CYBERCRIME BEHAVIOR MODE THROUGH E-COMMERCES

Dewi Ummiyati[1], Alexander Anggono[2]
[1]dewiummiyati19@gmail.com, [2]alexander.anggono@trunojoyo.ac.id
[1,2,]Universitas Trunojoyo Madura

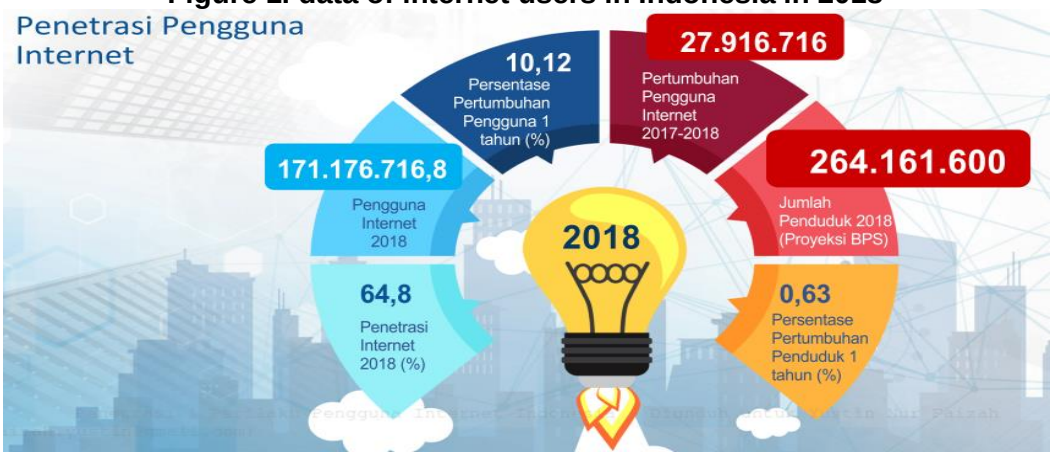
Abstract: The purpose of this study is to reveal the mode of behaviour through e-commerce. This research is a qualitative research using phenomological methodology to reveal the mode of crime. Data obtained by conducting interviews. As a result, online transactions can help sellers to market their products to a larger market share and help consumers to make it easier to meet their needs. The modes and tricks of the crimes committed by the perpetrators in various ways. Creating cloned accounts to get lots of cashback points, hacking into people's owner accounts, hacking credit cards when paying for purchases of goods, and taking other people's product names and vilifying these products and asking for half the purchase price. Small cases are rarely reported to the realm of law because the consequences of litigation and other costs are calculated with the lost losses.

Keywords: Cybercrime, E-commerce, Mode, Online.

Introduction

Indonesia with a population of ± 250 million people places Indonesia in a very strategic position in the intensity of business transactions both domestically and internationally. The era of globalization is identical with advances in technology and information that are developing very rapidly and rapidly. This phenomenon occurs in all parts of the world regardless of developed or developing countries, including Indonesia. Globalization is the process of entering into the world scope (noun) [KBBI 2020]. The increasingly rapid development of information technology has changed human life to become easier because of its sophistication and effective and efficient working power. Initially, the existence of information technology was only used by certain groups, but now almost all levels of society have used it, both government and private agencies. The following is data of internet users in Indonesia in 2018 (APJII, 2018).

Figure 1. data of internet users in Indonesia in 2018



Private agencies or business entities that use information technology to manage all types of data by conducting online sales transactions (e-commerce). However, this information technology has a negative impact that can harm many parties due to unclear laws regulating the use of information technology, such as crime in the world of telematics (cybercrime) (Sidik, 2013). Cybercrime is an act against the law committed by using computer technology and the internet (www.lintasberita.com). Cybercrime is a crime committed by and utilizing technology in cyberspace (the internet) (Raharjo, 2020).

