International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Data Theft Related to Cyber Offences in Society

Gomathi S

B.A., LL.B., (Hons), Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences

Abstract-

Data theft is a act of the stealing computer based information from the unknowing victim with the intent of an compromising privacy or the obtaining confidential information. There is another way to steal data. The aim of the study is to know people's awareness about the data theft and information theft that are occurring nowadays, and to know whether people have experienced any data theft or information theft. The study deals with non descriptive research. The research is being done by simple random sampling method by providing evidence through surveys. It deals with both primary as well as secondary sources of data and various secondary sources books, articles, research papers etc which are used as reference. Nearly 200 members were surveyed for the analysis. The study deals with survey methods and the main tool for calculating or analysing the results in graphs. The method of collecting is through a survey method by getting people's opinion and answers to the questionnaires. The independent variables included age, gender, educational qualifications and occupation. The dependent variables are people’s awareness about the data theft and Information theft that is occurring nowadays and people’s experiences towards any data theft or information theft. The finding of this paper is that we should be more aware, identity theft is occurring at a higher phase as computer network systems become more vulnerable from attacks by hackers and viruses.

Keywords: Criminals, Data theft, Information technology, Online, Personal informations.

INTRODUCTION

The term ‘information theft’ is actually a misnomer. Under the Indian law, theft can only committed in the respect of movable property. Data is not a movable property, and hence the unauthorized act of taking away data electronically (by way of emailing it to oneself or by hacking into a computer system, for example) is not considered as theft. As we have a tendency to concentrate additional and additional of the worth of our economy into accessible styles of data, we have a tendency to worry additional and additional regarding the dark facet of the knowledge Revolution - stealing and abuse of knowledge. Information stealing refers to an unauthorized speech act of confidential knowledge to non-trusted parties, either accidentally or deliberately. Data breaches did not begin when the company began stored their protects the data digitally. In fact, data breaches has existed for as long as an individuals and company has maintained records and the stored private information or messages. Data Security breaches that could lead to identity theft are just a click away as computer network systems become more and more vulnerable from attacks by hackers and viruses. Databases are also accessed daily by workers who have the potential of misusing people‘s private information for financial gains.

Discovering Private information about someone is even easier today and can occur anywhere access to medical or personal information exists. Unlike the days before laptops and personal data storage devices, current technology makes it possible to download thousands of records into a single handheld device or take pictures of information appearing on screens in a few second. Data breaches increases in frequency in an 1980s, and in the 1990s and the early 2000s public awareness of a potential for the data breach began to rise. IT act plays a major role in protecting the data. Unpatched Security Vulnerabilities, Human Error, Malware, Insider Misuse, Physical Theft of a Data-Carrying Device these are major factors that cause data theft. At the top of a list of new trend is text-based “smishing” attack in which hackers use SMS text messages to carry out phishing attack against the unsuspecting users.More over, hackers are experimenting emerging with new technologies to carry out their attacks. Data breach incident in India has been higher compared to a global averages. **The aim of the study is to understand various kinds of data theft, to know the people’s awareness about the data theft.**

OBJECTIVES

- To know the people’s awareness about the data theft and information theft that are occurring nowadays
- To know whether people have experienced any data theft or information theft.
- To Analyse the various kinds of information theft and data theft
- To understand about the punishment that is provided under the Information Technology Act, 2000.

