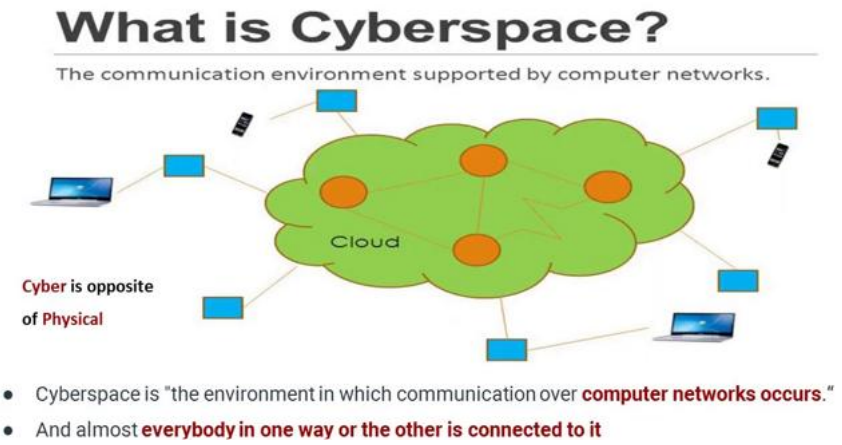
# Unit-1

## Cyber Crime

## Cyber Space:

Cyber Space is a virtual world where all digital, internet, and computer-based activities take place. It is an invisible and interconnected environment where people, systems, and devices communicate and exchange data through the internet.

In simple terms, Cyber Space is the global digital ecosystem where information is shared, transactions occur, and online activities take place.




### Key Features of Cyber Space:

1. Internet & Networking: Websites, social media, emails, cloud storage, etc.
2. Cyber Security: Protecting online data through antivirus, encryption, and firewalls.
3. Cyber Crimes: Activities like hacking, phishing, identity theft, and fraud.
4. Digital Communication: Chatting, video calls, and online meetings.
5. E-Commerce & Digital Transactions: Online shopping, banking, and cryptocurrency.

### Importance of Cyber Space:

- Connects people worldwide through the internet.
- Helps businesses and governments operate efficiently.
- Provides easy access to information and communication.
- Supports digital payments and financial transactions.
- Requires cybersecurity to prevent data breaches and cyber attacks.

In short, Cyber Space is the digital universe where technology, people, and data interact, shaping the modern world.

## Cyber Crime:

**Cyber Crime** refers to illegal activities carried out using computers, networks, or the internet. It involves crimes like hacking, identity theft, online fraud, and data breaches that can harm individuals, businesses, or governments.

In simple words, **Cyber Crime means any criminal activity done in the digital world using technology.**

### Types of Cyber Crime:

1. **Hacking:** Gaining unauthorized access to a computer or network.
2. **Phishing:** Fake emails or messages to steal sensitive information like passwords.
3. **Identity Theft:** Using someone else's personal data for fraud.
4. **Online Fraud & Scams:** Fake websites, lottery scams, or financial fraud.
5. **Cyber Bullying:** Harassment or threats through social media or messages.
6. **Malware Attacks:** Viruses, ransomware, or spyware that harm devices and steal data.
7. **Data Breaches:** Stealing confidential information from companies or individuals.
8. **Online Piracy:** Unauthorized downloading or sharing of movies, software, or music.

**How to Stay Safe from Cyber Crime?**

- Use strong passwords and enable two-factor authentication.
- Avoid clicking on suspicious links or downloading unknown files.
- Keep your devices and software updated.
- Use antivirus and firewall protection.
- Be cautious while sharing personal details online.
- Report cyber crimes to authorities if needed.

**Conclusion:**

Cyber Crime is a growing threat in the digital world. With the increasing use of the internet, it is important to be aware of online risks and take preventive measures to stay safe.

