# Project Report on ELP (Experiential Learning Programme) on Cyber Security


**Name:** Ghausiya Bashir

**Semester:** II

**Department**: B.Com

**College Roll No:** 57

**CU Roll No:** 241027-11-0006

**CU Registration No:** 027-1211-0131-24

**College Name:** Government Girls' General Degree College

**Supervisor Name:** Dr. Mumu Chakraborty

Programme Officer, NSS Unit-I

**Unit:** NSS

# Project Report on ELP (Experiential Learning Programme) on Cyber Security

**SUBMITTED BY:**

**Name:** Ghausiya Bashir

**Semester:** II

**Department**: B.Com

**College Roll No:** 57

**CU Roll No:** 241027-11-0006

**CU Registration No:** 027-1211-0131-24

**College Name:** Government Girls' General Degree College

**Unit:** NSS

_____

Signature of the Student

**SUBMITTED TO:**

**Supervisor Name:** Dr. Mumu Chakraborty

Programme Officer, NSS Unit-I

_____

Signature of the Student

# Report on ELP (Experiential Learning Programme) on Cyber Security

# Introduction

In today's digital age, cybersecurity has become a critical concern for individuals, organizations, and governments alike. The increasing reliance on technology and the internet has led to a rise in cyber threats, making it essential to develop effective security measures to protect sensitive information and systems. This project aims to explore the various aspects of cybersecurity, including threat analysis, vulnerability assessment, and incident response.

Through this Experiential Learning Program (ELP), I will gain hands-on experience in cybersecurity practices and tools, develop skills in identifying and mitigating potential security threats, and contribute to the development of effective security solutions. This project report documents my experiences, learnings, and findings during the internship, providing insights into the world of cybersecurity and its importance in today's digital landscape.

The Experiential Learning Programme (ELP) on Cyber Security was designed to provide hands-on experience and practical training to students in the field of cyber security. The programme aimed to equip participants with the skills and knowledge required to identify, analyze, and mitigate cyber threats.

# BACKGROUND OF THE PROJECT

The background of the project on Cybersecurity for the ELP (Experiential Learning Program) internship could include:

1. **Overview of Cybersecurity:**

Cybersecurity is a critical aspect of protecting computer systems, networks, and sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. With the increasing reliance on digital technologies, cybersecurity threats have become more sophisticated and frequent.

2. **Importance of Cybersecurity:**

The importance of cybersecurity cannot be overstated. Cyber threats can lead to financial losses, reputational damage, and compromise sensitive information. Effective cybersecurity measures are essential for individuals, organizations, and governments to safeguard their digital assets.

3. **Current Challenges:**

The cybersecurity landscape is constantly evolving, with new threats and vulnerabilities emerging regularly. Some of the current challenges include:

- Advanced persistent threats (APTs)
- Ransomware attacks
- Phishing and social engineering
- IoT security risks
- Data breaches

4. **Project Purpose:**

The purpose of this ELP project is to gain hands-on experience in cyber security practices and tools, analyze potential security threats, and develop skills in [specific skills, e.g., penetration testing, security auditing, etc.].

5. **Objectives:**

The objectives of this project are to:

- Understand the fundamentals of cyber security
- Identify and analyze potential security threats
- Develop skills in [Cyber security]
- Apply theoretical knowledge to real-world scenarios

6. **Scope:**

The scope of this project includes [specific areas of focus, e.g., network security, cloud security, etc.]. The project will involve [specific activities, e.g., research, tool usage, etc.].

# Project Objectives

Here are detailed objectives of the ELP project on Cyber security:

## Primary Objectives:

1. **Gain Hands-on Experience:** To gain practical experience in cybersecurity practices and tools, including threat analysis, vulnerability assessment, and incident response.

2. **Analyze Security Threats:** To identify and analyze potential security threats, including malware, phishing, and other types of cyber attacks.

3. **Develop Cybersecurity Skills:** To develop skills in specific areas of cybersecurity, such as penetration testing, security auditing, and security configuration.

## Secondary Objectives:

1. **Understand Cybersecurity Frameworks:** To understand and apply cybersecurity frameworks, such as NIST Cybersecurity Framework or ISO 27001.

2. **Improve Incident Response:** To develop incident response plans and procedures to effectively respond to cybersecurity incidents.

3. **Enhance Security Awareness:** To raise awareness about cybersecurity best practices and promote a culture of security within organizations.

## Specific Objectives:

1. To conduct a thorough risk assessment of a selected system or network.

2. To identify and prioritize vulnerabilities and threats.

3. To develop and implement effective security controls and countermeasures.

4. To analyze and respond to simulated cybersecurity incidents.

These objectives provide a clear direction for the project and ensure that the intern gains valuable experience and skills in cybersecurity.

# Description of project activities

## Data Collection:

1. Portal Analysis: Analyzing the existing e-Learning Portal to identify strengths, weaknesses, and areas for improvement.

2. User Feedback: Collecting feedback from users (students, teachers, administrators) to understand their needs and pain points.

3. Content Review: Reviewing existing content on the portal to ensure accuracy, relevance, and engagement.

## Data Analysis:

1. User Engagement Metrics: Analyzing metrics like page views, time spent on the portal, and user retention to understand user behavior.

2. Feedback Analysis: Analyzing user feedback to identify trends, patterns, and areas for improvement.

## Improvement Suggestions:

1. Content Enhancement: Suggesting improvements to existing content, including new topics, formats, and multimedia elements.

2. User Experience (UX) Enhancements: Recommending UX improvements to enhance navigation, accessibility, and overall user experience.

3. Feature Additions: Suggesting new features to enhance the portal's functionality and user engagement.

## Tools and Technologies:

1. Portal Development Frameworks: Familiarity with frameworks like Moodle, Drupal, or WordPress.

2. Analytics Tools: Using tools like Google Analytics to track user behavior and engagement metrics.

3. Collaboration Tools: Working with tools like Trello, Asana, or Slack to collaborate with team members.

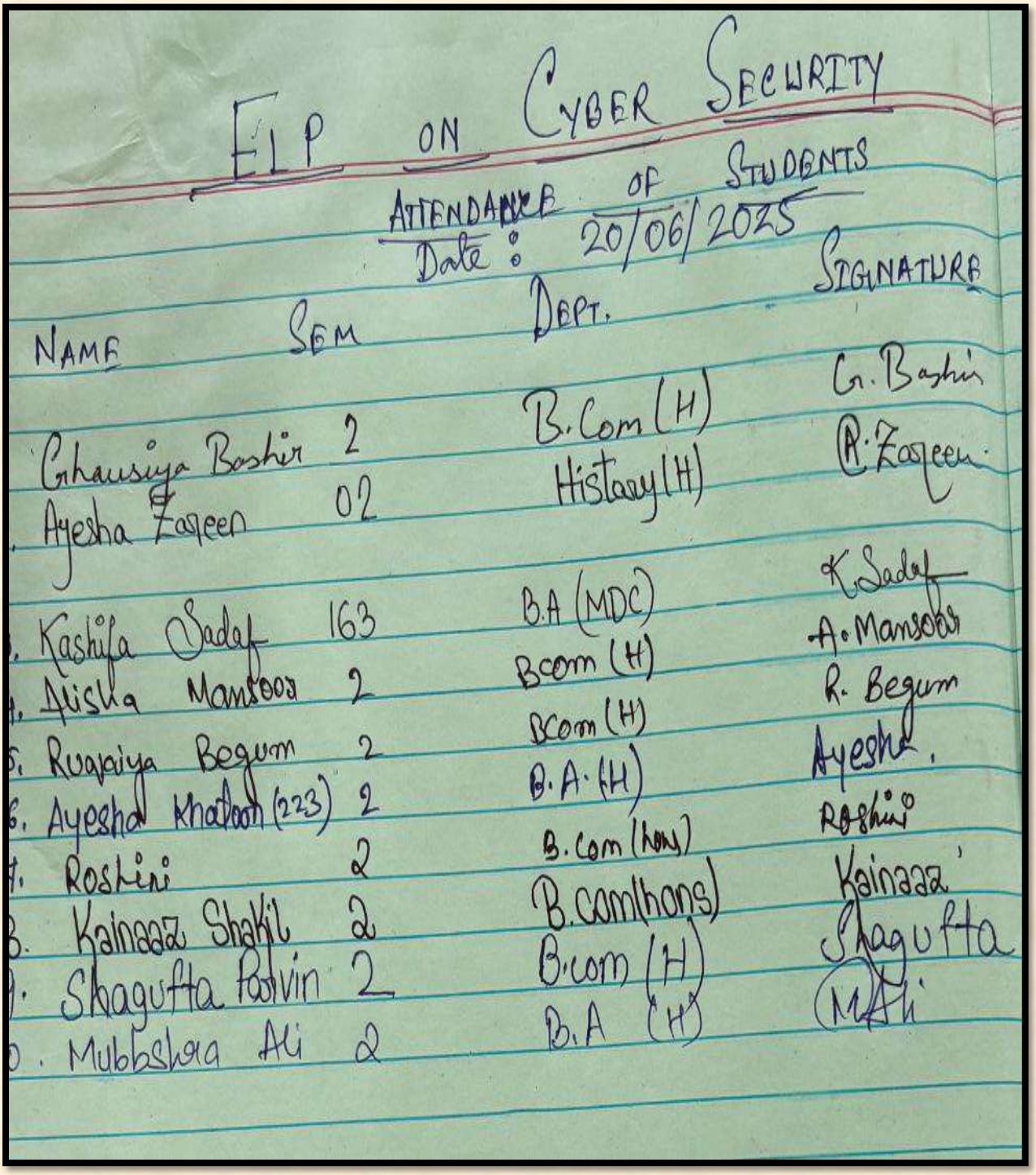
# Descriptions of the activities date wise

