Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 13, December 2019

Cybercrimes

Amit Sharma
Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

ABSTRACT:Cybercrime is a huge threat to humanity, but it can be particularly devastating to people who become victims. A detailed and topical overview of cybercrime affecting individuals is included in this chapter. It also discusses the motive of offenders who commit such attacks and the main human factors and psychological factors that lead to the success of cybercriminals.Social engineering (e.g., dating scams, phishing, cat fishing), internet abuse (e.g., cyber bullying, revenge porn, stalking, hate crimes), data-related crimes (e.g., identity theft, doxing), hacking (e.g., malware, account hacking,crypto jacking), and denial-of-service offences are main fields evaluated. As part of its contribution, if systematic interdisciplinary initiatives are not undertaken, the chapter provides a summary taxonomy of cybercrimes against individuals and an argument on whether they will continue to occur.

KEYWORDS: Cryptojacking, denial-of-service (dos), cyber bullying, phishing, identity theft, cautions.

INTRODUCTION

Latest data indicates that over the last two decades, there has been a substantial growth in the number of crimes using information technology (IT) technologies, although the rate of typical crimes has declined. In the United Kingdom, crime figures currently reveal that 'crime has not necessarily plummeted but changed, switching to newer modes of crime. Some researchers find that cyber-crime rates for property crime indicate a crime surge that 'will override the gains that Americans have enjoyed as a result of the gradual decline in conventional forms of property crime.'These modern offences take place in a digital environment where, unlike more conventional types of violence, the space and time of criminals and victims do not converge physically[1]. This begs the question of whether cybercrime offending and victimization can be compensated for by conventional correlates of offending and victimization.

For typical offences, a substantial body of evidence has found that victims are likely to commit violent acts and that perpetrators are relatively likely to be victimized. Among other aspects, this study has found that suspects and perpetrators share risk factors such as poor self-control, repetitive habits or a dangerous lifestyle and social demographics that increase both their risk of crime and victimization.Offending can also explicitly cause victimization or vice versa. It should be remembered that only a portion of the population of criminals is at risk of being abused, and not all victims commit offences. In order to clearly distinguish the variations in underlying risk factors, researchers recently emphasized the significance of examining victims-only, offenders-only, and victim-offenders as distinct categories[2].

While cybercrime criminal and victimization have been mostly independently observed, there is evidence of common risk factors, such as poor self-control and dangerous online routine behaviors. Cybercrime crimes have actually been shown to be a risk factor for victimization, and vice versa. This suggests that cybercrime offending and victimization share close underlying similarities and, as such, as is apparent in conventional offences, can be investigated in parallel.One research to date has directly discussed the likelihood of a victim-offender overlap amongst young people in cybercrime. This analysis showed a major crossover in the offending and victimizing of financial cybercrime correlated with poor self-control, revenge, high online dis-inhibition, and routine online practices. Although this research focuses exclusively on youth financial cybercrime, it is unclear if the overlap is visible in adult samples and in other cybercrime forms.

Furthermore, previous study would not equate cybercrime empirically with conventional crime, restricting our interpretation of any similarity in the associations of these forms of crime. The present research aims to overcome these literature limitations by using former offenders from the Netherlands' adult high-risk community to determine their patterns of cybercrime and conventional offending and victimization.Among offending-only, victimization-only and victimization-offending classes, for technological computer-dependent cybercrime (like hacking, data stealing, defacing, and etcetera) and conventional crime, the risk factors for offending and victimization are contrasted[3]. Danger variables include poor self-control, repetitive tasks online and offline, and IT skills. The research would demonstrate to what degree cybercrime offending and victimization can be explained by these risk factors in a manner close to conventional crime.

