What is Cybercrime?

intellipaat.com/blog/what-is-cybercrime

July 2, 2021

Previous
Next

Any criminal activity carried out over the internet is referred to as cybercrime. With 4.5 million attacks in July 2024, India was the country with the highest number of attacks, making it vital to raise awareness about cybercrime.

The first incident of cybercrime was documented in 1973. A computer was used by a teller at a New York bank to pilfer over two million dollars. The first email spam was sent in 1978.

In this blog, we will learn about cybercrime and the several risks and prevention strategies associated with it. Let us take a look at what is going to be covered in this blog.

Table of Contents

What is the Definition of Cyber Crime?

Let us start with the definition of cybercrime. Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and

highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime.

Cybercriminals or hackers who want to generate money, commit a majority of cybercrimes. Individuals and organizations are both involved in cybercrime. Aside from that, cybercriminals might utilize computers or networks to send viruses, malware, pornographic material, and other unlawful data.

To make money, cybercriminals engage in a range of profit-driven criminal acts, including stealing and reselling identities, gaining access to financial accounts, and fraudulently utilizing credit cards to obtain funds.

Cybercrimes Examples

1. Stolen credit card information

The most common cybercrime is when a person's credit card information is stolen and used unlawfully to acquire or purchase goods or services over the Internet. The stolen information is observed to be sold on the dark web to make fraudulent purchases or withdrawals, or used to commit identity theft. The consequences of stolen credit card information can result in severe financial losses, damaged credit ratings, and legal issues.

2. Hacking into a Government Website

Another type of cybercrime is tampering with sensitive government data. Hacking into a government website refers to unauthorized access to a government's computer system or network. Considered a highly illegal and unethical act that involves exploiting vulnerabilities in the system's security to gain access to sensitive information, and manipulate the system for malicious purposes. Such actions can lead to severe consequences, such as fines, imprisonment, and damage to national security.

3. Account Takeover (ATO) Fraud

Account Takeover (ATO) Fraud is a form of identity theft in which a fraudster manages to gain access to a victim's bank or credit card accounts and uses them to make unauthorized transactions. Yahoo experienced a serious data breach from 2013 to 2016 that resulted in the theft of three billion user accounts. The attackers gained access to private information and passwords that were used to access user accounts on other online services. Most of this data is available even today on the dark web.

4. Compromised IoT devices

In 2016, over one million connected devices in the IoT were compromised by attackers who took advantage of existing software vulnerabilities. It is the largest DDoS attack to date and one that caused outages in the global DNS affecting popular services including Netflix, PayPal, Twitter, and many more.

5. Loss of control and access to content

The WannaCry attack, which was allegedly launched by North Korea, in 2017, unleashed ransomware that locked down content on user devices. This ransomware rapidly spread itself and infected 300,000 computers worldwide. The victims had to pay hundreds of dollars to restore their data.

6. Phishing campaigns

The phishing campaigns infiltrate corporate networks by sending authentic-looking fraudulent emails to users in an organization and tricking them into performing actions such as downloading attachments or clicking on links**.** The viruses or malware then spreads to the systems, and, eventually, ends up in the organizations' networks.

Some other common examples of cybercrimes include the sale of illegal items, such as drugs, arms, or counterfeit goods, illegal gambling, solicitation, production, distribution, or possession of child pornography, etc.

Classification of Cyber Crimes

Cybercrimes are broadly categorized into three fields:

1. Individual

The act of sharing illegal or harmful content over the internet by a lone individual is considered a cybercrime. Examples include the distribution of pornography, human trafficking, and online stalking.

2. Property

For the property sector, cybercrime involves accessing personal bank or credit card information to perform unauthorized transactions or phishing schemes and attempts to obtain personal information.

3. Government

Similarly, hacking into government computer systems or official websites, although not frequent, is still regarded as a serious offense.

Types of Cyber Crime

There are diversified types of cybercrime recorded across the globe, and some of the noteworthy examples are email fraud, social media fraud, banking fraud, ransomware attacks, cyber espionage, identity theft, clickjacking, and spyware. Let's explore how these crimes are carried out.

1. Malware

Malware is a broad term that comprises a wide range of cyberattacks such as Trojans, viruses, and worms. Malware can simply be described as code written to steal data or destroy things on a computer.

