EXPERIENTIAL LEARNING PROGRAMME

NSS UNIT-I

NAME: MUBBSHRA ALI

Sem: 2 ROLL NO: 204

DEPT: ENGLISH HONOURS

TOPIC: REPORT OF ELP ON CYBER SECURITY

COLLEGE: GOVT GIRLS' GENERAL DEGREE COLLEGE

UNIVERSITY: CALCUTTA UNIVERSITY

REPORT

ON

EXPRIENTIAL

LEARNING

PROGRAME ON

CYBER

SECURITY!

INTRODUCTION

In an increasingly digital world, cyber security has become one of the most essential areas of focus for individuals, businesses, and governments. The growing threats of cyber-attacks, data breaches, identity theft, and online fraud highlight the urgent need for professionals and citizens to be equipped with the knowledge and skills to stay safe in the digital space. Traditional classroom learning often provides only theoretical knowledge, which is not enough to face real-world cyber threats. To address this gap, the Experiential Learning Programme (ELP) on Cyber Security has been designed to offer a more hands-on, practical approach to learning.

This programme focuses on learning by doing, where participants actively engage in simulations, real-time case studies, projects, and problem-solving exercises. It allows learners to understand cyber threats and defences through direct experience, rather than just reading or listening about them. Whether it is detecting phishing emails, analysing malware, or protecting a network from intruders, the experiential learning model helps learners build confidence and competence in applying cyber security tools and techniques.

The programme also aims to develop critical thinking, teamwork, and ethical awareness, alongside technical knowledge. By working on real-world scenarios and collaborative tasks, participants learn how to make informed decisions under pressure, respond to threats responsibly, and understand the legal and moral aspects of cyber security.

In essence, this Experiential Learning Programme is not just about acquiring knowledge, but about transforming that knowledge into practical skills and awareness that can be used to protect digital systems and data in everyday life and professional settings.

WHAT WE UNDERSTAND FROM ORIENTATION MEETING

The orientation meeting on cyber security serves as the first step to understanding the goals, expectations, and structure of the Cyber Security Experiential Learning Programme. It provides a clear picture of what the programme is about and how participants can benefit from it.

From the orientation, I understand that cyber security is a vital skill in today's digital world where online threats are increasing rapidly. The meeting explained the importance of learning how to protect personal and organizational data from cyber-attacks like hacking, phishing, malware, and identity theft.

The orientation also introduced the experiential learning approach, which means that instead of just reading about cyber security, we will actually practice it through hands-on activities, real-life simulations, and group projects. This practical learning style will help us understand cyber concepts more clearly and apply them in real situations.

In addition, the meeting gave information about:

The topics and tools we will learn (such as firewalls, ethical hacking, and data protection),

The schedule and timeline of the programme,

Our roles and responsibilities as participants,

And the support system available, including mentors and resources.

Overall, the orientation meeting helped set a strong foundation by building awareness about cyber safety, encouraging active participation, and motivating us to take the programme seriously to become more cyber-aware and secure in the digital world.

OBJECTIVES OF THE PROJECT

The main aim of a cyber-security project is to equip learners with practical knowledge, skills, and strategies to understand, detect, and defend against cyber threats. Here are the key objectives of a cyber-security project:

1. Identify and Analyze Cyber Threats:
To help participants recognize various types of cyber-attacks such as malware, phishing, ransomware, and data breaches, and understand how they occur.

2. Apply Security Tools and Techniques:
To train learners in using real-world cyber security tools (like firewalls, antivirus software, and intrusion detection systems) to protect systems and data.

3. Promote Safe Online Practices:
To raise awareness about digital hygiene, strong passwords, two-factor authentication, and other good cyber habits to prevent threats.

4. Build Technical and Problem-Solving Skills:
To enhance learners' ability to troubleshoot issues, respond to incidents, and design secure systems through practical tasks and challenges.