CYBERCRIMECATEGORIES

- ***Phishing***

Is the effort to deceive clients into revealing their personal security information by masquerading as trustworthy companies in an e-mail; their credit card numbers, bank account records, or other confidential information? Their messages can ask recipients to "update" their account information, "validate" or "confirm" them. Phishing is a two-time fraud, taking the identity of a corporation first and then using it to victimize customers by stealing their credit identity.The term phishing (also known as spoofing) derives from the fact that internet scammer’s use more advanced lures as they "fish" for the financial information and login information of users. Since it is very easy to execute, phishing is the most widely used social engineering attack to date since no direct contact between hacker and target is needed (i.e., hacker does not need to phone their prey, pretending that they are a technical support staff, etc.)[4].The risk of getting someone addicted is enhanced by sending mass e-mails to thousands of possible victims. In order for such attacks to operate, there are normally three distinct steps:

1. Setting up a mimic web account.
2. Sending out a convincingly bogus e-mail, drawing consumers to the imitation website.
3. To get details, users are then redirected to the actual site.

- ***HACKING***

Hacking is one of the most frequently studied and explored types of cyber-criminal activity, acting as an acute topic for societal fears regarding the danger to society that such activity presents. "Unauthorized access and subsequent use of the computer systems of other people" is the simple concept of hacking. The early hackers had a love of technology and a compelling desire to learn how it all worked, and their aim was to drive systems past what they were supposed to achieve.The term hacker did not, as it does today, have a negative connotation. The attacks take place in many stages, such as collecting or reconnaissance information, searching and ultimately accessing the target system. The processing of information requires means of accessing information or opening security gaps. That is much about the way the typical kind of theft is done. Before making an attempt, the thief can find out all of the details about the location he needs to steal.

The machine intruder would attempt to uncover details about the target much like this. One such tool used by an attacker to get knowledge is Social Engineering. There are two major categories, machine or technology-based deception and human-based deception, in which all social engineering attempts can be categorized[5]. The technology-based strategy is to trick the user into thinking that the "real" computer device communicates and to get the user to supply sensitive information.By deceit, by taking advantage of the innocence of the perpetrator, and the inherent human desire to be friendly and liked, the human solution is accomplished. Organized offenders have the means to access the requisite people's facilities. As the ability to reach, monitor and disrupt our technological and defense infrastructure increases at an equal pace, the challenge of organized crime and terrorist activity becomes even more subtle.Today, the most widely used means of correspondence and exchange of information are definitely e-mail and the Internet. Every day, well over 2 billion individuals access the Internet. This is called cyber child labor by criminal cartels "buying" thrill-seeking hackers and "script kiddies" to supply the skills and resources.

- ***SPAM***

Another form of cybercrime is spam mail, which is arguably the most profound result of the capacity of the Internet to put unparalleled influence in a single individual's hands. The sending of bulk e-mails selling goods, services or investment programs is spam mail, which could well appear to be fraudulent. The aim of spam mail is to confuse or hide clients into thinking that, usually at a discounted price, they will receive a legitimate product or service.The spammer,

though, asks for money or fair security details before the deal happens, such as credit card number or other personal information. The customer will never hear from the spammer after revealing his security details[6]. Today, according to a Symantec Intelligence Survey, spammers who spread malicious code and phishing e-mails are also searching for the perfect way to hit computer users by leveraging social engineering and technological advancements,Spam levels continued to decline from the 89 percent highest in 2010, to 68 percent of global e-mail traffic in 2012. Partisan spam returned to operation in April 2012, targeting mostly the US and French community. In Syria, the complicated situation has also been the target of spam e-mails. In 2012, the United States was ranked number 5 after India for spam origination with China.

- ***CYBER HARASSMENT***

Using electronic data and networking platforms such as e-mail, email messaging, text messages, blogs, cell phones, pagers, instant messages and defamatory websites to bully or otherwise abuse an individual or group by personal attacks or other means is cyber-harassment or bullying."There is a beginning and an end, at least in a physical fight, but when the taunts and humiliation follow a child into their home, it's 'torture,' and it doesn't stop". Among young people, cyber-bullying, taunts, threats and abuse over the Internet or text messages received from cell phones have been common, with disastrous results in some situations.Derek Randel, a motivational speaker, retired teacher and founder of StoppingSchoolViolence.com, claims that with new social technology, such as Facebook and text messaging, cyber-bullying has become so widespread that it has impacted every school in every nation.

