DOI: http://dx.doi.org/10.26483/ijarcs.v10i1.6349

Volume 10, No. 1, January-February 2019

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

INTERNET FRAUD TO DECEIVE EMAIL BY USING DIFFERENT TECHNOLOGIES

Mohammad Ali Bani Younes
Dep. of Computer Science
Ajloun National University
Jordan

Abstract: This research presents e-fraud types and clarifies the suggestions that have been reached to deal with the problems of electronic fraud so as not to be victims of this fraud, and explains how to act when detecting electronic fraud, especially with the spread of the Internet through institutions to make them more secure. Therefore, Arab countries must take a series of steps and strategies at all levels, particularly those organizational steps, which make many texts and provisions used effectively to prevent cybercrime. States should therefore take all legal measures to punish various types of attacks on information systems.

Keywords: crimes; cybercrime; Fraud; Monument; Stealing; victims

I. INTRODUCTION

Online fraud defined as a monument. The term also refers to any kind of trick or trick that uses one or more Web services, such as chat rooms, email, Internet forums, or websites, to direct deceptive calls to potential Web victims. Online fraud is often aimed at deceiving users by stealing their money by stealing their credit card numbers or by sending money transfers or checks or by pushing them to disclose personal information for the purpose of espionage, impersonation, or access to their account information in a sensitive situation [1].

Online fraud has turned into a new phenomenon that allowed its perpetrators to enter homes and offices, cross borders and access victims very easily, especially as the Internet is an important means of providing financial and banking services. Cybercriminals create new ways of drowning their victims and hacking them. Electronic scammers professional around the clock to invent new ways and find gaps through which to carry out their tasks, the information security companies and with banks and financial institutions and banking created sections Specialized technology to protect customers and secure financial transactions through the Internet. They discover bankers and computer experts on a daily basis about many of the new tools used in online fraud, including e-mail messages, daily conversation conversations and other types of communication. The entry into the Internet has become an unaccountable risk, as the hackers spread on their sides, waiting for the first prey to hit them [2].

With the increase in piracy, cybercrime has emerged. These crimes are different from conventional crimes. He sits in his house and does not bother to press the button to enter the Internet. He begins to catch the victims. It is no longer limited to the penetration of networks and the destruction or theft of information from them, but also included moral crimes such as kidnapping, extortion, murder, and others [6].

The majority of research studies and the economic, social and legal strategy have tended to follow the description of the information age over the period from the 1970s until now, while some consider the beginning of the era of the information at the beginning of the 1980s. The means of processing, storage, transmission and exchange of information, i.e., computer systems with their physical components, devices, morals, software, data, and communication systems, as well as their physical and moral components [4].

A legal system is a vital entity that reflects the tendencies and needs of the society and its tendencies to regulate and protect individual and collective rights through the rules of legislation in its different branches.

It is natural that its relations and the bases of its legislation will be influenced by the high impact of technology and the resulting new types of legal relations through a legislative movement reflecting the response of legislation to the new and new in this field. The Internet is the most controversial.

It is an interconnected and interconnected world that raises the most important question: Does the Internet need a legal framework that regulates its affairs and challenges? Or is it a new image of a society whose elements have not yet been integrated, which should be regulated? If there is a need for legal regulation of the Internet, what has the Arab countries accomplished so far? They are required to have unfinished tasks [10].

II. COMPUTER AND INTERNET CRIMES

What is the meant by cybercrime from the point of view of some jurists, researchers, and critics? We will also deal with technical fraud and piracy through the Internet [5].

Crimes affecting knowledge, use, trust, security, profit, money, reputation, and mind. All this is a matter of information, but the information in its various forms in the digital environment is slowly becoming knowledge of the means of use and its purpose, confidence, profit, and money.

Jurists and scholars have defined the crime of the computer with a quite few differentiated definitions depending on the subject matter of the science, according to the standard definition itself, researchers have differed in the phenomenon arising from the use of computers technically [19].

III. TECHNICAL FRAUD

The technical methods fraud by professionals has been done through their search in each operating system spy for penetration, noting that many sites and programs of penetration are available on the Internet and trading without difficulties to carry out piracy, theft, and fraud [7].

