Cyber Crime : History ,Types and Preventive Actions

Cybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information.

Cybercrimes are at an all time high, costing companies and individuals billions of dollars annually. What's even more frightening is that this figure only represents the last 5 years with no end in sight. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users' homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

What is Cybercrime?

Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online.

History of Cybercrime

The malicious tie to hacking was first documented in the 1970s when early computerized phones were becoming a target. Tech-savvy people known as “phreakers” found a way around paying for long distance calls through a series of codes. They were the first hackers, learning how to exploit the system by modifying hardware and software to steal long distance phone time. This made people realize that computer systems were vulnerable to criminal activity and the more complex systems became, the more susceptible they were to cybercrime.

Fast Forward to 1990, where a large project named Operation Sundevil was exposed. FBI agents confiscated 42 computers and over 20,000 floppy disks that were used by criminals for illegal credit card use and telephone services. This operation involved over 100 FBI agents and took two years to track down only a few of the suspects. However, it was seen as a great public relations effort, because it was a way to show hackers that they will be watched and prosecuted.

The Electronic Frontier Foundation was formed as a response to threats on public liberties that take place when law enforcement makes a mistake or participates in unnecessary activities to investigate a cybercrime. Their mission was to protect and defend consumers from unlawful prosecution. While helpful, it also opened the door for hacker loopholes and anonymous browsing where many criminals practice their illegal services.

Crime and cybercrime have become an increasingly large problem in our society, even with the criminal justice system in place. Both in the public web space and dark web, cybercriminals are highly skilled and are not easy to find.

Cybercrimes can generally be divided into two categories:

Crimes that target networks or devices	Crimes using devices to participate in criminal activities
Viruses	Phishing Emails
Malware	Cyberstalking
DoS Attacks	Identity Theft

Categories of Cybercrime

There are three major categories that cybercrime falls into: individual, property and government. The types of methods used and difficulty levels vary depending on the category.

- **Property:** This is similar to a real-life instance of a criminal illegally possessing an individual’s bank or credit card details. The hacker steals a person’s bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use a malicious software to gain access to a web page with confidential information.
- **Individual:** This category of cybercrime involves one individual distributing malicious or illegal information online. This can include cyberstalking, distributing pornography and trafficking.
- **Government:** This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

Types of Cybercrime

DDoS Attacks

These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

Botnets

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

Identity Theft

This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically, cyber stalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyber stalker knows their victim and makes the person feel afraid or concerned for their safety.

Social Engineering

Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

PUPs

PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.

Phishing

This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

Prohibited/Illegal Content

This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Online Scams

These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are “too good to be true” and when clicked on can cause malware to interfere and compromise information.

Exploit Kits

Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user’s computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

Impact of Cybercrime on Society

Cybercrime has created a major threat to those who use the internet, with millions of users’ information stolen within the past few years. It has also made a major dent in many nations’ economies. Below mentioned statistics show shocking impact on cybercrime’s impact on our society to date.

- **The global cost of cybercrime will reach $6 trillion by 2021**
- **According to the Ponemon Institute’s 2016 Cost of Data Breach Study, Global**
- **Analysis organizations that suffered at least one breach in 2016 lost an average of $4 million.**
- **48% of data security breaches are caused by acts of malicious intent.**
- **Cybersecurity Ventures expects ransomware costs will rise to $11.5 billion in 2019.**
- **Cybercrime will more than triple the number of unfilled cybersecurity jobs by 2021**

How to Fight Cybercrime

It seems like in the modern age of technology, hackers are taking over our systems and no one is safe. The average dwell-time, or time it takes a company to detect a cyber breach, is more than 200 days. Most internet users are not dwelling on the fact that they may get hacked and many rarely change their credentials or update passwords. This leaves many people susceptible to cybercrime and it’s important to become informed. Educate yourself and others on the preventive measures you can take in order to protect yourself as an individual or as a business.

1. Become vigilant when browsing websites.
2. Flag and report suspicious emails.
3. Never click on unfamiliar links or ads.
4. Use a VPN whenever possible
5. Ensure websites are safe before entering credentials.
6. Keep antivirus/application systems up to date.
7. Use strong passwords with 14+ characters
8. Report cybercrime on cybercrime.gov.in or call 1930