## Field Work

**Day 1 Date: 20.06.2025**
**Awareness Programme on Cyber Security for Senior Citizens**

It has been observed that the senior citizens are mostly attacked by hackers. Keeping this in mind, an awareness programme on cyber security was organized for senior citizens to protect them from cyber frauds. In this programme, We NSS volunteers interacted with the senior faculty members in 1:1 ratio and made them aware of all possible cyber crimes and the preventive measures. We volunteers also demonstrated how to do online shopping, net banking, online ticket booking etc. with 100% safety.
Feedback from a senior faculty member: https://youtu.be/dUosy0MbLgQ

***NSS Volunteers with a Senior Faculty Member***



# ELP ON CYBER SECURITY

ATTENDANCE OF STUDENTS

Date: 20/06/2025

| NAME | SEM | DEPT. | SIGNATURE |
|---|---|---|---|
| Ghausiya Bashir | 2 | B.Com (H) | G. Bashir |
| Ayesha Zaqeen | 02 | History (H) | A. Zaqeen |
| Kashifa Sadaf | 163 | B.A (MDC) | K. Sadaf |
| Alisha Mansoor | 2 | Bcom (H) | A. Mansoor |
| Rupaiya Begum | 2 | Bcom (H) | R. Begum |
| Ayesha Khatoon (223) | 2 | B.A. (H) | Ayesha. |
| Roshini | 2 | B.Com (hons) | Roshini |
| Kainaaz Shakil | 2 | B.Com(hons) | Kainaaz |
| Shagufta Parvin | 2 | B.Com (H) | Shagufta |
| Mubbshra Ali | 2 | B.A (H) | M Ali |

***Attendance sheet***

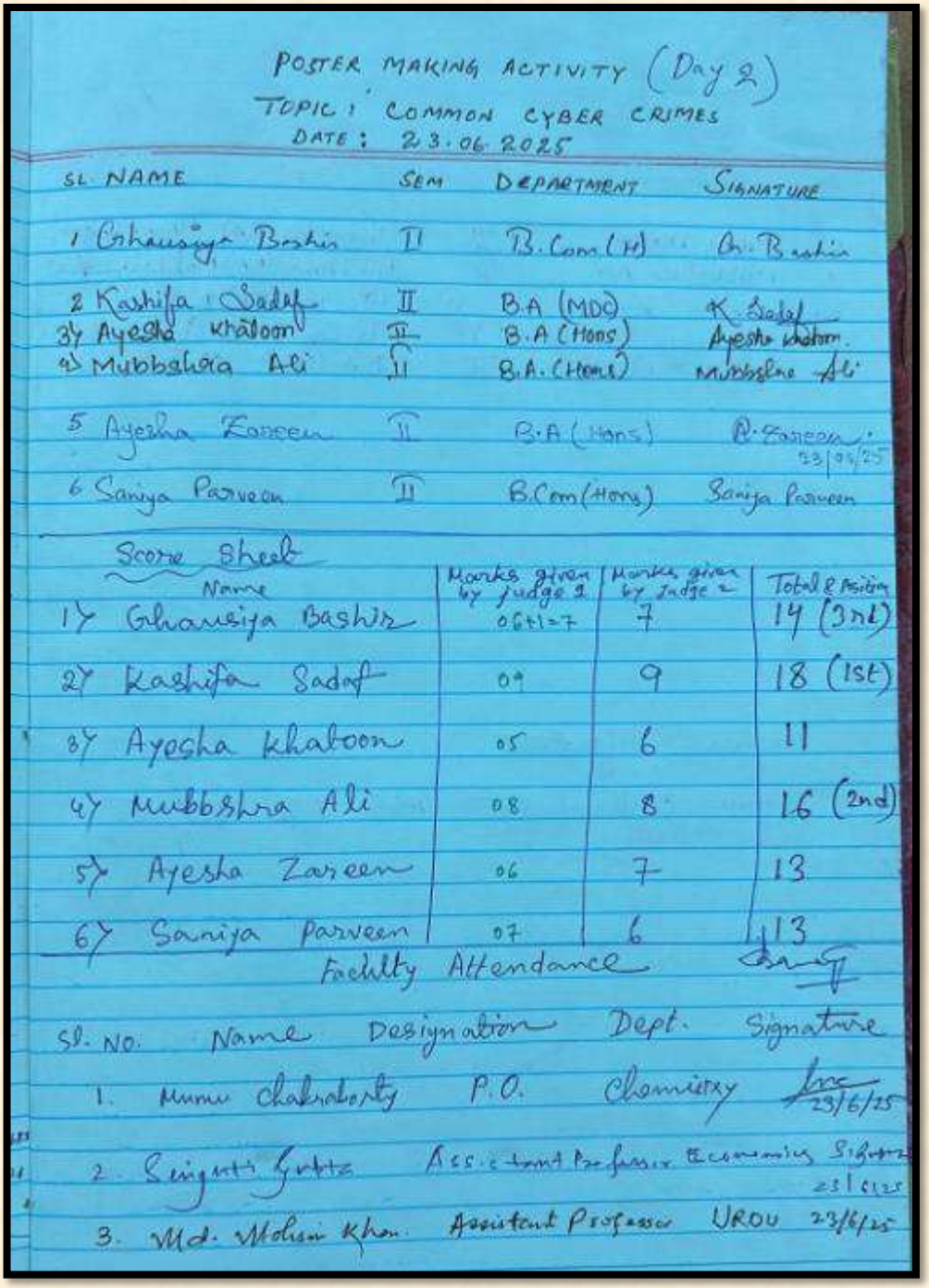
**Day 2 Date: 23.06.2025**

**Poster Competition on 'Common Cyber Crimes'**

A poster competition on the topic 'Common cyber crimes' was organized on 23rd June, 2025. The posters were judged by the Principal and IQAC coordinator of the college. This was a field based activity with weightage 8. Me and my friends Volunteers participated in this event with great enthusiasm and prepared some excellent posters on cyber crime. By this activity, We also came to know about the common cyber crimes in India and will definitely stay alert from these.




Evaluation of the posters by the Principal and IQAC Coordinator of the college



POSTER MAKING ACTIVITY (Day 2)

TOPIC : COMMON CYBER CRIMES

DATE : 23.06.2025

| SL | NAME | SEM | DEPARTMENT | SIGNATURE |
|---|---|---|---|---|
| 1 | Ghaniya Bashir | II | B.Com (H) | G. Bashir |
| 2 | Kashifa Sadaf | II | B.A (MDC) | K. Sadaf |
| 3 | Ayesha khatoon | II | B.A (Hons) | Ayesha khatoon. |
| 4 | Mubbshra Ali | II | B.A. (Hons) | Mubbshra Ali |
| 5 | Ayesha Zareen | II | B.A (Hons) | A. Zareen. 23/06/25 |
| 6 | Saniya Parveen | II | B.Com (Hons) | Saniya Parveen |

Score Sheet

| Name | Marks given by judge 1 | Marks given by judge 2 | Total & Position |
|---|---|---|---|
| 1) Ghaniya Bashir | 06+1=7 | 7 | 14 (3rd) |
| 2) Kashifa Sadaf | 09 | 9 | 18 (1st) |
| 3) Ayesha khatoon | 05 | 6 | 11 |
| 4) Mubbshra Ali | 08 | 8 | 16 (2nd) |
| 5) Ayesha Zareen | 06 | 7 | 13 |
| 6) Saniya Parveen | 07 | 6 | 13 |

Faculty Attendance

| Sl. NO. | Name | Designation | Dept. | Signature |
|---|---|---|---|---|
| 1. | Mumu Chakraborty | P.O. | Chemistry | 23/6/25 |
| 2. | Sangita Gupta | Assistant Professor | Economics | 23/6/25 |
| 3. | Md. Mohsin Khan | Assistant Professor | URDU | 23/6/25 |

***Attendance sheet and result of poster competition***

## Day 3 Date: 24.06.2025
## Digital leaflet making activity on cyber security

On the third day of the fifteen-day-long ELP We volunteers prepared digital leaflets on cyber crime and its prevention. Also we were taught on how to submit the tasks in My Bharat portal after its completion. Any doubt related to the portal and ELP were also addressed on this day.