REVIEW OF LITERATURE

Yang et al, (2015) The main aspects are the customary strategies for verifying systems, for example, firewalls and interruption identification frameworks are conveyed at the limit between an endeavor's interior system and its Internet association. **Bogomolov et al, (2014)** From the aspects of the author, control instruments are not adequate either, in light of the fact that much of the time the aggressors are approved clients and there is just no entrance control infringement when the secret data is taken. Other potential arrangements include:restricting utilization of removable media on the end client's PC. **Balzotti et al, (2018)** In the article it shows that the private data may incorporate item outlines, advertising plans, client records and business numbers in the configuration of Microsoft Office, Adobe pdf, HTML, and so forth. **John Sebes, (2007)** examined that, Associations ordinarily process the data by sharing those advanced records from ensured document servers and circulating them by downloads or email messages. Contrasted to the conventional print position, the computerized arrangement can fundamentally improve the productivity of taking care of the classified data just as keeping up its unwavering quality. **Scheffer, (2009)** studied the implications of networks‛ collection of personal information data. Issues identifying with violations in the internet and tending to them, nations can attempt to keep up for their residents a similar security in the data society that they have customarily delighted**. Gareth, (2018)** Pharming is an extraordinary kind of PC related assault which happens when the aggressor embed certain PC information in a Domain Name System's IP distribution table dependable with directing the unfortunate casualty's PC program solicitations to counterfeit website pages or to other web assets constrained by the assailant. **Bequai, (1997)** explained the institutional framework in which identity theft occurs and discussed some policy issues. Wholesale fraud is the illegal utilization of another person's distinguishing actualities to execute a financial extortion by opening a ledger, acquiring credit, applying for bank or retail establishment cards, or renting autos or lofts for the sake of another. **Saunders, (1999)** In 2004, 3.6 million families, speaking to 3% of the families in the United States, found that in any event one individual from the family unit had been the casualty of wholesale fraud during the past a half year.The households most likely to experience identity theft. **Zucker, (2006)** examined the robbery of telecommunications services like "telephone phreakers" of three decades prior and set a trend for what has become a significant criminal industry. **Hannken-Illjes, (2009)** examined the nature of identity theft and looked at the factors that led to its growth. It also examined whether or not the markets for goods and services could limit the risk that identity theft poses to the payment system. Government regulations are need to be protect the integrity and the efficiency of the payment system in order to overcome market failures. **Ng and Keung, (2018)** examined Customary ways to deal with taking character incorporate "dumpster plunging" to recover individual information from disposed of creditcard or service charges. when people input individual distinguishing proof data, paying off representatives to hand over close to home client data, and physically taking secret records or PC hard drives in which personality data is put away. **Hadnagy, (2015)** discussed the differences among financial frauds associated with identity theft which he believed necessitate additional distinction and treatment by consumers, lenders, financial institutions, and law enforcement agencies in order to better understand these kinds of criminal behaviour. **Syngress, (2002)** discussed about the chance that the risk of misfortune or robbery can't be stayed away from, anticipation countermeasures can be utilised to diminish the probability that cell phones may be lost or taken and to keep other individuals from getting to and male volently utilising the gadgets, information, and remote administrations. Passwords and information encryption are the most generally applied aversion countermeasures. **Von Ah Morano, (2019)** examined the numerous sellers that can give different countermeasures, for example, client verification, gadget blocking, and remote gadget wipe administrations, to avoid unapproved get to when gadgets are lost or taken. **Warburton, (2013)** look into directed in April demonstrates that a huge number of customers unwittingly succumb to phishing assaults — email interchanges intended to take purchaser account data, for example, charge card information, places of residence and phone numbers. Purchasers have motivation to be anxious. Phishing assaults undermine their trust in the realness of email originators, compromising customer trust in the very establishment of Internet-based correspondences. **Fincher, (2015)** discussed that there are various procedures and techniques that character cheats have created to take unfortunate casualties' close to home distinguishing data including low tech (disconnected) and cutting edge (on the web) methods. Government managed savings numbers give moment access to an individual's close to home data and are generally utilized for distinguishing proof and record numbers by insurance agencies, colleges, satellite TV organizations, military ID, and banks. **Copes, (2009)** examined that criminals can take a wallet or tote, work at an occupation that bears him/her entrance to credit records, buy the data from somebody who does or discover exploited people by taking mail, dealing with the junk, or via looking through the Internet. **Gill, (2006)** Sorted out rings may "plant" a representative in a home loan bank's office, specialist's office, or HR office to get to information. Different hoodlums have detailed purchasing data from different guilty parties, for example, whores, criminals, tranquilize addicts, and other road tricksters. **Vieraitis, (2012)** For instance, Copes and Vieraitis' meetings with character cheats found that some of them developed advanced ploys to initiate exploited people to uncover individual data, for example, setting up counterfeit work locales or organizations, while others essentially persuaded a companion or comparative with assistance the guilty party out of a troublesome monetary situation. **Lampke, (2010)** discusses that online techniques may incorporate hacking into organizations that keep up data authentically or using phishing, which includes spam email battles that request data from would-be unfortunate casualties. Underground sites and discussions sell taken data (e.g., Mastercard and financial balance numbers) for generally modest prices.