5. Simulate Real-Life Cyber Scenarios:
To provide hands-on experience through simulations of cyber attacks and defenses, helping learners apply theory in realistic situations.

6. Encourage Ethical Understanding:
To make learners aware of the ethical and legal aspects of cyber security, such as ethical hacking, privacy rights, and cyber laws.

7. Develop Teamwork and Communication:
To improve collaboration and communication through group projects, discussions, and role-based cyber security exercises.

8. Prepare for Future Careers:
To build a strong foundation for careers in cyber security by providing practical exposure and boosting confidence in handling real-time challenges.
These objectives ensure that participants not only understand cyber security in theory but are also well-prepared to handle and prevent threats in both academic and professional environments.

DESCRIPTION OF PROJECT ACTIVITIES

As interns in the Cyber Security Experiential Learning Programme, our primary role was to actively engage in hands-on activities that helped us understand, analyze, and respond to real-world cyber threats. These project activities were designed to develop both technical and practical knowledge while encouraging teamwork, ethical thinking, and problem-solving.

Our Responsibilities as Interns:

Threat Identification: Learning to recognize various cyber threats such as phishing, malware, and ransomware.

Network Analysis: Using tools to scan and assess the vulnerabilities in a computer network.

Ethical Hacking Practices: Performing controlled and legal simulations to test system security.

Data Collection & Awareness Campaigns: Gathering data on cyber awareness among users through surveys and conducting awareness drives.

Case Study Analysis: Studying real-life cyber incidents and presenting findings with prevention strategies.

Documentation & Reporting: Keeping records of all activities, findings, and learnings in a detailed report and sharing presentations.

Tools and Platforms Used for Data Collection and Learning:

Tool/Platform	Purpose
Google Forms:	Used to create and distribute surveys to assess cyber Awareness.
Wireshark:	For monitoring network traffic and detecting suspicious Activities.
Nmap:	To perform network scanning and vulnerability Assessment.
Kali Linux:	A platform for practicing ethical hacking and penetration
Google Docs/Sheets:	For documenting activities, responses, and And preparing final report.
Canva / MS PowerPoint:	To design awareness posters and campaign Presentation.

Additional Activities:

Participating in phishing simulations and learning how to detect fake emails or malicious links.

Conducting awareness sessions among peers on safe internet use and password hygiene.

Engaging in group discussions to reflect on weekly tasks and share best practices.

These project activities gave us the opportunity to apply theoretical knowledge to practical scenarios and gain meaningful experience in tackling cyber security issue

DESCRIPTION OF THE ACTIVITIES

DAY-1

DATE: 20.06.2025

Awareness Programme on Cyber Security For senior citizens.

