Internet crimes: definition, types, and prevention

Technology, Internet

Abstract

Nowadays internet crimes are a common problem in the world, and everyone exposes to these crimes. These crimes can cause very serious damage to the individual and society. Many people and companies had suffered from the impact of these types of crimes. To protect us from these we have a cyber-security and some precautions. This paper accordingly discusses and summarize these types of crimes and their preventions. introduction: The purpose of this report is to investigate internet crimes. This report will also recommend preventive measures from internet crimes. Internet crimes, also known as cybercrimes, are illegal activities that occur through the internet and done by either hackers or ordinary computer users. In the past few years, internet crimes became a significant issue, and it expanded rapidly and globally. The purpose of these activities varies from a person to another, some do it to revenge, and others do it to earn personal benefits.

Moreover, internet crimes have several types. For instance, virus spreading, global confidential information theft, personal information hacking, blackmailing, cyberbullying, penetration of online financial services, illegal online trading, identity theft, and cyber defamation. Considering these crimes, cyber bullying and cyber defamation are common crimes and are considerably increasing, especially in social media. Without a doubt, it’s noticeable that youth and children are the most targeted part of society. They get easily influenced by the negative effects of social networks. As a result, many young people who became a victim of cyberbullying and defamation, end up suiciding or getting depression. In fact, not only young people but recently much famous people get affected by such crimes since they get an incredible amount of hate. Discussion: Internet crimes are a common type of crimes at this century, and everyone using the computer exposed to be a victim of these type of crimes, it threatens everyone from the individuals, societies, organizations or a government. What is a cybercrime: A cybercrime or internet crimes are defined as any illegal activity that involves a computer, network device or a network.

Classification of Cybercrime:

1. The computer as Target.
2. The computer as an instrumentality.
3. The computer as an incidental of other crime.
4. Crime associated with the prevalence of computers.

These classifications are connected to each other. Some crimes can extend from one category to another. internet crime types: Internet crimes are categorized in many different categories also it has different methods.

The criminal can be an individual or a group of people targeting the same target. That’s what makes internet crimes more complicated than it occurs in various geographic areas. So, finding and penalizing guilty participants is complicated.

- Email phishing/spoofing: is a cyber crime which attempts to collect sensitive information such as personal information passwords, credit card details through emails, text messages or telephone. The criminal or the (phishers) often send a message that it’s often asking the user to enter personal information on a fake website which looks like a legitimate site.

- Cyberbullying: is using the technology to cause harm such as threaten or insulting someone. Usually, this type of crimes is common among young people, and it can affect them in a very serious way.
- Blackmail/ Extortion: the act of forcing someone to do something by threatening them to expose a secret, harm them to get money or any other benefit from them. This type of crimes affects the victim in a very serious way and it can cause financial problems also the victim can hurt himself or other people life.
- Viruses: which is spreading viruses to the victim computer and damage the system software or the data on the computer.
- Copyright Violation: it is the act of stealing people or companies' ideas, inventions or any creative expressions which are known as " intellectual property" which can include anything such as movies and music.
- Child Pornography: which is known as any sexual activities involving children using media such as emails, Facebook or any other media, which in the first place targeting children.
- Espionage (Spying): the use of media or technology to obtaining a secret or confidential information without permission of the holder of the information. There are certainly more types, but these are the most common types through the Internet. With progress and development the technology through this years, the internet crime with all kinds has become more worrisome to users and making them

stress, the security, and safety of the networks used when using the internet to avoid any crime.

Also, making users more cautious when dealing with unreliable websites to avoid hacking. Of course, there are ways to solve these problems and crimes. But they are expensive and sometimes complicated. Internet crime statistic: " The graph presented in Fig. 1 gives the comparison of the total number of complaints reported under the various categories – Economic, Facebook, Mail and Phone Calls in 2014 and 2015". (Arora, 2016)The impact of the internet crimes: Cybercrime is increasing in our generation, and it is creating large losses at the company and individual level. One of the most important effects on the individual and society:

- Identity theft
- Stealing his credit card
- Extortion and threat
- The theft and use of confidential information
- Disable Internet
- Stealing money

Many companies buy security software to keep their information secret from hackers or to protect against viruses. Using anti-virus tools, setting passwords and encryption can reduce the incidence of these crimes. Anti-cybercrimes laws in KSA: It's is not a secret what happened to Aramco Company in 2012 when they got hacked by a group called cutting sword of justice. Due to that many of their computers got destroyed by a virus. Aramco company isn't the only company that got hacked. It's a problem that faced everyone. Unfortunately, the number of companies, people and organizations that got hacked are increasing massively. Kingdom of Saudi Arabia as any country cares about her citizens, so protecting their rights and their safety is number one priority to them. Not to forget, that cyber crimes can create so much danger. In order to prevent that danger, Kingdom of Saudi Arabia publishes Anti-cyber crimes laws.

These laws consist of 16 articles. They first got published on 26 March 2007. To list one of them: Anyone who commits on of the following cybercrimes wither it was Spying on data, accessing to computers with the intention to threaten or hacking a web site with intention to destroy its URL. will be in jail for a period not exceeding one year and will be garage a fine not exceeding five hundred thousand Saudi riyals. How to be protected from cyber-crimes: Due to the increase in internet crimes nowadays, cybersecurity experts gave people some advice and precaution to avoid being a victim of these crimes:

- Using a safe password: choosing a password that no one will easily guess, making sure it’s long, and it’s highly recommended to use a different password for each website.
- Keeping the operating system up-to-date: older software may contain bugs or exploitable holes in the code that will make you an easy target to the hackers. By making your operating system running on the most recent update, you will improve your level of security.
- Being caution of the email links and attachment: Using email links and attachment’s is the most common way to spread viruses and malware.
- Using tow-factor-authentication: it’s a method that confirms user identity by using a combination of two factors. Something the user

knows and something they have. This will provide the user with an extra layer of security.

- Being protected from viruses: users should make sure that they install an anti-virus on their device or at least have a windows defender running on their computer.
- Being wary of public Wi-Fi: all information being sent to and from your computer can be intercepted and read by someone nearby. Users shouldn’t transfer sensitive data on public wi-fi.
- Being aware of what is being shared on social media: users should think before sharing something on the internet, once something been shared users can’t control how people use it.

Conclusion: The main aim of these illegal activities differs from a person to another. Understanding the causes of these crimes and the ways that cyber-criminals use them, will help people to defeat these types of crimes. People should be aware of these activities because it can cause serious damage to them or society. People should be taking big steps to protect themselves. There are various available methods that people can use such as cyber-laws, education, and policy making. All of them will help people to overcome the cybercrimes and their impacts.