How malware causes harm can assist us in classifying the type of virus that we are dealing with. So, let us talk about it!

1.1 Viruses

Viruses, like their biological namesakes, attach themselves to clean files and infect other clean files. Viruses can spread uncontrollably, causing damage to the core functionality as well as deleting and corrupting files. Viruses usually appear as executable files downloaded from the internet.

1.2 Trojan

This type of malware masquerades as legitimate software that can be hacked. It prefers to function invisibly and creates security backdoors that allow other viruses to enter the system.

1.3 Worms

Worms use the network's interface to infect a whole network of devices, either locally or via the internet. Worms infect more machines with each successive infected machine.

2. Phishing

Phishing frequently poses as a request for information from a reputable third party. Phishing emails invite users to click on a link and enter their personal information.

In recent years, phishing emails have become much more complex, making it impossible for some users to distinguish between a real request for information and a fraudulent one. Phishing emails are sometimes lumped in with spam, but they are far more dangerous than a simple advertisement.

There are five steps to phishing:

2.1 Preparation

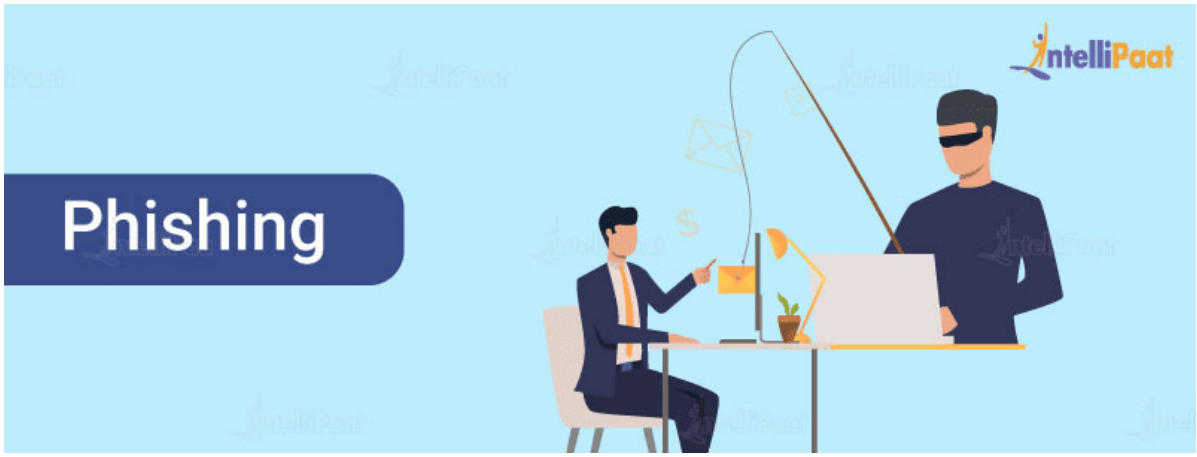
The phisher must pick a business to target and figure out how to obtain the email addresses of that business' customers.

2.2 Setup

Once the phisher has decided which entity to mimic and who the victims will be, the setup process can begin. The phisher constructs and distributes communications and collects data.

2.3 Carry out the attack

This is a process that most people are familiar with. The phisher sends a fake message that appears to come from a well-known source.



2.4 Recording data

The phisher keeps track of the information that victims submit to websites or pop-up windows.

2.5 Identity theft and fraud

The phisher uses the collected information to make unlawful transactions or perform other forms of fraud; up to a quarter of the victims never fully recover.

3. DDoS Attack

As the name suggests, a denial-of-service (DoS) attack focuses on disrupting network service. Attackers transmit a large amount of data traffic via the network until it becomes overloaded and stops working. A DoS attack can be carried out in a

variety of ways, but the most common is a distributed denial-of-service (DDoS) attack. It involves the attacker sending traffic or data, by utilizing several machines, that will overload the system.

In many cases, an individual may not recognize that their computer has been hijacked and is contributing to the DoS attack. Disrupting services can have major ramifications for security and internet access; many large-scale DoS attacks have occurred in the past. Many instances of large-scale DoS attacks have been implemented as a sign of protest against governments.