Related to cybercrime [Raharjo, 2020] classifies cybercrime into two, namely computer fraud and computer crime. The factors that cause cybercrime. These factors include; unlimited internet access, computer user negligence, easy to do with minimal security risk and no super modern equipment is required (Sunard, 2020). The perpetrators are generally intelligent, curious, and fanatical about computer technology, weak network security systems and a lack of public and law enforcement control.

Forms of attack or computer crime on computer systems, among others; interruption, interception (unauthorized party successfully accessing assets or information), modification, and fabrication (unauthorized party inserting fake objects into the system) [Rahardjo, 2020]. Several other forms of computer fraud include; falsification of evidentiary data values, data alteration, computer sabotage, disclosure of trade and industrial secrets and illegal data acquisition. The intention of conducting cybercrime has a positive effect on the occurrence of cybercrime (Anwar, 2012). There are three forms of fraud, namely: discount price fraud on National Online Shopping Day (Harbolnas) 2015, goods fraud that does not match orders and fraud pretending to sell goods (Fauzi and Primasari, 2018).

A survey conducted by Kaspersky Lab and B2B International revealed that Indonesia is a country where 26 percent of consumers are the target of online crime. This survey also found that 48 percent of consumers were the target of fraudulent acts designed to deceive and obtain sensitive information and financial data for criminal acts [Wardani, 2016]. A survey conducted by buying and selling site Bukalapak.com found 1 in 5 Internet users had been victims of online fraud. Based on the survey, it was found that online fraud was carried out through social media sites, be it forums, Facebook or Twitter. As many as 46 percent of respondents based on this survey admitted to having experienced fraud through buying and selling forums, while another 24 percent of respondents via Facebook, while 16 percent were deceived via the web and 14 percent of short message services (Iqbal, 2020). Online scams are in principle the same as conventional scams. The difference between online fraud and conventional fraud is the means of action, namely using an electronic system through computers, the internet and telecommunications devices (Melisa, 2013). Various modes of fraud through online media continue to emerge and the perpetrators are getting tidier in smoothing out their actions in fraud, this can be seen from the many fake buying and selling websites that are made and purchases with fictitious accounts.

Based on the above explanation, this researcher raises the cybercrime behaviour mode on buyers and sellers through e-commerce. This study is different from previous studies because this study looks at the behaviour of individuals in committing crime through e-commerce transactions. The contribution of this research is to first provide a new concept in the world of investigative technology to understand the behaviour of cybercrime value-commerce. Second, to provide examples of modes of criminal behaviour in the world of e-commerce and their relationship to the policy of Law No. 19 of 2016.

Methods

This study uses an interpretive paradigm with a qualitative approach. With a qualitative research approach, it is hoped that a conclusion generated in this study will become a quality information. The definition of qualitative research is as follows:

Qualitative research is research carried out in certain settings in real life (natural) with the intention of investigating and understanding phenomena: what happened, why did it happen and how did it happen? (Moleong, 2016).

To achieve the research objectives and obtain answers to the experiences and understanding of subjects in a situation and conditions they are experiencing, therefore researchers use phenomenological methods. In phenomenology, the differences in perceptions between perpetrators and victims are important and interesting things to be explored to produce important statements that will become the forerunners of the formation of a theme [R, Raco, 2010]. To get this meaning, phenomenology uses five elements, namely (1) noema, (2) noesis, (3) epoche, (4) intentional analysis, and (5) eiditic reduction as data analysis.

The informants needed in this study are informants who are directly involved in buying and selling activities in e-commerce. The informants used in this research are actually doing buying and selling interactions using e-commerce. The informant's name was deliberately disguised because of the informant's request.

Table 1. List of informants

No	Name (Pseudonym)	Gender
1.	Veny	woman
2.	Faizah	woman
3.	Miftah	man
4.	Rizki	man

The data collection method used in this research is an unstructured interview technique. Interviews were conducted by visiting restaurant X and interviewing the three key informants. In addition, conversations via cellphones, both telephone and SMS, are also carried out if there is an urgent matter.