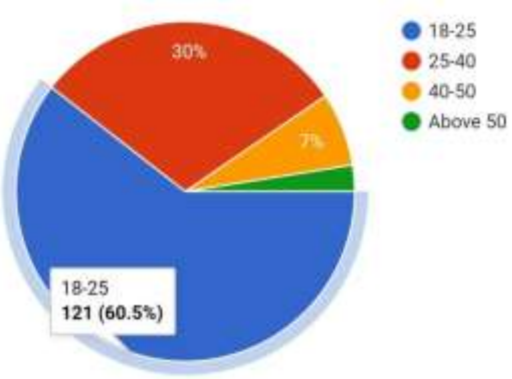
MATERIALS AND METHODS

- The research method followed here is an empirical research. A total of 200 samples have been taken out of which is taken through a simple random sampling method.
- The independent variable taken here is age, gender and educational qualifications and occupation.
- The dependent variables are people aware about the data theft and information theft that is occurring in society, people have experienced any data theft or information theft, ways to prevent data theft.

- The statistical tools used by the researcher is graphical representation like bar charts.

ANALYSIS

Age



Gender

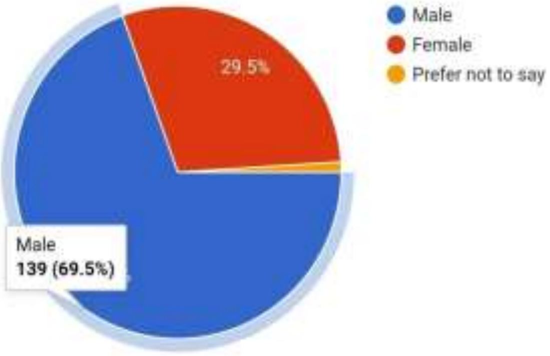
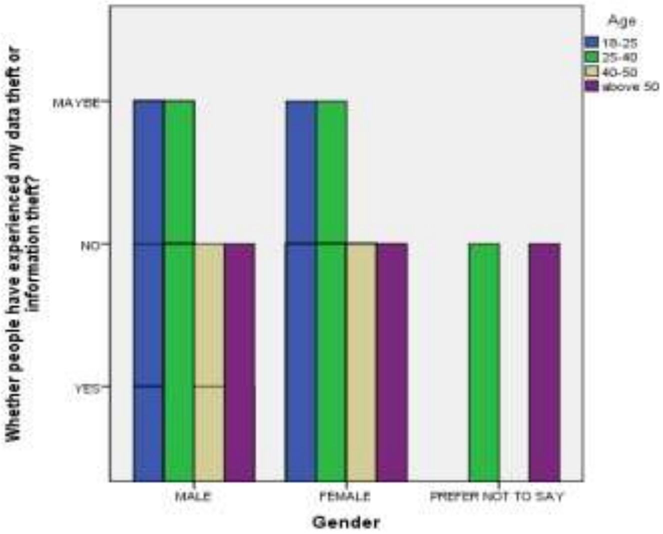
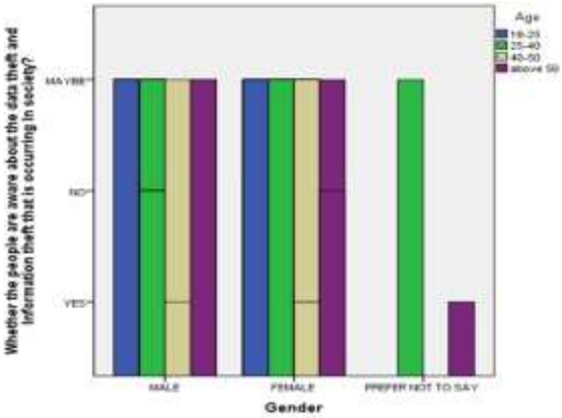


