UDC 681.321; 322:621.395

Problems of Computer-Based Crimes

Shevchuk I.S., Voronyak L.Ya.

email: i.s.shevchuk@ukr.net
Department of Theoretical Physics and Methods of Teaching Physics,
Ivan Franko Drohobych State Pedagogical University,
3 Stryis'ka St., Drohobych,UA–82100, Ukraine

In this article we consider needs for information security and discuss problems of computer-based crimes, explain the threats connected with hacking, fishing, and cyberstalking. The study concerns information security policies which can be applied to solve or reduce the risks of personal data breach and data theft. We also take into consideration benefits of effective protection measures against modern computer-based crimes.

Key words: computer-based crime, hacking, fishing, cyberstalking, spamming, flaming, information security, privacy of information.

INTRODUCTION

Nowadays illegal exploitation of computer technologies rapidly develops. Unfortunately, cybercrime is on the rise, having a global nature and causing both financial and personal damage to the victims it affects (Joffee, 2010). Such criminal activities as electronic frauds, misuse of devices, identity theft and data theft as well as system interference are considered to be computer crimes. They can range from the catastrophic to merely annoying ones. Some of them are dangerous to national security, others can drive a company out of business; still others, like cracker's prank, do not actually cause damage at all, but might cause annoyance. It is evidently that computer crimes have a multipurpose nature: some are created for kicks, some for social or political causes; others are the serious business of professional cyber criminals. Their activities involve the breach of human and information privacy, as also the theft and illegal alteration of system critical information. Kshetri, studying the problem of cybercrime in the early 21st century, states that "in 2005 nine-tenths of American companies lost over $67 billion as a result of cybercrime" [1]. There are various types of computer crimes, but we would like to develop a decision-making process on such issues as hacking, phishing, and cyberstalking which, to our mind, are the most prevalent.

Researches Nicolle, Parsons-Pollard (Virginia State University) and Laura J. Moriarty (Virginia Commonwealth University) have been studying the problem of cyberstalking for some period of time and have numerous articles and books focused on this issue. Their article *Cyberstalking: Utilizing What We Do Know* provides policy implications and necessary steps, which can increase our knowledge about cyberstalking to better assist and aid its victims [2]. Cyberstalking is a relatively new form of the computer-based crime, but it quickly spreads as technology has been constantly developing. Unfortunately, its boundaries cannot be vividly cut and people have different views what cyberstalking is. In general, people know that it includes harassing, threatening, or flaming. Cyberstalking victims are followed and pursued on line, receiving multiple threatening emails or text messages per day, electronic viruses, extreme amounts of spamming, abusive phone calls or finding their personal information (names, phone numbers, email addresses, street addresses) posted without their consent. They can even experience sexual harassment via online posts, emails or cell phones, including posting and/or creating sexually explicit images, or being subscribed to

pornography and unwanted advertising without their knowledge or consent, etc. Cyberstalkers often target the users by means of chat rooms, message boards, discussion online forums, listening devices, hidden cameras and social networking websites. They gather the information and harass the users on the basis of the information gathered. Regrettably, current state laws, dealing with cyberstalking, have numerous gaps. A deeper understanding of the cyberstalking phenomenon, adequate cyberstalking laws and increased enforcement will prevent us from becoming cyberstalkers' victims.

Defining the notion of cyberstalking, different authors stress on the lack of comprehending what the constituents of this computer-based crime are. Nowadays people have a limitless access to technology and it is sure that the ways to use this technology to harass, threaten, abuse or stalk others will increase. College students, being the main users of technology become the most frequent cyberstalking victims. Every day the harm of cyberstalking incidents increases from simple harassment to full-scale threats that can result in suicides. We agree with the points of view that this happens because the way the law addresses cyberstalking is very confusing. There exists the necessity of more effective cyberstalking laws and increased enforcement in our society. The researchers also prove that the people do not realize the extent of the problem as there is no official data. Though cyberstalking has indeed become a societal problem, it is largely anecdotal and informal. The most positive point of the abovementioned article is that its authors try to find out new ways to increase cyberstalking victims' awareness and provide additional resources that can help people to fight against this fast-growing cybercrime.

