Comprehensive Internship Report:
Practical Insights into Cybercrime Investigation

Mr. Nandipati Avinash Chowdary
Intern

Host Institution:
Cyber Crime Police Station, Vijayawada, Andhra Pradesh Police

Internship Period:
April 25, 2025 – May 25, 2025

Introduction

This comprehensive report outlines my in-depth learning and practical experiences during my internship at the Cyber Crime Police Station, Vijayawada, under the Andhra Pradesh Police. This internship, from April 25, 2025, to May 25, 2025, provided a unique opportunity to understand the real-world aspects of cybercrime investigation and how law enforcement operates in our digital world.

Understanding Cybercrime: What I Learned

During my time at the Cyber Crime Police Station, I gained a much clearer picture of cybercrime – how varied it is and the clever ways criminals use technology for illegal activities.

Different Types of Cyber Offenses

Cybercrime covers many illegal acts done using computers and the internet. Here are the main types I learned about:

1. **Money-Related Frauds and Scams:**
   - **Phishing:** This is like a tricky email or message that pretends to be from a trusted source (like your bank or a famous company). It tries to get you to click a link or give away personal details like your passwords or bank account numbers.
   - *Example:* You get an email that looks exactly like it's from your bank, saying your account is locked and asking you to click a link to "verify" your details. If you click and enter information, criminals steal it.
   - **Identity Theft:** This happens when someone steals your personal information (like your name, birth date, or Aadhaar number) and uses it to pretend to be you, often to open fake accounts or commit financial fraud.
   - *Example:* A criminal gets your PAN card number and uses it to apply for a loan in your name without you knowing.
   - **Business Email Compromise (BEC):** Here, criminals pretend to be a senior person in a company (like the CEO) or a trusted business partner, sending emails to employees to trick them into sending money to wrong bank accounts.
   - *Example:* An accountant receives an urgent email, seemingly from the CEO, asking them to immediately transfer a large sum of money to a new vendor account, which is actually controlled by the criminals.
   - **Net Banking/ATM Frauds:** This includes tricks like putting a device on an ATM to steal card details (skimming) or getting your online banking login through fake calls (vishing) or malware.
   - *Example:* You use an ATM, and a hidden device copies your card details and PIN, which criminals then use to withdraw money from your account.
   - **Online Transaction and Investment Scams:** These are schemes where criminals promise huge returns on fake investments (like in cryptocurrency) or ask for money for non-existent lottery winnings or goods you ordered online but never receive.
   - *Example:* You see an ad for a cryptocurrency investment promising double your money in a week. You invest, but the platform disappears, and your money is gone.
   - **Loan and Job Frauds:** Criminals offer easy loans or fantastic job opportunities, but first, they ask you to pay "processing fees" or "security deposits," which they take without providing any actual loan or job.
   - *Example:* You're offered a dream job overseas, but to get it, you're told to pay a "visa processing fee" to a specific bank account, and then you never hear back.

2. **Crimes Against Data and Computer Systems:**
   - **Hacking:** This is when someone gets into your computer, phone, or network without your permission. They might just look around, or they might try to steal data or cause damage.
   - *Example:* An unauthorized person breaks into a company's computer network to access confidential customer information.

- **Data Theft:** This is the act of illegally copying, taking, or deleting important digital information, like company secrets, customer lists, or personal records.
- *Example:* An employee secretly copies the entire client database of their company before leaving to join a competitor.
- **Ransomware Attacks:** This is a type of harmful software that locks up your computer files or your entire system. The criminals then demand money (a "ransom"), usually in cryptocurrency, to give you the key to unlock your files.
- *Example:* All your photos and documents on your computer suddenly become unopenable, and a message pops up demanding money to unlock them.
- **Malware Distribution (Viruses, Worms, Trojans):** This involves creating and spreading harmful software. **Viruses** attach to programs, **worms** spread themselves through networks, and **Trojans** pretend to be useful programs but secretly cause harm.
- *Example:* You download a free game, but it's actually a Trojan that secretly installs spyware on your computer to steal your passwords.

3. **Crimes Involving Content and Online Harassment:**
   - **Publishing/Transmitting Obscene Material:** This covers the illegal sharing of indecent or sexually explicit content, especially child pornography, which has very strict laws and severe punishments.
   - *Example:* Someone shares a private, inappropriate video of another person online without their permission.
   - **Cyberstalking:** This is when someone repeatedly uses the internet or digital messages to harass, threaten, or follow another person, often causing them fear or distress.
   - *Example:* A person constantly sends threatening messages and posts false rumors about someone on social media, making them feel unsafe.
   - **Cyberbullying:** This is when someone uses electronic communication (like social media or messaging apps) to bully, intimidate, or upset another person, often teenagers.
   - *Example:* A group of students repeatedly posts embarrassing photos and mean comments about a classmate on a public social media group.