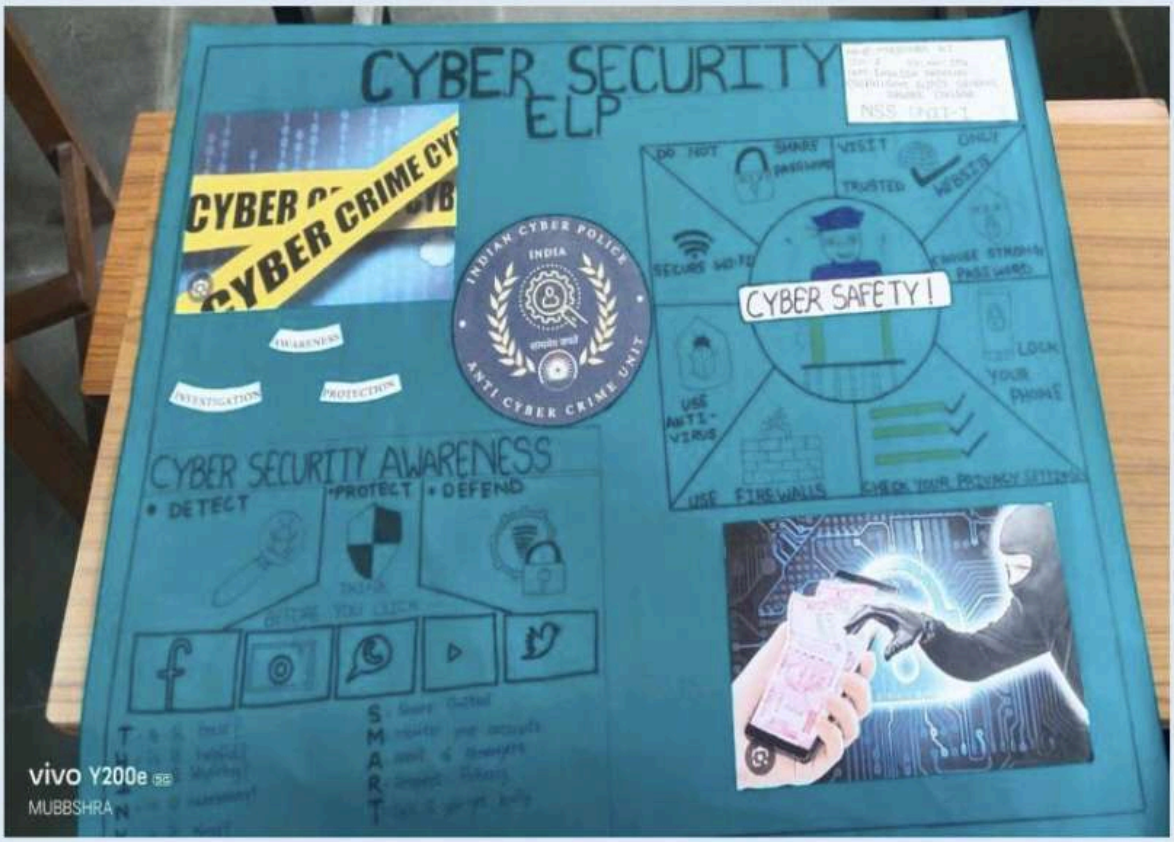
It has been observed that the senior citizens are mostly attacked by hackers. Keeping this in mind, an awareness programme on cyber security was organised for senior citizens to protect them from cyber frauds. In this programme, we the NSS volunteer interact with our senior faculty members in 1:1 ratio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

DAY: 02

DATE: 23.06.2025

Poster Competition on 'Common Cyber Crimes'.

A poster competition on the topic 'common cyber crimes' was organised 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. We 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.



DAY: 3

DATE: 24.06.2025

Digital Leaflet Making on Cyber Security.

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

DAY: 4

DATE: 25.06.2025

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

On the fourth day of the ELP, we 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'.

DAY: 5

DATE: 26.06.2025

Awareness Programme for the Students of the College.

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

DAY: 6

DATE: 30.06.2025

Door To Door Distribution of Leaflets in Cyber Security in the Adopted Slum.