***Making Digital leaflet on cyber security***

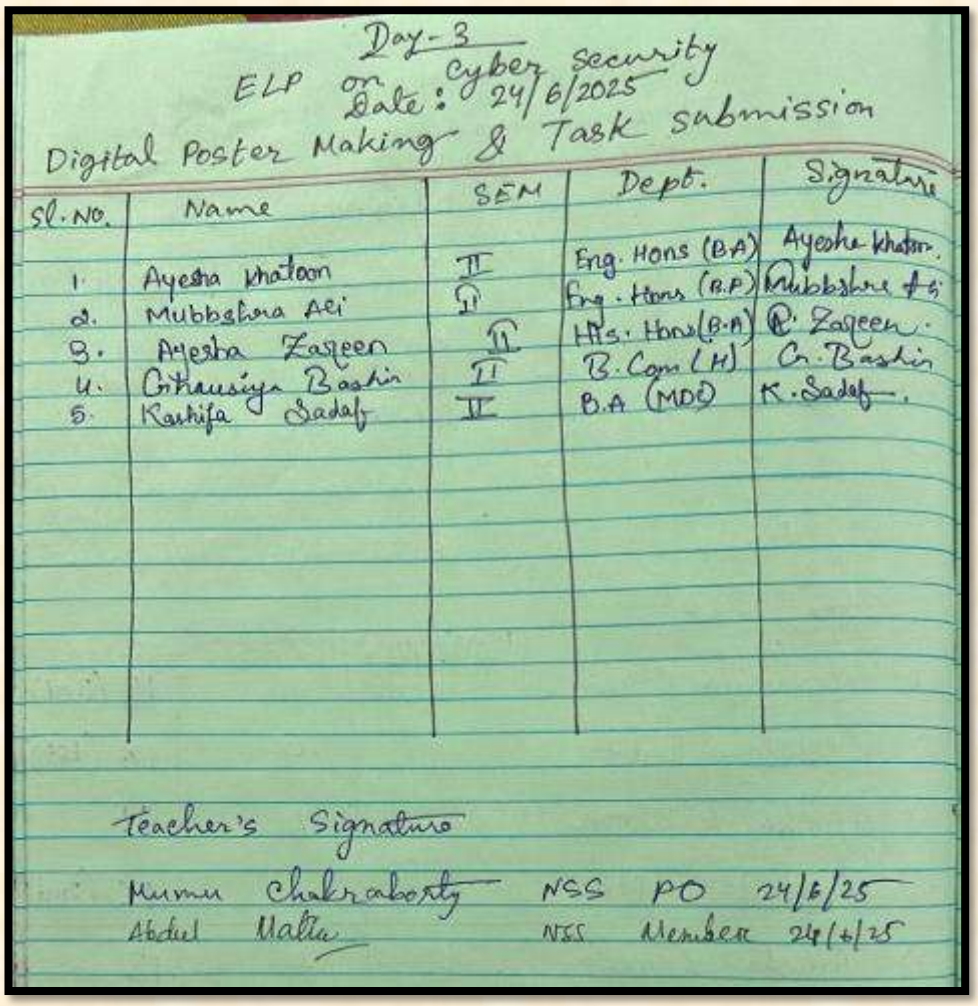

Designed by nss(unit 1)
Government Girl's General Degree College
Volunteer:AYESHA ZAREEN
Dept:History (hons)
Are you SAFE??
In digital world
△HACKED SOCIAL ACCOUNT
△MISUSE OF YOUR PERSONAL INFORMATION
△HACKERS USE SPYWARE TO SECRETLY ACCES YOUR CAMERA,
OR MESSAGES.
△SEND FAKE EMAIL/LINK TO STEAL PASSWORD.
△LOCK YOUR FILE & DEMANDING TO UNBLOCK
△FAKE JOB SCAMS.
ONE WRONG STEP CAN LEAD TO CYBER TRAP
Your awareness can be someone else's protection
«SHARE, SPEAK, SECURE»


CYBER CRIME SAFETY
THINK BEFORE YOU CLICK BECAUSE ONE WRONG MOVE CAN COST EVERYTHING
Don't get caught in the web – stay cyber smart
Hackers don't need a door when you leave a window open
HERE ARE SOME SAFETY TIPS
• Use strong, unique passwords
• Enable 2FA (Two-Factor Authentication)
• Think before you click
• Keep software updated
• Avoid public Wi-Fi for banking
• Back up your data
• Don't overshare online
• Check accounts regularly
• Use antivirus protection
• Stay informed, stay safe
THINK BEFORE YOU CLICK
DESIGNED BY – NSS UNIT-I
GOVERNMENT GIRL'S GENERAL DEGREE COLLEGE
NAME OF THE VOLENTEER: KASHIFA SADAF
DEPARTMENT: B.A. ( MDC)


CYBER SECURITY
Be aware be safe
Designed by NSS UNIT – I
Govt. Girls' General Degree College
Name of the volunteer:-
Ghausiya Bashir
Dept:- B com


Cyber security
Design by NSS unit -1
Govt.Girls' General Degree College
Name of the volenteer:- Ayesha Khatoon
Dept: English honours
Roll No: 223
Awareness
• Cyber security is everyone's responsibility, not just for the IT professionals.
• In today's digital world, cyber threats are constantly evolving. Stay informed .
• Be cautious about what you download and where you click online.
• Educate yourself and others about cyber security best practices.
DON'T GET HOOKED!
Think Before You Click.
Tackling cyber crime
"Be aware of the security settings on your social media and mobile devices."
CYBER CRIME: 'WE'RE ALL TARGETS'
Cyber attack
NATIONAL CYBER SECURITY AWARENESS MONTH


STAY SAFE FROM CYBER CRIME
Cybercrime awareness – Part 1
"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it"!
Everybody should be aware that we have the cyber tools necessary to investigate cyber crimes, and to be prepared to defend against them to bring people to justice who commit it!
Insure against cyber attacks: Experts
The dark side of internet: Cybercrime against women
"Every women deserves to be safe online. Let's challenge cyber crimes and promote digital equality".
Designed by NSS UNIT–I
Govt. Girls' General Degree College
Name of the volunteer:- Mubbshra Ali
Dept:- English Honours



Day-3

ELP on Cyber security

Date: 24/6/2025

Digital Poster Making & Task submission

| Sl. No. | Name | SEM | Dept. | Signature |
|---|---|---|---|---|
| 1. | Ayesha khatoon | II | Eng. Hons (B.A) | Ayesha khatoon. |
| 2. | Mubbshira Aei | II | Eng. Hons (B.A) | Mubbshira Aei |
| 3. | Ayesha Zaqeen | II | Hist. Hons (B.A) | A. Zaqeen. |
| 4. | Ghausiya Bashir | II | B. Com (H) | G. Bashir |
| 5. | Kashifa Sadaf | II | B.A (MDC) | K. Sadaf. |

Teacher's Signature

Mumu Chakraborty NSS PO 24/6/25

Abdul Malik NSS Member 24/6/25

***Attendance of Day 3 of ELP***

**Day 4 Date: 25.06.2025**

**Awareness Programme on cyber security for the non-teaching staff**

On the fourth day of the ELP, we students visited the offices and library in the college, interacted with the non-teaching staff and made them aware about the risks of doing banking, shopping, hotel booking, tickets booking etc. in online platforms. We also discussed on how to stay safe from this new enemy called ‘Cyber Scam’.


***volunteers with non- teaching staff***



DAY – 4

ELP on Cyber Security

Date : 25-06-2025

Awarness Programm on Cyber Security for the Non-teaching Staffs

| Sl No | Name | Sem | Dept. | Signature |
|---|---|---|---|---|
| 1. | Chhausiya Bashin | II | B.Com (H) | Ch. Bashin |
| 2. | Ayesha Zaheen | II | B.A (H) | A. Zaheen |
| 3. | Kashifa Sadaf | II | B.A (MDC) | K. Sadaf |
| 4 | Ayesha Khatoon | II | B.A (Hons) | Ayesha Khatoon |

Teacher's Signature

| | | | | |
|---|---|---|---|---|
| 1. | PUPA BANERJEE NEE SAMADPATI | Associate Professor | Bengali | P Banerjee |
| 2. | SUSMITA BASU | Ass. Prof. | Education | S. Basu 25/06/25 |
| 3. | Abdul Malik | Asst. Prof. | Arabic | 25/6/25 |

Non-teaching Staff

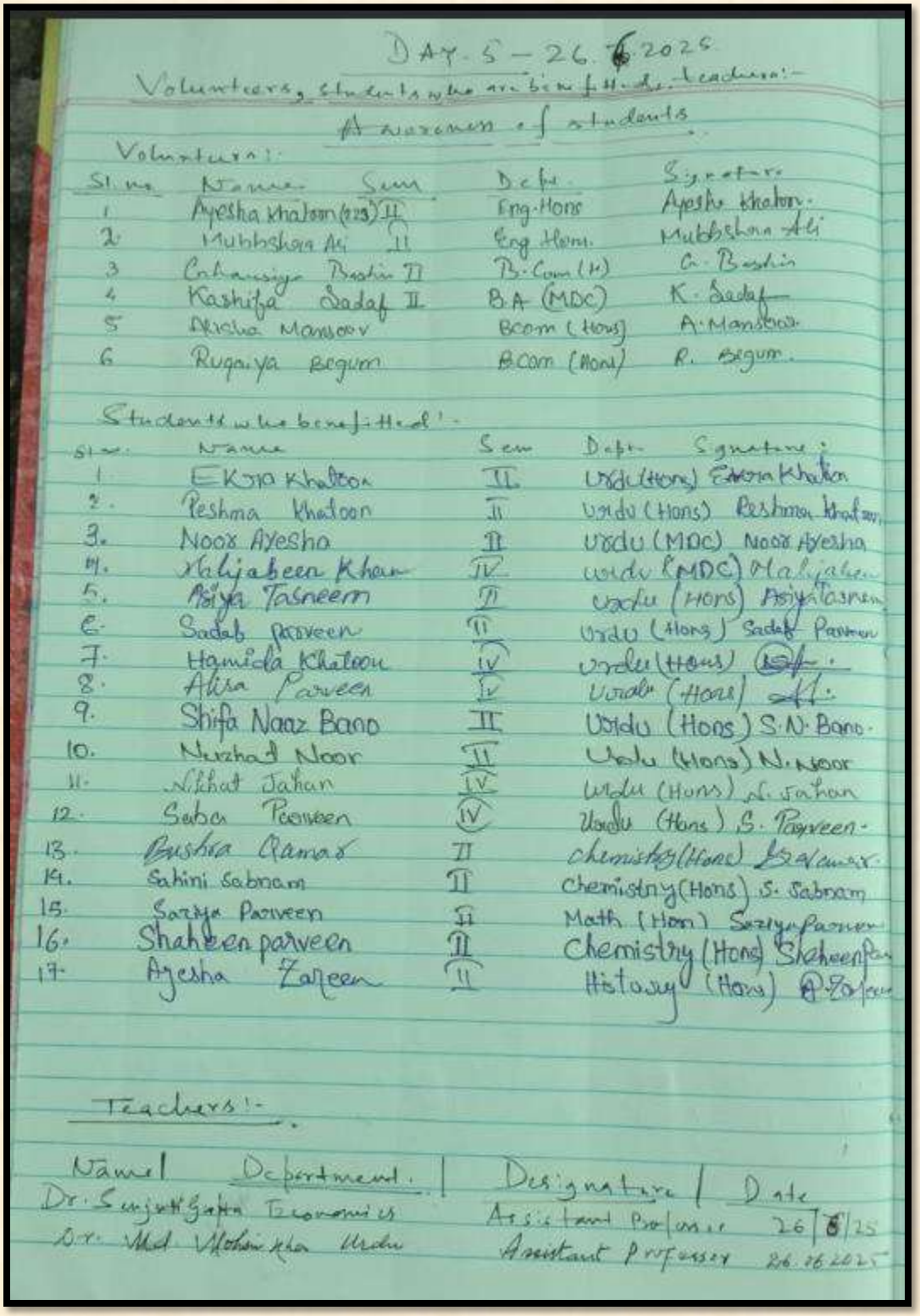
| Sl. No. | Name | Designation | Contact No. & Sign |
|---|---|---|---|
| 01. | Sovanil Roychowdhury | U.D.C. | 9836257292 25/06/25 |
| 02 | Asha kumari Shaw | Lab. Attend. | 9804828203 25.06.25 |
| 03 | Rajdip Ghosh | D.E.O. | 9038174968 |
| 04 | Sourav Hati | D.E.O | 8100989571 |
| 05 | Arup kumar Ghosh | Laboratory Attendant | 9007944539 25/06/25 |
| 06 | Kuntal Roy | L.D.C | 9749252357 |
| 07 | [illegible] | Office Peon | 9432[illegible] |
| 08 | Binoy Das | laboratory Attendant | 8537804123 |
| 09 | Putul chattopadhyay | Establishednonteaching | 9051416637 |
| 10 | Subhajit Koley | Storekeeper | SK 8013350155 |
| 11 | ARNAB GHOSH | DEO | 8906187666 |
| 12 | Amna Begum | Office Staff | 9088349229 25/06/25 |

