern and non-traditional ways.

The study of Muhammad (Kaabi :2009,p.14) also confirmed this, it aimed to examine the challenges and obstacles that threaten commercial activity, and the most important of these challenges are cybercrime. Continuing in technology, reviewing the Law on Combating Information Mobilization No. 2 of 2006, as well as reviewing the Electronic Transactions and Commerce Law No. 1 of 2006 and the need to amend the Criminal Procedures Law in line with the nature of information crime. Some of the reasons for the attractiveness of the internet to criminals, extremists and others are due to some of its characteristics, as it is a free medium without regulatory barriers between the sender and the future, and young people accept this method or way greatly.

Izzat Fahim's study (2008,p.1) aimed to uncover the impact of globalization on changing the methods and patterns of crime in the Egyptian society. The study concluded that the vast majority of perpetrators of information technology crimes fall into the age group (20-30 years) and that the category of youth is either graduates or those who They are still in education the most common categories of perpetrators of information technology crimes. This is due to the fact that this period triggers individual desires that many of these young people fail to control, which makes them feel emptied and unable to achieve what they desire, and accordingly some tend to commit criminal behaviors. The internet has achieved great benefit for the children of the internet generation, but the biggest concern is that the children of the internet generation make a serious mistake, which most of them do not realize, which is that they disclose their personal data on social networks and others (Tapscott: 2011,p. 36).

In today's interconnected world, when a person connects his or her home or company network to the internet, he or she becomes on the edge of the world and the beginning of (World Wide Web) as pirates seek to exploit the unwary (Thomas: 2004, 19). Electronic technology is considered, despite its positive aspects, but it is one of the reasons for the spread of electronic crimes in the university society, which had a great impact on

the achievement of some of its goals and the existence of institutional tension.

With respect to methods and patterns of crime in Egyptian society, the study found that the vast majority of perpetrators of information technology crimes fall in the age group (20-30 years) and that young people, whether graduates or still in education, are the most common groups who commit information technology crimes, due to the fact that this period is triggered by individual desires that many of these young people fail to control, which makes them feel emptied and unable to achieve what they desire, and accordingly some tend to commit criminal behaviors. There are foreign universities abroad deal with the issue as a complete curriculum in graduate and post-graduate studies because of its importance in that period. Universities have a great role in confronting that negative electronic thought. The rapid technological developments in the modern era, foremost of which are information and communication technologies, are among the most important challenges facing educational institutions to achieve their goals, which have brought about various changes in their centers, conditions and relations.

This is what (Al-Hadi's :2012,p.33) indicated, which focused on identifying the role of globalization and information and communication technology in transforming social work institutions and faculties into the digital image and confronting them with various electronic problems, and concluded that the success of the digital transformation process for universities does not depend on the effectiveness of the transformation process itself. Rather, it requires pivotal competencies on the part of members of the university's upper management, middle and executive levels.

Also, the success of technology in educational institutions is linked to the elements affecting the provision of services, such as "technology development", and attention to human resources, which are the basis for improving the level of services through training individuals and providing them with various skills within the framework of the optimal investment of systems and information technology and raising their awareness of its risk.

As the interest in educating people and educating them, especially university youth, in order to reach them to the highest levels of mastery of cognitive and performance skills, especially electronic skills that exist in our time - and those expected to exist in the near future - is not considered a kind of social luxury, nor an academic innovation, is one of the foundations and standards of institutional quality , and it is a necessity for our survival in a world in which those who achieve supremacy and sovereignty in it now and tomorrow are the ones who produce scientific knowledge and its applications in life, through educational and global

systems that are economically and humanly highly efficient at all times, relying on themselves and their capabilities on the one hand, and their eyes on learning and teaching others on the other hand.

They learn from their advanced systems to develop their education system in order to respond to the requirements of the information age based on the continuous flow of information and the rapidly increasing information progress to face the problems and negatives of this development. Many research studies confirm the existence of a strong link between social work institutions and faculties and confronting the electronic crimes problems with training and awareness for all groups in the university society. Various experiences have shown the role of awareness, education and training programs in this regard. Based on this, higher education is entrusted with playing an important role, especially in countries especially developing countries.

The education system is an important factor in transmitting development perceptions to individuals, as well as linking them to the general development goals, in addition to providing individuals with technical skills and preparing leaders transformation of the various levels of the general social situation, with its political and economic dimensions, and facing electronic problems.