## Jurisdictional Concerns:

**Jurisdictional Concerns in Cybercrime**

Jurisdiction refers to the authority of a country or legal system to prosecute a crime. Cybercrimes often create **conflicts in jurisdiction** because:

1. **Cross-Border Crimes:** Cybercriminals operate from different countries, making it difficult to determine which country's laws apply.
2. **Diverse Legal Frameworks:** Different countries have varying cyber laws, making cooperation complicated.
3. **Extradition Issues:** Many countries lack extradition agreements, preventing cybercriminals from being prosecuted in another jurisdiction.
4. **Data Sovereignty Conflicts:** Data stored in foreign servers is subject to the laws of that country, leading to legal disputes.
5. **Anonymity & Encryption:** Criminals use VPNs, the dark web, and encryption, making it hard to trace their real location.

## Key Challenges in Fighting Cybercrime

1. **Lack of International Cooperation:** Differences in legal frameworks hinder investigations and prosecution.
2. **Attribution Problems:** Identifying the real perpetrator is difficult due to sophisticated hacking methods.
3. **Fast-Evolving Threats:** Cybercriminals constantly update their tactics, making defense strategies outdated.
4. **Lack of Resources & Expertise:** Many law enforcement agencies lack trained personnel and technology to combat cybercrime effectively.
5. **Privacy & Surveillance Concerns:** Striking a balance between security and individual privacy rights is challenging.

## Types of Jurisdictional Issues in Cybercrime

1. **Territorial Jurisdiction:** Which country has the authority to prosecute cybercriminals operating across multiple regions?
2. **Personal Jurisdiction:** Can a country prosecute a person who commits a cybercrime against its citizens from abroad?
3. **Subject-Matter Jurisdiction:** Does a specific court have the authority to handle cybercrime cases?
4. **Extraterritorial Jurisdiction:** Can a country apply its laws to cybercriminals operating beyond its borders?

**Conclusion:**Jurisdictional concerns in cybercrime create challenges in law enforcement, investigation, and prosecution. Strong international cooperation, standardized laws, and advanced cybersecurity measures are needed to combat cybercrime effectively.

# What is Jurisprudential Inconsistency?

Jurisprudential inconsistency refers to contradictions, variations, or lack of uniformity in legal decisions, principles, or interpretations of the law across different courts, jurisdictions, or time periods. It occurs when similar cases result in different rulings due to differing legal interpretations, judicial philosophies, or legislative ambiguities.

## Types of Jurisprudential Inconsistency

1. **Intra-Jurisdictional Inconsistency**
    - Occurs when courts within the same jurisdiction (e.g., different courts in one country) deliver conflicting rulings on similar cases.
    - Example: Different high courts in a country interpreting the same law differently.
2. **Inter-Jurisdictional Inconsistency**
    - Happens when courts in different jurisdictions (e.g., different countries or states) apply the same legal principle in different ways.
    - Example: A cybercrime act being legal in one country but punishable in another.
3. **Temporal Inconsistency**
    - Arises when courts change their interpretation of laws over time, leading to differing rulings for similar cases in different periods.
    - Example: A Supreme Court reversing its stance on a fundamental right.
4. **Hierarchical Inconsistency**
    - Happens when lower courts deliver rulings that contradict higher court precedents.
    - Example: A trial court refusing to follow a Supreme Court ruling.
5. **Legislative-Judicial Inconsistency**
    - Occurs when judicial interpretations contradict legislative intent or statutory provisions.
    - Example: Courts interpreting laws in ways that differ from what lawmakers originally intended.

## Key Challenges of Jurisprudential Inconsistency

1. **Legal Uncertainty**
    - Citizens and businesses may not know how the law applies due to contradictory rulings.

2. **Erosion of Public Trust**
    - Inconsistencies in judicial decisions can reduce trust in the legal system.
3. **Delays in Justice**
    - Conflicting rulings lead to prolonged legal battles and appeals.
4. **Difficulties in Law Enforcement**
    - Police and regulatory bodies struggle to apply laws consistently when courts interpret them differently.
5. **Impact on International Law**
    - Different legal standards across countries create challenges in global legal matters like human rights, trade, and cyber law.
6. **Hindrance to Precedent-Based Systems**
    - Inconsistencies weaken the doctrine of **stare decisis**, where courts rely on past rulings to decide cases.