***Attendance of volunteers, non-teaching staff and faculty members***

## Day 5 Date: 26.06.2025
## Awareness Programme for the Students of the College

On the fifth day of ELP, volunteers visited all the classrooms and laboratories of the college to make maximum number of students aware of cyber crime and cyber security. They also requested the benefited students to spread this knowledge in their locality.


***Awareness programme for the students of the college***



DAY-5 – 26.6.2025

Volunteers, students who are benefitted by the teachers:-

Awareness of students.

Volunteers:

| Sl. no. | Name | Sem | Dept. | Signature |
|---|---|---|---|---|
| 1 | Ayesha Khatoon (223) | II | Eng. Hons | Ayesha Khatoon |
| 2 | Mubbshera Ali | II | Eng. Hons. | Mubbshera Ali |
| 3 | Channiya Bastin | II | B.Com (H) | C. Bastin |
| 4 | Kashifa Sadaf | II | B.A (MDC) | K. Sadaf |
| 5 | Alesha Mansoor | | Bcom (Hons) | A. Mansoor |
| 6 | Rugaiya Begum | | Bcom (Hons) | R. Begum. |

Students who benefitted:-

| Sl no. | Name | Sem | Dept. | Signature |
|---|---|---|---|---|
| 1. | Ekra Khatoon | II | Urdu (Hons) | Ekra Khatoon |
| 2. | Peshma Khatoon | II | Urdu (Hons) | Peshma Khatoon |
| 3. | Noor Ayesha | II | Urdu (MDC) | Noor Ayesha |
| 4. | Khajabeen Khan | IV | Urdu (MDC) | Khajabeen |
| 5. | Asiya Tasneem | II | Urdu (Hons) | Asiya Tasneem |
| 6. | Sadab Parveen | II | Urdu (Hons) | Sadab Parveen |
| 7. | Hamida Khatoon | IV | Urdu (Hons) | |
| 8. | Afsa Parveen | IV | Urdu (Hons) | |
| 9. | Shifa Naaz Bano | II | Urdu (Hons) | S.N. Bano. |
| 10. | Nazhat Noor | II | Urdu (Hons) | N. Noor |
| 11. | Nikhat Jahan | IV | Urdu (Hons) | N. Jahan |
| 12. | Seba Perveen | IV | Urdu (Hons) | S. Parveen. |
| 13. | Bushra Qamar | II | Chemistry (Hons) | Bushra Qamar |
| 14. | Sahini Sabnam | II | Chemistry (Hons) | S. Sabnam |
| 15. | Sazia Parveen | II | Math (Hons) | Sazia Parveen |
| 16. | Shaheen parveen | II | Chemistry (Hons) | Shaheen Parveen |
| 17. | Ayesha Zareen | II | History (Hons) | Ayesha Zareen |

Teachers:-

| Name | Department | Designation | Date |
|---|---|---|---|
| Dr. Sanjeet Gupta | Economics | Assistant Professor | 26/6/25 |
| Dr. Md. Mohsin Khan | Urdu | Assistant Professor | 26.06.2025 |

***Attendance Day 5***

## Day 6 Date: 30.06.2025

## Door to door distribution of leaflets in cyber security in the adopted slum x

On the sixth day of ELP, we volunteers visited all the classrooms and laboratories of the college to make maximum number of people aware of cyber crime and cyber security. They also requested the benefited students to spread this knowledge in their locality

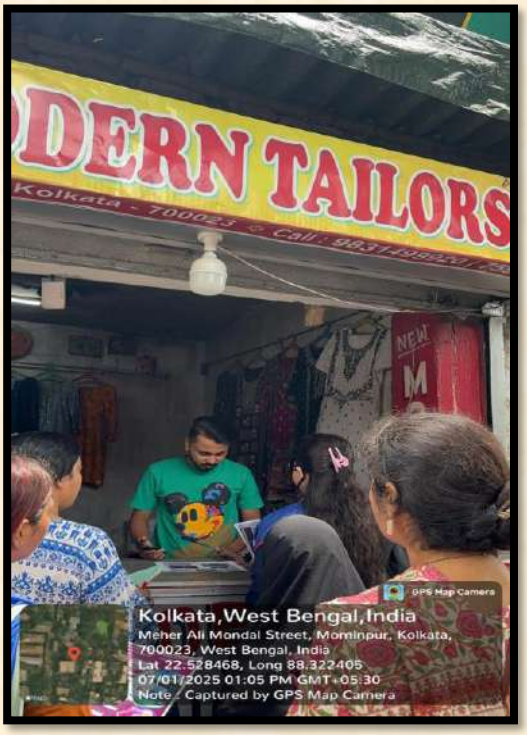


***Door to door distribution of leaflets in cyber security in the adopted slum***

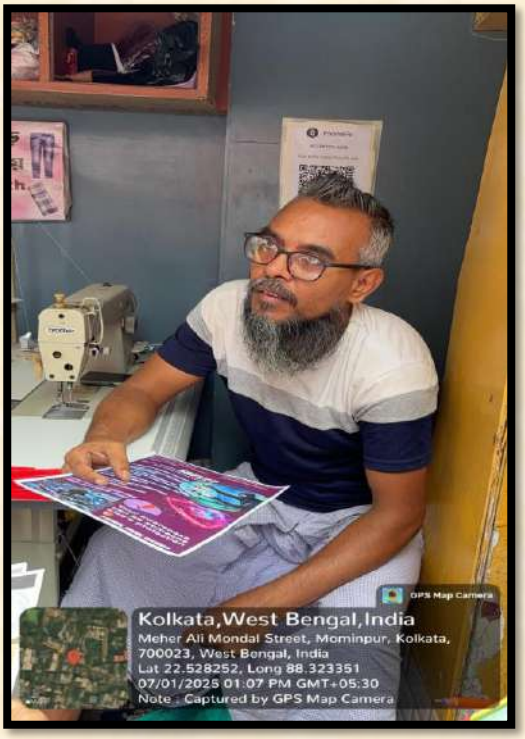
## Day 7 Date: 01.07.2025

## Campaigning programme on cyber security in nearby locality and shops of the college

- ***Distributed informative brochures and pamphlets on cyber security tips and best practices.***
- ***Conducted interactive sessions and demonstrations on:***
  - ***Password management and online safety***
  - ***Phishing and social engineering attacks***
  - ***Safe online transactions and e-commerce practices***
- ***Provided guidance on how to identify and report cyber crimes.***
- ***Engaged with the local community and college students, addressing their queries and concerns related to cyber security.***


**Campaigning programme on cyber security in nearby locality and shops of the college**



**Day 8 Date: 02.07.2025**

**Seminar on cyber security and interaction with victims of cyber crime**

The seminar provided a valuable opportunity to learn about cyber security and interact with victims of cyber crime. Key takeaways include:


## Cyber Security Insights:

**1. Threat Landscape:** Understanding the evolving threat landscape and emerging cyber threats.

**2. Best Practices:** Learning best practices for protecting personal and organizational data.

**3. Incident Response:** Understanding incident response procedures and strategies.


## Interaction with Victims:

**1. Real-Life Experiences:** Hearing from victims of cyber crime about their experiences and challenges.

**2. Emotional Impact**: Understanding the emotional impact of cyber crime on individuals and organizations.

**3. Lessons Learned:** Gaining insights from victims on how to prevent and respond to cyber crime.

## Key Learnings:

1. **Cyber Security Awareness:** The importance of cyber security awareness and education.
2. **Vigilance:** The need for vigilance in protecting personal and organizational data.
3. **Support Systems:** The importance of support systems for victims of cyber crime.

## Takeaways:

1. **Stay Informed:** Staying informed about cyber security threats and best practices.
2. **Be Proactive:** Being proactive in protecting personal and organizational data.
3. **Support Victims:** Supporting victims of cyber crime and promoting awareness about cyber security.

The seminar provided a valuable learning experience, highlighting the importance of cyber security and the impact of cyber crime on individuals and organizations.

**Day 9 Date: 03.07.2025**

**Drawing competition on cyber crime and cyber security**

The drawing competition was a creative way to raise awareness about cyber crime and cyber security. Participants expressed their understanding of cyber security concepts through art.