The emergence of information societies remarkably means new objective conditions, the basis of which is the development of information and communication technologies on the one hand, and the entry into the phase of globalization on the other hand, and there is no doubt that these new objective conditions dictate a new perception of the education profession and the social work profession, requiring a review of the role of educational institutions, and the social institutions to define the features of their role in spreading science and knowledge, providing data and information, and adopting the culture of both knowledge management and management by knowledge.

This new role is very important to clearly define it, because thinking about developing social work institutions and faculties in Egypt means thinking about the features of a society of tomorrow, which must prepare to face the many challenges of the future. In view of the enormity of the challenges that social work institutions and faculties face, including that they are somewhat far from the development plans in the Arab countries due to the preoccupation of these institutions with their daily problems, which multiply with the increase in the social demand for education. The existence of a working mechanism that responds to the issues facing Arab countries.

The future trends in universities became limited, and thus social work institutions and faculties became independent of planning for the future, which is the basis for effective participation in development plans, and

given that the nature of the era in which we live is characterized by rapid change and amazing progress in various educational, economic, social and political fields, and towards accelerated change highlights the urgent need for reforms and innovations in social work institutions and faculties in order to prepare people who are able to adapt to the changes and problems of the current era. Among these problems is the perpetration of some electronic crimes inside social work institutions and faculties.

**In the light of the above, the study problem can be identified in determining the requirements of social work institutions and faculties in confronting electronic crimes.**

**The study Aims:**

The main aim of the study is to identify the reality of the requirements of social work institutions and faculties in confronting electronic crimes.

The sub-aims of the study were as follows:

- 1- Determining the preventive requirements electronically for the social work institutions and faculties in confronting electronic crimes.
- 2- Determining the communication and informatics requirements electronically for the social work institutions and faculties in confronting electronic crimes.
- 3- Determining the educational requirements electronically for the social work institutions and faculties in confronting electronic crimes.
- 4- Determining the requirements for building the strategic planning capacity of the social work institutions and faculties in confronting electronic crimes.
- 5- Monitoring some of the obstacles that face the social work institutions and faculties in confronting electronic crimes.
- 6- Presenting some recommendations and suggestions that could contribute to confronting electronic crimes within the social work institutions and faculties.

**The Study Importance :**

- 1- The current study can contribute to shedding light on electronic crimes and the importance of the role of social work institutions and faculties in confronting it.
- 2- Seeking to diagnose the reality of electronic crimes in social work institutions and faculties by applying it to faculty members and to address the effects of electronic crimes.

- 3- Developing an implementing vision that may help to improve the current reality of social work institutions and faculties in a positive way in confronting this kind of crimes.

### **The Study Questions:**

The main question of the current study is: what are the requirements of social work institutions and faculties in confronting electronic crimes from the view point of a non- random sample of faculty members in social work institutes and faculties?

The sub-questions of the current study were as follows:

- 1- What are the preventive requirements electronically for social work institutions and faculties in confronting electronic crimes?
- 2- What are the communication and informatics requirements electronically for social work institutions and faculties in confronting electronic crimes?
- 3- What are the electronic awareness requirements for social work institutions and faculties in confronting electronic crimes ?
- 4- What are the requirements for building the strategic planning capacity of social work institutions and faculties and confronting electronic crimes?
- 5- What are the obstacles that obstruct social work institutions and faculties in confronting electronic crimes?

### **The Study Concepts:**

- **Electronic crimes :**

Electronic crime or cybercrime or on line crime is a criminal activity that either targets or uses a computer, computer network, or networked device. It is a crime committed using computer devices or the network, or it is committed on information systems or the network. Also, it is any act committed, including the use of a computer or an information network, in violation of the provisions of the law and the law. Most, but not all, of electronic crimes are committed by cyber criminals or hackers who want to make money. It is carried out by individuals or cybercrime organizations.

Some criminals are organized, use advanced techniques and are highly technical. Others are novice hackers. Electronic crime seldom aims to harm computers for non-profit reasons. Here are some examples of the different types or kinds of electronic crimes:

- 1- Fraud via e-mail and the Internet.
- 2- Cyber bullying
- 3- Data unlawfully intercepted or stolen.

- 4- Interfering with systems in a way that exposes the network to danger.
- 5- Copyright violation.
- 6- Selling illegal goods over the Internet.
- 7- Demanding, producing or possessing child pornography.
- 8- Identity fraud (where personal information is stolen and used).
- 9- Theft of financial data or payment data with the card.
- 10- Stealing and selling corporate or corporate data.
- 11- Electronic blackmail (asking for money to prevent a threatening attack).
- 12- Electronic espionage (where hackers gain access to government or company data).