4. **Attacks on Systems and Networks:**
   - **Distributed Denial of Service (DDoS) Attacks:** This is like sending a huge flood of internet traffic from many different computers to a website or online service. The goal is to overwhelm it so it crashes and normal users can't access it.
   - *Example:* A popular online shopping website suddenly becomes unavailable because millions of fake requests hit its servers all at once, overwhelming it.
   - **Web Defacement:** This is a form of digital vandalism where hackers change the look of a website without permission, often to display their own messages or images.
   - *Example:* A hacker changes the homepage of a government website to display a political message or a humorous image.
   - **Cyber Terrorism:** This involves using computer systems to cause major disruption, fear, or violence, often targeting important computer systems like power grids or banking networks, for political or ideological reasons.
   - *Example:* A group tries to hack into a country's power grid to cause a widespread blackout and create panic.

How Cybercriminals Operate: Their Methods

Cybercriminals are always finding new ways to trick people and systems. Here are some key methods I learned about:

1. **Tricking People (Social Engineering):**
   - **Spear Phishing:** Unlike general phishing, this is a very targeted attack where the criminal researches a specific person or company to make their fake emails or messages seem incredibly real and personal.
   - *Example:* An employee receives an email that appears to be from their HR department, mentioning their recent appraisal and asking them to click a link to view details, but the link leads to a fake login page.
   - **Pretexting:** The criminal creates a fake story or situation (a "pretext") to get information from you. They might pretend to be someone important, like an IT support person or a bank manager.
   - *Example:* Someone calls you pretending to be from your bank's fraud department, saying they've detected suspicious activity and need your full card number to "verify" your identity.
   - **Baiting:** This involves leaving something tempting (like a free USB stick labeled "Company Payroll Data" in a public place) that, when used, infects your computer with malware.
   - *Example:* An employee finds a USB drive in the office parking lot, plugs it into their work computer out of curiosity, and unknowingly infects the company network.

2. **Exploiting System Weaknesses (Technical Vulnerabilities):**
   - **Malware Injection:** This means secretly putting harmful software (like viruses that damage files, spyware that watches what you do, or keyloggers that record your typing) onto your computer through infected downloads, email attachments, or bad websites.
   - *Example:* You download a free software program from an untrusted website, and it secretly installs a keylogger that records all your passwords as you type them.
   - **Exploiting Software/System Flaws:** Attackers look for security holes (like un-updated software or weak settings) in operating systems, apps, or websites. They then use these flaws to get in without permission or run their own harmful code.
   - *Example:* A company's old web server has a known security flaw. A hacker finds this flaw and uses it to gain control of the server and steal data.
   - **Brute-Force and Dictionary Attacks:** These are automated attempts to guess your passwords. "Brute-force" tries every possible combination, while "dictionary attacks" use lists of common words and phrases as passwords.
   - *Example:* A hacker uses a program that rapidly tries thousands of common passwords like "password123" or "qwerty" to break into an online account.
   - **SQL Injection (SQLi):** This is a trick used on websites where criminals put special code into input boxes (like search bars). If the website isn't secure, this code can trick the website's database into revealing sensitive information or letting the criminal take control.
   - *Example:* A hacker types a specific code into a website's login field. If the website is vulnerable, it might accidentally show them all the usernames and passwords stored in its database.
   - **Man-in-the-Middle (MITM) Attacks:** In this attack, the criminal secretly puts themselves between you and the website or service you're trying to connect to (often on public Wi-Fi). They can then listen in, steal your login details, or change the information you're sending without you knowing.

- *Example:* You connect to free public Wi-Fi at a café. A criminal on the same network intercepts your connection to your banking app, stealing your login details.