The primary problem with the research is that it does not contain a clear definition of cyberstalking. They define cyberstalking as "an extension of stalking that utilizes computers and other electronic devices or as a completely separate action that has some of the elements of stalking but utilizes a different mode of delivery" [2, 435]. In our opinion, they had better resort to the contrastive analysis that could show effectively the differences between cyberstalking and spatial or offline stalking. Though these concepts have many similarities in content and intent, for sure, they are not synonymous. Cyberstalking is different from offline stalking, however it sometimes leads to it, or is accompanied by it. Goodno claims that traditional stalking statutes fall short of addressing cyberstalking because there are five crucial ways in which cyberstalking differs from offline stalking:

"(1) Cyberstalkers can use the Internet to instantly harass their victims with wide dissemination. (2) Cyberstalkers can be physically far removed from their victim. (3) Cyberstalkers can remain nearly anonymous. (4) Cyberstalkers can easily impersonate the victim. (5) Cyberstalkers can encourage "innocent" third-party harassment." [3 129-132).

It is quite evident that the authors' aim was to convince the readers that they should be aware of cyberstalking in order not to become its victims. With the help of utilizing vivid details and interesting examples they prove that cyberstalking causes harm. They describe the most dangerous cyberstalking incidents and reinforce them with the current data. Unfortunately, the public cannot see the full range of this cybercrime as there is a lack of official data. Firstly, that is because many cyberstalking victims do not report the conduct to law enforcement, and, secondly, because law enforcement agencies have not had adequate training in how to deal with this crime. However, there are some reports that suggest that cyberstalking is ever-growing. The U.S. Department of Justice reports that there exist cyberstalking resources, like CyberAngels, GetNetWise, the National Center of Victim and Crime, Privicy Rights Clearinghouse, Working to Halt Online Abuse, that assist cyberstalking victims. It was estimated that in 1999 there were approximately 63,000 Internet stalkers in the United States and 474,000 victims world-wide [4]. It is difficult even to imagine the exact number of today's cyberstalkers and their victims.

We should note the fact that the authors also point out the resources which do not only provide the assistance to cyberstalking victims, but give educational programs, referral services, and law enforcement assistance. To

the abovementioned they add the National Coalition Against Domestic Violence, the National Domestic Violence Hotline, the National Organization for Victim Assistance, the Safety New Project, and WiredSafety. In contrast to online resources some law enforcement agencies, handling cyberstalking cases, have no idea that cyberstalking laws even exist. Now, we are in the situation when, on the one hand, law enforcement agencies do not investigate or prosecute cyberstalking cases, on the other, they report a large number of cyberstalking incidents.

Having analyzed numerous researches, Parsons-Pollard and Moriarty agree that college students, especially females, are cyberstalking victims. Regrettably, they leave out that children can be also at risk. This is even more dangerous because parents are sometimes not able to recognize the core warning signs that their kid may be in trouble and in need of help. Some cyberstalkers who are experienced online predators and pedophiles know exactly how to manipulate their victims.

It is very positive that by their article Parsons-Pollard and Moriarty tried to draw legislatures' attention to the problem. They are convinced that the society needs clear state laws specifically prohibiting cyberstalking. In the USA cyberstalking laws vary from state to state and what is the worst not all states have these laws. Only forty-six states now include electronic communications in their stalking and harassment laws. The status of American cyberharassment law remains inconsistent. For sure, without effective cyberstalking laws the fight against cyberstalkers will give no results. Having completed a profound analysis of existing cyberstalking laws, the researchers stated their main shortcomings. They draw correct conclusions. First, the laws shortcomings lie in the methods they are presented. Unfortunately, most of them are written in "a list or general prohibition method" [2, 438]. According to them, the list method is very restrictive while the general prohibition method is too broad. Second, they "do not address third party" [2, 438]. Fortunately, *Boston College Law Review* reports that federal and state legislatures have adopted certain mechanisms to reconcile the interests of the victim and alleged harasser. These mechanisms involve "(1) an objective or subjective reasonable person test based on the victim's perspective, (2) an objective reasonable person test based on the harasser's perspective, (3) a specific intent element, or (4) some combination of the above" [5, 302]. As technology changes, so should the laws. Legislatures should review the stalking and harassment laws to ensure that they are adequate to address the new crime of cyberstalking [3, 157].