Fig 1: People have experienced data theft or information theft



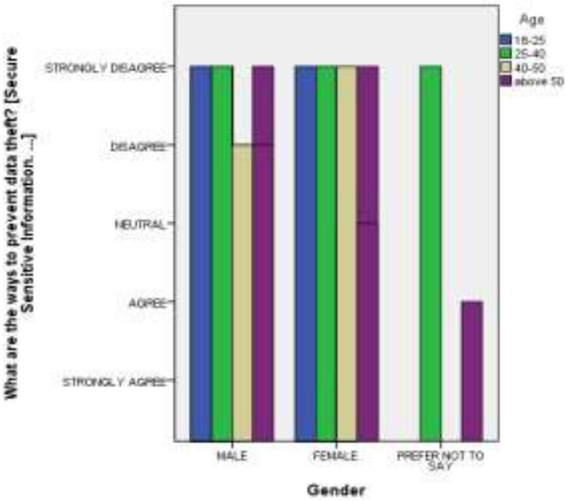
Legend: The above chart shows the responses that people have experienced any data theft or information theft between gender and age of the people.

Fig 2: Are people aware about the data theft and information theft that is occurring in society



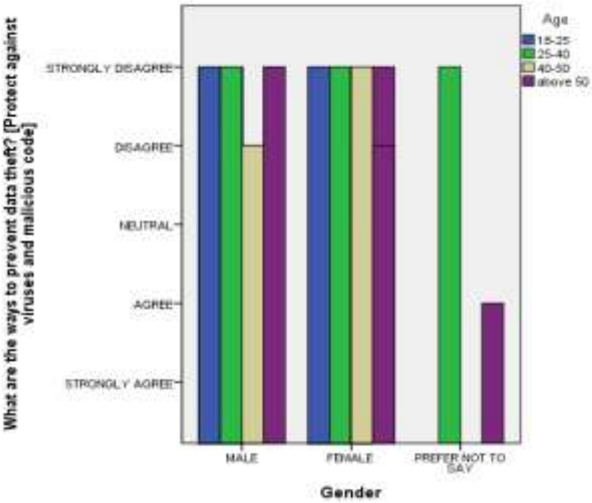
Legend: The above chart shows the responses are people aware about the data theft and information theft that is occurring in society by analysing between gender and age of the people.

Fig 3: The ways to prevent data theft (secure sensitive information)



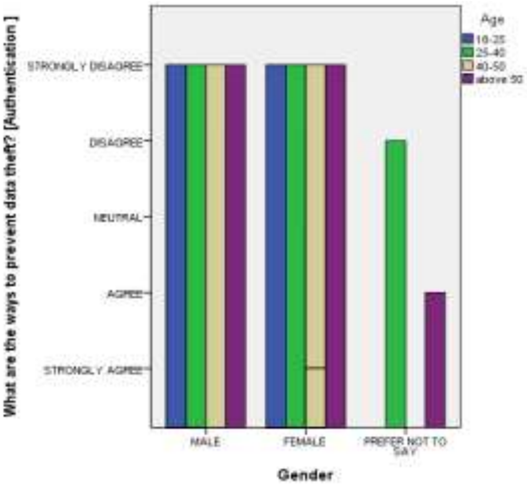
Legend: The above chart shows that people answered that ways to prevent data theft is by (secure sensitive information) by analysing between gender and age of the people.

Fig 4: The ways to prevent data theft (protect against viruses and malicious code)



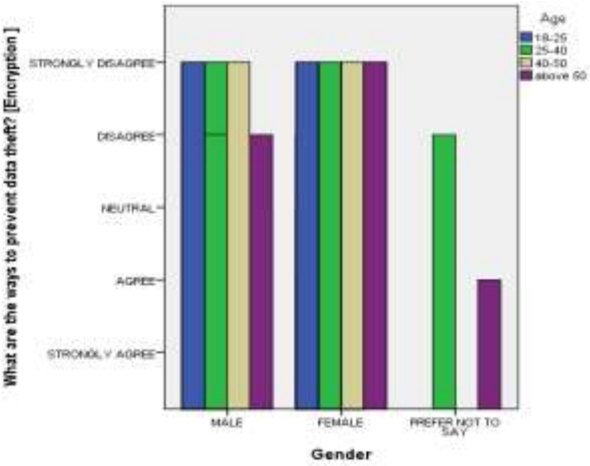
Legend: The above chart shows that people answered that ways to prevent data theft is by (protect against viruses and malicious code) by analysing the gender and age of the people.