4. Man-in-the-middle Attack

A man-in-the-middle attack can obtain information from the end-user and the entity with which they are communicating by impersonating the endpoints in the online information exchange.

Let us take a look at an example to learn more about this attack.

If the user is banking online, the man in the middle would communicate with the user by impersonating the bank. The man in the middle would receive all information transferred between the user and the bank including sensitive data related to bank accounts.

5. Drive-by Download Attack

To become infected, we no longer need to click to accept a download or install a software update. Simply opening a compromised webpage may now allow dangerous code to be installed on our device. We only need to visit or drive by a website by clicking accept for any software and malicious code will be downloaded in the background on our device.

The unintentional download of a virus or malicious software onto a computer or mobile device is referred to as a download from these pages.

Drive-by downloads typically take advantage of or exploit an out-of-date browser, app, or operating system with security flaws.

Effects of Cybercrime

As per a report from Cybersecurity Ventures, the worldwide expenses incurred due to cybercrime are predicted to touch $10.5 trillion by 2025. The report also highlights an estimated growth rate of 15% annually for cybercrime over the next five years.

Financial loss is one of the obvious effects of cybercrimes, and it can be quite significant. But cyber crimes also have several other disastrous consequences for businesses, such as:

1. Investor perception can become a huge problem after a security breach causes a drop in the value of businesses.
2. Businesses may also face increased costs for borrowing, and raising more capital can be challenging as well after a security breach.
3. Loss of sensitive customer data can result in penalties and fines for failing to protect customer data. Businesses may be sued over data breaches.
4. Due to a loss of reputation and damaged brand identity after a cyberattack, customers' trust in a business will decline. Businesses not only end up losing current customers but also find it difficult to gain new customers.
5. Direct costs may also be incurred such as the cost of hiring cybersecurity companies for remediation, increased insurance premium costs, public relations (PR), and other services related to the attack.

How to Prevent Cyber Crime?

1. Backup all Data, System, and Considerations

To ensure optimal cyber security, it is advisable to include data backups, system backups, and related considerations within your security strategy. This is because mismanagement of backups can eventually lead to security breaches and compromise sensitive information.

2. Enforce Concrete Security and keep it up-to-date

The selection of the perfect firewall is important as it has functionalities to safeguard against harmful hackers, viruses, and malware, which helps companies detect and react to potential security breaches promptly. Thus, it is important for all individuals to implement strong security measures to ensure optimal Cybersecurity.

3. Never Share Personal Information to a stranger

One of the simplest yet most effective ways to safeguard personal information is to refrain from sharing it with individuals who are not known or trusted. This includes avoiding sharing sensitive information such as one's full name, date of birth, social security number, address, and financial information with strangers online.

4. Integrate Antivirus Software

Using antivirus software helps to recognize any threat or malware before it infects the computer system. Never use cracked software, as it may impose a serious risk of data loss or malware attack.

5. Use Virtual Private Networks (VPNs)

VPNs can be used for a variety of purposes, including protecting online privacy, bypassing internet censorship, and securing online communications. In fact, VPNs help to prevent online tracking and surveillance, as well as safeguard against cyber attacks and identity theft by encrypting data and hiding the user's IP address.

Cyber Security and CyberCrime

In today's interconnected world, Cybersecurity is of paramount importance in safeguarding our digital lives. Think of it as a digital fortress that protects our computer systems, networks, and sensitive information from unauthorized access, damage, and theft. It encompasses a range of measures and practices designed to ensure the confidentiality, integrity, and availability of our digital assets.

Just as we lock our doors and install security systems to protect our physical possessions, Cyber security involves authentication and access control, network security, data encryption, malware protection, and security awareness training. It empowers us to navigate the digital landscape with confidence, knowing that our information is protected and our systems are fortified against potential threats.

In the shadows of the digital world lurks the realm of Cybercrime, where individuals with malicious intent seek to exploit vulnerabilities and wreak havoc. Cybercrime refers to illegal activities conducted in cyberspace, targeting computer systems, networks, and individuals for financial gain or disruption. These nefarious activities include phishing, ransomware attacks, identity theft, hacking, and distributed denial-of-service (DDoS) attacks, among others.

Cyber security gives in-depth knowledge about how to control or recover from cyberattacks.