In general, the discussed references achieved its overall purpose as they broadened the boundaries of public awareness on the issue. They drew law enforcement and the legal community attention to this crime. We share their conviction that "more effective laws and increased enforcement will lead to more reliable data collection methods and hopefully a deeper understanding of cyberstalking" [2, 440]. We'd like to add that research in this field would be more valuable if a proper differentiation of cyberstalking and offline stalking was included. It would give the readers a clearer understanding of cyberstalking and its prevalence.

1. COMPUTER HACKING

Cybercriminals (hackers, phone phreakers, blue boxers, virus writers, pirates, cypherpunks, anarchists, cyberpunks, etc.) employ diverse kinds of security attacks. Still hackers are believed to be the most frequent and the most dangerous of them. Hacking is the activity of breaking into a computer system to gain an unauthorized access. Hackers can intentionally gain unauthorized access to computer systems. Most feared motives for hackers' attacks are data breach, data theft, money or simply system damage. It has become a big problem concerning Internet security. The worst thing is that it can happen and one even won't know about it. Hackers use a robot scanning the Internet for available ports and openings in the computer that allows data to pass back and forth from a network connection like the Internet. Having found unprotected ports on the computer, they can simply insert viruses and spam. To minimize the risk of becoming a hacking victim it's important to disconnect the computer from the

Internet when using it, as well it's necessary to install and activate a competent firewall as it provides a layer of Internet security to strengthen the defenses of the computer and it will help protect against any hacking attempts on the system. One should download and install any security updates as soon as they become available because not installing all of the recommended updates is the same as leaving the computer open for the hackers to walk through. The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another highly dangerous computer crime is the hacking of Internet Protocol (IP) addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities. To avoid hacking one should never post the IP address in a public place.

2. FISHING AS A KIND OF SOCIAL ENGINEERING

Phishing is another type of computer crimes. It is an example of social engineering techniques used to deceive users and exploit the poor usability of current web security technologies, usually leading to financial losses. Modern phishers are "dynamic and depend more on social engineering techniques rather than software vulnerabilities" [6]. Phishing scams pretend to be a legitimate business like a bank or credit company or they can include phony emails about a bogus inheritance, jobs overseas handling money transactions for a large salary and illegitimate loan approvals. Phishing typically attempts to acquire sensitive personal information in e-communications. These communications can range from popular social web sites, auction sites, online payment processors or IT administrators. They are commonly used to tempt the unsuspecting public as a trustworthy source. Phishing is usually carried out by e-mail. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that will be used for identity theft. If the user does this, the Web site steals this information. Phishing emails attempt to recruit the victims as mules for a funds transfer scam [7]. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Dhinakaran, C., Nagamalai, D., Lee, J.K. [3] developed an anti-phishing methodology and implemented in the network. Their approach is highly effective to prevent phishing attacks. It reduced more than 80% of the false negatives and more than 95% of phishing attacks in our network. Martin., et al. [8] describes a framework to better classify and predict the phishing sites using neural networks. A neural network is a multilayer system which reduces the error and increases the performance. To avoid phishing one should not e-mail personal or financial information and be cautious about opening any attachment or downloading any files from e-mails. One should neither reply the e-mails asking for personal and financial information nor click on the link in the pop-up messages. People should always use the anti-virus and anti-spyware software and update them regularly.

3. CYBERSTALKING AS A CRIMINAL OFFENSE

Cyberstalking is also a form of computer related crime as it refers to harassment or unwanted communication via some form of technology including computers, global positioning systems, cell phones, cameras and more. Cyberstalking can include harassing, threatening or obscene emails, excessive spamming, live chat harassment otherwise known as flaming, inappropriate messages on message boards or online guest books, dangerous electronic viruses sent, unsolicited email, and electronic identity theft. Parsons-Pollard and Moriarty [2] stress that people can be followed and pursued on line, receiving multiple emails or text messages per day, unsolicited threatening emails and/or death threats, electronic viruses, extreme amounts of spamming, abusive phone calls; experiencing sexual harassment via online posts, emails or cell phones, including posting and/or creating sexually explicit images; find their personal information (phone numbers, email addresses, and street addresses) posted without their consent; being subscribed to pornography and