Most electronic crimes fall into two main categories, namely:

- 1- Criminal activity targeting computers.
- 2- Criminal activity that uses computers to commit other crimes.
- 3- Or practicing both criminal activities together.

- **Requirements:**

Requirements are plural of a requirement, and a linguistically speaking is a command or action to be fulfilled, or something basic and indispensable.

The concept of requirements has equivalent terms that contribute to explaining this concept, namely: supplies, needs, necessities, and necessities... Requirements means identification of existing or potentially available materials, programs and collaborative efforts to link and coordinate these resources; in order to avoid duplication, conflict or competition and determine the scope and quality of the services provided. In the current study, requirements can be defined as the set of conditions and capabilities that must be available to social work institutions and faculties in confronting electronic crimes.

**The Study Methodology:**

**The Study Type:**

The current study is considered a descriptive / analytical and field study.

**The Study Method:**

The current study is guided by the social survey method.

**The Study Fields / limits :**

- 1- **The objective limit:** The study was limited to identifying the requirements of social work institutions and faculties in confronting electronic crimes, and the obstacles face these institutions and faculties in addressing this type of crimes.

- 2- **The human field / limit:** a non- random sample of faculty members in some institutes and faculties of social work, the size of which is 50 faculty members.
- 3- **The time field / limit :** Data were collected from the study sample by the researcher during the first semester of the academic year 2020-2021

**The Study tool:**

The current study tool consisted of an electronic questionnaire form, divided into five axes:

The first axe: the initial data & information.

The second axe: The reality of the requirements of social work institutions and faculties in confronting electronic crimes.

The third axe: The role of social work institutions and faculties in confronting this type of crimes at the level of prevention and treatment.

The fourth axe: The obstacles that obstruct social work institutions and faculties in confronting electronic crimes

The fifth axe: the suggestions to overcome the obstacles facing social work institutions and faculties in confronting electronic crime.

**First:** Presenting and analyzing the results of the study on the requirements of social work institutions and faculties in combating cybercrime from the perspective of how society is organized

**(A) Primary data:**

Table No. (1) Distribution of respondents in social work institutions and faculties (n = 50)

No.	Type	F	%	F	Educational Status	F	%
1	Male	22	44	1	Professor	15	30
2	Female	28	56	2	Assistant Professor	16	32
No.	Age	F	%	3	Lecturer	8	16
1	26	1	2	4	Assistant lecturer	11	22
2	27	1	2	No.	Number of years of experience as	F	%
3	28	2	4	1	Less than 3 years old	1	2
4	29	2	4	2	3 years - 6 years	18	36
5	30	4	8	3	6 years - 9 years	17	34
6	31	4	8	4	9 years and over	14	28

7	32	5	10	No.	Access to training courses as	F	%
8	33	5	10	1	Yes	27	54
9	34	4	8	2	No	23	46
10	35	4	8	No.	The organization that organized these courses as	F	%
11	36	3	6	1	Governmental organizations	4	8
12	38	2	4	2	General Federation of NGOS	9	18
13	40	4	3	3	The organization in which you work	10	20
14	42	1	2	4	International body	5	10
15	43	2	2	5	Others	22	44
16	44	3	6	No.	Extent of benefit from training courses as	F	%
17	45	1	2	1	Yes	14	28
18	47	2	4	2	to some extent	13	26
19	48	1	2		No	23	46
20	49	1	2				

The previous table shows that female respondents occupy the first rank at a rate of (56%) of the study sample, while male beneficiaries came in second place at a rate of (44%). Cybercrime from the perspective of the way society is organized.

The table also shows the age status of the respondents, as it indicates, in general, 80% are over 33 years of age, (12%), arrived in the first order, followed by the 32-year-old group (10%), and this shows the turnout of the respondents in various categories to know the extent to which the requirements of educational institutions The higher level in combating cybercrime from the perspective of the way society is organized, and they strive to develop themselves to confront and prevent electronic crimes.