Fig 5: The ways to prevent data theft (authentication)



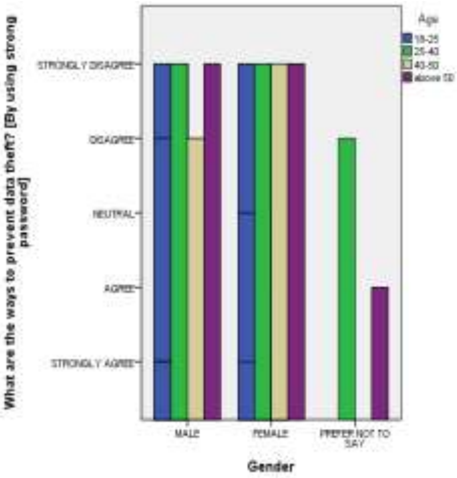
Legend: The above chart shows that people answered that ways to prevent data theft is by (authentication) by analysing between gender and age of the people.

Fig 6: The ways to prevent data theft (encryption)



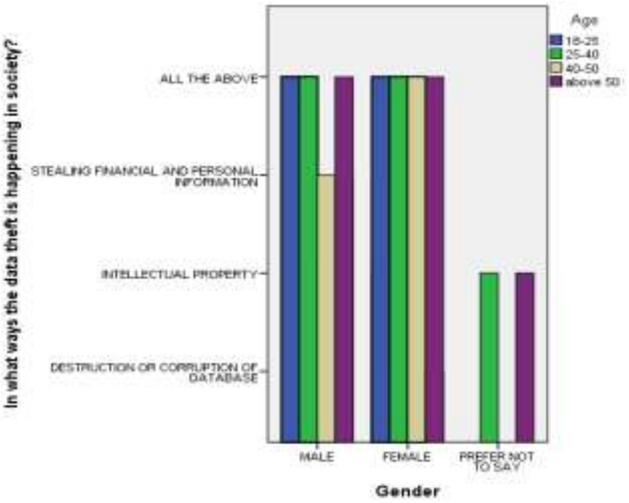
Legend: The above chart shows that people answered that ways to prevent data theft is by (encryption) by analysing between gender and age of the people.

Fig 7: The ways to prevent data theft (by using strong password)



Legend: The above chart shows that people answered that ways to prevent data theft is by (by using strong password) by analysing between gender and age of the people.

Fig 8: Ways that data theft is happening in society



Legend: The above chart shows the responses of the people in what ways that data theft is happening in society by analysing between gender and age of the people.

RESULT

In **figure 1**, the above chart shows the responses that people have experienced any data theft or information theft. 64% of the people answered that they have not experienced any data theft, 30% of them have experienced data theft in the society. From 18 to 25 years of age, people answered that they are not experiencing the data theft and some of them were affected and experiencing the data theft. For over 50 years they have not responded. In **figure 2**, the above chart shows the responses are people aware about the data theft and information theft that is occurring in society. 45.5% of the people were not merely aware about the data theft. 47.5% of the people respondent answered that they are aware about the data theft. 7% of the respondents are not aware. Between 25 to 40 they are saying no and 40 to 50 years of age they are saying that data theft and information theft is occurring in society. In **figure 3,** the above chart shows that 80% of the people strongly agree that ways to prevent data theft are by (secure sensitive information) by analysing between gender and age of the people. 55.5% of the people agree and 40% of the people are neutral. In **figure 4**, The above chart shows that people answered that ways to prevent data theft is by (protect against viruses and malicious code) by analysing between gender and age of the people. 85% of the people were strongly agreeing and 60% were agreeing and some of them are neutral. In **figure 5,** The above chart shows that people answered that ways to prevent data theft is by (authentication) by analysing between gender and age of the people. 95% of the people strongly agreed and 25% were neutral. In **figure 6**, the above chart shows that people answered that ways to prevent data theft is by (encryption) by analysing between gender and age of the people. 80% of the people strongly agree and 50% of them are neutral. In **figure 7,** The above chart shows that people answered that ways to prevent data theft is by (by using a strong password) by analysing between gender and age of the people. 75% of the people strongly agree and 55% agree and 45% of them are neutral. In **figure 8,** The above chart shows the responses of the people in what ways that data theft is happening in society and by analysing between gender and age of the people. 75.5% of the people answered that data theft is happening in all the ways, 10% were by stealing, 6.5% were by destruction.