A user Internet is exposed to daily piracy, cannot be limited or predict their number, the most serious is that the fraudster has a card reader to capture any bank credit card or ATM card; it copies the code on it and then uses it.

In light of the tremendous advances in information technology, and because of the large number of individuals and institutions who visit this network, it has become easy to commit the worst crimes against its users, whether individuals or institutions or entire conservative communities.

Cybercriminals impersonating the characters, deceiving young people, and tarnish the reputation of the victims, who are usually individuals or businesses. Furthermore, they try to tarnish the reputation of entire societies, especially Muslim communities [10].

As the Internet emerged, all fields have entered the computer from individual use, institutional, and governmental use as a means of facilitating the lives of everyday people. Cybercrime moved into the Internet, becoming known as cybercrime as a basic tool, as in cybercrime. It may also be a goal of crime and manage it.

Internet crimes have been divided into various categories, such as computer-related data theft, data tampering, tampering with stored information, personal identity or life-related data, intellectual property rights-related crimes and other illegal Internet fraud, harassment, prosecution, one of the most common cybercrime crimes, especially among young users of the network [8].

IV. INTERNET FRAUDS

The types of fraud vary from a lottery to lottery, where the person is notified that he is a winner in the lottery and only sends a sum of money to receive his prize. There is also a method (romantic fraud) by convincing the victim to find a lover for a sum of money. In addition to doing well and try to convince the victim to donate for humanitarian issues of wars and epidemics and famine [8].

There is also a way to contact institutions or banks and say that there is an explosive device and they have to pay to ensure that the place is not blown up. It is interesting to mention one of the most monumental roads in the memorial, it is a meeting with the victim in one of the places and make him see a bag filled with fake dollars and convince him that the real problem is that each one of them can remove the blue seal only by using a kind of chemical solution, and this solution needs to be paid thousands of dollars and so on [9].

A. Types and methods of fraud

The Internet is one of the worst roads which is witnessing monument operations annually, online fraud cases have been rampant since the early 1980s and are growing at a high rate every year, with the number of losses from fraud in 2014 reaching $30 billion. These crooks always rely on the greed or ambition of some people, or play on the tendon of ignorance and inexperience, and usually use innovative means and are extremely savvy, in addition to the great skills in impersonating others to make them easily trap, most fraud and corruption Revolves around the following points [12]:

- **Stealing others' money**

  It is certainly the main target of all scammers around the world is to center around most cases of fraud and fraud through money transfers or the purchase of fake things or stealing money from them indirectly.
- **Get personal information**

  Such as name, mobile number, address, zip code or other data, and are usually used for physical purposes or for sale to third parties or for use in other monumental processes.
- **The theft of social accounts**

  Such as email or theft of your accounts on social networking, sites either for marketing purposes or for personal purposes related to the account holder, or for their exploitation in other matters as explained above in the previous point.
- **Get commissions**

  There are many cases of monument do not be the aim of theft, but to deceive others to do some things that these people may get as commissions, such as signing up or registering in a site, uploading a specific application on your mobile, etc. The principle of the commission is legitimate and not rejected, but the real problem in the fraud methods used to attract others is immoral.
- **Free access to services**

  It is used by the fraud to use certain persons or to induce them to make false promises to obtain their services without giving them any compensation.
- **Theft of the Intellectual Rights**

  Some people attempt to steal the efforts of others, whether through photographs, designs, works of art, publications, publications, etc., or the theft of ideas or industrial secrets belonging to some companies. These materials are copyrighted and may be exclusive or difficult to obtain. Therefore, they start to trick some creators to get it.

B. Some prominent methods that these people follow to Monument or fraud against others:

- **Job offers:**

  Job offers may be one of the most attractive areas for young people, usually, job offers in high-end companies, salaries, and huge benefits, or jobs in other countries. These jobs are ultimately unrealistic, and maybe the goal is to get the funds or personal data.
- **Unreal awards**

  Some users receive messages telling them that they have won a car or a recent mobile, and they asked them to send the rest of their data, some of may ask people for a copy of their passports or identity cards, which later prove to be a fake prize.
- **Deceptive pages**

  Some people create pages that may be a replica of the famous sites. In order to enter the information victim without knowing what leads to theft. The fraudsters usually pose situations or problems that may make the user fall into this trap naively, such as an email that telling him that his account will be closed if it is not activated within 24 hours with a link to a fake page, and users usually rush without confirming the link to this page.