unwanted advertising without their knowledge or consent, etc. Cyberstalkers often target the users by means of chat rooms, message boards, discussion online forums, listening devices, hidden cameras and social networking websites to gather information and harass the users on the basis of the information gathered. Being emotionally weak and unstable, women and children are at the greatest risk for cyberstalking. We witness the "social" era of the Internet. Social networking sites (SNSs) such as Facebook, YouTube, MySpace, Twitter, Blogger, Tumblr, LinkedIn, etc have paved the way for easier communication to friends and family, but more importantly, their friends and family are connected to others, resulting in potential new networks. They allow users to create their own personal virtual space that includes applications like photo-sharing, instant messaging, and blogs. Social networking continues to gain momentum. In the USA the most popular social network is Facebook, followed by YouTube, Twitter, MySpace, Blogger, Tumblr, and LinkedIn. In U.S. 68% of women and 54% of men use social media to keep in contact with their peers, meet new people, listen to music, share ideas, join organizations, play games, or participate in other activities that the world of social networking has to offer**.** 9 out of every 10 U.S. Internet users visit a social networking site in a month, and an average Internet user spends more than 4 hours on these sites each month. Americans spend 23% of Internet time on social networks [9]. There are now more social-networking accounts than there are people in the world. According to Social Networking Watch [9], in 2010 there were approximately 10 billion social-networking and online-world accounts and almost 4.5 billion of these are active. 1 out of every 8 minutes online is spent on Facebook. Facebook users upload about 3,000,000,000 photos every month. The "average (Facebook) user has 130 friends on the site ... (and) spends more than 55 minutes per day on Facebook" [10]. This data, which illustrates the skyrocketing proliferation of social networking, use-tells us that, like it or not, this new technology is here to stay. As wonderful as it is for individuals to share their daily lives online with friends and family, Internet users are open to moral attacks or may experience harassment or stalking through these social networking media.

SNSs have both positive and negative effects on their users. On the one hand, they provide an environment that facilitates increasing one's social circle of friends. On the other, they provide an environment where cyberstalkers and cyberbullers can easily target their victims. Social networking sites rely on connections and communication, so they encourage SNSs users to provide a certain amount of personal information, which can be used by cybercriminals to threaten, insult, or harass the victims. Social networking sites make personal information more available to individuals who may wish to use this information for illegal activities. On SNSs such ethical principles as privacy of information, accuracy of sharing and verifying information, property of the posted information, and access to the shared information are usually violated. SNSs have both positive and negative effects on their users. On the one hand, they provide an environment that facilitates increasing one's social circle of friends. Internet users can avail themselves of many different applications in one place. Forums, chat rooms, email, instant-messaging, daily status posts, and photo sharing allow individuals to communicate in multiple ways. On the other hand, SNSs provide an environment where cyberstalkers can easily target their victims. Social networking sites rely on connections and communication, so they encourage SNSs users to provide a certain amount of personal information. It is personal information – "both held by the site provider and posted either by the user or by friends and family of the user – that can become a source of vulnerability" [11, 940).

Light and McGrath [12] claim that social networking sites such as Facebook are not ethical as they violate privacy. They say that privacy settings have gone further and further away into the background on Facebook that's why more than 800 million active Facebook users can find themselves at risk of cyberstalking or identity theft if they do not pro-actively adopt the necessary privacy settings.

Cyberstalkers and cyberbullers use the Internet to seek and compile victim's personal

information. They send e-mails that threaten, insult, or harass, disrupt e-mail communications by flooding a victim's e-mail box with unwanted mail or by sending a virus. They even can use the victim's e-mail identity to send false messages to others or to purchase goods and services. According to a new study by the British Electronic Communication Harassment Organization (ECHO), cyberstalking has become more prevalent than offline stalking. Researchers surveyed 250 participants between the ages of 14 and 74 and found out that cyberstalkers commonly used social networks as channels for harassment and intimidation. 20% of victims were tracked through their social networks, compared to 4% who were targeted via dating sites [9]. Computer monitoring software or spyware allows a cyberstalker to monitor a SNS user. It can be installed in many ways, either physically or remotely, and a victim may be unaware of its installation. "Once installed, spyware will send the abuser all of the victim's computer activity, including passwords to e-mail and social networking sites" [11, 942].