## Themes:

**1. Cyber Crime Awareness:** Depicting the impact of cyber crime on individuals and society.

**2. Cyber Security Measures:** Illustrating ways to protect against cyber threats.

**3. Safe Online Practices:** Showcasing safe online behaviors and habits.

## Judging Criteria:

**1. Creativity:** Originality and creativity in conveying the theme.

**2. Relevance:** Relevance of the artwork to the theme of cyber crime and cyber security.

**3. Message:** Effectiveness of the artwork in conveying a message about cyber security.

## Outcomes:

**1. Awareness:** Raised awareness about cyber crime and cyber security among participants and viewers.

**2. Creativity:** Encouraged creative thinking and expression among participants.

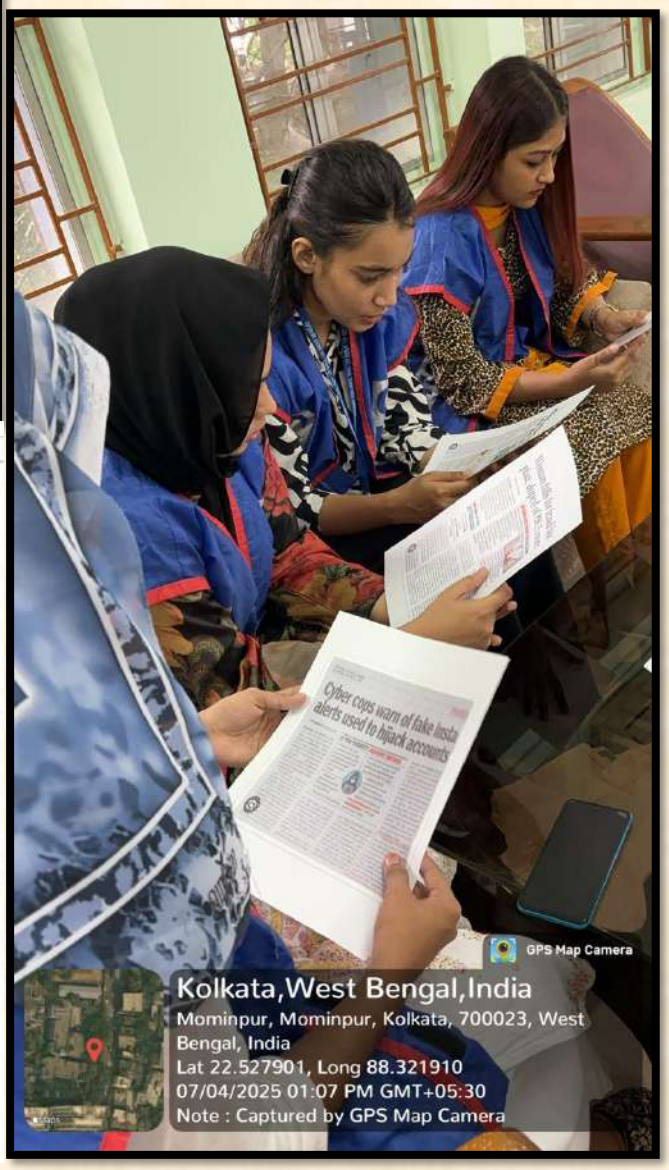
**3. Engagement:** Fostered engagement and discussion about cyber security issues.

The drawing competition was a fun and interactive way to promote cyber security awareness and creativity.

**Day 10 Date: 04.07.2025**

**Real case studies on cyber crime from newspaper**

Day 10 was about case studies on cyber crime from newspaper and make a poster from it.


THE TIMES OF INDIA, AHMEDABAD/SURAT
TUESDAY, NOVEMBER 12, 2024

TIMES

# Int'l cybercrime ring busted in Surat; 200 cases detected

## Stolen Money Sent To Dubai Via Hawala

TIMES NEWS NETWORK

**Surat:** Three months of investigation into several cyber frauds led Surat police to bust a major international cybercrime ring and detect 200 cases registered in 15 states and Union territories.

In the 24 hours ended Monday night, police arrested four members of the gang who were allegedly involved in at least 200 cybercrime FIRs lodged across the country. Police said the FIRs were lodged in 200 cases out of the total 866 complaints registered on the national cybercrime portal.

"Our investigation revealed that the gang not only executed cyber frauds but also laundered the siphoned-off money worth crores by sending it to international gangs operating from Dubai, China, Myanmar, Thailand, Indonesia, and other countries," said Anupam Singh Gahlaut, police commissioner, Surat.

Gahlaut said this is India's first detection of cyber-crime which as many as 200 FIRs registered across the country were detected in one of the various cyber frauds, including digital arrests, were registered this year alone. We detected transactions worth Rs 111 crores made from 623 bank accounts that the gang was operating," said Bhavesh Rojiya, deputy commissioner of police (crime).

Those arrested were Ajay Italiya, Vishal Tusamia, and Jalpesh Nadiyadara, apart from Hiren Barwaliya, who was nabbed at the Mumbai airport on Sunday night before he could flee to Dubai. Others on the run are Milan Vaghela and Jagdish Ajudiya, who are suspected to be in Dubai; Ketan Vekariya and Dashrath Dhandhaliya.

"Ajay Italiya, Milan Vaghela, and Ketan Vekariya are the masterminds of the scam," Rojiya added.

They would withdraw the money siphoned in different cyber frauds from these accounts and transfer money to other accounts being operated from Dubai and other countries. "After withdrawing money, it was sent to Dubai via hawala over through wallets after conversion into cryptocurrency," he explained.

In the last three months, the police raided two places in Sarthana and Mota Varachha areas of the city and booked 25 people. So far, the police seized 139 debit cards, 196 passbooks, 35 cheques, 356 SIM cards, 36 mobile phones, and 16 bank kits, apart from laptops and computers.

Looking at the scale of organised crime, police will soon invoke the stringent Gujarat Control of Terrorism and Organised Crime (GujCTOC) Act-2015 against the gang members.

The first raid was conducted outside a nationalised bank in Sarthana in which 17 people were booked, of which six were arrested.

During the investigation, the cops found out that Vaghela and Italiya were also involved as they raided their office in Mota Varachha last month and found a large number of bank accounts and transaction details from their office and computers.

### CYBER LAUNDERING

### HOW THE CROOKS OPERATED

- Gang would find poor, lower middle-class and jobless people and lure them with **money to open bank accounts**
- After assisting them in opening accounts in their preferred banks, **they would give them Rs 10,000 to Rs 15,000**
- After paying them money, **gang would take their kit including cheque book**, passbook and debit card
- International gangs would **use these accounts to receive money**
- Money was transferred from one account to another **to avoid probe and freezing**
- **The money was withdrawn mainly in Dubai** and distributed among the gang members
- Money was also **converted into cryptocurrency** and sent back to Dubai

**ILLICIT MONEY RECEIVED IN 375 ACCOUNTS:** Out of 623 bank accounts found on them, 370 were used to receive the illicit money obtained through digital arrest, task frauds, or some stock or investment frauds from different states. Out of these 370 accounts, 275 are such that they have more than one cybercrime attached to them

**200 CRIMES DETECTED:** The probe helped detect 51 cyber fraud complaints lodged in Karnataka and Telangana, 41 in Maharashtra, 18 each in Tamil Nadu and Delhi, eight in Andhra Pradesh, seven in Gujarat, six in Odisha, two each in West Bengal, Rajasthan, Punjab, Madhya Pradesh, and Chhattisgarh, and one each in Bihar and Andaman & Nicobar Islands

**ED TO BE INFORMED:** The police will appoint a special team of chartered accountants to look into transactions done by the gang members. The sheer number of bank accounts has necessitated engagement of financial experts to decipher the nature of transactions. The Enforcement Directorate, Income Tax and other agencies will also be informed. The role of some bank employees is also not being ruled out

**Day 11 Date: 07.07.2025**
**Quiz competition**

The quiz competition was a fun and engaging way to test knowledge and awareness about cyber security.


## Quiz Details:

**- Topics:** Cyber security, cyber crime, online safety, and digital literacy.

**- Format:** Multiple-choice questions.

**- Participants:** Students, professionals.

## Benefits:

**- Knowledge Assessment:** The quiz helped participants assess their knowledge and understanding of cyber security concepts.

**- Awareness:** The quiz raised awareness about cyber security threats, best practices, and online safety tips.

**- Engagement:** The quiz encouraged engagement and discussion about cyber security issues.


## Prizes:

**- Winners:** Received prizes or recognition for their performance.

**- Participation:** All participants received a certificate of participation or a similar recognition.

The quiz competition was a valuable learning experience, promoting cyber security awareness and knowledge among participants.

**Day 12 Date: 08.07.2025**
**Prepare report on ELP**

Today's day was about report for ELP. Mumu ma'am has given us format of the ELP report and explain us, about how to write the report but in online form because due to heavy rainfall sudden holiday was announced. The day was all about ELP report.

**Day 13 Date: 09.07.2025**
**Campaigning by poster**

Poster campaigning is a visual and impactful way to raise awareness about cyber security threats and promote safe online practices.


## Benefits:

**1. Visual Impact:** Posters can grab attention and convey messages effectively.

**2. Wide Reach:** Posters can be displayed in public places, schools, colleges, and workplaces.


**3. Cost-Effective:** Posters are a cost-effective way to disseminate information.

## Designing Effective Posters:

**1. Clear Message:** Ensure the message is clear, concise, and easy to understand.

**2. Eye-Catching Visuals:** Use eye-catching visuals and graphics to grab attention.

**3. Call-to-Action:** Include a call-to-action, such as visiting a website or reporting suspicious activity.

## Placement Strategies:

**1. Public Places:** Display posters in public places, such as malls, bus stations, and community centers.

**2. Educational Institutions:** Display posters in schools, colleges, and universities.

**3. Workplaces:** Display posters in workplaces, especially in industries that handle sensitive information.

## Examples of Poster Campaigns:

**1. Cyber Security Awareness:** Posters highlighting the importance of strong passwords, two-factor authentication, and safe online practices.

**2. Phishing Awareness:** Posters warning people about phishing scams and how to identify suspicious emails or messages.

**3. Online Safety:** Posters promoting online safety tips, such as being cautious when sharing personal information online.