It also shows the distribution of the study sample according to the educational status as follows: Where the category (Assistant Professor) came in first place at a rate of (32%), followed by the (Professor)

category in the second place by (30%), while (Assistant lecturer) ranked third with a percentage of (22%), the (lecturer) category is ranked fourth with (16%) in the table. This is due to the respondents' contribution to achieving the requirements of social work institutions and faculties in combating cybercrime from the perspective of how society is organized. It also shows the results of the distribution of respondents according to years of experience, where the percentage of (3 years - 6 years) occupies the first place with (36%) the highest percentage, followed by the category (6 years - 9 years) with (34%), while the category (9 years and more) with (28%), a category (less than 3 years), at a rate of (2%) in the table. This is due to the importance of gaining experience for the respondents in the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way society is organized.

The results of the distribution of the study sample according to obtaining training courses in the field of combating cybercrime indicate as follows: Where (those with training courses) came in first place with (54%), while the percentage (did not receive training courses) was (46%) This may be due to the respondents' keenness to develop their capabilities and gain more experiences.

The results of the study sample distribution also show the extent of benefiting from training courses in the field of combating cybercrime as follows: Where it came in first place (those who did not benefit from the training courses) with a rate of (46%), while the percentage of (those who benefited from the training courses came in second place) (28%), while the percentage (who benefited to some extent) was (6%). This may be due to the extent of the respondents' keenness to develop their capabilities and gain more experience.

Table No. (2) Distribution of the beneficiaries according to the uses of the training courses (N = 50)

No	How to benefit from the training courses?	Yes		to some extent		No	
		F	%	F	%	F	%
1	Acquiring new experiences in electronic technology	20	40	23	46	7	14
2	Identifying electronic crimes and how to confront them	17	34	21	42	12	24
3	How to prevent cybercrime in social	15	30	22	44	13	26

	work institutions and faculties						
4	How to build coping mechanisms within social work institutions and faculties	16	32	25	50	9	18
5	Gaining new experiences on the techniques of electronic work for prevention and confrontation	23	46	17	34	10	20
	<b>total</b>	50	100	50	100	50	100

The results of Table (2) also indicate that the respondents see the need to benefit from training courses in the field of combating cybercrime as follows: the necessity of acquiring new experiences on the techniques of electronic work for prevention and confrontation by (46%), and gaining new experiences in electronic crimes by (40%) The need to know about cybercrime and how to confront it was (34%), followed in order by how to build coping mechanisms within social work institutions and faculties by (32%), and how to prevent cybercrime inside social work institutions and faculties by (30%), which indicates On the awareness of the respondents in acquiring new experiences and developing themselves. Second: The requirements of social work institutions and faculties in combating cybercrime from the perspective of how society is organized Table No. (3) Distribution of respondents according to the reality of (preventive power electronically ) of the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way society is organized (n = 50)

No	reality of preventive power electronically	Responses						arithmetic mean	standard deviation	Arrangement
		Yes		to some extent		No				
		F	%	F	%	F	%			
1	The necessity to integrate a knowledge part in the courses on cybercrime and its effects	45	90	3	6	2	4	2.86	0.45	1

2	Investing the mental and knowledge capital of the youth in various activities	43	86	4	8	3	6	2.8	0.53	5
3	Continuous participation of the opinions and perspectives of university youth on this phenomenon	38	76	10	20	2	4	2.72	0.53	2
4	Awareness initiatives for young people inside and outside the university about risks and causes	42	84	6	12	2	4	2.8	0.49	5
5	Shifting from teaching information to thinking about solutions to problems	35	70	12	24	3	6	2.64	0.59	3
6	Investing the youth's e-efforts in positive activities	46	92	3	6	1	2	2.9	0.36	4
7	Using clerics to raise religious awareness	35	70	9	18	6	12	2.6	0.7	6
	The variable as a whole							2.76	0.5	is a high level

As for the reality of (preventive power electronically) with the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way the society is organized as determined by the respondents, the results of Table (3) indicate that the preventive force electronically contributes in the first place in the need to integrate a knowledge part in the courses on cybercrime and its effects on average It is weighted (2.86), and in the second order came a continuous participation of the opinions and views of university youth about that phenomenon with a weighted average (2.72), and in the third order came the shift from teaching information to thinking about solutions to the problem with a weighted average (2.64), and in the fourth order came investment efforts E-youth in positive activities with a weighted average

(2.9), and in the fifth order came investment of mental and cognitive capital for young people in various activities, awareness-raising initiatives for young people inside and outside the university of risks and causes with a weighted average (2.8), while it came in the order of late to seek the help of clergy and the church for religious awareness Weighted average (2,6)

The researchers conclude from this the results of the reality of preventive power electronically the necessity to integrate a knowledge part in the courses on cybercrime, continuous participation of the opinions and perspectives of university youth, investing the youth's electronic efforts in positive activities, in social work institutions and faculties. This indicates that the results of the table indicate that the general average, as determined by the respondents, is (2.76), which means a high level and the actual protective force electronically.