DISCUSSION

In **figure 1**, the above chart shows the responses that people have experienced any data theft or information theft. From 18 to 25 years of age, people answered that they are not experiencing the data theft and some of them were affected and experiencing the data theft. For over 50 years they have not responded, this may be due to not having knowledge on the cyber offences and not knowing the difference between the other crimes. In **figure 2**, the above chart shows the responses are people aware about the data theft and information theft that is occurring in society. 45.5% of the people were not merely aware about the data theft. 47.5% of the people respondent answered that they are aware about the data theft. 7% of the respondents are not aware, this is due to some lack of awareness on data theft. Between 25 to 40 they are saying no and 40 to 50 years of age they are saying that data theft and information theft is occurring in society. In **figure 3,** the above chart shows that 80% of the people strongly agree that ways to prevent data theft are by (secure sensitive information). 55.5% of the people agree and 40% of the people are neutral. Because this is not the permanent preventive method and also forgetting the sensitive information may lead to this crime. In **figure 4**, The above chart shows that people answered that ways to prevent data theft is by (protect against viruses and malicious code). 85% of the people were strongly agreeing and 60% were agreeing and some of them are neutral. Because not upgrading and using the other unwanted sources will affect the software. In **figure 5,** The above chart shows that people answered that ways to prevent data theft is by (authentication). 95% of the people strongly agreed and 25% were neutral. This type of authentication will be prevented but if we ignore this type of authentication it will lead to data theft or any kind of viruses. In **figure 6**, the above chart shows that people answered that ways to prevent data theft is by (encryption). Because encryption is the method by which information is converted into secret code that hides the information's true meaning. In **figure 7,** The above chart shows that people answered that ways to prevent data theft is by (by using a strong password). 75% of the people strongly agree and 55% agree and 45% of them are neutral. Few people only answered because of the use of weak passwords and any kind of stealing of information. In **figure 8,** The above chart shows the responses of the people in what ways that data theft is happening in society, 75.5% of the people answered that data theft is happening in all ways, because nowadays there are many cyber offences that are happening in the society.

LIMITATION

The major limitation of my studies is the sample frame. The lack of education being major drawback. Their restrictive area of sample size was also a major drawback. The physical factors are the most impactful and a major factor and most of the people are unaware of the impacts. Privacy concern sometimes data collection might breach the privacy of the customer as their informations such as purchases, online transactions, and subscriptions are available to company whose services they are using.

CONCLUSION

Data security breaches that could lead to identity theft are occurring at a higher phase as computer network systems become more vulnerable from attacks by hackers and viruses. The lack of education is also the major problem when it's from the common public view. The number of customers victims of identity theft has also been rising over the years. As per the analysis through the graph, the findings of this paper are that the majority of the male respondents were aware about the data theft and the information theft that is occurring nowadays when compared to the female respondents, the majority of the people who have attended the survey responded that they have experienced data theft or information theft. Identity theft could be one of a main criminal issue in the future. The growing number of case only proves this tendency. It is difficult for the authorities to detect criminals who are going to commit identity theft. Because not upgrading and using the other unwanted sources will affect the software. That is why people should always be careful with the personal information. And my suggestion is we should be more careful in using sensitive information and should not share with any people. We should use all the security by using a strong password, authentication method, encryption and also other useful protection like upgrades, protection against viruses and malicious code.

REFERENCES

1. Balzotti, Caterinae, Andrea Braggnini, Maye Briani, and Emilianno Crestiani. 2017. “Understanding that mortal Mobility Flows there be Added up Mobile Phone Data ∗ ∗This Work Was Supported by Funding from Project MIE - Mobilità Eco sostenibile Cluster ‘Tec-Nologie per Le Smart Communities." vol. 68, no. 4, 2020, pp. 1116–1131.