V. TYPES OF INTERNET FRAUD

The email spoof shows that the sender of the message is a person with a particular position (as a company manager or a

member of the Webmail maintenance team). The "phishing message" may ask the user for information about his or her account on the pretext of what the user is doing. This is a type of social engineering [2].

If the page is falsified for a sensitive site (a bank's website, for example), the deceptive user may enter their account data on the counterfeit page, which will steal this information. This trick may sometimes be associated with its predecessor, and the URL of the Website is sent in a false mail message.

Fraudulent financial transactions, where the deceptive party By email message, in general, the party deceived by a large amount of fake wealth estimated in millions provided that the deceived user first make some arrangements to receive the money. These arrangements include sending money to the first party for some reason (for example, money transfer transactions), thus the user has been the victim of fraud and lost his money [13].

Mail messages of this type are classified in many e-mail systems as spam mail. A mouse click trick is a website that requires the user to register and click on their ads or run a program that displays ads on their device for a certain amount (for each particular number of ads or the duration of the program).

The result of these tricks is the marketing of free advertising for these sites against the "nothing" material obtained by the user in return.

Deceived opportunities at home, these tricks require the user to send a certain amount of money up to a few hundred dollars for materials to start his work to send to him, but the user pays without getting the materials/information paid for. These tricks sometimes require registering on the site and sending a site link to other users to increase their profit rate.

Some users who are victims of an Internet scam misrepresent these frauds and confirm their validity and credibility (whether ignorant or not), resulting in more victims [13].

VI. Psychological effects on victims

The tens of thousands of people have been fallen victim to the monument, and the main feeling is the sense of treachery or rape and the fact that this kind of monument may lead to psychological and neurological problems may turn into physical diseases. There are cases all over the world for the victims of this kind of fraud, and in return, the victims have become fraudsters, and they have practiced the same methods of fraudsters who stole everything they have [10].

VII. Professionalism in fraud

Fraudsters send you documents which are very vigorously forged documents, including government papers so be careful to ensure that the person does not commit fraud.

How do I protect myself from online fraud? Be wary of any message or anyone asking you for your personal data such as your full name, birth date, account number, credit card number, or your identity or social security number [13].

If you receive a message from the bank or financial site that you are using and it asks you to send the login data to the site, immediately contact the bank to inquire about the message. Do not use links in mail messages and manually type links in the browser address bar [20].

Check that the anti-virus program on your computer is blocking fraudsters. Most modern controls virus has this feature, so be sure to update the anti-virus program constantly. As well as, Report any message they suspect fraudulent. Most email sites offer the possibility to report suspicious messages [21].

VIII. Recommendations

- Taking all legal measures aimed at punishing various types of attacks on information systems.
- The preparation of laws on the fight against information crimes
- Reach solutions that face the technical challenges and recognize the state of change and development in the legal needs to face the digital age.
- Legislative institutions should intervene to protect information, protect consumers and protect the user in the regulation of standards of technical standards.
- Organization of infrastructure in measures to ensure the development and employment properly of technology and appropriately to the needs of society [15].
- Protecting the programs and databases produced by creators in the era of technology as well as protecting the production of companies
- The necessity of legislative intervention is to organize and process personal data and organize the storage and exchange of data in banks and databases.
- Using the latest security systems, that provides a high degree of insurance for all banking transactions over the Internet.
- Cooperation between the States to establish common organizational rules and solutions that call for the organization and endeavor to expand this work.
- Focus on the key role that the States and regional organizations in the region can play in the field of information technology crimes.
- Conducting intensive courses for human cadres working in the field of investigation and investigation, and the prosecution of crimes related to automated data processing systems, computer applications, and related crimes, and considering the inclusion of criminal investigation curricula in colleges, police training institutes and topics on cybercrime [16].
- The need to create a new social culture, that condemning cybercrime while activating the method of awareness and refinement among users of the global telecommunications network and urging them to use these technologies optimally.
- The need to spread digital awareness among users and how to avoid encroachment on their personal data and to inform them of the magnitude of the risk that monitors them in the absence of precaution
- Encouraging universities and the research centers to organize many seminars and conferences that deal with the information development of crime, and how to combat cybercrime and reduce its impact.
- Teaching a new branch in all universities and colleges of law means legal studies that specialize in legal informatics [17].

