Cyber Crime

Name : Yoga Permana Tanaya

Student ID: 1400464 /140010326

BACHELOR OF INFORMATION AND TECHNOLOGY (HONS)

STMIK STIKOM BALI

**Chapter I**

Introduction

* 1. Background

The Development of Technology is good for the people nowadays. The development of technology is technology from many years that developed rapidly. Many benefit could be used from the development of technology such as you can find a place like restaurant, bar or anything you want in foursquare, You can find many friend on the social media(facebook, path, Instagram, etc)Or you can discuss something with the other people in twitter or Kaskus, finding a jokes in 1cak or 9gag. And also doing an e-commerce.

What is e-commerce ? E-commerce (electronic commerce or EC) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the Internet *source:* [*http://searchcio.techtarget.com/definition/e-commerce*](http://searchcio.techtarget.com/definition/e-commerce)

In the Outside of Indonesia we all know [www.ebay.com](http://www.ebay.com) or in Indonesia we’re familiar with [www.olx.co.id](http://www.olx.co.id) or [www.tokopedia.com](http://www.tokopedia.com) all kind of them are e-commerce website. You can find anything you want from there and off course you must pay for that if you wanna buy something. On the e commerce website they usually request the buyer to transfer some of money from the bank account. Off course this is so many risk, as we know the cyber crime threaten us.

The cyber criminal is dangerous as the real bad guy in the real world. Imagine when you had an e-commerce transaction the cyber-bad guy can threaten you. They can hack your bank account, steal your money, or steal your private information on the social media. Maybe you have watch news about many tragedy could happen on the internet like kidnapping, money laundry, deception and many else. And now we must aware from this situation because the bad guy now had a skill in computer and threaten us.

* 1. **Problem Of the Study**

From the background above, as the writer of this paper I formulate some question that can be the conclusion at the end. The questions are :

1. *What is Cyber Crime?*
2. *What the effect of Cyber Crime in Development of Technology nowadays?*
3. *What is kinds of cyber criminal that happening nowadays?*
4. *Why we must aware from the Cyber Criminal?*
5. *How to prevent us from the Cyber Criminal?*

**Chapter II**

2.1. Discussion

2.2.

1. *What is Cyber Crime?*

* [Cyber](http://www.webopedia.com/TERM/C/cyber.html) crime encompasses any criminal act dealing with [computers](http://www.webopedia.com/TERM/C/computer.html)and [networks](http://www.webopedia.com/TERM/N/network.html) (called [hacking](http://www.webopedia.com/TERM/H/hacker.html)).

*Source:* [*http://www.webopedia.com/TERM/C/cyber\_crime.html*](http://www.webopedia.com/TERM/C/cyber_crime.html)

* Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

*Source:* [*http://www.techopedia.com/definition/2387/cybercrime*](http://www.techopedia.com/definition/2387/cybercrime)

* Cybercrime is criminal activity done using computers and the Internet.

*Source :* [*http://techterms.com/definition/cybercrime*](http://techterms.com/definition/cybercrime)

* From all three(3) definition above as a writer I conclude that Cyber Crime is a Criminal Activity done using Computer and internet(hacking, phishing, and spamming) or used a tool to commit an offense

1. *What the effect of cyber crime in Development Technology nowadays?*

* The effects of a single, successful cyber-attack can have far-reaching implications including financial losses, theft of intellectual property and loss of customer confidence and trust. The overall monetary impact of cybercrime on society and government is estimated to be billions of dollars per year.

*Source:* [*http://itsecurity.vermont.gov/featured/cybercrime*](http://itsecurity.vermont.gov/featured/cybercrime)

* Criminals take advantage of technology in many different ways. The Internet, in particular, is a great tool for scammers and other miscreants, since it allows them to ply their trade while hiding behind a shield of digital anonymity. Cyber crime affects society in a number of different ways, both online and in the offline world.

*Source:* [*http://science.opposingviews.com/effects-cyber-crime-1704.html*](http://science.opposingviews.com/effects-cyber-crime-1704.html)

Therefore, cyber crime effect for Development of Information and Technology nowadays are many implication like financial losses, theft of intellectual property and loss of customer confidence and trust. The cyber crime is dangerous as the real crime in the real world the criminal had many ways for scammer, hacking or phishing. They’re so harmful for their victim.