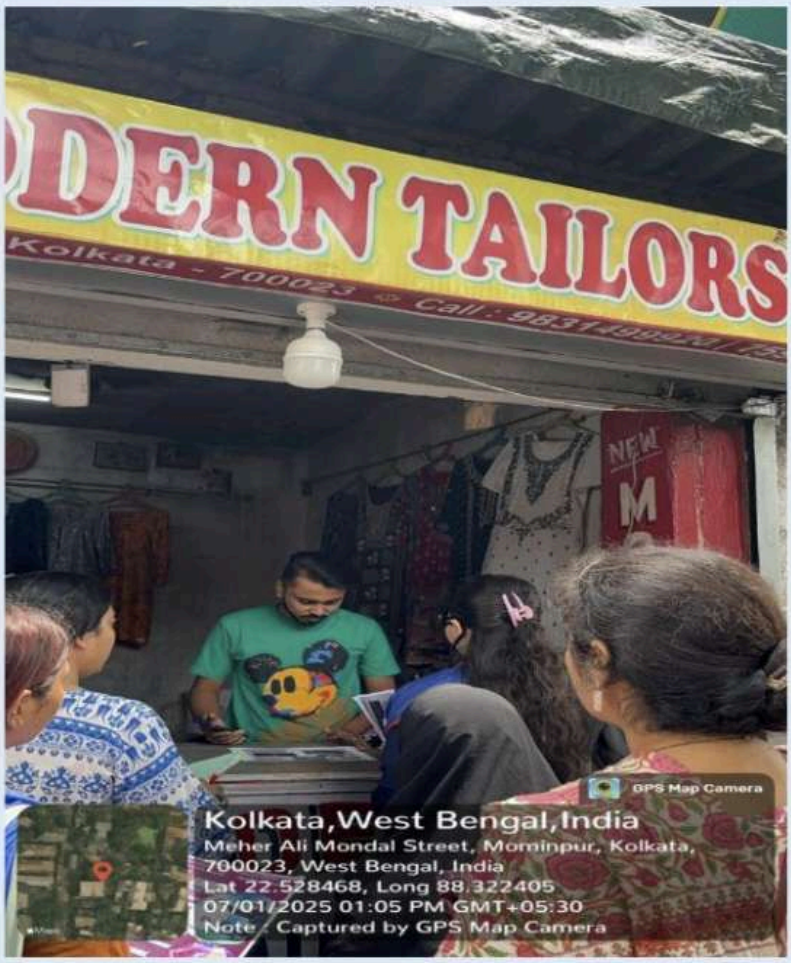
On sixth day of ELP we distribute leaflets on door to door in the adopted slum area to make people aware about cyber crime. We also taught people about how they protect themselves and their family from cyber attack.

DAY: 7

DATE: 01.07.2025

Campaigning Programme on Cyber Security in Nearby Locality and Shops of the College.

On day seven we went on the nearby locality and shops of the college to make more people aware about cyber crime and cyber security. We explain how they protect themselves from hackers. We also told them to spread this awareness with their family and friends.



DAY: 8

DATE: 02.07.2025

Seminar on Cyber Security and Interaction with Victims of Cyber Crime.

On 2nd July we attend a seminar on cyber security. In a seminar we came know lots of things related to cyber crimes and understand how we protect ourselves and others from cyber attck.We also interact with victims of cyber crime and know that how hackers were attacks innocent peoples.

DAY: 9

DATE: 03.07.2025

Drawing Competition on Cyber Crime and Cyber Security.

On the ninth day of ELP we have a drawing competition.We are making drawing on cyber crime and cyber security. Through the drawing we try to make people aware that how we should keep ourself secure.

DAY: 10

DATE: 04.07.2025

Real Case Studies on Cyber Crime from Newspaper.

On fourth July we studied real cases on cyber crime from newspaper to understand how hackers attack people through online frauds and deduct innocent people's money. We also list some real case on cyber crime from newspaper.

DAY: 11

DATE: 07.07.2025

Quiz Competition on Cyber Security.