Findings

E-Commerce Service Users in Buying and Selling Transactions

The era of globalization has had a considerable impact on all countries as well as Indonesia. Indonesian internet users in 2018 surpassed 171 million people (APJII, 2018). Internet information and communication technology is now used for business activities. The transaction activities of the business world have all shifted to the virtual world which is often called e-commerce. Access to sale and purchase feels helped by the assistance of the internet by opening stalls in cyberspace, making it easier for consumers and sellers.

E-commerce business activities provide great opportunities for young people to develop their businesses even with small capital. Cyber business was started by Bukalapak, Tokopedia, Shopee, Lazada, and OLX and other businesses started marketing their products via the internet. As with the expression bak veny:

> "Buying and selling via the internet is more convenient and simple. You don't have to open a stall and have to have a stand or shop. Selling can be done at home while taking it easy, at best if we buy goods we need to take it "

Based on the above expression, it provides an illustration that business in cyberspace or via the internet has a positive impact on the world of age. Businesses that usually require a lot of capital, can now be more effective by marketing their wares via the internet. Sellers only need to market their wares by displaying their products via the internet either in the form of applications or other sites such as WhatsApp, Facebook,

Instagram, YouTube and others. Its consumer market reach is wide and its merchandise sells quickly. Consumers only choose the desired item then just order from the user or the owner of the stall. This is in line with the statement from faizah:

> "I prefer selling via the internet because goods are sold faster and the market share in marketing is able to reach a wide market both in cities and out of town to different islands."

A wide market share provides considerable product sales opportunities. Not only inside the city but can go beyond outside the city. In addition, consumers are more interested in moving to purchase transactions via the internet, especially among young people. The interest of young people in shopping has mushroomed in cyberspace, almost all activities of basic or secondary needs have been through online purchases. As stated by brother Miftah:

> “When I am often in the city to buy necessities or products online, it is my habit now at home. I still buy necessities usually online because there is cashback and points that can be redeemed "

Online transactions have almost become a habit, not only among young people, but for almost all elements of society, from children to adults. This habit has an impact on economic growth and supports convenience as a strategic step in running a business. The ease of facilities in online purchasing services has a positive impact that provides access to consumers to be more interested in buying products. Especially for entrepreneurs who need a lot of goods, ordering via online will provide their own benefits because they get large points. As stated by kak risky:

> “I usually buy vochers online in large quantities. Usually I get an ovo point which can be exchanged for goods later, no need to use money. If you get cashback, cash is usually transferred "

Giving cashback in the form of points gives positive values to consumers. Giving cashback serves to attract consumer sympathies to spend more. The use of buying and selling online has a strategic impact on running a business and increasing public interest. The use of e-commerce or internet services in running a business is increasing every year. The market demand for business in cyberspace has been increasing graphically in the last five years.

Selling and buying through e-commerce is more effective and efficient in terms of finance, labor, and there is no need for a warehouse. Storage places for goods can be placed at home and not as difficult as making a storage warehouse such as sun or hypermart. The delivery service can use anything as long as the goods are able to arrive at their destination safely and the goods ordered are not damaged. Even though the item is damaged, the user will replace the item if the error is on his part. If the fault lies with the consumer, the user does not want to replace it. The terms for selling and buying goods online are usually listed and can be trusted.

Cybercrime Mode in E-Commerce Transactions

The development of a business via online or the internet has a positive impact on society. Buying and selling transactions via online provide benefits from both parties, both from consumers and sellers. The community is facilitated by the existence of business facilities through e-commerce that can reach all market segments, both within the city or outside the city. This business provides an opportunity for someone with moral hazard to commit fraud or theft via online or internet media. Various tricks or modes performed by individuals who are not responsible for their own interests to gain income.