By using posters as a campaigning tool, organizations can effectively raise awareness about cyber security threats and promote safe online practices.

**Day 14 Date: 10.07.2025**
**Online campaigning**

Online campaigning is a powerful way to raise awareness, engage audiences, and drive action on various topics, including cyber security.


## Types of Online Campaigns:

**1. Awareness Campaigns:** Educate people about cyber security threats, best practices, and online safety tips.

**2. Engagement Campaigns:** Encourage people to participate in discussions, share their experiences, and provide feedback.


**3. Call-to-Action Campaigns:** Motivate people to take specific actions, such as reporting cyber crimes or adopting secure online practices.

## Online Campaigning Channels:

**1. Social Media:** Utilize platforms like Facebook, Twitter, LinkedIn, and Instagram to reach a wide audience.

**2. Influencer Marketing:** Partner with influencers to amplify the campaign's reach and credibility.

**3. Email Marketing:** Send targeted emails to subscribers, stakeholders, or specific groups.

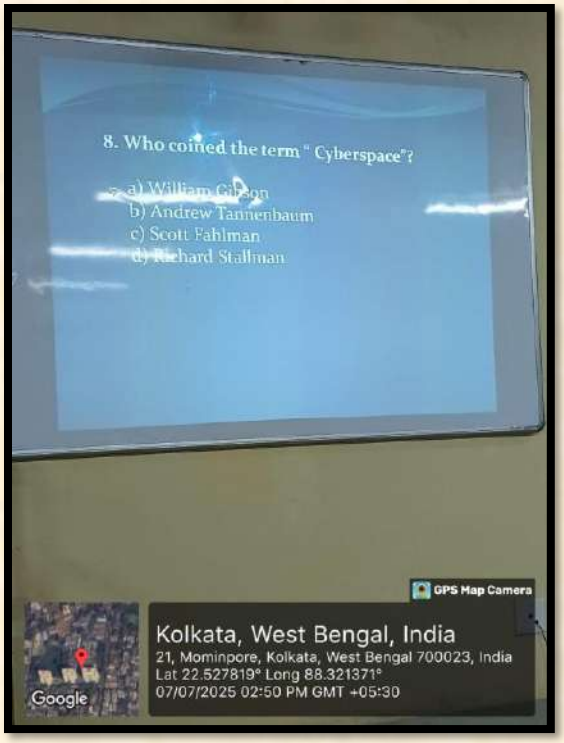
**4. Content Marketing:** Create and share valuable content, such as blog posts, videos, and infographics.

## Benefits:

**1. Increased Reach:** Online campaigns can reach a large audience, regardless of geographical location.

**2. Cost-Effective:** Online campaigns can be more cost-effective than traditional offline campaigns.

3. **Measurable Results:** Online campaigns provide measurable results, allowing for data-driven decision-making.




## Best Practices:

**1. Clear Objectives:** Define clear objectives and goals for the campaign.

**2. Targeted Audience:** Identify and target the specific audience for the campaign.

**3. Compelling Content:** Create engaging and relevant content that resonates with the audience.

**4. Continuous Monitoring:** Monitor the campaign's progress and adjust strategies as needed.

**Day 15 Date: 11.07.2025**
**Feedback and report submission**

The final day of the Experiential Learning Programme (ELP) on Cyber Security was a culmination of intense learning and hands-on experience. The day was filled with valuable feedback sessions and report submissions, marking the completion of the programme.


Key Highlights:

**- Constructive Feedback:** Participants received constructive feedback from industry experts, highlighting their strengths and areas for improvement**.**


**- Report Submission:** Participants submitted their final reports, showcasing their learning and project outcomes.

- **Peer Review:** Participants engaged in peer review sessions, sharing insights and feedback on each other's work.

## Takeaways:

**- Improved Understanding:** The feedback sessions helped participants gain a deeper understanding of their strengths and weaknesses.

**- Enhanced Reports:** The report submission process enabled participants to refine their documentation skills and present their findings effectively.

**- Networking Opportunities:** The final day provided opportunities for participants to network with peers and industry experts, fostering potential collaborations and future connections.

## Overall Experience:

The last day of the ELP on Cyber Security was a fitting conclusion to an enriching programme. The feedback and report submission process helped participants reflect on their learning, identify areas for improvement, and showcase their skills and knowledge.

# What are the learning from the internship

The internship provided valuable hands-on experience and exposure to various aspects of cyber security. Some key learnings include:

**1. Technical Skills:** Gained practical experience with cyber security tools, techniques, and technologies.

**2. Threat Analysis:** Developed skills in identifying, analyzing, and mitigating cyber threats.

**3. Collaboration and Teamwork:** Learned the importance of teamwork and collaboration in addressing cyber security challenges.

**4. Problem-Solving:** Improved problem-solving skills, particularly in responding to complex cyber security issues.

**5. Communication:** Developed effective communication skills, essential for conveying technical information to stakeholders.

## Issues Dealt With:

**1. Cyber Threats:** Identified and analyzed various types of cyber threats, including malware, phishing, and ransomware.

**2. Vulnerability Assessment:** Conducted vulnerability assessments to identify potential security weaknesses in systems and networks.

**3. Incident Response:** Developed incident response plans and procedures to respond to cyber security incidents.

**4. Data Protection:** Implemented measures to protect sensitive data and ensure compliance with data protection regulations.

**5. System Security:** Implemented security measures to protect systems and networks from cyber threats.

## Key Takeaways:

**1. Cyber Security is a Continuous Process:** Cyber security requires ongoing monitoring, evaluation, and improvement.

**2. Staying Up-to-Date:** It's essential to stay current with the latest cyber security trends, threats, and technologies.

**3. Collaboration is Key:** Collaboration between teams and stakeholders is critical in addressing cyber security challenges.

These learnings and experiences will be valuable in future endeavors, particularly in the field of cyber security.

# What are the over all learnings

The internship provided a comprehensive learning experience, equipping me with valuable skills and knowledge in:

## Technical Skills:

**1. Cyber Security Tools:** Familiarity with various cyber security tools and technologies.

**2. Threat Analysis:** Ability to identify, analyze, and mitigate cyber threats.

**3. Vulnerability Assessment:** Skills in conducting vulnerability assessments and penetration testing.

**4. Incident Response:** Knowledge of incident response procedures and best practices.

## Soft Skills:

**1. Teamwork and Collaboration:** Ability to work effectively in a team **environment.**

**2. Communication:** Improved communication skills, including technical writing and presentation.

**3. Problem-Solving:** Enhanced problem-solving skills, particularly in responding to complex cyber security issues.

**4. Time Management:** Developed time management skills, prioritizing tasks and meeting deadlines.

## Domain Knowledge:

**1. Cyber Security Fundamentals:** Understanding of cyber security concepts, threats, and best practices.

**2. Compliance and Regulations:** Familiarity with relevant laws, regulations, and standards.

**3. Risk Management:** Knowledge of risk management principles and practices.

## Personal Growth:

**1. Confidence:** Gained confidence in tackling cyber security challenges.

**2. Adaptability:** Developed adaptability in responding to new technologies and threats.

**3. Continuous Learning:** Recognized the importance of ongoing learning and professional development.

These skills and learnings will be valuable in future endeavors, particularly in the field of cyber security.

# Case Studies

## Case I

News / Crooks Pose As Firm MD, Trick COO Into Paying 2 Cr

### Crooks pose as firm MD, trick COO into paying 2 cr

Dwaipayan Ghosh / Jul 11, 2025, 23:46 IST


Kolkata: The COO of a firm, Haldia Water Services Pvt Ltd, was conned into transferring Rs 2 crore to fraudsters, who impersonated the company's MD on WhatsApp.

Two men from Bamongola in Malda—Mantu Das and Papai Das—have been arrested for providing SIM cards to the accused. The SIM cards were used to create the fake WhatsApp account of the MD and send the message. Initial probe reveals the involvement of an inter-state cybercrime gang with Cambodia links, said police.

COO Nikhil Mahanta got a message on June 26, ostensibly from his MD's number, telling him to transfer money to a private bank account of "a Bangalore IT firm". It was after he sent Rs 2 crore through RTGS that Mahanta noticed errors in the message and reported it to the National Cyber Crime Reporting Portal, with the help of West Bengal Cyber Crime Wing. Police coordinated with the private bank's Domlur branch in Bangalore, froze Rs 1.3 crore, which was later reversed.

# Case II

## Sr executive loses 1.7 cr in 2 bank 'transactions'

Dwaipayan Ghosh / Jul 06, 2025, 05:05 IST


Kolkata: A 51-year-old resident of a condo in south Kolkata, working as a senior executive, fell victim to a bank fraud, losing Rs 1.7 crore through unauthorized transactions, police reported on Saturday. The incident prompted the city's detective department to issue new cyber security guidelines.

The victim, a resident of the Survey Park area, received two SMS alerts on July 3, indicating debits of Rs 86 lakh and Rs 88 lakh from his bank account, allegedly transferred to a private firm account. The SMS updates arrived much after the transactions got completed, said investigators.

Upon verification with the firm, it was confirmed that the company did not receive any such payment. Cops believe he might have fallen victim to a SIM swap fraud unless there are other ways the victim gave away his personal information.

The fraud comes amid a surge in such cases across Kolkata and its suburbs, with total losses exceeding Rs 3 crore in recent months. In response, the bank fraud section of the detective department has released detailed security protocols for mobile banking users."Forwarding messages to dedicated server numbers and sudden loss of tower connection in well-connected areas are major red flags," said a senior officer.

# Case III

## Forex trader 2nd to be arrested in 1 cr digi-arrest fraud case

Jul 05, 2025, 23:34 IST


Kolkata: The Bidhannagar Police on Saturday arrested Debabrata Ghosh, a forex trader from Kazipara in Barasat, for duping an 86-year-old Salt Lake resident of Rs 1.1 crore between Aug 14 and Aug 29 last year with ‘digital arrest' threats.