**Conclusion**

Jurisprudential inconsistency poses significant challenges in maintaining a fair, predictable, and efficient legal system. Solutions include better judicial training, legislative clarity, and stronger legal harmonization efforts across jurisdictions.

## eCash Security: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

### What is eCash?

eCash (Electronic Cash) refers to digital money used for online transactions, stored in electronic wallets, and transferred securely over the internet. Examples include cryptocurrencies (e.g., Bitcoin), digital wallets (e.g., PayPal), and central bank digital currencies (CBDCs).

### 1. Security Characteristics of eCash

eCash security is crucial to prevent fraud, hacking, and unauthorized transactions. The key security characteristics include:

**a) Anonymity & Privacy**

- Users can conduct transactions without revealing personal details (e.g., cryptocurrencies like Monero).
- However, some systems maintain traceability for compliance (e.g., CBDCs).

**b) Authentication & Encryption**

- Digital signatures, multi-factor authentication (MFA), and cryptographic techniques secure transactions.
- Public and private key cryptography ensures only authorized users can access funds.

**c) Non-Repudiation**

- Once a transaction is completed, neither party can deny its occurrence, ensuring accountability.

**d) Double-Spending Prevention**

- Blockchain and cryptographic protocols prevent users from spending the same eCash multiple times.

**e) Integrity & Tamper Resistance**

- Transactions are verified through decentralized ledgers (blockchain) or trusted central authorities to prevent tampering.

---

## 2. Key Challenges in eCash Security

Despite its advantages, eCash faces multiple security challenges:

**a) Cybercrime & Fraud**

- Hackers exploit system vulnerabilities to steal eCash through phishing, malware, and ransomware attacks.

**b) Regulatory & Legal Issues**

- Lack of a unified global framework makes enforcement difficult.
- Criminals exploit anonymity for money laundering, terrorism financing, and tax evasion.

**c) Scalability & Performance**

- Blockchain networks face transaction speed limitations (e.g., Bitcoin's slow processing time).
- High computational power is required for secure transactions.

**d) Lack of Consumer Protection**

- Transactions are irreversible in decentralized systems, leading to challenges in fraud recovery.
- Unlike banks, crypto wallets are not insured against losses.

**e) Identity Theft & Account Takeover**

- Phishing attacks and social engineering scams target users to steal eCash.

---

## 3. Risks Associated with eCash in Cybercrime

### a) Financial Losses

- Hacking, fraud, and Ponzi schemes lead to massive losses.
- Example: Exchange hacks (e.g., Mt. Gox, FTX collapse).

### b) Money Laundering & Terrorist Financing

- Criminals use eCash to launder illicit funds via decentralized exchanges and mixers.

### c) Ransomware & Dark Web Transactions

- Cybercriminals demand ransom in cryptocurrencies due to their untraceable nature.
- eCash is widely used in illegal activities on the dark web.

### d) Smart Contract Vulnerabilities

- Bugs in blockchain smart contracts can lead to exploits and stolen funds.
- Example: DAO hack on Ethereum.

---

## 4. Security Mechanisms to Protect eCash

### a) Cryptographic Security

- **Public Key Infrastructure (PKI):** Ensures secure encryption and decryption.
- **Elliptic Curve Cryptography (ECC):** Enhances security while reducing computational requirements.

### b) Blockchain & Distributed Ledger Technology (DLT)

- Ensures tamper-proof transactions with decentralized verification.
- Reduces risks of double-spending and fraud.

### c) Multi-Factor Authentication (MFA)

- Combines passwords, biometrics, and OTPs to prevent unauthorized access.

### d) Secure Wallets & Cold Storage

- **Hardware wallets (Ledger, Trezor):** Store eCash offline to protect against hacks.
- **Multi-signature wallets:** Require multiple approvals for transactions.

**e) AI & Machine Learning-Based Fraud Detection**

- AI-driven monitoring detects suspicious transaction patterns.