3. **Large-Scale Operations and Data Usage:**
   - **Botnets:** This is like an army of infected computers (called "bots") that criminals secretly control. They use this network to send huge amounts of spam, launch massive DDoS attacks, or even mine cryptocurrency, all from a hidden central computer.
   - *Example:* A criminal controls a botnet of thousands of infected home computers. They use this botnet to launch a massive DDoS attack that takes down a major company's website.
   - **Dark Web Operations:** The Dark Web is a hidden part of the internet where people can be anonymous. Criminals use it to buy and sell stolen personal data (like credit card numbers or IDs), exchange hacking tools, or communicate securely for their illegal businesses.
   - *Example:* After a company data breach, the stolen customer credit card numbers are sold in bulk on a hidden marketplace on the Dark Web.
   - **Cryptojacking:** This is when a criminal secretly uses your computer's power to mine cryptocurrency (like Bitcoin) without your permission. It makes your computer slow down and use more electricity.
   - *Example:* You visit a seemingly normal website, but in the background, without your knowledge, it uses your computer's processing power to mine cryptocurrency for the website owner, slowing your computer down.

Understanding Victim Profiling: How Cybercriminals Pick Their Targets

Victim profiling in cybercrime investigation is a clever way to figure out *why* certain people or organizations become targets. It's like putting together a puzzle to understand the victim's habits, weaknesses, and online behavior to see how criminals might have chosen them.

1. **Finding Weaknesses in Victims:**
   - **Lack of Online Smartness:** Victims often don't know enough about how to stay safe online. They might fall for simple tricks, use weak passwords, or click on suspicious links without thinking.
   - *Example:* An elderly person who isn't very familiar with technology might easily believe a fake pop-up message saying their computer has a virus and calling a fake support number.
   - **Online Habits:** People who share too much personal information on social media, click on every ad, download software from unofficial places, or visit risky websites are more likely to be targeted.
   - *Example:* Someone frequently posts details about their vacation plans on social media, making their home an easy target for burglars who track their online activity.
   - **Personal Situations:** Criminals often target people based on their age (e.g., elderly people for lottery scams), financial situation (e.g., those looking for quick money for investment scams), or emotional state (e.g., lonely individuals for romance scams).
   - *Example:* A lonely individual seeking companionship online is targeted by a scammer who builds a fake romantic relationship over months, eventually asking for money for a fabricated emergency.
   - **Company Weaknesses:** For businesses, vulnerabilities might include using old software, not updating systems, having weak security on their networks, or employees who aren't trained on cybersecurity.
   - *Example:* A small business still uses an outdated email system that has a known security flaw, making it easy for hackers to break into their email accounts.

2. **How Criminals Choose Their Targets:**
   - **Using Public Information (OSINT):** Criminals are like detectives. They scour public sources like social media profiles, company websites, and online news to find out details about potential victims' interests and habits. This helps them create very convincing fake messages.
   - *Example:* A criminal finds out on LinkedIn that an employee just got promoted. They then send a highly personalized "congratulations" email with a malicious link, knowing the employee is more likely to open it.
   - **Buying Stolen Information:** Details from past data breaches (like lists of emails and passwords) are often sold on hidden parts of the internet. Criminals use these lists to try to log into other accounts where people might use the same password.
   - *Example:* A list of email addresses and passwords from a hacked online forum is sold. Criminals then try to use these same email and password combinations to log into people's banking or shopping accounts.
   - **Automated Scanning:** For technical attacks, criminals use special programs that automatically scan thousands of computers on the internet looking for common weaknesses, like open doors in a network or outdated software.
   - *Example:* A hacker runs a tool that scans millions of computers on the internet, looking for specific software that has a known security hole. When it finds a computer with that flaw, it's marked as a potential target.

- **Targeted Research for Big Scams:** In advanced scams like Business Email Compromise, criminals do deep research into a company's structure and how money is usually transferred. This allows them to perfectly imitate a boss or a supplier.
- *Example:* A criminal studies a company's financial reports and internal communication for weeks to learn who approves payments and how the payment process works, before sending a very convincing fake invoice.

Handling Digital Evidence: The Core of Investigations

For any court case, showing reliable evidence is key. In cybercrime, digital evidence (like files on a computer or messages on a phone) is very delicate and can be easily changed or destroyed. So, handling it correctly is super important to make sure it can be used in court. I learned about these strict steps:

1. **Finding the Evidence (Identification):** This first step is about spotting where digital evidence might be. It could be on computers, laptops, phones, company servers, cloud storage, or even smart home devices.

2. *Example:* After a ransomware attack, investigators identify the affected office computers, network servers, and backup drives as potential sources of digital evidence.