Ghosh, a resident of DL Block in Salt Lake, is the second to be arrested in the case. Earlier, Nirmal Vijay from Nagerbazar was arrested. They have been booked under BNS sections for digital fraud and impersonation.The victim.

Shambhu Nath Choudhury, a resident of Sector II, Salt Lake, was targeted by the scamsters, who posed as officers from "Ambani Police Station". The fraudsters claimed his Aadhaar card was linked to a money laundering case and threatened him with arrest.

During the raid on Friday, police seized various documents and articles from Ghosh's possession that were linked to the forex trading aspect of the scam. The total amount siphoned from the victim reached Rs 1,10,93,000, transferred from his accounts in three banks. The Bidhannagar Cyber Crime PS is continuing its investigation to identify and apprehend other members of the fraud ring.

# Case IV

## Kolkata: Trader loses Rs 1.5 crore after ‘digital arrest’ follows investment fraud; cops suspect larger racket targeting senior citizens

Dwaipayan Ghosh / TNN / Updated: Jul 05, 2025, 10:02 IST



A Tollygunge trader lost ₹1.5 crore in a sophisticated scam involving cryptocurrency,...

KOLKATA: A 56-year-old resident of Tollygunge fell victim to a combination of scams, involving cryptocurrency, investment, and share trading, followed by ‘digital arrest' fraud and lost about Rs 1.5 crore through multiple transactions between May and June this year.

The victim, a trader by profession, has lodged a complaint at Regent Park Police Station.

The victim was lured into joining a legitimate WhatsApp group claiming to represent a share trading and securities firm on May 26.

The group promised lucrative returns through Over The Counter (OTC) trading and IPO investments. The scammers then convinced him to join a Telegram group on June 6.

Over the him to make several large transfers amounting lakhs of rupees through RTGS payment mode for investment purpose.

# Case V

## Two arrested for 1.1 cr cyber frauds

Dwaipayan Ghosh / Jun 29, 2025, 00:25 IST


Kolkata: The Bidhannagar Police has arrested two men in two cases of digital fraud, which together led to a loss of Rs 1.1 crore.

In the first case, Nirmal Vijay was arrested from Nagerbazar for defrauding an elderly Salt Lake resident, Shambhu Nath Choudhury, of Rs 1 crore by posing as police officers and intimidating him over calls. Documents related to the crime were recovered from Vijay.

In another incident, Jharna Basak, from Bidhannagar East PS area, lost Rs 9 lakh in an OTP fraud. Accused Vikas Kumar Nishad was arrested from Jharkhand for his alleged involvement. He was brought to Kolkata on transit remand.

Also, an FIR was registered at the Bidhannagar cyber cell on Friday against an investment scam, which defrauded multiple victims of Rs 4.4 lakh through a fake trading app.

# NSS (National Service Scheme)


The acronym NSS stands for National Service Scheme. It is a government-sponsored public service program in India that aims to develop the personality and character of student youth through voluntary community service.

The National Service Scheme is a public service program run by the Indian government's Ministry of Youth Affairs and Sports. It began in 1969. The goal is to develop students' personalities and build character through voluntary community service. Its motto is “NOT ME, BUT YOU,” which stresses selfless service to the community.

Students in 11th and 12th grades, along with undergraduate and postgraduate students in India, can participate in the NSS. Upon finishing the program, participating students receive certificates to acknowledge their service.

In a medical context, specifically for infants, NSS can also mean Non-nutritive sucking. This refers to the sucking reflex in newborns that is not for feeding, such as sucking on a pacifier. It helps with oral development and self-regulation.


GPS Map Camera
Kolkata,West Bengal,India
Mominpur, Mominpur, Kolkata, West Bengal 700023, India
Lat 22.528041, Long 88.321580
07/09/2025 01:39 PM GMT+05:30
Note : Captured by GPS Map Camera


Government Girls' General Degree College


GPS Map Camera
Kolkata,West Bengal,India
Mominpur, Mominpur, Kolkata, West Bengal 700023, India


Cyber cops warn of fake insta alerts used to hijack accounts
GPS Map Camera
Kolkata,West Bengal,India
Mominpur, Mominpur, Kolkata, 700023, West Bengal, India
Lat 22.527901, Long 88.321910
07/04/2025 01:07 PM GMT+05:30
Note : Captured by GPS Map Camera


GPS Map Camera
Kolkata,West Bengal,India
Mominpur, Mominpur, Kolkata, West Bengal 700023, India
Lat 22.527848, Long 88.321818
07/10/2025 12:55 PM GMT+05:30
Note : Captured by GPS Map Camera


Kolkata,West Beng
Mominpore Road, Mominpur, West Bengal, India
Lat 22.527713, Long 88.3219
06/24/2025 12:54 PM GMT+
Note : Captured by GPS Map


GPS Map Camera
Kolkata,West Bengal,India
Mominpur, Mominpur, Kolkata, West Bengal 700023, India
Lat 22.527777, Long 88.321581
07/09/2025 12:40 PM GMT+05:30
Note : Captured by GPS Map Camera

THE TIMES OF INDIA, AHMEDABAD/SURAT
TUESDAY, NOVEMBER 12, 2024

TIMES

# Int'l cybercrime ring busted in Surat; 200 cases detected

## Stolen Money Sent To Dubai Via Hawala

TIMES NEWS NETWORK

**Surat:** Three months of investigation into several cyber frauds led Surat police to bust a major international cybercrime ring and detect 200 cases registered in 15 states and Union territories.

In the 24 hours ended Monday night, police arrested four members of the gang who were allegedly involved in at least 200 cybercrime FIRs lodged across the country. Police said the FIRs were lodged in 200 cases out of the total 866 complaints registered on the national cybercrime portal.

"Our investigation revealed that the gang not only executed cyber frauds but also laundered the siphoned-off money worth crores by sending it to international gangs operating from Dubai, China, Myanmar, Thailand, Indonesia, and other countries," said Anupam Singh Gahlaut, police commissioner, Surat.

Gahlaut said this is India's largest detection of cyber-CYBER LAUNDERING which as many as 200 registered across the were detected in one

"The 866 complaints of various cyber frauds, including digital arrests, were registered this year alone. We detected transactions worth Rs 111 crores made from 613 bank accounts that the gang was operating," said Bhavesh Rojiya, deputy commissioner of police (crime).

Those arrested were Ajay Italiya, Vishal Tummar, and Jalpesh Nadiyadara, apart from Hiren Barwaliya, who was nabbed at the Mumbai airport on Sunday night before he could flee to Dubai. Others on the run are Milan Vaghela and Jagdish Ajadiya, who are suspected to be in Dubai; Ketan Vekariya and Dashrath Dhandhaliya.

"Ajay Italiya, Milan Vaghela, and Ketan Vekariya are the masterminds of the scam," Rojiya added.

They would withdraw the money siphoned in different cyber frauds from these accounts and transfer money to other accounts being operated from Dubai and other countries. "After withdrawing money, it was sent to Dubai via hawala or through wallets after conversion into cryptocurrency," he explained.

In the last three months, the police raided two places in Sarthana and Mota Varachha areas of the city and booked 25 people. So far, the police seized 128 debit cards, 198 passbooks, 35 cheques, 336 SIM cards, 36 mobile phones, and 16 bank kits, apart from laptops and computers.

Looking at the scale of organised crimes, police will soon invoke the stringent Gujarat Control of Terrorism and Organised Crime (GujCTOC) Act 2015 against the gang members.

The first raid was conducted outside a nationalised bank in Sarthana in which 17 people were booked, of which six were arrested.

During the investigation, the cops found out that Vaghela and Italiya were also involved as they raided their office in Mota Varachha last month and found a large number of bank accounts and transaction details from their office and computers.

### HOW THE CROOKS OPERATED

- Gang would find poor, lower middle-class and jobless people and lure them with **money to open bank accounts**
- After assisting them in opening accounts in their preferred banks, **they would give them Rs 10,000 to Rs 15,000**
- After paying them money, **gang would take their kit including cheque book**, passbook and debit card
- International gangs would **use these accounts to receive money**
- Money was transferred from one account to another **to avoid probe and freezing**
- **The money was withdrawn mainly in Dubai** and distributed among the gang members
- Money was also **converted into cryptocurrency** and sent back to Dubai

**ILLICIT MONEY RECEIVED IN 375 ACCOUNTS:** Out of 623 bank accounts found on them, 370 were used to receive the illicit money obtained through digital arrest, task frauds, or some stock or investment frauds from different states. Out of these 370 accounts, 275 are such that they have more than one cybercrime attached to them

**200 CRIMES DETECTED:** The probe helped detect 51 cyber fraud complaints lodged in Karnataka and Telangana, 41 in Maharashtra, 19 each in Tamil Nadu and Delhi, eight in Andhra Pradesh, seven in Gujarat, six in Odisha, two each in West Bengal, Rajasthan, Punjab, Madhya Pradesh, and Chhattisgarh, and one each in Bihar and Andaman & Nicobar Islands

**ED TO BE INFORMED:** The police will appoint a special team of chartered accountants to look into transactions done by the gang members. The sheer number of bank accounts has necessitated engagement of financial experts to decipher the nature of transactions. The Enforcement Directorate, Income Tax and other agencies will also be informed. The role of some bank employees is also not being ruled out

# Woman falls for fraud biz plan, duped of ₹18.5 crore

TIMES NEWS NETWORK

**Hyderabad:** A sexagenarian was lured into a business expansion plan floated by her son's tenant and was duped of ₹18.5 crore. The suspect, Anil Kumar, initially offered to buy the victim's multi-storied apartment complex at Nacharam. In exchange for the building, he offered her a share in the business.