**f) Regulatory Compliance & KYC/AML Measures**

- **Know Your Customer (KYC)**: Verifies users' identities.
- **Anti-Money Laundering (AML):** Tracks suspicious activities.

**Conclusion**

eCash security is essential to prevent cybercrime, financial fraud, and identity theft. Strong encryption, secure storage, blockchain technology, and legal regulations are necessary to enhance protection against evolving threats.

## Prepaid Cards: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Prepaid cards are financial instruments that are loaded with a fixed amount of money beforehand. Users can make purchases or payments until the balance runs out, without linking the card to a bank account.
- **Types**:
    1. **Open-loop cards**: Issued by Visa/Mastercard; accepted at multiple merchants.
    2. **Closed-loop cards**: Restricted to a particular retailer or brand (e.g., Amazon gift cards).
    3. **Reloadable cards**: Can be refilled with funds for continuous use.
    4. **Non-reloadable cards**: Can be used only until the initial balance is exhausted.
- **Key Features**:
    - Fixed spending limit based on the loaded amount.
    - Not linked to any bank account.
    - Often used anonymously or without credit checks.
- **Benefits**:
    - Safe alternative to cash.
    - Helps with budgeting and controlled spending.
    - Can be given as gifts or used for travel.
- **Characteristics**:

- Available in physical or virtual formats.
- Usually PIN-protected.
- Accepted widely (for open-loop types).

- **Challenges/Risks**:
  - May charge activation or inactivity fees.
  - If lost or stolen, balance may be unrecoverable.
  - Limited consumer protections compared to credit cards.
- **Security Mechanisms**:
  - EMV chip and PIN for authentication.
  - Card tokenization for online use.
  - SMS or email alerts for transactions.
- **Examples**:
  - HDFC Forex prepaid card for international travel.
  - SBI prepaid card for employees' salary disbursement.
  - Amazon gift cards.

---

## Stored Value Cards: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Stored value cards are cards that store monetary value either on the card itself or in an associated database, used for specific services or vendors.
- **Types**:
  1. **Smart cards**: With embedded chips storing data.
  2. **Magnetic stripe cards**: Data encoded on a magnetic stripe.
  3. **Contactless cards**: Use RFID/NFC for quick tapping.
- **Key Features**:
  - Can be used without internet connection.
  - Reloadable in most cases.
  - Transactions are usually quick and seamless.

- **Benefits**:
  - Useful for frequent small payments.
  - Ideal for closed environments (e.g., campuses, metros).
  - Reduces dependency on cash.
- **Characteristics**:
  - Usually tied to a specific service provider.
  - Balance stored on card or backend.
  - May come with usage restrictions.
- **Challenges/Risks**:
  - Lost card = lost value.
  - Usually not accepted outside designated areas.
  - Susceptible to card tampering.
- **Security Mechanisms**:
  - Data encryption in chips.
  - Unique card IDs and PINs.
  - Backend verification in hybrid systems.
- **Examples**:
  - Delhi Metro card.
  - Employee cafeteria cards.
  - Student ID cards with prepaid balance.

---

## Mobile Payments: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Mobile payments refer to financial transactions conducted via mobile devices using mobile apps, wallets, or contactless technologies such as NFC.
- **Types**:
  1. **NFC-based payments**: Tap-to-pay systems like Apple Pay or Google Pay.

2. **QR Code payments**: Apps like Paytm and PhonePe use QR scanning for fast payments.
3. **USSD and SMS payments**: Used in rural or low-internet areas for simple bank transfers.
4. **Mobile wallets**: Apps like Mobikwik or Amazon Pay store prepaid balance for payments.