This is what the study "Madiha: 2011,p.12" indicated, which emphasized in its results the central role of the university, as it is linked to society, interacts with it and affects it, but has become responsible for educating and protecting young people against contemporary dangers and threats facing them, especially those related to the cultural and informational aspect that It has become the predominant feature in this era, and the crimes or moral deviations resulting from them may befall them while dealing with these technological applications.

Table No. (4) Distribution according to the forms of (communication and information power) as one of the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way society is organized (n = 50)

No .	Power communicative and informational	Responses						arithmetic mean	standard deviation	Arrangement
		Yes		to some extent		No				
		F	%	F	%	F	%			
1	The existence of cooperation and partnership efforts between the various colleges and institutes to confront cybercrimes	46	92	3	6	1	2	2.9	0.36	4
2	Continuous communication	45	90	3	6	2	4	2.8	0.60	5

	with the security authorities to find out the causes of electronic crimes									
3	Coordination between internal and external bodies to create a complete societal awareness of cybercrime	43	86	5	10	2	4	2.82	0.48	3
4	The existence of a continuous communication mechanism between the colleges within the university to solve the problem and raise awareness of its risks	44	88	3	6	3	6	2.82	0.52	3
5	Consolidating the institutional efforts to create a complete preventive system within universities and institutes	46	92	3	6	1	2	2.9	0.36	4
6	Existence of continuous preventive programs between departments within the organization	47	94	2	4	1	2	2.92	0.34	1

7	Presence of a virtual communication mechanism with social media directly	45	90	4	8	1	2	2.88	0.38	2
The variable as a whole								2.8	0.4	is a high level

As for the forms of (communication and information power ) as one of the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way the society is organized as determined by the respondents, the results of Table (3) show that the communication power and information contribute in the first order to the existence of continuous preventive programs between departments within the institution with a weighted average (2.92), and in the second order came the existence of a virtual communication mechanism with social media directly with a weighted average (2.88), and in the third order came coordination between internal and external bodies to create a complete community awareness of the phenomenon, and the existence of a continuous communication mechanism between colleges inside the university to solve the problem and awareness of its risks with a weighted average (2.82), and in the fourth order came the existence of cooperation and participation efforts between the various colleges to confront this phenomenon, unify the institutional efforts to create a complete preventive system within the universities with a weighted average (2.9), and in the fifth order came the continuous communication with the security authorities to find out the causes the phenomenon with a weighted average (2.8)

The researchers conclude from this the results of communication and information strength, there must be continuous preventive programs between departments within the institution, a virtual communication mechanism with social media directly, coordination between internal and external bodies to create a complete community awareness of the phenomenon, and a continuous communication mechanism between colleges within the university to solve the problem and awareness of its risks in social work institutions and faculties. This indicates that the results of the table refer that the general average, as determined by the respondents, is (2.8), which means a high level of communication and information strength. This is what was confirmed by the study of Ibrahim bin Muhammad: 2007". The study aimed to measure the extent of students 'fear of mobile crimes. The most important results of its findings revealed a lack of awareness among young people using this technology

of its positiveness, and the weakness of religious faith among mobile users. This is followed by the lack of knowledge of penalties, as well as the emptiness of the youth.

Table No. (5) Images (planning power) as one of the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way society is organized (n = 50)

No.	strength schematic	Responses						arithmetic mean	standard deviation	Arrangement
		Yes		to some extent		No				
		F	%	F	%	F	%			
1	And the existence of preventive plans within institutions to reduce cybercrimes	47	94	2	4	1	2	2.92	0.34	1
2	There is cooperation in planning efforts between educational institutions and the concerned authorities. Cybercrime	46	92	3	6	1	2	2.9	0.36	3
3	The existence of a database on the impact of cybercrime on different groups in colleges and institutes	45	90	3	6	2	4	2.86	0.45	2
4	Having a study of the strengths, weaknesses, opportunities and threats facing colleges and institutes in dealing with cybercrime	47	94	2	4	1	2	2.92	0.34	1
	The variable as a whole							2.9	0.3	is a high level