On SNSs such ethical principles as privacy of information, accuracy of sharing and verifying information, property of the posted information, and access to the shared information are usually violated. Studying the users' ethical behavior (as opposed to the technology and how the two intertwine), Light and McGrath comment that "developers don't always know how the technology is going to work in practice, and the users don't, so it becomes a case of: 'who's moral obligation is it? Is it the users? Is it the developers?" [12, 307].

Social networking sites make personal information more available to individuals who may wish to use this information for illegal activities. Even if the user does not post personal content on the Internet and does not have a page of his/her own, an abuser may be able to track down this information if a family member, child, or friend posts a picture or other personal information about the SNS user. When sharing information on SNS, it is not only necessary to consider the privacy of one's personal information, but the privacy of the information of others who may be tied to the information being shared.

Additionally, social networking sites do not check into whether a user who creates a profile is in fact a real person, so the creation of a fake profile is as easy as the creation of a real profile. According to Baughman, "a fake profile may allow an abuser to access the site of a victim or victim's family member, when an authentic profile would act as a red flag" [11, 944]. It is the responsibility of the SNS user to determine the authenticity of a person or program before allowing the person or program access to the shared information.

Though cyberstalking is very dangerous it can be easily prevented. First of all, parents should be careful about their children. They should monitor their child, their access to electronic communications and their activities online, install a reliable Internet filter and enable parental controls where available and check the child's privacy settings. Adults, especially women, should be extremely cautious about meeting online acquaintances in person and make sure that their Internet Service Provider and Internet Relay Chat network have an acceptable use policy that prohibits cyberstalking. And if the network fails to respond to the complaints, it's better to switch to a provider that is more responsive to user's complaints. If a situation online becomes hostile, it is necessary to log off or surf elsewhere. In case the user's fear increases, it is better to contact a local law enforcement agency.

CONCLUSIONS

Knowledge and comprehension of computer crimes such as hacking, phishing, and cyberstalking is the key to prevent people from becoming a victim. The utilitarian approach comes closest to our ethical decision making. It shows that the moral worth of preventing computer-based crimes is determined by its resulting outcome and maximizes the overall good of the society.

REFERENCES

[1] Kshetri N. Positive Externality, Increasing Returns, and the Rise in Cybercrimes / N. Kshetri // *Communications of the ACM* – 2009. –V. 52, № 12. – P. 141-144.

[2] Parsons-Pollard N. Cyberstalking: Utilizing What We Do Know / N. Parsons-Pollard, L. J. Moriarty // *Victims & Offenders* – 2009. – V. 4, № 4. – P. 435-441.

[3] Goodno N. H. Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws / N. H. Goodno // *Missouri Law Review* – 2007. –V. 72, № 1. – P. 125-198.

[4] *1999 Report on Cyberstalking: a New Challenge for Law Enforcement and Industry* / U.S. Department of Justice, USA, 2003; http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

[5] Murray Megan W. A Balance of Convenience: the Use of Burden-Shifting Devices in Criminal Cyberharassment Law / Megan W. Murray // *Boston College Law Review* – 2011. –V. 52, № 1. – P. 289-338.

[6] Dhinakaran C. Multilayer Approach to Defend Phishing Attacks / C. Dhinakaran, D. Nagamalai, J.K. Lee // *Journal of Internet Technology (JIT)* – 2010. –V. 72, № 1. – P. 112-117.

[7] Joffee, R. Cybercrime: the Global Epidemic at Your Network Door / R. Joffee // *Network Security*, – 2010. –№ 7. – P. 4-7.

[8] Martin A. A Framework for Predicting Phishing Websites Using Neural Networks / A. Martin, et al. // *International Journal of Computer Science Issues (IJCSI)*, – 2011. – V. 8, № 2. – P. 330-336.

[9] Social Networking Watch: All Social Networking Statistics / *Courtland Brooks*, 2011; http://www.socialnetworkingwatch.com

[10] Statistics. *Facebook,* USA, 2011; http://www.facebook.com/press/info.php?statistics

[11] Baughman L. L. Friend Request or Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators / L. L. Baughman // *Widener Law Journal* – 2010. –V. 19, № 3. – P. 933-966.

[12] Light B. Ethics and Social Networking Sites**:** a Disclosive Analysis of Facebook / B. Light, and K. McGrath // *Information Technology & People* – 2010. –V. 23, № 4. – P. 290-311.