- **Key Features**:
  - Real-time processing, works online/offline (some services), linked with banks or wallets.
  - Easy UI with integration into retail and utility platforms.
- **Benefits**:
  - Fast and convenient, reduces need for cash, and helps keep a digital record of spending.
  - Supports remote transactions like online shopping or bill payments.
- **Characteristics**:
  - App-based interface, requires device and account registration, includes authentication.
  - Compatible with smart devices and widely accepted in urban setups.
- **Challenges/Risks**:
  - Prone to cyber frauds, phishing, and data leakage if device is lost or unsecured.
  - Dependent on mobile network or internet availability.
- **Security Mechanisms**:
  - Biometric locks, multi-factor authentication, tokenization, and device verification.
  - Alerts and OTPs for every transaction add an extra layer of protection.
- **Examples**:
  - Using Google Pay for grocery payments.
  - Scanning Paytm QR at a petrol pump.
  - Paying a bill with Airtel Thanks app.

---

## Internet Payment Services: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: These are platforms that facilitate online financial transactions, allowing individuals and businesses to send or receive money over the internet.
- **Types**:
    1. **Payment Gateways** (e.g., PayPal): Process and secure online payments.
    2. **Merchant Account Providers**: Enable businesses to accept online payments.
    3. **All-in-One Solutions** (e.g., Stripe): Combine payment processing and merchant accounts.
- **Key Features**:
    - Integration with e-commerce platforms, real-time payments, multi-currency support.
    - Encrypted data transmission for secure payments.
- **Benefits**:
    - Global reach, allows 24x7 transactions, and reduces manual payment handling.
    - Increases convenience for online shoppers and businesses.
- **Characteristics**:
    - Works with credit/debit cards, digital wallets, or net banking.
    - Can be embedded into websites and mobile apps.
- **Challenges/Risks**:
    - Risk of hacking, fraud, and data breaches.
    - Downtime or technical glitches may delay transactions.
- **Security Mechanisms**:
    - SSL encryption, PCI-DSS compliance, fraud detection systems.
    - Tokenization and secure API calls protect sensitive data.
- **Examples**:
    - Stripe used by e-commerce stores.
    - Razorpay integrated with Indian startups.
    - PayPal for international freelance payments.

## Cyber Stalking: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Cyber stalking involves repeated use of digital platforms to harass, monitor, or threaten an individual, often causing fear or emotional distress.
- **Types**:
    1. **Email stalking**: Sending threatening or unwanted messages.
    2. **Social media stalking**: Monitoring and commenting aggressively on a person's posts.
    3. **Location stalking**: Using GPS tracking or apps to track someone's physical movement.
- **Key Features**:
    - Repetitive behavior, anonymity of stalker, psychological impact on the victim.
    - Often includes fake profiles and impersonation.
- **Benefits (for victims)**:
    - Awareness allows early intervention, use of reporting and blocking tools.
    - Law enforcement may provide legal protection if reported early.
- **Characteristics**:
    - Often difficult to trace as stalkers use fake IDs and proxy IPs.
    - Victims may experience anxiety, fear, or trauma.
- **Challenges/Risks**:
    - Emotional and mental health issues for the target.
    - May escalate to real-world stalking or violence.
- **Security Mechanisms**:
    - Strong privacy settings, reporting features on platforms, using VPNs and blocking users.
    - Cyber laws and digital forensics help track and punish offenders.
- **Examples**:
    - A student repeatedly messaged by a stranger online.
    - An ex-partner tracking social media activity aggressively.

- Using spyware to follow someone's location.

---

## Cyber Extortion: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Cyber extortion is a crime where attackers demand money or favors by threatening to damage, steal, or leak data from individuals or organizations.
- **Types**:
  1. **Ransomware attacks**: Files encrypted and held hostage until payment is made.
  2. **DDoS threats**: Services are disrupted unless ransom is paid.
  3. **Data breach blackmail**: Threatening to leak sensitive data unless extorted.
- **Key Features**:
  - Involves threats, monetary demands, use of anonymous platforms for communication.
  - Often paid in untraceable crypto like Bitcoin.
- **Benefits (preventive awareness)**:
  - Helps businesses implement better security.
  - Encourages insurance and risk mitigation strategies.
- **Characteristics**:
  - Cybercriminals operate from anonymous, global networks.
  - Targets are often high-value data holders like hospitals or corporations.
- **Challenges/Risks**:
  - Business disruption, reputation loss, and financial damages.
  - Legal obligations if customer data is exposed.
- **Security Mechanisms**:
  - Backups, endpoint protection, incident response plans, network segmentation.
  - Use of honeypots and early detection tools.
- **Examples**:
  - WannaCry ransomware attack.
  - An e-commerce site receiving DDoS ransom threats.