As for the reality of (planning power) with the requirements of social work institutions and faculties in combating cybercrime from the perspective of the method of organizing society as determined by the respondents, the results of Table (3) show that the planning force contributes in the first order to the existence of preventive plans within institutions to reduce the phenomenon, and the existence of a study of points The strength, weakness, opportunities, and threats facing the institution in dealing with the phenomenon with a weighted average (2.92), and in the second order there is cooperation in the planning efforts between educational institutions and the parties concerned with the phenomenon with a weighted average (2.86). In the third order, there is

cooperation in planning efforts between the institutions educational and concerned parties with the phenomenon with a weighted average (2.9)

The researchers conclude from these results the reality of preventive power electronically and the existence of preventive plans within institutions to reduce the phenomenon, the existence of a study of the strengths, weaknesses, opportunities and threats facing the institution in dealing with the phenomenon, in social work institutions and faculties. This indicates that the results of the table indicate that the general average, as determined by the respondents, is (2.9), which means a high level, the reality of planning power.

Table No. (6) Obstacles facing institutions of higher education in combating cybercrime from the perspective of how society is organized (n = 50)

No .	Obstacles	Responses						arithmeti c mean	standard deviation	Arra nge ment
		Yes		to some exte nt		No				
		F	%	F	%	F	%			
1	Lack of a long-term strategy and reliance on short-term planning	4	8	3	6	3	6	2.82	0.52	4
2	Weak support from different departments within the colleges and institutes	4	9	3	6	2	4	2.86	0.45	3
3	Weak youth participation to reduce cybercrime	4	8	4	8	3	6	2.8	0.53	7
4	Weak cooperation of security and concerned authorities to	4	8	7	1	3	6	2.74	0.56	6

	prevent and confront cybercrime									
5	Weak institutional communication between the different colleges	4 6	9 2	2	4	2	4	2.88	0.43	2
6	Weak societal and media support to reduce cybercrime	4 1	8 2	7	1 4	2	4	2.78	0.50	5
7	Weakness of deterrence laws for cyber criminals	4 7	9 4	2	4	1	2	2.92	0.34	1
	The variable as a whole							2.8	0.4	is a high level

With respect to obstacles facing the social work institutions and faculties in combating cybercrime from the perspective of the way the society is organized as determined by the respondents ,the results of the table show that obstacles contribute in the first order to weak deterrence laws for perpetrators of these cybercrimes with a weighted average (2.92), and in the second order the weakness of institutional communication between the different colleges with a weighted average (2.88), and the third order is the weakness of the presence of support from the different departments within the university with a weighted average (2.86), and in the fourth order the lack of a long-term strategy and reliance on short-term planning with a weighted average (2.82). Weak societal and media support to reduce the phenomenon came in the fifth order with a weighted average (2.78). In the sixth order the weak cooperation of the security authorities and concerned parties to prevent and confront the phenomenon with a weighted average (2.74). In the last order weakness of youth participation to reduce the phenomenon with a weighted average (2.8).

The researchers conclude from this the results of the reality of the obstacles that the deterrence laws are weak for the perpetrators of these cybercrimes, the second is the weakness of institutional communication between the different colleges, the weakness of the support from the various departments within the university, in social work institutions and

faculties. This indicates that the results of the table indicate that the general average, as determined by the respondents, is (2.8), which means a high level of obstacles.

**The answer to questions of the study and general discussion:**

The study answered the study's questions represented in the main question: What are the requirements of social work institutions and faculties in facing cybercrime?

The results proved the following:

- 1- Females occupy the first place in the study sample, and this may be due to the effective role of females in achieving the requirements of social work institutions and faculties in combating cybercrime from the perspective of the way society is organized.
- 2- The study data related to obtaining training courses shows the extent of the respondents' keenness to develop their capabilities and gain more experiences. The reality of the preventive force came electronically as follows: the necessity of integrating a knowledge part in the courses on cybercrime, the importance of the continuous participation of the opinions and perspectives of university youth, and the need to invest the efforts of electronic youth in positive activities in social work institutions and faculties.
- 3- The reality of the communication and information power came as follows: the necessity of continuous communication and information programs between departments within the institution, the existence of a virtual communication mechanism with social media directly, coordination between internal and external bodies to create a complete community awareness of the phenomenon, and the existence of a continuous communication mechanism between Faculties within the university to solve the problem of cybercrime and raise awareness of its risks in social work institutions and faculties.
- 4- As for the reality of the planning power electronically, it came as follows: There must be plans within institutions to limit the phenomenon, and a study of the strengths, weaknesses, opportunities and threats (quadruple analysis) facing the institution in dealing with the phenomenon in social work institutions and faculties.
- 5- As for the obstacles, they were: the weakness of the deterrence laws for the perpetrators of these cybercrimes, the weakness of

institutional communication between the various colleges, and the lack of adequate support from the various departments within the university and in social work institutions and faculties.

