Community Development Project

On

Cybersecurity

Submitted By:
Aryan Singh

Registration Number: 12410314

In partial fulfillment for the requirements of the award of

the degree of "B.Tech CSE"

School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab.

Certification by the NGO regarding the Student Project:

LOVELY PROFESSIONAL UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

ARYINDUTTAB9C46SONOTH

LOVELY PROFESSIONAL UNIVERSITY

Introduction :

In today's increasingly digital world, cybersecurity has become a vital skill for individuals across all age groups. Recognizing this critical need, the WNS Cares Foundation, in collaboration with Lovely Professional University, initiated a cybersecurity training program aimed at empowering young minds with essential knowledge and practices for online safety. As part of this initiative, a group of 40 students was selected to undergo structured training focused on building awareness, technical skills, and responsible digital behavior.

The training sessions were designed to be engaging, hands-on, and informative, covering core cybersecurity topics such as online threats, password security, phishing, ethical hacking basics, social engineering, and safe browsing practices. The objective was not only to introduce students to the fundamentals of cybersecurity but also to cultivate a proactive attitude toward protecting personal and organizational data learning but should also help a person develop their character and sense of social responsibility.

This report outlines the goals, structure, content, and outcomes of the training program. It also reflects on the students 'learning journey, feedback received, and the overall impact of the initiative. Through this project, we aim to contribute meaningfully to digital literacy and promote a safer online environment for the youth.

Problem Identification and the Cause of the Problem:

With the rapid growth of digital technology, students are increasingly exposed to cyber threats such as identity theft, phishing scams, cyberbullying, and data breaches. However, many lack the awareness and skills to recognize or respond to these threats effectively. The root cause lies in the absence of formal cybersecurity education at the foundational level. This knowledge gap leaves young users vulnerable, highlighting the urgent need for structured training programs to promote safe and responsible digital practices.

Objective to be Achieved:

The primary objective of this training program is to equip students with fundamental knowledge and practical skills in

cybersecurity to help them navigate the digital world safely and responsibly. By introducing key concepts such as cyber threats, online privacy, password protection, social engineering, and ethical hacking, the program aims to build a strong foundation of cyber awareness among participants.

Additionally, the training is designed to encourage critical thinking and proactive behavior when using digital platforms. It seeks to foster a sense of digital responsibility, enabling students to identify potential risks, take preventive measures, and promote cyber safety within their communities. Through interactive sessions, real-life examples, and hands-on activities, the goal is to not only educate but also empower students to become cybersecurity ambassadors and contribute to building a safer online ecosystem.

Various Steps Taken to Achieve the Objectives:

To fulfill the objective of raising cybersecurity awareness among a total of 40 participants, multiple interactive sessions were conducted at a local school, a coaching institute, and within the community for neighbours, friends and relatives. This initiative was carried out under the WNS Cares Foundation program and aimed to make participants more aware of online safety measures and responsible

digital behavior. The following steps were taken to ensure the sessions were informative, interactive, and memorable for participants of different age groups and digital literacy levels:

1. Pre-Session Planning and Coordination

The first step involved reaching out to relevant authorities and community members to secure venues and confirm participation. I coordinated with:

School authorities to schedule a student-focused awareness session and ensure the availability of infrastructure like a projector, speakers, and internet access.

Coaching institute management to arrange a classroom session for learners who regularly use online academic platforms.

Neighbours, friends and relatives by inviting them for informal gatherings at my home or community space.

For each audience, a customized session plan was prepared. The school content was made age-appropriate, the coaching institute session focused on technical safety practices, and the community session included simplified explanations for beginners. Key topics selected for all sessions included:

Key topics selected for the session included:

- What is Cybersecurity?

- Common Cyber Threats (Phishing, Viruses, Online Scams)
- Safe Browsing Habits
- Password Protection
- Cyberbullying and Online Behavior
- Real-Life Examples of Cybercrime

2. Interactive Presentation and Visual Aids

Each session began with a well-structured visual presentation to introduce cybersecurity concepts in an engaging way. Slides were designed with infographics, analogies, and minimal text to make them accessible to all participants. Visual aids included:

Animated videos explaining phishing and malware.

Screenshots of real phishing emails to highlight red flags.

Online password strength tools to show the difference between weak and strong passwords.

These visual elements ensured participants could connect abstract cybersecurity terms with real-life examples, making the concepts easier to understand.

3. Real-Life Stories and Scenario-Based Learning

To make the sessions relatable and memorable, real-life cybersecurity incidents were shared. Examples included:

A case of social media hacking due to weak passwords.

Phishing attempts disguised as scholarship offers.

Cyberbullying cases and their consequences.