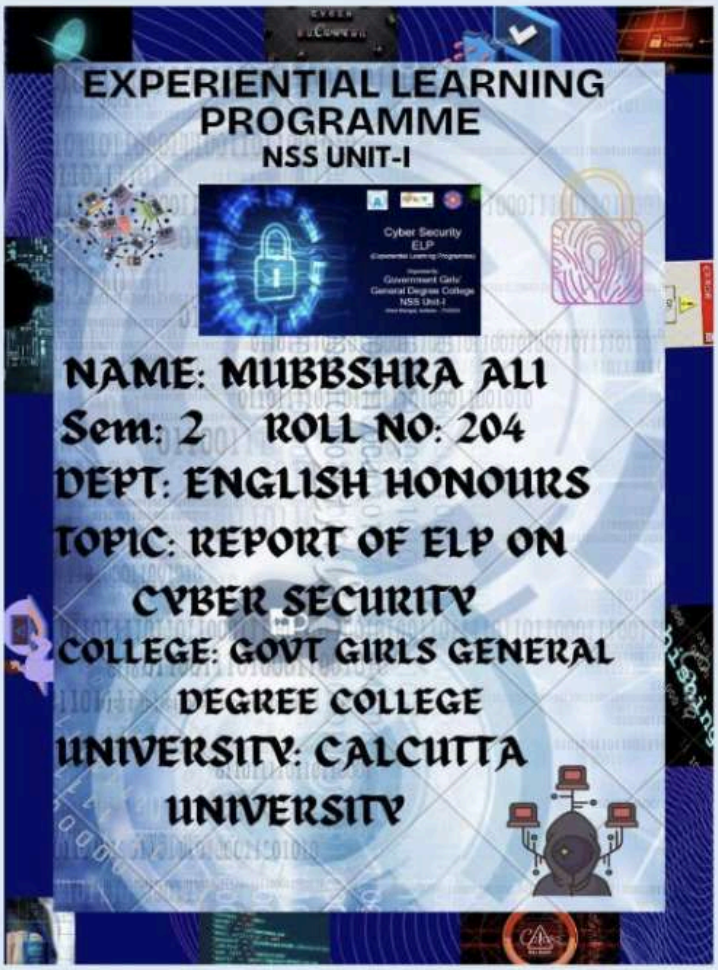
On the eleventh day of ELP our teachers organised a quiz competition on cyber security to test our knowledge that how much we know about cyber crime and cyber security. Through this competition we also came to know our ability and knowledge about cyber crime.

DAY:12

DATE: 08.07.2025

Prepared Report on ELP

On 8th of July we preparing a report on Experiential Learing programme on cyber security to make a hardcopy of our work that what we learn from this ELP and how we make others aware about cyber crime.



DAY: 13

DATE: 09.07.2025

Campaigning Through Posters

On day fourteenth of ELP our teachers organize a campaign through posters. We stick posters on college wall to attract people's attention on cyber security.

WHAT ARE THE OVERALL LEARNING SKILLS

The Cyber Security Experiential Learning Programme provided a strong foundation in both technical and practical aspects of cyber safety. Throughout the internship, we gained a wide range of valuable skills that are essential for protecting digital information and handling real-world cyber threats.

1. TECHNICAL SKILLS:

Network Scanning and Vulnerability Assessment:

Learned how to scan systems using tools like Nmap to identify potential security weaknesses.

Ethical Hacking:

Gained basic skills in ethical hacking and penetration testing to understand how attackers exploit systems.

Malware Detection and Analysis:

Understood different types of malware and how to detect and analyze them.

Encryption Techniques:

Learned how data encryption works and how it protects sensitive information.

Firewall Configuration & Network Security:

Acquired knowledge about securing a network using firewalls and access control.

2. ANALYTICAL AND PROBLEM-SOLVING SKILLS:

Developed the ability to assess threats, find solutions, and respond to security incidents.

Learned to think critically while working on real-world case studies and simulated attacks.

Understood how to investigate breaches and determine their causes and impacts.

3. CYBER AWARENESS AND BEST PRACTICES:

Gained awareness of common online threats like phishing, ransomware, and identity theft.

Learned how to practice safe browsing, manage passwords securely, and avoid suspicious links.

4. COMMUNICATION AND COLLABORATION:

Improved communication skills through group discussions, awareness presentations, and campaign planning.

Worked effectively in teams during simulations, drills, and peer learning activities.

5. RESEARCH AND REPORTING:

Developed the ability to gather, organize, and interpret data through surveys and tools.

Learned how to document findings and present them in clear, structured reports and presentations.

6. ETHICAL AND LEGAL UNDERSTANDING:

Understood the importance of ethics in cyber security, such as respecting privacy and using knowledge responsibly.