### OFFERED BIZ SHARE FOR BUILDING

- Woman lured into biz plan floated by her son's tenant
- Duped of ₹18.5cr by suspect Anil Kumar
- Accused offered to buy victim's multi-storied apartment at Nacharam
- In exchange for building, he offered her share in business
- Made her director & obtained Rs18.5cr from bank by mortgaging her apartment


- However, without lady's knowledge, accused diverted loan amount for fraudulent activities
- With non-payment of EMIs, bank served woman legal notices
- Woman lodged complaint, man hunt on to nab suspect

### DON'T PANIC. GET HELP

Cyber crime awareness, Prevention helplines

- National Cybercrime Reporting Portal: **1930**
- Website: **www.cybercrime.gov.in**
- TG Cyber Security Bureau: **8712672222**

Further, he made her a director in the new business he floated and obtained ₹18.5 crore loan from bank by mortgaging her apartment. But without her knowledge, Anil Kumar, along with his associates, diverted the loan amount to their personal accounts and indulged in fraudulent activities.

With non-payment of [illegible] the bank served legal [illegible] asking her to clear dues and cautioned her about attaching her mortgaged apartment. The woman has now lodged a complaint with the Cyberabad police, who have launched a hunt to nab the suspect.

The woman, a retired state govt employee currently residing at Madhapur, became acquainted with Anil Kumar a couple of years ago. He paid her ₹5 lakh as advance to buy the Nacharam apartment and bought some time to pay the complete amount and execute a sale deed. He then claimed that he was not able to arrange the amount on time and proposed to offer her a 93% share in their new business — Silk Saree Malls.

Accordingly, her property was mortgaged, and she was also made a director and designated partner without any role in the management of the companies and a 93% share as promised. But later, she found that her shares in the company were reduced from 93% to 25% without any information or board resolution, and also the suspect used the loan amount for other business expansion purposes.

When she resigned from board membership and questioned the accused on the fund diversion, they threatened her, saying that they would not release her personal guarantee from the bank and would make the loan account a non-performing asset. Subsequently, the bank issued her notices regarding irregularities in the loan accounts.

S CITY

# Beware, instant loan apps can be lasting nightmare

## No Regulations Against Such Cos; Harassment Plaints On Rise

**APPS NOT REGISTERED WITH RBI**

Most of the applications have not been registered with the RBI and hence they are not authorised to lend money. However, the Google Play Store has hundreds of such illegal Chinese apps which are evidently flourishing. Each of these apps have more than 10 lakh downloads within months of their launch.

CASE 1 | For a loan of ₹1,000 taken on May 20, one woman's friend had to pay ₹2,152 in just one week. The additional ₹562 which is 43% of the principal — is called interest, processing fee and GST at 18% on that fee. After a few months, he again took a loan of ₹10,000 for a month. The company deducted the processing fee and interest in advance and disbursed ₹7,157

CASE 2 | Kapil Mittal had borrowed ₹1,000 from the app but he delayed payment by a day. "They started abusing some of my personal photos received by me as a 'friend'. It was quite harrowing. They harassed me with threatening calls throughout the day. They said they would inform the police and send collection agents. They also harassed my contacts," he said.

Applications offering micro loans at high interest rates have mushroomed in the country in the past few years ...

No action can be taken against recovery agents: Cyber experts

READ APP POLICIES VERY CAREFULLY

# Crime thrives online, little action on ground

**LOW CONVICTIONS** Experts blame lack of manpower, poor training

Vijay Kumar Yadav & Jayprakash S Naidu

MUMBAI: The state government in April this year, approved the setting up of four new police stations dedicated to tackling the rising cases of cyber crime in Mumbai. It also sanctioned creating 186 new posts, most of them to be filled by assistant police inspectors.

These units are yet to start work, but meanwhile, cases of cyber crime — which range from data theft to credit and debit card frauds and advertising — have steadily risen over the past three years. Convictions, however, have remained disproportionately low. According to the National Crime Records Bureau's (NCRB) 2016 report on crime, Mumbai ranked first in the country for cyber crime cases. From 2015, up until May 2018, 10,275 cyber crime cases were filed in Maharashtra. While 3,680 of these were solved by the police, just 10 of these cases went to trial. In all, since 2015, there have been convictions only in 28 cases.

"The detection (solving) rate depends on several factors," said Balaji Rajput, the superintendent of police (cyber).

"It is difficult to extract information in cyber crime cases. Though many agencies investigate on the internet service providers are the ones who provide such content online, inter-connectors like the banks and technology service providers. There is also the issue of international jurisdictions."

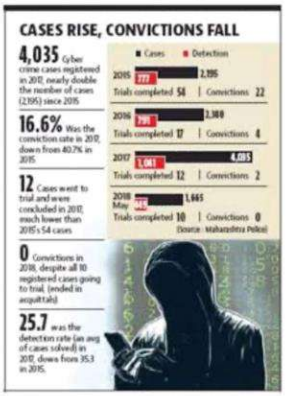
Rajput pointed out how in many cases, the fraudsters use SIM cards that they get after providing false information.

"The bank account of an illiterate person is used, after these fraudsters promise them a commission."

Former Maharashtra director general of police and cyber crime expert, D Sivanandhan, said one of the main reasons for low detection and conviction rates was the lack of manpower and poorly trained police officers.

CONTINUED ON P10
RELATED REPORTS, P2

### CASES RISE, CONVICTIONS FALL




**4,035** Cyber crime cases registered in 2017, nearly double the number of cases (2,195) since 2015

**16.6%** Was the conviction rate in 2017, down from 40.7% in 2015

**12** Cases went to trial and were concluded in 2017, much lower than 2015's 54 cases

**0** Convictions in 2018, despite all 10 registered cases going to trial, (ended in acquittals)

**25.7** was the detection rate (an avg of cases solved) in 2017, down from 35.3 in 2015.



## Crime thrives...

"Further, the law permits only officers from the rank of police inspectors and above to register and investigate the cyber crimes," he said, and added that the since cyber criminals operate online, many times from another state, it becomes difficult for the police to arrest them. "For this, we need a good inter-state and international network of officers, and improved coordination among investigative agencies."

At the trial stage, prosecutors and the judges also need to be updated about the growing incidents cyber crimes and the technology that is being used to cheat people. "This may help them better examine evidence, trials will be done faster, and conviction rates will improve. This is the missing link," Sivanandhan said. Special inspector general of police (cyber crime) Brijesh Singh also stressed on the need to better training and improved technology. "In the near future, we will have a centre for excellence where special training and information pertaining to cyber crimes and its investigations are provided to police, prosecutors and the judiciary. We will also have 44 cyber police units that have state-of-the-art technology."

THE TIMES OF INDIA, MUMBAI
SATURDAY, JANUARY 2, 2021

TIMES

# Cyber cops warn of fake Insta alerts used to hijack accounts

V.Narayan@timesgroup.com

**Mumbai:** Maharashtra police's cyber cell has issued an alert warning citizens against sharing confidential details such as their usernames and passwords of Instagram accounts after receiving fradulent copyright infringement SMSes or emails. Fraudsters misuse these details to hijack accounts for blackmail, cyber cell police said.

The fake text notification reads: "Accounts will be suspended within 24 hours for violating Instagram's copyright law". The email notice says, "Account will be permanently deleted for copyright infringement". The fake email [illegible] looks official as it uses [illegible]ram logo, said police. [illegible]ber cell tweeted that [illegible]ckers are targeting [illegible]m users in a bid to hijack their accounts. "As soon as your data goes to the scammers, they can take over your Instagram profile and modify the information. They can then demand a ransom to return the hijacked account or start spreading spam and all kinds of malicious content through it."

The attack begins with a phishing email or a direct message being distributed as part of this fake campaign that claims the user's account will be suspended within 24 hours for violating Instagram's copyright law. "It sends the user a copyright notice. The users who wish to refute the claim can do so by clicking the 'Copyright Objection Form' link or button provided in the email or direct message. The message has several grammatical errors. Clicking on the link redirects the user to a fake Instagram page. The URL of the page doesn't end in '.com' but '.cf'. The page asks the user to share the email ID, date of birth and Instagram password. After obtaining all the private information, the phishing page redirects the user to the official Instagram login page for maintaining the illusion that the copyright objection form was authentic," said joint commissioner of police Yashasvi Yadav.

Cyber expert Ritesh Bhatia said this is a case of phishing and warned the hacked contents can be even sold for terrorist activities. "Hackers are not just gaining access to celebrity accounts but also of any user with a large number of followers. The idea of these hackers is to sell these hacked accounts on the dark web," said Bhatia.

### IF YOU SUSPECT ACCOUNT MISUSE

- When you enter your credentials and can still access the account, check if the mobile number and email ID associated with it have been changed
- Change your password which will automatically log you out of all devices
- If you have lost full control of your account, you need to report it to Instagram Security; it will confirm your identity through your phone number and email
- Enable two-factor authentication on social media to protect your identity and private details
- Report such instances at www.cybercrime.gov.in or www.reportphishing.in or visit your nearest police station

# Acknowledgements

I would like to express my heartfelt gratitude to everyone who supported and guided me throughout the Cybersecurity Experiential Learning Programme (ELP). This journey has helped me gain real knowledge about the importance of cyber safety in today's digital world.

First and foremost, I sincerely thank our respected Principal for giving us the opportunity to be part of this important programme. I would also like to specially thank our NSS Unit Officer, Mumu Chakraborty Ma'am, for her constant support, guidance, and encouragement. My thanks also go to our cyber security officer, whose insights helped me better understand the concepts of cybersecurity.

As part of this programme, I interacted with senior faculty members, non-teaching staff, college students, local shopkeepers, and residents of slum areas. These activities helped me understand how aware (or unaware) people are about online threats and how we can help them stay safe digitally.

I also learned a lot by attending seminars, reading real-life cybercrime case studies from newspapers, and using the Bharat Cybersecurity Portal to stay updated on cyber laws and practices. One such case study involved a fake job offer scam that led to financial loss for several people – a reminder of how serious cyber frauds can be.

This programme has given me both practical experience and valuable lessons that I will carry forward. I am truly grateful for this opportunity.