2. Bequia, August. 1997. “E*merging Research and openings*. Management’s part.” computer System *inspection Update,* vol. 44, no. 9, pp. 1139–1154, September 2014.

3. Bogomolov, Andrew, Bruno Lepri, Jakopo Staiano, Nuriae Oliver, Fabio Pianesi, and Alex Pentland. 2014.*Proceedings of the national meetings on Multimodal Interaction,* vol. 10, no. 3, pp. 339–359, 2008.

4. Curtains, Heith, and Lynne M. Vieraitis. 2009. “Bounding of Rationality of thieves: Using that offender- predicated Exploratory the Information Policy.” *Criminology & Public Policy*, vol. 19, no. 2, pp. 185–201, 2017.

5. Caterina, 2012. *Identity stealers: Motives and styles.* UPNE vol. 22, no. 1, pp. 93–101, 2019.

6. Duffin, Edwin. 2006. “Defibrillator.” *Medically biased and computer Systems*, vol. 65, no. 2, 2018, pp. 477–493.

7. Gareth, Grainger. 2018. "Problem Concerning *Emerging Research and openings*. Implicit International Cooperation Principles 1.” *The International Confines of Cybercrime,* vol. 278, no. 2, pp. 578–595, 2019.

8. Gill, Richard. 2006. “learning.” *Offensive and Defensive Sides,* vol. 55, no. 3, pp. 497–511, 2009.

9. Hadnagy, Christopher, and Michele Fincher. 2015. *Phishing Dark Waters: The Offensive and Defensive Sides of vicious Emails*. John Wiley & Sons, vol. 82, pp. 181–192, 2019.

10. Holt, Thomas J., and Erric Lampke. 2010. “Traverse be theft Data requested online:Products and shops Forces.” lawless *Justice Studies*, vol. 67, no. 2, pp. 466–482, 2020.

11. Kozin, Alexander, Kati Hannken-Illjes, and Thomas Scheffer. 2009. “Before the Law and the Narrative about Raising Access to Theft Defense.” *Zeitschrift Für Rechtssoziologie*, vol. 50, no. 12, pp. 5049–5057, Dec. 2020.

12. Ng, and Alex Chi Keung. 2018. *Contemporary Identity and Access Management infrastructures: Emerging Research and openings: Emerging Research and openings*. IGI Global, vol. 126, pp. 49–65, 2019.

13. Saunders, Kurt M., and Bruce Zucker. 1999. “Neutral robbing in the information Age: The Identity crime.” *International view of Law, Computer system & Technology*, vol. 15, no. 1, 1972, pp. 143–149.

14. Sebes, E. John, E. John Sebes, and Mark Stamp. 2007. “Soluble Problems in Enterprise Digital Rights Management.” Messaging *Management & System Security*, vol. 97, no. 1, pp. 20–29, 2019.

15. Statistics, United States Department of Justice Office of Justice Programs Bureau of Justice, and United States Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. 2006. “International cybercrime Victimization" vol. 89, no. 5, pp. 1097–1115, 1999.

16. Syngress. 2002. *Hack Proofs the Identity of the Messaging Age*. Ellsevier, vol. 30, no. 1, 1999b, pp. 1–21.

17. Teu, Zhilling, Ofir Turrel, Yuffei Yuan, and Norm Archear. 2015. "Guard Risks Regarding Portable Device Loss or Theft: An Empirical Test." *Information & Management*, vol. 54, no. 3, 2006, pp. 602–604.

18. Von Ah Morano, Ana E., Gilson P. Dorneles, Alessandra Peres, and Fábio S. Lira. 2019. *Journal publications of Cellular Physiology*, September, vol. 278, no. 3, pp. 783–795, 2019.

19. Warburton, Christopher E. S. 2013. “abstract Property Theft.” *The Encyclopaedia of a Criminologist and CriminalJustice*, vol. 283, no. 3, pp. 929–941, 2020.

20. Yang, Yuanguan, Dep of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY, Usa 11790, Cong Wang, and Ji Li. 2015. “Portable RechargeSensor Networks - Status and next Trends.” *Journal of Dispatches*, vol. 54, no. 10 (October 2008), pp. 1759–1773.