1. *What is kinds of cyber criminal that happening nowadays?*

* **Script kiddies**: A wannabe hacker. Someone who wants to be a hacker (or thinks they are) but lacks any serious technical expertise. They are usually only able to attack very weakly secured systems.
* **Scammers:** Your [email inbox](http://www.faronics.com/news/article/webinar-inside-the-mind-of-todays-cyber-criminal/?p=27522) is probably full of their work. Discount pharmaceuticals, time-shares, personal ads from available women in Russia…sound familiar?
* **Hacker groups:** Usually work anonymously and create tools for hacking. They often hack computers for no criminal reason and are sometimes even hired by companies wanting to test their security.
* **Phishers:** Gotten an email recently claiming your bank account is about to expire? Don’t fall for these jerks. They want your [personal information](http://www.faronics.com/news/blog/fish-for-information-don%e2%80%99t-let-it-phish-you/) and, most likely, your identity, by directing you to a phony websites.
* **Political/religious/commercial groups:** Tend to not be interested in financial gain. These guys develop malware for political ends. If you think this group is harmless, think [Stuxnet](http://en.wikipedia.org/wiki/Stuxnet" \t "_blank). The Stuxnet worm which attacked Iran’s Atomic Program of Its Nuclear Facilities was believed to be created by a foreign government.
* **Insiders**: They may only be 20% of the threat, but they produce 80% of the damage. These attackers are considered to be the highest risk. To make matters worse, as the name suggests, they often reside within an organization.
* **Advanced Persistent Threat (APT) Agents**: This group is responsible for highly targeted attacks carried out by extremely organized state-sponsored groups. Their technical skills are deep and they have access to vast computing resources.

*Source :* [*http://www.faronics.com/news/blog/7-types-of-cyber-criminals/*](http://www.faronics.com/news/blog/7-types-of-cyber-criminals/)

1. *Why we must aware from cyber criminal ?*

Cyber crime is a dangerous criminal that happen on the internet or criminal using Computer as the media. Of course its dangerous because we didn’t know who is the actor behind itself. Maybe you often heard about ‘anonymous’



**Cracker and Hacker**

Yes, anonymous is a group hacker that sometimes make us scared, because they had incredible hacking skill. But a question coming ‘is that a hacker dangerous?’ , and the answer is maybe yes maybe not. The dangerous hacker is when they are hack into some system and they’re crack and destroy them and its called ‘Cracker’. But if they’re only do an hacking not to crack or destroy, then it still safe.

Many good hackers around the world actually give benefit for many people or companies.

the different between hacker and cracker :

Hacker use their skill for observe, discover and recover the weakness of the security system in computer system or software

And cracker get into the others system and had destructive tend, usually in computer network, by-passing password, deliberate counter to computer security system, defacing, data stealer, or deleting the someone’s data.

At this time why we must had an awareness because wherever we stand, even in the cyber space certainly has a crime.

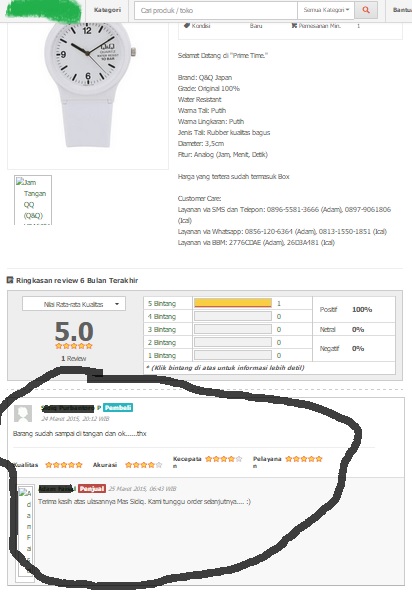
1. *How to prevent us from cyber criminal?*