Modes or tricks can be done by either the seller or the consumer to get their own benefit and harm one of the parties. Crime in business transactions via online often occurs and cases of business fraud through online media are rampant. One of the modes or tricks performed by a person or individual is telling consumers that they get a cashback

from "S" (the initials of one of the market places) and will be sent if following the procedure has been followed. As conveyed by Brother Miftah below:

> "I often shop online and have been able to cashback to" S ". However, I was almost cheated because someone claimed to want to send a cashback gift. He asked for an email address and password, account number, password to enter the application "S" to process the cashback and finally I gave him. When I found out that he changed the password I quickly stopped his action and finally saved my account".

The above expression provides an explanation that the trick or mode of the perpetrator is to hack into the account and use it to shop online using your miftah's account. This will affect the ownership of the account being transferred and individuals freely using Miftah's account to carry out the action. As stated by [Clough, 2014] specifically and comprehensively deals with identity theft and forms of identity theft provisions. In addition, the person asked for an account number to drain the entire contents of the account but fortunately the bank balance at that time had run out so that the individual could not drain the account balance.

Brother Miftah then blocked the account number in anticipation that the person would retake the account when the bank balance was topped up again. This happened to Ms. Faizah, whose case was the same about hacking a bank account, especially her credit card when she wanted to pay for the product she bought. This was expressed by him as follows:

> "I ordered goods then I wanted to pay using a credit card, when I paid using a credit card there were people who knew my account number and hacked it so I lost 3 million in cash".

Hacking via credit card when shopping online is quite rife in the wider community. As noted by [Guillen, and Christopher Westland, 2012] Credit card fraud costs consumers and the financial industry billions of dollars every year. Uses real-time data from credit card transactions from international credit card operations for transaction aggregation and model estimation. The tricks and modes of the people are always more creative in carrying out their actions compared to security from various parties, both from financial institutions or online businesses. Online business activists provide sufficient extra security for consumers to avoid cyber crimes such as account hacking.

The case that Miftah experienced was related to the hacking of her account, it is different from the case of risky brother's admission of making multiple accounts to get lots of cashback points to benefit him. A different account was deliberately created to buy quite a lot of her needs because she bought vocher to resell it. If you only buy from one account, you will not get many points and the old account with the new account has a different effect. As expressed by kak risky as follows:

> "I created 9 accounts, one cellphone and one account so that I didn't find out that the account was a clone account."

Creating different accounts has a pretty good effect on gaining points. This mode or trick is powerful enough so far to not get caught and smooth the action. One cellphone for one account is a strategic way that is quite effective because it is assumed that someone who has a cellphone must have the application. This gap is taken to shop on a large scale with various accounts so that you get a fairly large cashback point. The old account and the new account have a big effect on the awarding of points. As stated by kak risky below:

> “The old account and the new account are definitely different in giving cashback points. The old account has a bigger cashback than the new account. If I combine all of the accounts I will get around 10 million cashback points "

An expression that is quite surprising and tempting to do this way to buy goods online. One cellphone for one account may be an effective way to trick their prey for now because the security of each application and cashback method is now starting to be reduced by users. Other methods may exist which are more sophisticated to deceive their prey and more elegant. Multiple security systems and prevention methods must be optimized because cybercrime is increasingly developing with different tricks and modes.

Ms. Veny experienced different modes and tricks because she had been tricked by her retailer by vilifying her product and the person changed Ms. Veny's product with a different packaging and sold it twice as much. The following is Ms. Veny's confession:

> "I sell masks through the" S "application and then there are retailers who want to sell my products too and the price is higher than my price and I allow them to sell them via wathsap, facebook, instagram, youtube etc., don't sell them on" S "either. It turned out that he cheated on me by selling the same product with different packaging in the "T" application and vilified my product in cyberspace by saying my product was spotty and accompanied by evidence from a dermatologist. Not only that, he asked for half the price he had bought. Now he sells my product on "T" by changing the packaging and the price has doubled and is now selling really well "

Ms. Veny's statement illustrates that what this person does is not only committing cybercrime but also sabotaging products belonging to goods by changing the packaging without permission or often called taking copyright or property rights. This trick and mode is actually subject to layered articles if it is reported to the authorities because there are two crimes involved. Not only subject to the ITE Law but also the product copyright protection law and the defamation law.