How to File an Online Cyber Crime Complaint in India?

1. **Visit the Official Website of the Cyber Crime Reporting Portal:** The Indian government has launched the Cyber Crime Reporting Portal (https://cybercrime.gov.in/) specifically for reporting cybercrimes.
2. **Click on "File a Complaint":** On the homepage of the portal, you will find the option to "File a Complaint." Click on it to proceed.

3. **Provide your Personal Details:** Fill in the required information, such as your name, contact details, address, and email ID. Ensure that the information provided is accurate and up-to-date.

4. **Choose the Appropriate Complaint Category:** Select the relevant category that corresponds to the type of cybercrime you have experienced. The options may include hacking, phishing, online fraud, cyber harassment, or others.

5. **Provide Detailed Information:** Describe the incident in detail, providing all relevant information such as the date, time, and nature of the cybercrime. Include any supporting evidence you may have, such as screenshots, emails, or messages.

6. **Attach Supporting Documents:** If you have any supporting documents or evidence related to the cybercrime, upload them as attachments. Ensure that the files are in the specified formats and within the size limit mentioned on the portal.

7. **Submit the Complaint:** Review the information you have provided and ensure its accuracy. Once you are satisfied, submit the complaint by clicking on the “Submit” button.

8. **Note the Complaint Reference Number:** After submitting the complaint, you will receive a unique reference number. Make a note of this number for future reference and tracking.

9. **Follow up with the Authorities:** The cyber crime cell or law enforcement agency responsible for handling cybercrime complaints will review your complaint. It is essential to follow up with them periodically, providing any additional information or cooperation they may require.

How to Withdraw Cyber Crime Complaint?

Once a cybercrime complaint has been filed, it is generally not possible to withdraw it unilaterally. Cybercrime complaints are taken seriously by law enforcement authorities, and they initiate investigations based on the information provided in the complaint. However, if you have a valid reason to withdraw a cybercrime complaint, you can follow these steps:

1. **Contact the Investigating Officer:** Reach out to the law enforcement agency or the investigating officer assigned to your case. Explain your reasons for wanting to withdraw the complaint and discuss the situation with them.
2. **Provide Documentation:** Prepare a written request to withdraw the cybercrime complaint. Clearly state your reasons and attach any supporting documentation that may be necessary to support your request.
3. **Seek Legal Advice:** Consult with a legal professional who specializes in cybercrime or criminal law. They can provide guidance on the specific legal implications and procedures involved in withdrawing a complaint.

4. **Follow the Legal Process:** If the investigating officer agrees to your request, they will guide you through the necessary legal procedures for withdrawing the complaint. This may involve submitting an affidavit or appearing before a magistrate or court to formalize the withdrawal.

Cyber Crime Helpline Numbers

The central cyber helpline number is 1930. As per https://cybercrime.gov.in/, here is how you can reach out to cybercrime officers.

S.No	State/UT's	Email
1	UTTAR PRADESH	sp-cyber.lu@up.gov.in
2	ANDHRA PRADESH	spwpc_cid@ap.gov.in
3	DELHI	ncrp.delhi@delhipolice.gov.in
4	KARNATAKA	spctrcid@ksp.gov.in
5	PUNJAB	aigcc@punjabpolice.gov.in
6	RAJASTHAN	igp.ybercrime@rajpolice.gov.in
7	W3EST BENGAL	digcyber@cidwestbengal.gov.in

Conclusion

In 2024, there was a significant increase in the number of attacks on government agencies in India, making it the country with the highest number of targets. Cyberattacks on government agencies are not uncommon. A considerable number of these attacks are sponsored and the objective is to obtain sensitive information or cause damage to the crucial infrastructure of other nations. This blog provides information about Cybercrime, the various risks it poses, and strategies for preventing it.

Ready to take the next step? Enroll in our Cyber security certification course today and and start building the skills you need to protect yourself and organizations from the growing threat of cyber crime!

Check out our free video on what cybercrime is and learn more!

About the Author

Shivanshu
Lead Penetration Tester

Shivanshu is a distinguished cybersecurity expert and Penetration tester. He specialises in identifying vulnerabilities and securing critical systems against cyber threats. Shivanshu has a deep knowledge of tools like Metasploit, Burp Suite, and Wireshark.