Stories were told in a simple, conversational manner to keep attention and spark curiosity. Participants were encouraged to share their own experiences or stories they had heard. This opened up meaningful discussions and created an environment of trust where participants felt comfortable asking questions.

4. Hands-On Activities and Demonstrations

Practical demonstrations were a central part of the sessions to move beyond theory. Examples included:

- Comparing a weak password like "12345" with a strong password that uses a mix of characters.
- Spot-the-scam: Students were shown screenshots of fake and genuine messages/websites to identify the differences
- A group brainstorming task on “What to do if someone hacks your social media account”

These activities helped reinforce the key messages and made the session more participatory.

5. Student Involvement and Q&A

All sessions followed an interactive format where participants were regularly asked short questions to maintain attention and check understanding. Volunteers were invited to explain their views, guess answers, or give personal examples.

The Q&A segments brought up genuine concerns such as:

- “How can I know if a website is safe?
- “Is it safe to use public Wi-Fi for online banking?”
- “What should I do if I get a suspicious message from a friend’s account?”

Answers were kept simple, practical and relevant to the audience’s daily lives.

6. Cyber Safety Pledge

At the end of the session, all students were asked to take a **Cyber Safety Pledge** — a short and powerful promise to practice safe internet habits. This symbolic activity helped reinforce the values discussed and left students with a sense of responsibility.

7. Feedback and Participation Recognition

A quick oral feedback session was conducted where students shared what they learned and liked most. Their responses indicated that the session successfully increased their awareness and interest in cybersecurity. Some students expressed their desire to learn more in the future.

Certificates of participation or small tokens of appreciation (if distributed) were acknowledged to further encourage interest.

8. Post-Session Reflection and Documentation

After the session, key points such as attendance, student engagement, questions asked, and feedback were documented. Photos were taken (if permitted) to be included in the report. These records will help in future scaling or repetition of such sessions in other schools.

Conclusion

The cybersecurity awareness initiative successfully reached the target of training 40 individuals from diverse backgrounds. By combining interactive presentations, real-life stories, hands-on activities, and open discussions, the sessions not only educated participants but also encouraged them to take active steps toward protecting themselves online. The initiative fulfilled the objective of

the WNS Cares Foundation program by making digital safety knowledge accessible, relatable, and practical for everyday life.

GEO-TAGGED PICTURES:

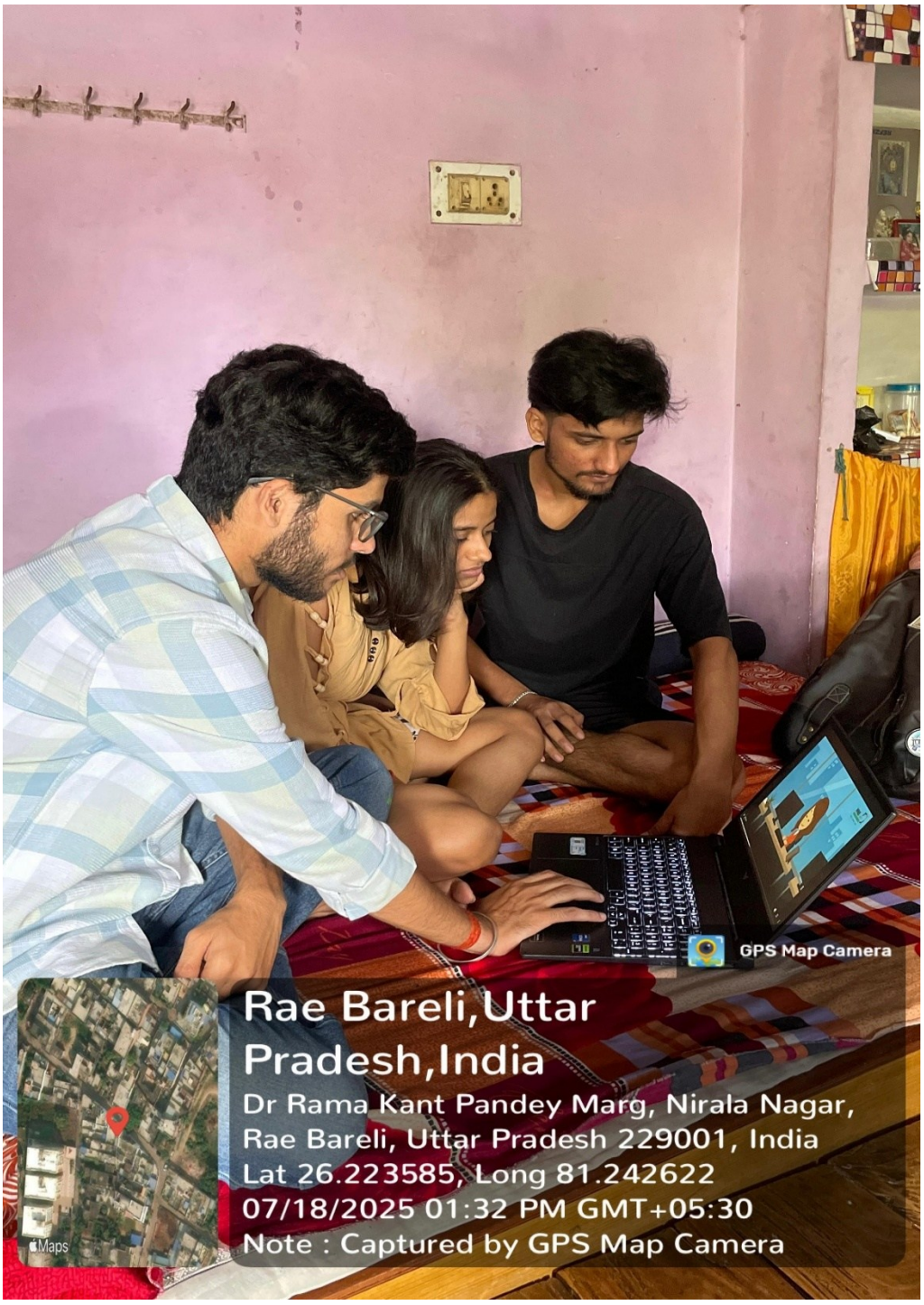
LOVELY PROFESSIONAL UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY



LOVELY PROFESSIONAL UNIVERSITY

Excel Sheet:

S. N	Name	Gender	Mobile Number	Aadhar Card Details	Certificate Reference ID
1	Yashika Khurana	Female	9056630455	9532 5856 6912	YASINDPUNC04F93SONOTH
2	Amrita Singh	Female	7307768652	4991 4108 1165	AMRINDUTT0ABB1BSONOTH
3	Isha Singh	Female	6307181005	4180 4742 4404	ISHINDUTTD61E6CSONOTH
4	Yasharth Pratap Singh	Male	6306326540	4684 3629 4314	YASINDUTTD2718DSONOTH
5	Avika Singh	Female	8355042192	Aadhar card not shared due to privacy concerns	AVIINDUTT86BCB2SONOTH
6	Jatin Kaushik	Male	9810837458	8349 2877 7736	JATINDHARFA43E4SONOTH
7	Akul Singh	Male	8467884697	2156 8266 0809	AKUINDUTTE76709SONOTH
8	Kashish Srivastava	Female	8470913683	5146 6266 1157	KASINDUTTBBD616SONOTH
9	Rishabh Pandey	Male	8864902606	Aadhar card not shared due to privacy concerns	RISINDUTT9FE937SONOTH
10	Avisha Singh	Female	6387684571	Aadhar card not shared due to privacy concerns	AVIINDUTTF1F974SONOTH
11	Kishan Yadav	Male	8299425612	9425 1903 5883	KISINDUTTF5D373SONOTH
12	Shikha Tripathi	Female	7905631518	Aadhar card not shared due to privacy concerns	SHIINDUTT4C0E4FSONOTH
13	Anjali Tripathi	Female	9580625599	6082 4239 9522	ANJINDUTT5C377BSONOTH
14	Anushka Singh	Female	7985390440	2196 2003 8800	ANUINDUTT2D917ESONOTH
15	Prince Yadav	Male	6307729618	2911 4202 9128	PRIINDUTTE65B82SONOTH
16	Abhay Pratap	Male	9445734162	4465 8144 3614	ABHINDMADC47F50SONOTH
17	Adarsh Kumar Maurya	Male	8736822204	6528 0856 4761	ADAINDUTT0541B9SONOTH
18	Alok Singh	Male	6387407797	6369 7487 2910	ALOINDUTTCEAE4ASONOTH
19	Swastik Shukla	Male	8948333032	6175 2615 7608	SWAINDUTT2F9064SONOTH
20	Sheersh Mishra	Male	9451011947	2942 2193 0650	SHEINDUTT5FDBF2SONOTH
21	Katyayni Singh	Female	9335937580	7962 3771 8914	KATINDUTT2A790ESONOTH
22	Vishal Kumar	Male	9835031347	9944 4109 1304	VISINDBIH757FF5SONOTH
23	Khushi Dwivedi	Female	6284155151	6888 5791 3711	KHUINDHARDF7C87SONOTH
24	Diksha Khurana	Female	9592989272	2906 3484 5527	DIKINDPUNF3C8C2SONOTH
25	Rohan Khurana	Male	8264297657	Aadhar card not shared due to privacy concerns	ROHPHISOU7460FAVONOTH
26	Sakshi	Female	7889249787	5375 5694 5728	SAKINDPUNFC9AEDVONOTH
27	Komal Rajput	Female	8198823860	4857 7578 0487	KOMINDPUNBF4ADVONOTH
28	Supriya Sinha	Female	9942992127	8886 4162 9165	SUPINDBIH4C75CFSONOTH
29	Khushi Patel	Female	6388056762	8645 9314 2852	KHUINDPUNDFE53FSONOTH
30	Ayush	Male	6280826930	5375 5694 5728	AYUINDPUN1BF187VONOTH
31	Guneet Khurana	Male	8544944161	Aadhar card not shared due to privacy concerns	GUNINDPUN0FC8EBSONOTH
32	Roshani Yadav	Female	7814714200	Aadhar card not shared due to privacy concerns	ROSINDPUNFD08B0SONOTH
33	Diya Malhotra	Female	9781534320	7705 4426 0561	DIYINDPUNA46D7CSONOTH
34	Krishna	Male	7719665549	4781 9299 9929	KRIINDPUNC12C5BSONOTH
35	Preeti Khurana	Female	6284938369	6368 0549 5604	PREINDPUNF81DC2SONOTH
36	Khushi	Female	6284155151	6888 5791 3711	KHUINDDEL3014FASONOTH
37	Deepak	Male	9977645321	3977 8800 0234	DEEINDPUN4BB4A9SONOTH
38	Abhey Khurana	Male	8544944161	Aadhar card not shared due to privacy concerns	ABHINDPUN892690SONOTH
39	Shivam Sharma	Male	9713952492	9068 3713 3191	SHIINDMAD81435FSONOTH
40	Sunita Mehra	Female	8968403048	5425 5179 7392	SUNINDPUN9F93FDSONOTH