The behavior of cybercrime using tricks and modes is the behavior of the individual itself. There is moral hazard in him that wants to benefit himself and harm others. This behavior is against ethics and can lead to criminal acts. If the loss is experienced by consumers or sellers, they can file a lawsuit and make an arrest warrant. Cybercrime in business will usually be prosecuted by law if the losses are large enough and one of the parties is disadvantaged.

Cybercrime Perspective in E-Commerce Transactions according to the ITE Law

Crime in the virtual world in business or online transactions is very vulnerable in Indonesia. Many criminal activities in the business world through online. The existence of cybercrime can be charged by the ITE Law if the case is reported by the injured party to the authorities. This is because the ITE Law provides a solution as a protection against crimes in the business world via online or often known as e-commerce.

As described in Law Number 11 of 2008 concerning Electronic Information and Transactions (“ITE Law”) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. This action is explained in article 30 paragraph 2 and 3, namely [Indonesian Constitution, 2008]:

> "Everyone knowingly and without right or against the law accesses Computers and / or Electronic Systems in any way for the purpose of obtaining Electronic Information and / or Electronic Documents.

Anyone who knowingly and without right or unlawfully accesses Computers and / or Electronic Systems in any way by violating, bypassing, bypassing, or breaking into security systems. When someone violates article 30, then the sanction for violating Article 30 of the ITE Law is contained in Article 46 of the ITE Law which reads (UUD,2016):

1. Every person who fulfills the elements as referred to in Article 30 paragraph (1) shall be sentenced to imprisonment for a maximum of 6 (six) years and / or a maximum fine of Rp. 600,000,000.00 (six hundred million rupiah).
2. Every person who fulfills the elements as referred to in Article 30 paragraph (2) shall be sentenced to imprisonment of not longer than 7 (seven) years and / or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiah).
3. Every person who fulfills the elements as referred to in Article 30 paragraph (3) shall be sentenced to imprisonment for a maximum period of 8 (eight) years and / or a maximum fine of Rp. 800,000,000.00 (eight hundred million rupiah).
4.

Meanwhile, if the violation of Article 30 of the ITE Law results in losses for other people, then he will be punished with imprisonment of up to 12 years and / or a maximum fine of Rp. 12 billion. Cyber business violation cases can affect consumers or sellers. This condition depends on the case experienced by certain parties such as experienced by Ms.Veny. Actually Ms. Veny could report her case to the police, but she did not want to extend the matter. Below is his statement:

> "I do not want to extend this matter, I am sincere. I prefer to change rather than deal with the authorities "

The above acknowledgment provides an explanation that he did not want to extend the matter and accepted it sincerely. Measuring the rate of reporting and non-reporting consequences provides its own judgment about the amount of loss and its consequences. Choosing not to report is a more effective option by measuring the level of losses experienced with legal consequences. As experienced by faizah who had her credit card hacked when buying goods online. Like the admission of Ms. Faizah who did not report her case to the authorities. Here is the explanation:

> "My card was hacked when I bought goods but I didn't report it because there were not too many of them and I didn't think about it anymore"

Ignoring the loss and refusing to report it is possible because the case is too trivial so Ms.Faizah does not want to lift the green shirt. Victims rarely perform legal lifting because the problem is small and the losses are not too big. Some only a few small cases are not reported under the law because the cases are experienced by individuals, usually the cases to be raised are large cases and those experienced by entrepreneurs.

Conclusion

The development of information technology in the era of globalization is very rapid in the millennial era. Internet access users in Indonesia, amounting to 171,176,716 people, certainly have an impact on all sectors. The sector that has benefited greatly is the business world, namely online trading or often called e-commerce. The results of the above discussion can be drawn from several conclusions. First, online transactions can help sellers to market their products to a greater market share and help consumers to make it easier to meet their needs.

