Mathematical Statistician and Engineering Applications
ISSN: 2326-9865
https://doi.org/10.17762/msea.v71i1.50

# Understanding the Types of Cyber Crime and Its Prevention

Dr. Antino Marelino
Department of Management Studies,
ARCET Malaysia

***Article Info***
***Page Number: 108 – 112***
***Publication Issue:***
***Vol 71 No. 1 (2022)***

***Article History***
***Article Received****: 18 November 2021*
***Revised****: 03 December 2021*
***Accepted****: 19 December 2021*
***Publication****: 28 January 2022*

***Abstract***

In the era of social media and online provisions, there are also a lot of crimes happening these days. Cyber-crime is linked to the online or crime committed over internet. Such types of attacks are done intentionally due to which they are classified as crime. There are many hackers who has the capability of hacking even the banking details of the user. This paper will explain the meaning of cyber-crime, different types of cyber-crime and also gives the reason as why crime can take place even in the world of internet. There are many tools available which helps to identify the nature of the security attack and helps to avoid it.

**Keywords**: - Cyber Crime, Categories of Cyber Crime, Methods to prevent, Causes.

---

Introduction: - Cyber-crime is the way of attacking the devices or computer available in internet network to gain profits. It is done intentionally to access the data of the user to serve their personnel purpose. The person who commits crime are called as hackers and are very technically strong person who knows how to interfere in personnel data of the user available online without even letting the user know. It is done for the aim of making profits for themselves. For example, the hacker can access banking websites and with the help of the hacking algorithms can crack the code and can login in user account and can withdraw all the balance in his own account. It is illegal access in computer, website, account, system etc available online. There are organisations who in order to compete their competitors hacks the other company's details to read their budgets and their investment plans and details of the projects or new plans in order to make profits for their own company. On the other hand, the hacker can be individual hacker whose aim is to have a control over user's banking credentials in order to withdraw money in to his own account. It is very essential that whoever works using internet and online services should also invest in good security protocols such that no hacker can crack the code and access that information. For this, the organisations can invest in training of the technical engineers who knows how to detect the crime before it takes place and should use such a code which is very difficult to decode and hack.

Causes that give rise to Cyber Crime: - [1]

1. Access Metric: - Since the technical details of the system are very complex, there is possibility of the inefficient code which is easily hacked by the hacker. The hacker's take advantages of the code which is not technically strong and can be easily hacked by the hacker. The code which is easily accessible and does not use sound and strong technical algorithms, can easily be cracked by the hackers to make profits for their own personal use.

2. Storage capacity: - The computer system has very less space for storing the data. This data can be easily hacked by the hacker and they can remotely login in devices which have data for their use.

3. Inefficient coding: - The coding of systems can be complex and difficult which takes a lot of time to implement. The coder needs to take care of many metrics and due to high technical and complex coding, they might make advantage of this inefficient code and can hack the system to serve their need.

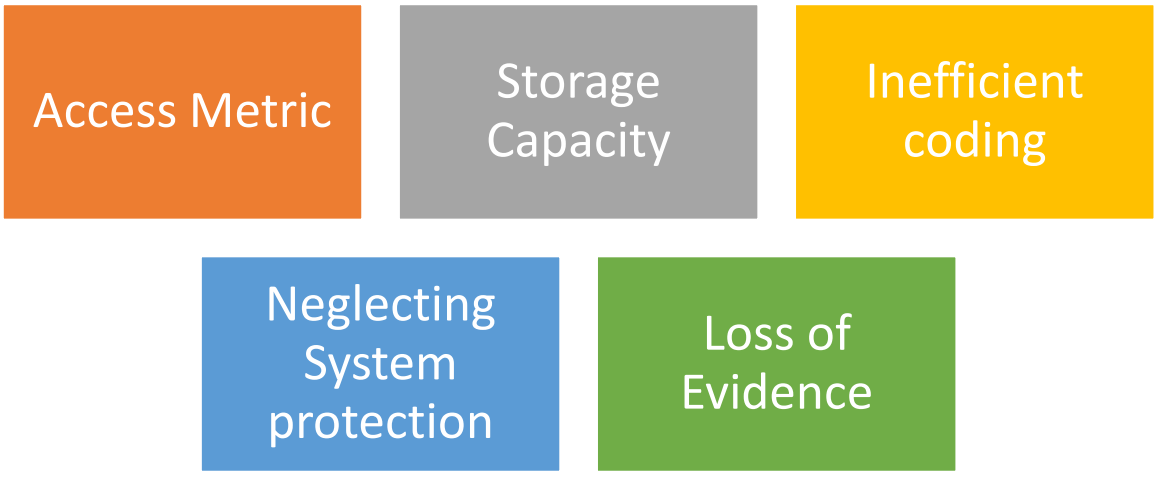


Figure 1 Causes of Cyber Crime

4. Neglecting System Protection: - While implementing measures to protect the system, if there is any sort of negligence from the designer's side then this can prove to be advantage to the hacker.
5. Loss of Evidence: - The hackers after the access into the system can easily destroy the data related to the crime. So due to loss of evidence of the data it is difficult to identify that who has hacked the system and from where.