3. **Collecting the Evidence Carefully:** Once found, digital evidence must be gathered without changing it.
   - **Live Data:** If a computer is still running, investigators might first collect temporary information like what programs are open or what's in the computer's memory, as this disappears when the computer is turned off.
   - **Making Copies:** The most important rule is to make an exact, perfect copy (called a "forensic image") of any storage device, like a hard drive. All analysis is then done on this copy, leaving the original untouched. Special tools are used.
   - **Tracking History:** Every step – who handled the evidence, when, and why – must be written down. This "chain of custody" proves the evidence hasn't been tampered with.
   - **Safe Packing:** Evidence is placed in special bags and secure boxes, then transported safely to a forensics lab.
   - *Example:* After seizing a suspect's laptop, a forensic expert uses a special device to create an exact digital copy of the hard drive. They then get a unique "hash" code for both the original and the copy to prove they are identical.

4. **Keeping the Evidence Safe (Preservation):** This part makes sure the digital evidence stays exactly as it was when collected.
   - **Unique Codes (Hashing):** Like a digital fingerprint, a unique code (called a hash) is generated for the original evidence and its copy. If these codes match later, it confirms the evidence hasn't been changed.
   - **Write Blockers:** These are tools that stop anyone from accidentally or deliberately writing new information onto the original evidence.
   - **Secure Storage:** All digital evidence is kept in safe, climate-controlled rooms with limited access.
   - *Example:* The digital copy of the laptop's hard drive is stored in a locked room, and its hash code is regularly checked to make sure it hasn't been altered.

5. **Analyzing the Evidence (Analysis):** This is where experts examine the copied digital data to find important information and figure out what happened.
   - **Looking at Files:** Experts examine how files are organized, recover deleted files, and check details like when a file was created.
   - **Internet Activity:** They check browser history, downloaded files, and temporary internet files.
   - **Communication:** They read emails, chat messages, and social media posts.
   - **Network Activity:** They look at records of internet traffic and security alerts.

- **Malware Study:** If there's harmful software, they study it in a safe environment to understand how it works.
- **Timeline Building:** They put together all the time-stamped digital pieces to create a clear timeline of events.
- *Example:* During analysis, deleted chat messages between the suspect and another person are found on the laptop, showing a plan to defraud a victim.

6. **Writing the Report:** Every step, finding, and decision is written down carefully. This detailed report explains how the investigation was done, what was found, and what conclusions were reached. This report is then used in court.

Cyber Law: The Rules for Digital Justice

My internship helped me understand the laws that fight cybercrime in India, mainly the **Information Technology Act, 2000 (IT Act)**. I also learned how general laws like the Indian Penal Code (IPC) and the Indian Evidence Act are used together with the IT Act.

1. **The Information Technology Act, 2000 (IT Act):** This is the main law for cybercrime. Some important sections include:
   - **Section 43 (Penalty for damage to computer etc.):** Deals with penalties if someone illegally accesses a computer, causes damage, messes with data, or disrupts services.
   - *Example:* If someone uses a virus to damage a company's computer system, they can be penalized under this section.
   - **Section 66 (Computer Related Offenses):** Specifically punishes hacking and related dishonest acts that cause harm or illegal gain.
   - *Example:* A person gains unauthorized access to a social media account and posts offensive content.
   - **Section 66C (Identity Theft):** Punishes stealing someone's digital identity, like their password or digital signature.
   - *Example:* A criminal steals your email password and uses it to send fake emails pretending to be you.
   - **Section 66D (Cheating by Personation):** Punishes cheating by pretending to be someone else online.
   - *Example:* Someone creates a fake social media profile using another person's photos and details to trick others.
   - **Section 66E (Privacy Violation):** Addresses publishing or sharing private images of someone without their permission.
   - *Example:* A person secretly records a video of someone in a private space and shares it online.
   - **Section 66F (Cyber Terrorism):** Punishes serious acts of cyber-terrorism that threaten India's safety or cause major disruption to important systems.
   - *Example:* A group tries to hack into a country's air traffic control system to cause chaos.
   - **Section 67 (Obscene Material):** Punishes sharing obscene or indecent material online.
   - **Section 67B (Child Pornography):** Deals with very severe punishments for sharing content involving child sexual abuse.
   - **Section 80 (Police Power):** Gives police officers (Inspector rank or above) the power to search public places and arrest people without a warrant if they suspect an IT Act offense.

2. **Indian Penal Code (IPC):** Many traditional crimes listed in the IPC can also be committed in the cyber domain. For instance:
   - **Section 420 (Cheating):** Used in many online financial frauds, like fake lottery or investment scams.

