What is Cybercrime? Types, Examples, and Prevention

cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

The term "cybercrime" was introduced after the latest evolution in the computer industry and networks.

Cybercrimes are considered a major risk because they can have devastating effects like financial losses, breaches of sensitive data, failure of systems, and also, it can affect an organization's reputation.

In this article, we will discuss more about cybercrimes, and what are they? How do they happen? Who are Cybercriminals? Also, we will demonstrate different types of cybercrimes.

What is Cybercrime?

Cybercrime can be defined as “The illegal usage of any communication device to commit or facilitate in committing any illegal act”.

A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm.

Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments.

Investigators tend to use various ways to investigate devices suspected to be used or to be a target of a cybercrime.

Who are The Cybercriminals?

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or teams.

Cybercriminals are widely available in what is called the “Dark Web” where they mostly provide their illegal services or products.

Not every hacker is a cybercriminal because hacking itself is not considered a crime as it can be used to reveal vulnerabilities to report and batch them which is called a “white hat hacker”.

However, hacking is considered a cybercrime when it has a malicious purpose of conducting any harmful activities and we call this one “black hat hacker” or a cyber-criminal.

It is not necessary for cybercriminals to have any hacking skills as not all cyber crimes include hacking.

Cybercriminals can be individuals who are trading in illegal online content or scammers or even drug dealers. So here are some examples of cybercriminals:

- Black hat hackers

- Cyberstalkers

- Cyber terrorists

- Scammers

Cybercriminals who conduct targeted attacks are better to be named Threat Actors.

How do Cybercrimes happen?

Cybercriminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment.

The security holes can be a form of using weak authentication methods and passwords, it can also happen for the lack of strict security models and policies.

Why are Cybercrimes Increasing?

The world is constantly developing new technologies, so now, it has a big reliance on technology. Most smart devices are connected to the internet. There are benefits and there are also risks.

One of the risks is the big rise in the number of cybercrimes committed, there are not enough security measures and operations to help protect these technologies.

Computer networks allow people in cyberspace to reach any connected part of the world in seconds.

Cybercrimes can have different laws and regulations from one country to another, mentioning also that covering tracks is much easier when committing a cybercrime rather than real crimes.

We are listing different below reasons for the big increase in cybercrimes:

- Vulnerable devices:

As we mentioned before, the lack of efficient security measures and solutions introduces a wide range of vulnerable devices which is an easy target for cybercriminals.

- Personal motivation:

Cybercriminals sometimes commit cybercrimes as a kind of revenge against someone they hate or have any problem with.

- Financial motivation:

The most common motivation of cybercriminals and hacker groups, most attacks nowadays are committed to profit from it.

Two Main Types of Cyber Crimes

- Targeting computers

This type of cybercrimes includes every possible way that can lead to harm to computer devices for example malware or denial of service attacks.

- Using computers

This type includes the usage of computers to do all the classifications of computer crimes.

Classifications of Cybercrimes

Cybercrimes in general can be classified into four categories:

1. Individual Cyber Crimes:

This type is targeting individuals. It includes phishing, spoofing, spam, cyberstalking, and more.

2. Organisation Cyber Crimes:

The main target here is organizations. Usually, this type of crime is done by teams of criminals including malware attacks and denial of service attacks.

3. Property Cybercrimes:

This type targets property like credit cards or even intellectual property rights.

4. Society Cybercrimes:

This is the most dangerous form of cybercrime as it includes cyber-terrorism.

Most Common Cyber Crimes

Now that you understand what cybercrimes are, let’s discuss some common cybercrimes.

1. Phishing and Scam:

Phishing is a type of social engineering attack that targets the user and tricks them by sending fake messages and emails to get sensitive information about the user or trying to download malicious software and exploit it on the target system.

2. Identity Theft

Identity theft occurs when a cybercriminal uses another person’s personal data like credit card numbers or personal pictures without their permission to commit a fraud or a crime.

3. Ransomware Attack

Ransomware attacks are a very common type of cybercrime. It is a type of malware that has the capability to prevent users from accessing all of their personal data on the system by encrypting them and then asking for a ransom in order to give access to the encrypted data.

4. Hacking/Misusing Computer Networks

This term refers to the crime of unauthorized access to private computers or networks and misuse of it either by shutting it down or tampering with the data stored or other illegal approaches.

5. Internet Fraud

Internet fraud is a type of cybercrimes that makes use of the internet and it can be considered a general term that groups all of the crimes that happen over the internet like spam, banking frauds, theft of service, etc.

Other Types of Cybercrime

Here are another 9 types of cybercrimes:

1. Cyber Bullying

It is also known as online or internet bullying. It includes sending or sharing harmful and humiliating content about someone else which causes embarrassment and can be a reason for the occurrence of psychological problems. It became very common lately, especially among teenagers.

2. Cyber Stalking

Cyberstalking can be defined as unwanted persistent content from someone targeting other individuals online with the aim of controlling and intimidating like unwanted continued calls and messages.

3. Software Piracy

Software piracy is the illegal use or copy of paid software with violation of copyrights or license restrictions.

An example of software piracy is when you download a fresh non-activated copy of windows and use what is known as “Cracks” to obtain a valid license for windows activation. This is considered software piracy.

Not only software can be pirated but also music, movies, or pictures.

4. Social Media Frauds

The use of social media fake accounts to perform any kind of harmful activities like impersonating other users or sending intimidating or threatening messages. And one of the easiest and most common social media frauds is Email spam.