Became aware of basic cyber laws and the legal consequences of cyber crimes.

Overall, the internship helped us build a solid foundation in cyber security and equipped us with practical skills that are not only useful for future careers but also essential for protecting ourselves and others in the digital world.

CASE STUDY ON CYBER SECURITY

In 2019, over 530 million Facebook users' personal data was exposed online due to a misconfigured server. The leaked data included users' phone numbers, full names, email addresses, locations, and birthdates. The breach affected users from more than 100 countries.

HOW THE BREACH HAPPENED:

The data was scraped from Facebook's public profiles through a technique called web scraping.

Attackers exploited a vulnerability in Facebook's "Contact Importer" feature, which allowed them to link phone numbers to user accounts.

This data was then compiled and posted on a hacker forum for free.

CONSEQUENCES OF THE BREACH:

Loss of user trust in Facebook's ability to protect personal information.

Risk of identity theft, phishing attacks, and fraud for affected users.

Facebook faced global criticism and investigations by data protection authorities.

WHAT WENT WRONG:

Lack of proper rate-limiting and security controls to prevent automated data scraping.

Failure to notify users when the data leak was discovered.

Inadequate privacy settings and user protection policies.

LESSONS LEARNED:

1. Data Minimization: Only collect and store necessary user data.

2. Stronger Access Controls: Features like "Contact Importer" should have limits to prevent abuse.

3. User Transparency: Inform users promptly if their data is compromised.

4. Regular Security Audits: Frequent testing and patching of systems to detect vulnerabilities.

5. Encryption and Anonymization: Sensitive data should be encrypted or anonymized, even if it's public.

CONCLUSION:

The Facebook data breach serves as a powerful example of how even the largest platforms are vulnerable if proper security measures aren't in place. It underlines the importance of strong cyber security practices, both at the organizational and user level, and highlights the need for ethical responsibility when handling personal information.

NSS UNIT- 1

The Government Girls' General Degree College has an active NSS (National Service Scheme) unit. NSS unit 1 in particularly, known for its involvement in various social service activities both inside and outside the college campus. The college also hosts events like awareness programs related to cyber security and many more, organized by the NSS unit.

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to everyone who supported and guided me throughout the Cyber Security Experiential Learning Programme.

First and foremost, I sincerely thank NSS Unit-1 for offering this valuable opportunity and creating a platform that enabled us to gain hands-on experience in the field of cyber security. Your commitment to practical learning and youth development is truly inspiring.

I am deeply grateful to our mentors and trainers for their expert guidance, continuous support, and insightful sessions that enhanced our understanding of complex cyber security concepts. Your patience and encouragement helped us grow both technically and personally.

Special thanks to the programme coordinators for organizing the sessions efficiently and for being approachable and supportive throughout the internship journey.

I would also like to acknowledge the contribution of my fellow interns and team members. Working with all of you was a wonderful experience, and our collaboration helped make the project activities more engaging and successful.

Lastly, I extend my gratitude to my family and friends for their constant encouragement, motivation, and belief in my abilities during this learning experience.

This internship has been a meaningful step in my academic and personal growth, and I am truly thankful to everyone who made it possible.

युवा कार्यक्रम और खेल मंत्रालय
MINISTRY OF
YOUTH AFFAIRS AND SPORTS

Indian Cyber Crime Coordination Centre
Working Together With Vigour

NATIONAL CYBERCRIME TRAINING CENTRE

Department of Youth Affairs (DOYA) & Indian Cyber Crime Coordination Centre (I4C), MHA

THIS CERTIFICATE IS AWARDED TO :

Mubbshra Ali

For successfully completing the '**Basic Cyber Security & Hygiene Course**'
Cyber Police Station, Cyber Crime Police Station, Lalbazar, Kolkata

This is a digitally generated certificate and does not require a physical signature.

July 10, 2025