Types of Cyber Crimes: -

There many types of cyber-crimes being committed. Following are the types of cyber crimes committed in brief: -

1. Spamming: - It is basically linked to sending the same messages over and over again to the same person or to same groups in order to advertise something or also to do phishing attack. In some instances, it is seen that a particular message is sent over and over again repeatedly due to which the person working can be disturbed and cannot concentrate to finish his daily tasks in the company. The types of spamming can be: -
   - Email spamming
   - Instant messaging
   - Messenger spamming
   - Forums
   - Newsgroups
   - Mobile etc

2. Phishing: - This is related to the illegal access in the banking websites to hack the users account etc. This type of crime is committed to get the financial details of the user and then the hacker can withdraw money from that account which can be used to make profits. The jackers in this way also withdraws money to buy other things like any expensive software etc. The hackers send attractive messages which tend to make the person fall in the trap. Like the hacker can send messages which says to click a particular link which gives guarantee that the person will win the lottery. In some scenarios the person may fall in this type of trap and as a result of which the hacker gets easy access to the password and login details of the person which the hacker can use for his own use. There are following main categories of phishing: - [2]
   - Spear Phishing: - This type of phishing is used by the hackers to target particular or specific user or group of people in order to get their information. The hacker can target to access the details of the admin's account so that he can use his login details to further access the account details of all the users of the company or the other information of the organisation.
   - Smishing: -This type of attack is done by exchange of the text messages which are sent to the customer in order to hack their details. These type of messages looks genuine and the person might click on it but it may result in giving full control to the hacker in individual's account. The person should always be careful about these kinds of messages and should not panic and they should cross check with their bank reception to check if really such message was being sent by the bank.
   - Whaling: -It is very dangerous type of phishing as it will target big companies or high-profile people to get their details. They will be asked via message that they are violating the rules and they need to send crucial information of the company. If the person replies to their message, then all the information of the company can be hacked by the hacker and can be exploited.
   - Vishing: - This is also one of the phishing attacks where the hacking is planned over the voice call. The person will get a call and be asked to press a button to confirm certain details. If the person who has received such a call responds and press the buttons being asked to press then the IP address and other crucial details of that particular person is hacked and can be used to serve the hacker's use.

3. Piracy or Theft: - This type of cyber crime is related to the stealing of copywrites of another person. In this type of attack the attacker can download the song or movie or music and make duplicate copies and sell them at a cheaper cost. The hacker then sells the pirated copies at a cheaper cost which helps him in making profits. The hackers also copy the script of a story and then give their name instead of the original director etc. The target people of this categories are movie directors etc.
4. System Damage: - This type of cyber attack is linked to the disruption of the working of the business or organisation by damaging the systems. In this type of cyber-attack, the hacker will send virus to damage the systems. If the computer is accessed during that particular time, then the virus can enter the system and can damage the working of the systems and hence affecting the work flow of the business.
5. Malicious Software: - It is a type of software program which is used by the hacker to infect the user system and has the capability to access the system and get the crucial data of the organisation. Its main target is to damage the software of the system which is been targeted by the hacker.

6. Fraud calls and messages: - In this type of attack the hacker will make a call to the user and pretend to be the person from bank and shall ask few details to authorise the data saved in the bank. The person should to get trapped in such kind of fraud calls as no bank will ask for personal crucial details like OTP or ATM pin by the bank. If the person falls in such a trap, then it is difficult to save the money from the hacker. The hacker can easily access the bank account of the user as the details will be provided by the user only.
7. Dark web market: - This market involves the black marketing of illegal products to be sold on internet. This is also a type of cyber-crime as the illegal products or software or programmes are sold online. Many people use this kind of online shopping for the purchasing of the products which otherwise cannot be bought easily offline as they are illegal products.
8. Cyber Stalking: -This is also one of the many kinds of cyber-crime. In this a person will continuously stalk a person which he thinks is enemy or something. They will continuously keep tracking the person and then harasses by trolling and commenting in that particular person's social media account.
9. Theft of person's identity: - In this type of cyber-crime, the hacker will hack the identity of the person and use his identification to use the ATM pin etc of the person and can use it to buy the online things available which will result in financial lose of that person.
10. Cyber Extortion: - Here the hacker will get access of the crucial data of the business or organisation by hacking the system. Then the hacker will demand for money in return of the data being stolen by them. This is very common these days and many companies are dealing with major profit loss and comes in crisis state.