- Leaked celebrity data used for blackmail.

---

## Cyber Terrorism: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Cyber terrorism is the use of digital technology to threaten or cause disruption, fear, or damage to critical systems, often with political or ideological motives.
- **Types**:
  1. **Website defacement**: Hacking government sites to spread propaganda.
  2. **Critical infrastructure attacks**: Targeting power grids or communication systems.
  3. **Cyber bomb threats**: Sending fake or real digital threats to incite panic.
- **Key Features**:
  - Politically motivated, aimed at mass disruption and fear.
  - Often targets national security or public safety systems.
- **Benefits (counter-strategy awareness)**:
  - Promotes national cybersecurity defense plans.
  - Encourages cooperation between countries to fight digital terrorism.
- **Characteristics**:
  - Highly skilled attackers, anonymous networks, global impact potential.
  - May include elements of physical and digital terrorism combined.
- **Challenges/Risks**:
  - Massive economic losses, public panic, or even loss of life.
  - Difficult to trace sources across borders due to decentralized nature.
- **Security Mechanisms**:
  - National cyber defense agencies, AI-based threat detection, and intelligence sharing.
  - Real-time monitoring of critical systems like transport or energy grids.
- **Examples**:
  - Cyber attack on Ukraine’s power grid.

- Terrorist organizations using social media to spread messages.
- Defacing national websites during conflict.

---

## Cyber Warfare: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Cyber warfare refers to hostile actions in cyberspace between nations or state-sponsored actors to damage, disrupt, or steal information from another country.
- **Types**:
  1. **Espionage**: Stealing classified data from rival governments.
  2. **Sabotage**: Disabling communication or military systems.
  3. **Propaganda**: Using digital platforms to influence or mislead populations.
- **Key Features**:
  - State-level planning, long-term espionage goals, politically or militarily driven.
  - Can paralyze vital systems during real-world conflicts.
- **Benefits (defensive readiness)**:
  - Countries strengthen cybersecurity strategies and develop cyber armies.
  - Promotes innovation in cyber defense tools and training.
- **Characteristics**:
  - Highly secretive, uses zero-day exploits, usually not acknowledged officially.
  - May involve both government and private sector infrastructures.
- **Challenges/Risks**:
  - Could trigger real wars, damage public trust, or disrupt economy.
  - Attribution is hard, making retaliation tricky.
- **Security Mechanisms**:
  - Firewalls, advanced threat intelligence, digital forensics, and red team testing.
  - Government CERT teams and international alliances like NATO's CCDCOE.
- **Examples**:
  - Stuxnet worm targeting Iran’s nuclear program.

- Russian cyber operations during geopolitical tensions.
- Chinese cyber espionage activities reported by multiple countries.

---

## Cyber Weapons: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Cyber weapons are software tools or malicious codes used by governments or hackers to carry out attacks in cyberspace that can cause real-world damage or disruptions.
- **Types**:
  1. **Malware tools**: Used to infiltrate or destroy systems.
  2. **Logic bombs**: Hidden code that activates under certain conditions.
  3. **Remote access trojans (RATs)**: Allow full control of target systems.
- **Key Features**:
  - Designed for stealth, control, destruction, or theft.
  - Can be customized for specific targets or systems.
- **Benefits (from defense POV)**:
  - Awareness leads to better digital defense architectures.
  - Can act as deterrents like nuclear weapons in cyber diplomacy.
- **Characteristics**:
  - Highly technical, may lie dormant for months, and hard to detect.
  - May exploit zero-day vulnerabilities not known to the public.
- **Challenges/Risks**:
  - Could be misused or leaked, leading to uncontrollable attacks.
  - Raises ethical concerns over digital warfare.
- **Security Mechanisms**:
  - Constant patching, threat simulations, red teaming, and digital surveillance.
  - Zero-trust architecture and endpoint monitoring help detect early signs.
- **Examples**:

- Stuxnet worm (again, as a cyber weapon).
- EternalBlue exploit used in WannaCry.
- Pegasus spyware for surveillance.