3. **Indian Evidence Act, 1872:** This law sets the rules for using electronic records (like emails or digital photos) as evidence in court, making sure they are real and haven't been changed.

How Law Enforcement Investigates Cybercrimes: Step-by-Step Procedures

Investigating cybercrimes is a complex process because digital clues can disappear quickly and criminals can be anywhere in the world. My internship showed me the detailed steps the Cyber Crime Police Station follows:

1. **Getting the Complaint and Initial Check:**
   - **Reporting:** It starts when a victim reports a cybercrime, giving all the details.
   - **First Look:** The police first check the complaint to see if it's a real crime and if it falls under their area. They talk to the victim and get any initial digital clues (like screenshots).
   - **Official Start (FIR):** If it's a serious crime, an official report (FIR - First Information Report) is made, which officially starts the investigation.
   - *Example:* A person loses 50,000 in an online fraud. They file a complaint, which the police verify and then register an FIR to begin the investigation.

2. **Starting the Investigation and Seizing Evidence:**
   - **Officer in Charge:** The case is given to a specially trained officer.
   - **On-Site Response:** For big company hacks, a special team might go to the location to collect digital clues right away before they are lost.
   - **Getting Legal Permission:** The officer gets legal papers (like search warrants) to legally take computers, phones, or access cloud data.
   - **Copying Evidence:** They make perfect copies of digital devices, ensuring no changes are made to the originals, which are carefully sealed and tracked.
   - *Example:* The investigating officer gets a court order to seize the suspect's phone and computer. They use specialized tools to create exact, verified copies of all data before analyzing it.

3. **Analyzing Digital Evidence and Gathering Information:**
   - **Lab Work:** Seized devices go to a special lab where experts use advanced software to look at the copied data.
   - **Finding Hidden Data:** They recover deleted files, check computer logs, internet history, emails, chat messages, and social media activity to piece together what happened.
   - **Network Checks:** They examine internet traffic records and security alerts to find out how an attack happened or if data was stolen.
   - **Studying Harmful Software:** If malware is involved, they study it in a safe environment to understand how it works and who created it.
   - **Online Research (OSINT):** Investigators use publicly available information from social media, news, and other websites to find clues about suspects or the crime.
   - **Tracing Digital Clues:** They use techniques like tracking IP addresses, checking who owns websites, and following cryptocurrency transactions to find the source of the attack and the criminals.
   - **Talking to People:** They interview victims, witnesses, and suspects to get more information.
   - *Example:* Forensic experts analyze the suspect's computer, recover deleted emails showing their communication with other scammers, and trace the IP address used for the fraud to a specific location.

4. **Connecting the Dots and Taking Action:**

- **Putting Pieces Together:** All the digital and non-digital evidence is carefully linked to build a strong case, showing the connection between the criminal, the victim, and the crime.
- **Forensic Report:** A detailed report is written explaining how the digital investigation was done, what was found, and the conclusions, all ready to be used in court.
- **Legal Check:** Lawyers review the evidence and report to make sure everything follows the law.
- **Arrest and Charges:** If there's enough evidence, suspects are arrested, and a formal accusation (charge-sheet) is filed in court.
- **Court:** The officer and experts might have to explain their findings in court.
- **Teamwork:** Because cybercrime often crosses borders, police work closely with other police forces, international agencies, and cybersecurity companies to catch criminals.
- *Example:* The collected evidence, including the recovered emails and IP tracing results, is compiled into a detailed forensic report, which is then submitted to the court, leading to the suspect's arrest and subsequent trial.

Conclusion: A Transformative Learning Journey

This extensive internship at the Cyber Crime Police Station, Vijayawada, has been an incredibly valuable and eye-opening experience for me. It wasn't just about learning theories; I got to see firsthand the real challenges and detailed steps involved in fighting cybercrime. Learning about the different types of cyber offenses, the clever methods criminals use, the crucial process of handling digital evidence, the specific laws governing cyber activities, and the careful procedures police follow has greatly expanded my knowledge and improved my analytical skills.

This experience has truly solidified my interest in cybersecurity and law enforcement. It has made me even more determined to work in a field where I can help protect people from online dangers and contribute to justice in the digital world. I am very thankful to the Andhra Pradesh Police and the dedicated team at the Cyber Crime Police Station, Vijayawada, for giving me such a thorough and insightful learning opportunity that will be a strong foundation for my future career.

Reference:

Internship Certificate from Cyber Crime Police Station, Vijayawada (uploaded:CYBERCELLVJA.pdf)