SCRIPT

Slide 1: WELCOME

Slide 2: CYBER CRIME AND CYBER SECURITY

Presented by: Kartik Sharma, Aman Verma, Aviral Srivastava, Devansh Chaudhary, Avikam Singh, Neelansh Singh, Aditya Agarwal, Ishaan Nigam.

Slide 3: What is Cyber Crime?

Cybercrime is any illegal activity that happens on a computer, a network like the internet, or uses the internet. Imagine someone trying to steal your toys but doing it through a computer - that's cybercrime!

Slide 4: Financial Cyber Crimes

These are bad things people do online to steal money or important information about your money. This can be like someone trying to sneak into your piggy bank using a computer!●

Hacking: Breaking into computer systems to steal information.●

Phishing: Tricking people into giving away personal information like passwords. Imagine someone pretending to be your friend to trick you into telling them a secret!●

Identity theft: Stealing someone's personal information to pretend to be them.

Slide 5: Identity Theft Crimes●

Stolen Identities: Criminals can steal your personal information to pretend to be you, especially to steal money or do other bad things.●

Data Breaches: Bad people can hack into computer systems to steal sensitive information like your secret passwords, credit card numbers or other important details.

Legal Consequences: Identity theft can lead to serious problems with the law, like being accused of doing something you didn't do. It can also damage your credit score, which is like a report card for how well you handle money.

Slide 6: Cyberbullying

This is when someone uses technology like phones or computers to harass, threaten, or embarrass someone else. It's like bullying, but it happens online, and can make people feel very sad and scared.

Slide 7: Hacking Cyber Crimes

Hacking is a type of cybercrime. Cybercrime means any illegal activity that happens on a computer, a network of computers, or the internet.

What Do Hackers Do?

Hackers are people who use hacking techniques, which are like sneaky tricks, to get into computer systems, networks, or data without permission. They do this with bad intentions.

Here's an example: Imagine a hacker like someone trying to break into a house. They might look for an unlocked window (that's like a vulnerability in a computer system) or try to trick someone into opening the door (that's like a phishing scam).

Why is Hacking Bad?

Hacking can have really bad consequences:•

Stealing Information: Hackers might steal sensitive information like passwords, credit card numbers, or personal details. That's like someone breaking into your house and stealing your jewellery!•

Disrupting Operations: Hackers can disrupt how things work, like shutting down websites or causing blackouts. Imagine if someone cut off the electricity to your whole neighbourhood - that's a bit like what a hacker can do!•

Holding Data for Ransom: Some hackers hold important data hostage and demand money to give it back. It's like kidnapping someone's pet and asking for money to return them!

Who Can Be Affected by Hacking?

Hacking can affect anyone:•

Individuals: Hackers might target your personal computers or devices.•

Businesses: Hackers could steal company secrets or disrupt business operations.•

Critical Infrastructure: Hacking can even affect important things like hospitals or power grids, which could put people's safety at risk.

The Impact of Hacking

The effects of hacking can be really serious:•

Financial Losses: People and businesses can lose a lot of money because of hacking.•

Reputational Damage: Imagine if a company lost all its customers' data because of hacking - people wouldn't trust that company anymore.●

Physical Harm: In some cases, hacking can even lead to physical harm, especially if it affects things like hospitals or traffic systems.

Slide 8: Cyber Security Fundamentals

This is how we protect ourselves and our information online!1.

Understanding Threats: It's important to know the different dangers online, like malware, phishing, hacking, and data breaches. Imagine learning about different types of germs so you know how to stay healthy.2.

Implementing Robust Security Measures: Just like a house needs strong walls and locks, computers need protection like firewalls, antivirus software, and encryption.3.

Fostering Security Awareness: Everyone needs to learn how to stay safe online, like spotting phishing attempts and using strong passwords.4.

Protecting Sensitive Data: Always back up important information, so you don't lose it if something bad happens. Imagine having spare keys just in case you lose the original.

Slide 9: Protecting Yourself from Cyber Threats

Here are some ways to stay safe online:●

Enable Two-Factor Authentication: This adds an extra layer of security to your accounts, like having two locks on your door! It usually involves a password and a special code.●

Use Strong and Unique Passwords: Make sure your passwords are long, tricky and different for each account. Think of it like having a different key for each of your valuable things.●

Keep Software Up-to-Date: Regularly updating your computer and phone software is like getting vaccinated - it protects you from new threats! ●

Be Cautious of Phishing Attempts: Don't trust emails or messages asking for personal information. Always double-check if something seems suspicious.

Slide 10: Cyber Security Best Practices

Protecting Your Accounts: Use strong passwords, enable two-factor authentication and avoid sharing personal information online!

Being Cautious Online: Don't click on suspicious links and be careful about what you download!

Protecting Your Privacy: Think carefully about what you share online and adjust your privacy settings to control who can see your information!

Slide 11: Online Etiquette

Just like we have good manners in real life, we need to be respectful and responsible online! This includes:●

1. Being polite and considerate to others.●
2. Being careful about what you post.●
3. Not sharing personal information.●

Telling a trusted adult if you experience or see something upsetting.

Slide 12: Careers in Cyber Security

If you're interested in computers and keeping people safe online, then a career in cyber security might be for you! Here are some cool jobs you could have:●

Cybersecurity Analyst: They protect organisations from cyber threats by monitoring networks and investigating suspicious activity!●

Ethical Hacker: They use their hacking skills to find weaknesses in systems and help make them stronger!●

Cybersecurity Educator: They teach people about cybersecurity and how to stay safe online!●

Chief Information Security Officer (CISO): They are the leaders in an organisation who make sure that everything is secure!

Slide 13: Future Prospects About Cyber Crime●

Rise of AI-Powered Defenses: Imagine super smart computers helping us fight cybercrime even faster! AI can detect and stop threats much quicker than humans.●

Increased Regulatory Oversight: Governments and organisations will create stricter rules and laws to protect people's information and punish cybercriminals!●

Proactive Threat Prediction: In the future, we might be able to predict cyber attacks before they happen, like having a superpower to see into the future!

Slide 14: Cyber Crime Statistics in India●

India is a big target for cyber criminals, with millions of cybercrimes reported every year!●

This costs the country a lot of money - over **$1 billion** annually!

Slide 15: Staying Safe

If you ever feel unsafe or bullied online, tell a trusted adult like a parent or teacher.

Slide 17: Conclusion

Cybersecurity is important, but it doesn't have to be scary. Always remember to be careful and use strong passwords. If you're unsure about anything, ask a trusted adult.

Slide 19: It's Quiz Time