IX. Acknowledgment

I would like to thank all the staff of the International Journal of Advanced Research in Computer Science, and I thank Ajloun National University for encouraging research in all fields, leading to building a knowledge society, promoting scientific research.

X. REFERENCES

[1] A. Singh Poonia, "Cyber Crime: Challenges and its classification," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS). vol.3, pp.119-121, November-December 2014.

[2] Rusch, Jonathan J. "The social engineering of internet fraud," In Internet Society Annual Conference, http://www. isoc. org/ 1999.

[3] M. Gercke, "Understanding cybercrime: Phenomena, challenges and legal response," e ITU publication, pp. 1-336, September 2012.

[4] H. Saini, Y. Shankar Rao and T.C.Panda, "Cyber-Crimes and their impacts: A Review," International Journal of Engineering Research and Applications (IJERA). vol..2, pp. 202-209, Mar-Apr 2012,.

[5] S. Malby, R. Mace, A. Holterhof, C.Brown, S. Kascherus, and E.Ignatuschtschenko (UNODC), the Comprehensive study on cybercrime (United Nations New York, Printed in Austria, February 2013).

[6] M. McGuire, S. Dowling, Cybercrime: A review of the evidence Chapter 1: Cyber-dependent crimes, (Home Office Research Report 75 October 2013).

[7] M. Pironet, C. Antunes , P. Moura , J. Gomes, "Classification for Fraud Detection with Social Network Analysis," Dissertation, October 2009.

[8] Y. Kou, C. T. Lu, S. Sinvongwattana, Y. P. Huang, "Survey of Fraud Detection Techniques," Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23, 2004 pp. 749-754.

[9] K.S. Koong, L. c. Liu, J. Wei, "An Examination of Internet Fraud Occurrences," Research Gate, January 2012, pp.441-449.

[10] KS. Koong, H. Qin, LC. Liu, T. Ying "Occurrences of online fraud complaints: 2002 through 2015," International Journal of Accounting and Information Management, vol. 25, pp. 484-504, August 2017.

[11] E. Echeburúa, P. Corral and P. J. Amor "Evaluation Of Psychological Harm in the Victims of Violent Crime," Copyright 2003 by the Colegio Oficial de Psicólogos, Spain, vol.7, pp. 10-18. 2003.

[12] L. Delamaire, H. Abdou, J. Pointon, "Credit card fraud and detection techniques: A review," Banks and Bank Systems, vol. 4, pp. 57-68, January 2009.

[13] T. Zeller Jr, A Common Currency for Online Fraud: Forgers of U.S. Postal Money Orders Grow". New York Times. (April 26, 2005.

[14] Ziegenfuss, Douglas E. "An examination of the professionalism of fraud examiners," Southern Business Review 27.1 (2001): 23.

[15] K. Frimpong, P. Baker, "Fighting public sector fraud: The growth of professionalism in counter-fraud investigators," Crime Prevention and Community Safety, 9(2), 130-137, 2007.

[16] B. Gavish, C. L. Tucci, "Reducing internet auction fraud," Communications of the ACM, vol 51, pp.89-97. 2008.

[17] C.E.H. Chua, J. Wareham and D. Robey, "The role of online trading communities in managing internet auction fraud," MIS Quarterly, pp.759-781,2007.

[18] A Teich, M.S. Frankel, R. Kling, and Y.C. Lee, "Anonymous communication policies for the Internet: Results and recommendations," of the AAAS conference. The Information Society, vol.15, pp.71-77. 1999.

[19] Casey, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.

[20] Lail, Bradley, J. MacGregor, J. Marcum, and M. Stuebs. "Virtuous professionalism in accountants to avoid fraud and to restore financial reporting," Journal of business ethics, vol. 140, pp.687-7044, 2017.

[21] Grazioli, Stefano, and S. Jarvenpaa. "Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers," IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans30, no. 4, pp. 395-410. 2000.