LOVELY PROFESSIONAL UNIVERSITY

Effectiveness of the Project:

The cybersecurity awareness session conducted under the WNS Cares Foundation proved to be highly effective in fulfilling its objective of sensitizing students to the importance of digital safety. The session witnessed active participation from all 40 students, with high levels of enthusiasm and curiosity displayed throughout. Complex topics such as phishing, password security, and cyberbullying were explained using simple language, real-life examples, and interactive demonstrations — which helped in better retention and understanding.

Students were highly engaged during activities such as spotting fake messages, creating strong passwords, and discussing online behavior. Their questions during the Q&A reflected a genuine interest in applying safe digital practices in their daily lives. The post-session feedback indicated that most students had never attended such a workshop before and found it both informative and enjoyable.

The session successfully met its goal of creating awareness and initiating a behavioral shift toward responsible internet use. It also laid the foundation for further cybersecurity training initiatives in schools, making it a meaningful and impactful effort.

Identified Societal Problems:

1.Lack of Cyber Awareness Among Students

In today's digital age, students are increasingly using the internet for learning, social interaction, and entertainment. However, many lack basic awareness of cybersecurity threats such as phishing, cyberbullying, identity theft, and unsafe browsing. This lack of awareness often leads to risky online behavior, making them vulnerable to cybercrimes. The absence of digital safety education in school curriculums further worsens the problem, leaving a large population of young users unprotected.

2.Increasing Cases of Cyberbullying and Online Exploitation

Cyberbullying and online harassment have become growing concerns among school-age children and teenagers. Many students face mental stress, social anxiety, or emotional trauma due to harmful online interactions, but they are often unaware of how to report or respond to such incidents. This societal issue is fueled by the misuse of social media and lack of digital etiquette education, requiring urgent intervention through awareness campaigns and training sessions.

LOVELY PROFESSIONAL UNIVERSITY

Conclusion:

The cybersecurity awareness session conducted under the WNS Cares Foundation initiative was a meaningful step toward empowering students with essential knowledge for safe digital engagement. In a world where cyber threats are growing rapidly, educating young minds about cybersecurity is not just beneficial — it is necessary. Through this one-day session, 40 students were introduced to the fundamental concepts of online safety, responsible digital behavior, and ways to identify and avoid common cyber threats.

The interactive nature of the session, combined with real-life examples and hands-on activities, ensured that students remained engaged and retained the key takeaways. Their active participation, curiosity, and willingness to learn highlighted the success of the program. The discussions on cyberbullying, password security, phishing, and digital etiquette encouraged students to reflect on their own online habits.

This project has shown that even a single well-designed awareness session can make a significant difference in how students perceive and respond to cybersecurity challenges. It also underscores the need for regular cybersecurity education in schools. Going forward, similar initiatives can be expanded to reach more students and create a larger impact in building a safer digital society. The session was a small yet powerful step in that direction.

Thank You.