In the light of these obstacles, the researchers find that universities must take important steps for prevention, treatment and planning through, for example, the application of environmental analysis for universities by monitoring the strengths, weaknesses, opportunities and threats to confront the phenomenon.

**First: The areas of strength available to confront the phenomenon:**

- 1- The availability of a very large number of faculty members, which can be invested in playing many roles that could contribute to facing this type of crime.
- 2- The presence of a large number of students in universities, which gives the university a great opportunity to contribute to facing this type of crime among a large number of young people.
- 3- The expansion of higher education, in terms of bringing it to new areas, and the geographical spread of universities in many and varied regions, which means more ability to confront this type of crime for a large sector of young people in various places.
- 4- The expansion of higher education in terms of the number and diversity of specializations, which means more ability to confront cybercrimes through these various disciplines.
- 5- The requirement of the International Computer Driving License for all graduates in Egyptian universities, which leads to the availability of greater skills among students that help them in effective dealing with the computer, and the acquisition of the skills associated with it.
- 6- Diversifying the roles and functions of university education, which allows universities to contribute more in various fields to confront electronic crimes among students.
- 7- Large numbers of students are keen to learn foreign languages, and the language requirement, especially for postgraduate students; This enables them to see the latest books on this topic, to know the latest protection programs for networks, and to be sent to missions and scholarships abroad for studies related to computer and its sciences.

- 8- The presence of many community service centers and units of a special nature that can be invested in facing this type of crime.
- 9- Attention to providing technological education; As there are some technological colleges in Egypt, which include many of the disciplines required by the times and which can be used in the development of some programs and specializations that help in facing these crimes among young people.
- 10- The tendency to cooperate with some ministries and authorities, which would help extend university services, and to increase the university's ability to perform its roles and functions.
- 11- The presence of a group of experts and specialists in many colleges, and from various disciplines, who can contribute to facing this problem for students, each according to his specialization.
- 12- The existence of a center for the protection of intellectual property in some universities, which can contribute to protection against some electronic crimes; especially those related to the various attacks on intellectual property in all its forms.
- 13- The existence of a futures center in some universities, and in the Supreme Council of Universities, that can be used in the preparation of future research studies related to computer science and the future dimensions of this type of crime and how to confront it.

**Second: The areas of opportunities available and that can be taken advantage to confront the phenomenon:**

- 1- Increasing societal demand for higher education, which gives universities the opportunity to guide and educate a large number of young people
- 2- .Existence of a structure of material capabilities represented in the buildings and sites occupied by the system units, which can be re-coordinated their use
- 3- Availability of technologies and capabilities of communication with the outside world, and advanced educational institutions, which allows universities and faculty members to communicate with some universities, and to learn about the experiences of some countries in facing this type of crime.

- 4- Paying attention at the societal level to developing new types of education, such as distance education and open education.
- 5- Increasing societal understanding and awareness of the seriousness of the internal and external challenges, the importance of the role that the higher education sector must play to face these challenges, and the negative effects that will result from them.
- 6- Societal interest in setting up some cybercrime legislation and the penalties that result from its commission.
- 7- Increasing societal awareness of the importance of civil society participation in many areas, which provides the opportunity for universities to seek partnership with civil society to solve this problem.

**Through the previous review, a number of recommendations can be made that can contribute to combating cybercrimes:**

- 1- Introducing the legal education subject, so that this article is general to all students, and this article deals in some parts of the legal and legislative aspects of cybercrime.
- 2- The importance of studying issues related to intellectual property issues, and educating students about it in various colleges.
- 3- Including this topic in the human rights course, which is one of the courses taught to all students in Egyptian universities.
- 4- A specialized diploma can be established in postgraduate courses in intellectual property or in information security. It is one of the new fields of study that the labor market needs, and thus a large number of students is expected to attend.
- 5- Including the topic of cybercrime in some courses, such as: the youth welfare course and the computer introduction course.
- 6- Focusing on teaching the problem of cybercrime on the ethics of using technology and making good use of it.
- 7- Organizing awareness seminars and campaigns, and distributing flyers and booklets to educate students of social work institutions and faculties of the efforts made by the Ministry of Interior in facing these crimes and the penalties that result from their commission, as well as how to act in the event of exposure to such crimes.