Prevention of Cyber Crime: -
The cyber crime can be prevented and a person can keep his data and information safe by using one of the following methods: - [3]

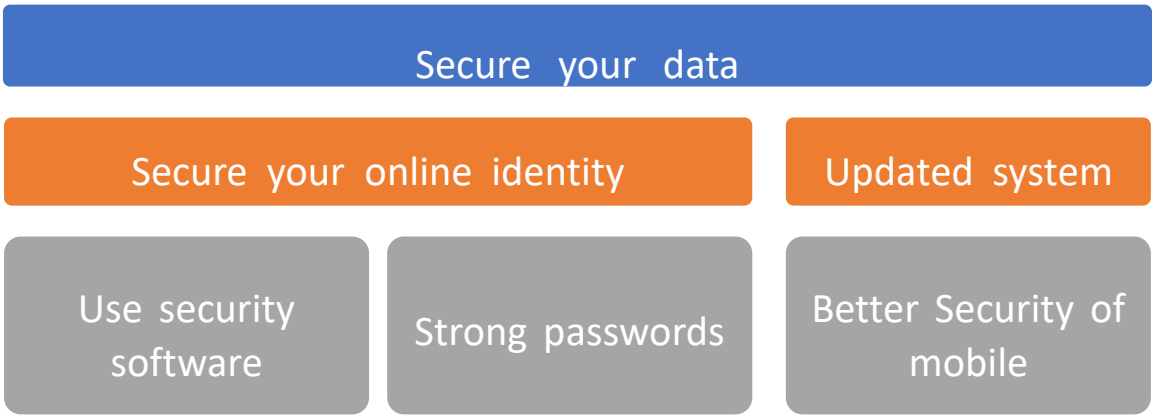


Figure 2 Prevention of Cyber Crime.

1. Secure data: - One should keep his data secure by using various encryption techniques available. The data which is crucial and has sensitive information about users account should be kept safe and secure so that the hacker cannot hack it easily. The person should keep himself updated about the type of phishing attacks used by the hackers and in this way, he can avoid getting trapped in any such hack used by the hacker.

2. Safeguard Online identity: - The person should be very careful as where he or she is using and giving his or her details like address, phone number and other details. The person should be very careful about the online transactions which he is making and make sure that the websites are safe enough to provide all the crucial details for the transaction.
3. Updated System: - One should always keep updating their personal system so that the antivirus etc can be updated which can help to avoid the security threats to the system.
4. Use Security Software: - There are many software available which helps to protect the system from security attacks. The user can make use of firewall installed in the system which can track the type of data and transaction being made and can report in case of any issues which is to avoid the cyber-crime.
5. Strong Passwords: - The person should use combination of alphabets, numerical, special characters etc to make a strong password which cannot be hacked by the hacker.
6. Mobile phone security: - While using mobile phones, the user should be careful as to what he is downloading in his mobile. Proper antivirus should be downloaded in mobile phones also.

Conclusion: - Hence it is seen that there are many types of hackers and cyber crimes in all the fields where the data and information is available online. There are many illegal actions taken by these hackers to make profit for their own use. The government and many agencies are hiring professionals who can identify these hackers and prevent the loss of persons data and financial crises. It is also the responsibility of individual to use online provisions carefully to avoid the security threats.

References: -

[1]. https://www.jigsawacademy.com/major-causes-of-cyber-crimes-you-must-be-aware-of/
[2]. https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html
[3]. https://krazytech.com/technical-papers/cyber-crime
[4]. Ronad, A. ., and M. . Madgi. “Online Platform for Agricultural Produce Livestock Marketing”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 9, no. 12, Dec. 2021, pp. 12-18, doi:10.17762/ijritcc.v9i12.5494.
[5]. Pallathadka, D. H. . (2022). Mining Restaurant Data to Assess Contributions and Margins Data . International Journal of New Practices in Management and Engineering, 10(03), 06–11. https://doi.org/10.17762/ijnpme.v10i03.128
[6]. Sherje, D. N. . (2021). Thermal Property Investigation in Nanolubricants via Nano- Scaled Particle Addition. International Journal of New Practices in Management and Engineering, 10(01), 12–15. https://doi.org/10.17762/ijnpme.v10i01.96
[7]. Gunasekara, S. ., D. . Gunarathna, and M. Dissanayake. “Advanced Driver-Assistance System With Traffic Sign Recognition for Safe and Efficient Driving”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 9, no. 9, Sept. 2021, pp. 11-15, doi:10.17762/ijritcc.v9i9.5488.