* Education and training
* Do all your employees understand the most common hacking tactics, such as phishing, social engineering, or packet sniffing (to name just a few)?
* Education and awareness across your staff will go a long way to protect yourself against many types of cybercrime.
* **Securing Computers, Digital Assets, and Networking**
* Is all software housed within your network continually up to date? Exploits in software are very common ways hackers gain access to systems and sensitive data. Updating software on network-connected machines should always be a top priority.
* Do you have business-class antivirus software installed (and up to date) on all office workstations and servers? Leading antivirus software can detect, remove, and protect your machines and network from malware.
* Do you scan your [website or web applications](http://www.thesba.com/web-services/)for malware? Many of us are used to checking for viruses and malware on our personal computers, but don’t realize that websites and web applications are just as susceptible.
* Do you have reliable backups of all of your critical [data](http://www.thesba.com/web-services/cloud-managed-services/)? Recovering from many types of common cybercrimes often involves restoring your data from a point prior to the event in question. Not having reliable and securely stored backups of your data is a significant liability.
* Is your network equipped to handle network-specific attacks? Earlier, we mentioned a common type of network attack called a DDOS. Unsophisticated networks are particularly susceptible to these, as DDOS mitigation devices and tools often require enterprise-sized budgets. If you own a small business, this type of luxury wouldn’t normally be practical, financially speaking. However, with the growing adoption of [cloud and utility computing services, using a quality cloud-computing partner](http://www.thesba.com/web-services/cloud-managed-services/)— one that has already invested the necessary capital to protect its network—is a cost-effective solution.

*Source:* [*http://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/*](http://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/) *with a little bit alteration*

In addition above method, there’s some other way to prevent from cyber crime from me as the writer after read so many source. Such as :

1. Do not open any link from the email you got. Especially the suspicious email. Because these are a phisher, cracker, malware threaten us there. Update your anti virus for routines to prevent this
2. When you meet someone that stranger(you didn’t know before) on the social media like facebook, twitter, or other else. And she/he wants you to do anything like send a money, invite you to meet him/her. Do not agreed their invite or request. This the modus for the deception or kidnapping
3. If you want to transaction on the e-commerce website. Observe the comment below the thing you want to buy like this



If you didnt see the comment below the item you want to order it possibility a deceiver. Deception like this usually happen in the social media like facebook or Instagram. And very seldom was found on the spesific e-commerce website If you find a phenomena like this please contact the seller about the item their sell.

1. Careful if you had a transaction with a credit card/ATM because this cyber crime was called Cyber Carding. This is some way to prevent the cyber carding:

* Secure your username and password

Username must use your real name so that be easier in the data process, use the unpredictable password. Do not use your birthday as the password or any relation with your family

* Carefull when doing a transaction

Try to always aware when your card being process in the bank, mall, or shop. And keep safe the receipt. The receipt may not missing. Match with the credit card/ATM billing when the payment

* Wifi could be dangerous

Using WIFI connection are so fun. Do not try to do a transaction via WIFI. It could be you are being monitored by the bad guys , and your password could be stolen .

* Carefully when you take a promo on the internet

Do not easily tempted with the promo which was offered. Because when you give your credit card personal identity. Then it only was a fake. Your credit card will be cracked by someone with no responsibility

Chapter III

Conclusion and Suggestion

3.1. Conclusion

Development of Information Technology give us more benefit. but In other side there’s a bad guy or criminal use Development of Information Technology for their crime.

3.2 Suggestion

We must use the Development of Information and Technology for kindness and be helpful for the other people. And we also has awareness of the bad guy or Cyber Criminal that develop rapidly concomitant with the Development of Information and Technology itself.

**Reference**

[*http://www.webopedia.com/TERM/C/cyber\_crime.html*](http://www.webopedia.com/TERM/C/cyber_crime.html)

[*http://www.techopedia.com/definition/2387/cybercrime*](http://www.techopedia.com/definition/2387/cybercrime)

[*http://techterms.com/definition/cybercrime*](http://techterms.com/definition/cybercrime)

[*http://itsecurity.vermont.gov/featured/cybercrime*](http://itsecurity.vermont.gov/featured/cybercrime)

[*http://science.opposingviews.com/effects-cyber-crime-1704.html*](http://science.opposingviews.com/effects-cyber-crime-1704.html)

*be accessed on April, 10th 2015*

[*http://www.faronics.com/news/blog/7-types-of-cyber-criminals/*](http://www.faronics.com/news/blog/7-types-of-cyber-criminals/)

[*http://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/*](http://www.forbes.com/sites/thesba/2013/08/28/how-to-prevent-cyber-crime/)

*be accessed on April, 11th 2015*