Second, the modes and tricks of the crimes that were carried out by various perpetrators. Creating cloned accounts to get lots of cashback points, hacking into

people's owner accounts, hacking credit cards when paying for purchases of goods, and taking other people's product names and vilifying these products and asking for half the purchase price. Third, small cases are rarely reported to the legal domain because the consequences of litigation and other costs are calculated with the lost losses.

This study provides a dimensional concept that the modes and tricks in committing cybercrime through e-commerce are increasingly creative. There are many ways that people do it elegantly. Suggestions for further research in making effective early prevention concepts to prevent cybercrime through e-commerce and adding informants from the authorities, academics in legal and business aspects, and the prosecutor's office as informants who understand the law.

References

kbbi, “kamus besar bahasa indonesia,” *http://kbbi.web.id/globalisasi*.diakses tanggal 26 april 2020.

apjii, “asosiasi penyelenggara jasa internet indonesia,” 2018.

s. sidik, “dampak undang-undang informasi dan transaksi elektronik (uu ite) terhadap perubahan hukum dan sosial dalam masyarakat,” vol. 1, p. 7, 2013.

a. raharjo, “kebijakan kriminalisasi dan penanganan cybercrime di indonesia,” *www.unsoed.ac.id*, 2006.diakses tanggal 26 april 2020.

b. rahardjo, “keamanan sistem informasi berbasis internet,” *http://budi.insan.co.id*, 2001.diakses tanggal 26 april 2020.

t. sunardi, “faktor-faktor penyebab cybercrime dan jenis kejahatan internet,” *http://qnoyzone.blogdetik.com*, 2008.diakses tanggal 26 april 2020.

a. s. h. anwar, “pengaruh intensi, pengalaman menggunakan internet, kondisi pemfasilitasan, dan undang undang informasi & transaksi elektronik no. 11/2008 terhadap cybercrime,” *jrak*, vol. 1, no. 1, p. 69, jul. 2011, doi: 10.22219/jrak.v1i1.501.

s. n. fauzi and l. primasari, “tindak pidana penipuan dalam transaksi di situs jual beli,” vol. 7, no. 3, p. 12, 2018.

a. s. wardani, “orang indonesia paling banyak jadi korban penipuan online,” *ttp:// tekno.liputan6.com/read/2519790/orang-indonesia-paling-banyak-jadi-korban-penip uan-online*, 2016.diakses tanggal 26 april 2020.

m. iqbal, “satu dari lima orang jadi korban penipuan online,” *https://m.tempo.co/read/news/2011/12/14/072371673/satu-dari-lima-orang-jadi-korban-pe nipuan-online*, 2011.diakses tanggal 26 april 2020.

m. s. melisa, “penipuan menggunakan media internet berpura jual beli online,” *lex crimen*, vol. 2, 2013.

l. j. moleong, *metodologi penelitian kualitatif (edisi revisi)*. jakarta: pt remaja rosdakarya, 2016.

j. r. raco, *metode penelitian kualitatif, jenis, karakteristik, dan keunggulannya*. grasindo, 2010.

j. clough, “towards a common identity? the harmonisation of identity theft laws,” *journal of financial crime*, vol. 22, no. 4, pp. 492–512, oct. 2015, doi: 10.1108/jfc-11-2014-0056.

s. jha, m. guillen, and j. christopher westland, “employing transaction aggregation strategy to detect credit card fraud,” *expert systems with applications*, vol. 39, no. 16, pp. 12650–12657, nov. 2012, doi: 10.1016/j.eswa.2012.05.018.

undang-undang republik indonesia, “undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.”

undang-undang republik indonesia, “undang-undang nomor 19 tahun 2016.” 2016 tentang informasi dan transaksi elektronik.”