5. Online Drug Trafficking

With the big rise of cryptocurrency technology, it became easy to transfer money in a secured private way and complete drug deals without drawing the attention of law enforcement. This led to a rise in drug marketing on the internet.

Illegal drugs such as cocaine, heroin, or marijuana are commonly sold and traded online, especially on what is known as the "Dark Web".

6. Electronic Money Laundering

Also known as transaction laundering. It is based on unknown companies or online business that makes approvable payment methods and credit card transactions but with incomplete or inconsistent payment information for buying unknown products.

It is by far one of the most common and easy money laundering methods.

8. Cyber Extortion

Cyber extortion is the demand for money by cybercriminals to give back some important data they've stolen or stop doing malicious activities such as denial of service attacks.

9. Intellectual-property Infringements

It is the violation or breach of any protected intellectual-property rights such as copyrights and industrial design.

9. Online Recruitment Fraud

One of the less common cybercrimes that are also growing to become more popular is the fake job opportunities released by fake companies for the purpose of obtaining a financial benefit from applicants or even making use of their personal data.

Cyber Crimes Examples

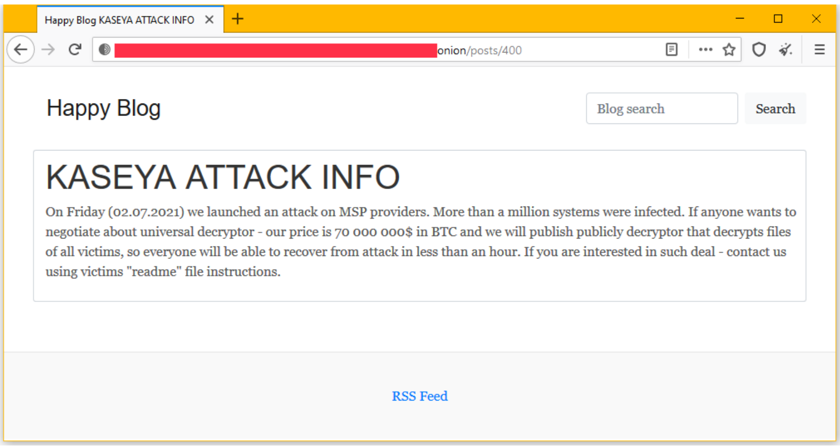
- REvil and Kaseya Ransomware

REvil is a Russian or Russian-speaking hacking group and it is known as a ransomware-as-a-service operation. The Kaseya incident took place in July - 2021.

The incident happened when one of the Kaseya's company's products was deploying the famous SODINOKIBI REvil ransomware to endpoints of Kaseya's customer network that attack surface was over 1000 Kaseya's customers worldwide.

A few hours later REvil took credit for the attack by posting on their Happy Blog website on the dark web and demanded a $70 million ransom to release a public decryptor that they claim can decrypt all the damaged devices.

The attack was so impactful that the United States government offered $10 million bounties to anyone that can give any information for arresting REvil members.



KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

Source

Yaroslav Vasinskyi, a 22 years Ukrainian, was charged with conducting the attack and unleashing the ransomware against Kaseya and other companies.

- Stuxnet

The Stuxnet incident is a famous incident that happened in 2010. Stuxnet is the name of a computer worm (type of malware) that targets SCADA (supervisory control and data acquisition) systems.

Stuxnet malware left devastating damage to Iran’s nuclear power program. It was spreading through USB drives and affected mainly Microsoft Windows operating systems.

The malware functionality was to search for machines that are working as PLCs (programmable logic controllers) and if it was found the malware updates its code over the internet through the attackers.

- Marriott Hotels

In November 2018, Marriott hotels group suffered from a massive data breach that affected more than 500 million customers.

The compromise happened for the guest reservation database by an unknown party. The information that was leaked contained payment information, mailing addresses, passport numbers, and phone numbers for customers.

Marriott Group has immediately conducted incident investigations with a group of security experts plus setting up a website and a call center.

They also sent emails to the affected customers and gave them free access to monitoring tools that monitor the internet and give an alert if any evidence of sharing personal information is found.

- RockYou Data Breach

RockYou is a company that works in the game field and was founded in 2005 by Lance Tokuda and Jia Shen. The company was working well until December 2009 when what is called “the biggest data breach of all time” happened.

The data breach exposed and leaked more than 32 million user account information from RockYou database.

The company was storing passwords in an unencrypted plain text format which made it easier for the hacker to have access to all passwords stored. The hacker used a very old and popular SQL vulnerability to leak all data from the database.

After this major breach, the total set of passwords that were leaked became a very helpful resource in penetration testing as hackers use this wordlist of passwords to test the security and password strength of accounts and products.

You can read more about top data breaches in this article.

How to Prevent Cybercrimes?

There are many tips and guidelines to protect yourself and your environment from the risk of cybercrimes such as:

1. Be sure that you are using up-to-date security software like antivirus and firewalls.

2. Implement the best possible security settings and implementations for your environment.

3. Don't browse untrusted websites and be careful when downloading unknown files, and also be careful when viewing Email attachments.

4. Use strong authentication methods and keep your passwords as strong as possible. You can find in this article tips on how to protect your password.

6. Educate your children about the risks of internet usage and keep monitoring their activities.

7. Always be ready to make an immediate reaction when falling victim to cybercrimes by referring to the police.

Further reading to protect yourself online:

A Quick Guide to Cybersecurity Incidents and How to Avoid Them?

Types of Cybersecurity Threats, and How to avoid them?

Work From Home Cybersecurity, Tips, and Risks