CYBER CRIME AND CYBER SECURITY

ALISHA
ASSISTANT PROFESSOR
CSE
CONTENTS

• INTRODUCTION
• HISTORY OF CYBER CRIME
• CATEGORIES OF CYBER CRIME
• TYPES OF CYBER CRIME
• CYBERCRIMES THREATENS NATIONAL SECURITY
• CYBER SECURITY
• ADVANTAGES OF CYBER SECURITY
• SAFETY TIPS OF CYBER CRIME
• CYBER LAW OF LAW
• CONCLUSION
INTRODUCTION

Cybercrime, also called computer crime, **the use of a computer as an instrument to further illegal ends**, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

Criminal activities carried out by means of computers or the internet.
HISTORY

History

• Cybercrime first started with hackers trying to break into computer networks. Some did it just for the thrill of accessing high-level security networks, but others sought to gain sensitive, classified material. Eventually, criminals started to infect computer systems with computer viruses, which led to breakdowns on personal and business computers.

• Computer viruses are forms of code or malware programs that can copy themselves and damage or destroy data and systems. When computer viruses are used on a large scale, like with bank, government or hospital networks, these actions may be categorized as cyberterrorism. Computer hackers also engage in phishing scams, like asking for bank account numbers, and credit card theft.
We can categorize cyber crime in two ways:

The computer of target:- using a computer to attacks other computers.
Eg. Hacking, virus, worms attack, dos attack etc.

The computer as a weapon:- using a computer to commit real world crime.
Eg. cyber terrorism, credit card fraud and porography etc.
TYPES OF CYBER CRIME

• Phishing: using fake email messages to get personal information from internet users;
• Misusing personal information (identity theft);
• Hacking: shutting down or misusing websites or computer networks;
• Spreading hate and inciting terrorism;
• Distributing child pornography;
• Grooming: making sexual advances to minors.
TYPES OF CYBER CRIME

• Denial-of-Service attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.
TYPES OF CYBER CRIME

• Phishing:
A technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You’ve probably received email containing links to legitimate appearing websites.

• Cyber stalking:
Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs).
TYPES OF CYBER CRIME

• Pornography:

Pornography falls under the category of obscenity and is punishable by law. Child pornography is a serious offence, and can attract the harshest punishments provided for by law. Pedophiles lurk in chat rooms to lure children.

The internet allows long-term victimisation of such children, because the pictures once put up, spread like wild-fire, and may never get taken down completely. Internet crimes against children are a matter of grave concern, and are being addressed by the authorities, but this problem has no easy solution.
Cybercrime threatens national security in India

• The issue of escalating cyber crime has once again caught our attention with Union Home Minister Shivraj Patil expressing concern over its disastrous effects at the seventh International Cyber Crime Conference held last Wednesday. Patil said that the rising level of cyber crime is an indication of an enormous threat to national security. He further urged law makers and law enforcement agencies to give immediate attention to the matter.

• Arun Kumar, an IT professional from Haryana says, “I feel it is a crime in itself to be part of such ridiculous fan clubs. This is a means to promote crime. If a criminal ends up having a number of fans all across the globe, it is crazy. This throws light on the mindset of the people. As for the anti-India, anti-Pakistan campaigns, we must realize that in the long run these antagonistic feelings can pose an irreversible threat to our very own existence and people behind these acts of notoriety should be penalized as they are somewhere fuelling a sense of hostility in the already estranged relations between the two countries.”
Cybercrime threatens national security in India

- Patil further says, “There is huge potential for damage to national security through cyber attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner. Online child pornography, trafficking in contrabands and e-commerce frauds are on the rise.”

In the words of Pavan Duggal, Supreme Court Lawyer, “Cyber crime is omnipresent and although cyber crime cells have been set up in major cities, most cases remain unreported due to lack of awareness.”

Duggal further opines,” Information Technology Act of 2000 is completely outdated and not fit to deal with cyber crimes.”
CYBER SECURITY

• Cyber security
Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

• Privacy policy
Before submitting your name, email, address, on a website look for the site’s privacy policy.

• Keep software up to date
If the seller reduces patches for the software operating system your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage. Use good password
CYBER SECURITY

• Disable Remote Connectivity

Some PDA’S and phones are equipped with wireless technologies such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use.
Cyber security's advantages and benefits

• It protects an individual's and an organization's personal and sensitive data from being stolen.

• The primary benefit of employing these effective cyber-security mechanisms is that networks can be protected from various false nodes attempting to gain unauthorised access to the network.

• The most important aspect is that it improves the system's cyber-security.

• It reduces the likelihood of machines being hacked, reducing the likelihood of system freezes and crashes.
Cyber security's advantages and benefits

• It improves the company's overall security mechanisms through the use of a better information framework, resulting in smooth business management activities.
• It identifies the flaws and weak entities that could aid an attacker in gaining access to the system or server. These vulnerabilities, once identified, will assist teams in securing systems and preventing such attacks from occurring.
Important Cyber Security Tips for Your Users

• Clicking Without Thinking Is Reckless
• Use Two-Factor Authentication
• Look Out for Phishing Scams
• Keep Track of Your Digital Footprint
• Keep Up With Updates
• Connect Securely
• Secure Your Mobile Device
• Back-Up Your Data
Cyber Laws In India

• In India, cyber laws are contained in the Information Technology Act, 2000 (“IT Act”) which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

• The Act now allows Government to issue notification on the web thus heralding e-governance.
Important of Law

- Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.
CONCLUSION

• Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

• So we make us a safer we must need cyber security.
THANK YOU