---

## ATM Frauds: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: ATM frauds are unauthorized activities involving ATMs to steal money or personal information from users.
- **Types**:
  1. **Card skimming**: Fake card readers that capture card data.
  2. **PIN capturing**: Hidden cameras or fake keypads to steal PINs.
  3. **ATM jackpotting**: Hacking the machine to eject all cash.
- **Key Features**:
  - Involves both physical tampering and digital methods.
  - Targets common people withdrawing money.
- **Benefits (after awareness)**:
  - People become cautious while using ATMs and banks upgrade technology.
  - Encourages biometric and chip-based systems.
- **Characteristics**:
  - Usually occurs at remote or poorly monitored ATMs.
  - Criminals may work in groups and use distraction techniques.
- **Challenges/Risks**:
  - Financial loss, emotional distress, and difficulty in getting refunds.
  - Can go undetected if user is unaware.
- **Security Mechanisms**:
  - EMV chip cards, ATM anti-skimming devices, transaction alerts.
  - Real-time monitoring and ATM surveillance cameras.
- **Examples**:

- A user's card cloned at a petrol pump ATM.
- An ATM hacked using malware to dispense cash.
- Fake keypad found on a city ATM.

---

## Phreaking: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Phreaking is the act of hacking into telecommunication systems to make free calls or manipulate telephone networks.
- **Types**:
  1. **Blue boxing**: Mimicking tones to access free long-distance calls.
  2. **VoIP phreaking**: Attacks on internet-based phone systems.
  3. **PBX hacking**: Breaking into corporate phone exchanges.
- **Key Features**:
  - Exploits telephone systems using tones, codes, or system flaws.
  - Historically popular before the internet, now used on VoIP systems.
- **Benefits (modern learning)**:
  - Helps telecom companies plug vulnerabilities.
  - Shows early evolution of cybercrime.
- **Characteristics**:
  - Involves technical skill, sound frequency knowledge, and physical access.
  - Usually targets call routing or billing systems.
- **Challenges/Risks**:
  - Unauthorized billing, loss of telecom revenue, and user privacy breaches.
  - Can be hard to detect on VoIP platforms.
- **Security Mechanisms**:
  - Strong authentication, call monitoring systems, and updated PBX firewalls.
  - Blocking suspicious IPs and real-time VoIP traffic analysis.
- **Examples**:

- Hacker using a laptop and modem to make international calls for free.
- VoIP fraud on a business phone system.
- Exploiting weak PBX to reroute calls.

---

## Internet Gambling: Characteristics, Challenges, Risks, and Security Mechanisms in Cybercrime

- **Definition**: Internet gambling involves betting money on casino-style games, sports, or lotteries through online platforms.
- **Types**:
  1. **Online casinos**: Slots, poker, and roulette games.
  2. **Sports betting**: Predicting sports results for money.
  3. **Fantasy leagues and lotteries**: Betting on team performances or numbers.
- **Key Features**:
  - Available 24/7, accessible globally, and usually requires digital payment.
  - Some are legal and regulated; others are illegal or in grey areas.
- **Benefits**:
  - Convenience of gambling from home, wide variety of games, and bonuses.
  - Can generate revenue for licensed operators.
- **Characteristics**:
  - Addictive nature, easy to access, often anonymous platforms.
  - May involve real or virtual currencies.
- **Challenges/Risks**:
  - Addiction, financial loss, illegal platforms scamming users.
  - Children and vulnerable users can be exploited.
- **Security Mechanisms**:
  - Age verification, responsible gambling tools, and encryption for payments.
  - Licensing and regulation by governments to ensure fairness.
- **Examples**:
  - Playing real-money poker on an international app.

- Betting on IPL results using fantasy sports apps.
- Online slot games from offshore websites.