- ***PLASTIC CARD FRAUD***

Plastic Card Fraud is the fraudulent use of plastic or credit cards to procure money or property, or the stealing of a plastic card number. Plastic card losses in 2011 were £ 341 million, according to APACS, the UK Payments Group, of which £ 80 million was the result of theft abroad.In countries that have yet to upgrade to Chip and PIN, this usually includes offenders using compromised UK card data at cash machines and supermarkets. The UK's largest form of fraud is card-not-present (CNP) fraud. CNP accounted for 65% of gross losses in 2011, which was £ 220.9 million (down 3%) in 2011. CNP fraud involves any fraud requiring payment of an online, mobile or postal order.The difficulty with countering this form of fraud lies in the fact that there is neither the card nor the cardholder at a physical point in a supermarket[7]. There are a range of methods used by fraudsters to access both cards and card information, such as phishing, submitting spam e-mails, or the database of hacking firms, as described above.

- ***IDENTITY THEFT***

In the UK, this is the fastest growing form of fraud. Identity theft is the act of acquiring, without his or her consent, personal information about another person and using this information to

commit theft or fraud. The Internet has given cyber attackers the chance to access certain information from the database of insecure enterprises. It has also allowed them to cause victims to assume that confidential personal information is revealed to a legitimate company; often as a response to e-mail requesting updating billing or membership information;it often takes the form of an invitation to publish a (fraudulent) work on the Internet. According to the All Party Parliamentary Community, the evidence available, both in the United Kingdom and internationally, shows that identity theft is a significant and growing issue due to the rising and changing ways of accessing and using personal data. Subsequently, over the coming years, it is expected to climb higher. This is a dilemma that is acknowledged at the highest government levels. About 150,000 victims of these identity offences were identified and covered by CIFAS, the UK Fraud Detection Agency, in 2012 alone.

CONCLUSIONS

It is impossible to imagine that physical crime has not been influenced by the IT revolution and the onset of cyberspace. With regard to the drop in crime, we have given counterarguments to Farrell and Birks that support two hypotheses: that, among other reasons, the use of cyberspace for leisure activities at home has reduced the amount of opportunities in the physical space for certain crimes, leading to certain types of drop in crime, especially for crimes associated with young people; and that there has been an increase in cyberspace criminal opportunities, which has also decreased criminal opportunities in physical space, particularly with regard to dual crimes. These dynamics related to the onset of cyberspace are analogous and, in some cases, etiologically related. Cybercrime has not triggered a decline in terrorism. There was no overarching cause caused by Tis, but the rise of cyberspace as a new field of illicit opportunity and cybercrime influenced particular forms of the decline in crime.

REFERENCES

[1] N. Kshetri, “The simple economics of cybercrimes,” *IEEE Security and Privacy*. 2006, doi: 10.1109/MSP.2006.27.

[2] S. Ghosh and E. Turrini, *Cybercrimes: A multidisciplinary analysis*. 2010.

[3] E. R. Leukfeldt and M. Yar, “Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis,” *Deviant Behavior*, 2016, doi: 10.1080/01639625.2015.1012409.

[4] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, “Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime,” *European Journal on Criminal Policy and Research*, 2017, doi: 10.1007/s10610-016-9332-z.

[5] A. Hassan, “Cybercrime in Nigeria: Causes, Effects and the Way Out,” *ARPN Journal of*

Science …, 2012.

[6] M. Levi, "Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change," *Crime, Law and Social Change*, 2017, doi: 10.1007/s10611-016-9645-3.

[7] D. Wall, "Cybercrimes and the Internet," in *Crime and the Internet*, 2010.