### References

- Al-Arabi Miloud: Dawar, a specialist in the Education Resources Center in the era of modern technology, Cybrarian Journal, Issue (25),
- Aghanim Souad: Judicial Administration and the Challenges of Digital Transformation: The Moroccan Experience as a Model Journal of Law and Business, Hassan I University - Faculty of Legal, Economic and Social Sciences - Business Law, p. 175
- Al Badaniyah Y Yab: Security and Information Warfare, Amman, Al Shorouk Publishing House, p. 114.
- Ali Osama: Digital Transformation of Egyptian Universities: Requirements and Mechanisms of Education, World Council of Comparative Education Societies.
- The Ministry of Higher Education and the State for Scientific Research: Higher Education Development Projects Management Unit: Evaluation of Egyptian Universities for Projects Funded by the Higher Education Development Project Fund: Evaluation of the Fund's Performance and University Studies Summary, Cairo: Higher Education Development Project Fund, March, pp. 39- 41.
- Amin Mustafa Ahmed: Digital Transformation of Egyptian Universities: Requirements and Mechanisms of Education, World Council of Comparative Education Associations.
- Tbach Philip GAL "University Reform: An International Perspective", Higher Education Research published by American, Association for Higher Education, No 10.p 6
- Abdel Hafeez Izzat Marzouq Fahim: The Impact of Globalization on the Methods and Patterns of Crime in the Egyptian Society, PhD Thesis, Minia University, Faculty of Arts, Department of Sociology.
- Orlikowski Wanda j., "The Duality of Technology in Organization' Organization Science., P402
- Al-Alfi Muhammad Muhammad (2007): The Electronic Court between Reality and Expectations "From the working papers of the sixth e-government conference entitled: The New Public Administration and E-Government, held from 9-12 December 2007 in Dubai, Arab Administrative Development Organization, p. 29.
- Al-Hadi Muhammad Muhammad: The Digital Organization in a Changing World, from the researches of the first Arab Conference on Information Technology and Management entitled "Towards a Digital Organization, held in Sharm El-Sheikh, from 1 to 4 October, Cairo, Arab Organization for Administrative Development."
- Al-Khodary Hanaa Odeh: Planning for institutional change in Egyptian university education in light of the requirements for integrating information and communication technology into the educational process.

PhD thesis, unpublished, presented to the fundamentals of education, Faculty of Education, Ain Shams University, Cairo.

Nasr Nawal: The relationship between university education and the world of work in the ninth (first Arab) national conference for the development of university education at the Faculty of Education, Ain Shams University “Arab university distance education: a future vision in the period from December 17-18, Cairo.

Al-Sayed Abbas Mahmoud: Total Quality Management as an Entrance to the Development of Secondary Education in Egypt, Journal of Education and Development, Issue 27, Eleventh Year.

Jamil Hilal,: Our universities are alienated from scientific research, The Palestinian Politics Journal, Ramallah, Palestine, 28-38

Al-Naqib Khaled Hassan: Al-Ahram Digital Website, Al-Ahram Al-Masai, Al-Ahram Publishing and Distribution Foundation,

[http // www.ahram.org.eg24 / 8/2014/4](http://www.ahram.org.eg24/8/2014/4): 45

Abdul Sadiq Adel (2012): Cyberspace and the Constitution: Al-Ahram Digital Website, Al-Ahram Foundation for Publishing and Distribution.

[http // www.ahram.org.eg8 / 12/2012/7](http://www.ahram.org.eg8/12/2012/7): 15.

Qutb Muhammad Ali: Information Crimes and Ways to Confront them (Part Two), Bahrain, Ministry of Interior, Royal Police Academy, Security Media Center, pp. 3-4

Al-Sukkari Ahmed Shafiq: Dictionary of Social Work and Social Services, Alexandria, University Knowledge House.

Law on Regulating Network Communication and Combating Information Crime, Syrian Arab Republic, Legislative Decree No. 17, p. 3

Cybercrime Law, Saudi Arabia, Cabinet, Council of Experts, P5.

Fakhry. Madiha (2011): A study on the role of Egyptian universities in facing cybercrime among students, Faculty of Education, Helwan University, p. 12

bin Muhammad Ibrahim A (2007): Fear of cell phone crimes, Society and Security Symposium, Riyadh, King Fahd Security College, April 5, 2007.