B.M.S COLLEGE OF ENGINEERING

Autonomous Institute, Affiliated to VTU

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(IOT & CYBERSECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)

SENSORED CLUB EVENT

CYBERSECURITY AWARENESS EVENT AT 'NEED BASE INDIA' (NGO)

DATE: 14th April, 2026

TIME: 3:30 PM – 5:30 PM

VENUE: Need Base India, beside Srirampura Police Station - 560021

SPEAKERS: Ms Durgashree R, Ms Keerthi S, Ms Sravya Munipalle

FACULTY COORDINATOR: Ms. Krupa K S

PARTICIPANTS: Students of Class 9th to 12th (NGO)

OBJECTIVE:

- To create awareness among school students about common cyber threats and online scams.
- To educate participants on cybersecurity concepts such as phishing, spam emails, hacking, OTP fraud, and social engineering attacks.

- To help students identify red flags in suspicious calls, messages, links, and social media interactions.
- To encourage safe digital practices and responsible use of mobile phones, social media, and online platforms.
- To familiarize students with the Cyber Crime Helpline Number (1930) and the importance of reporting cyber fraud incidents immediately.
- To promote interactive learning through roleplay activities and real-life scam scenarios.

DESCRIPTION:

The Cybersecurity Awareness Event was conducted for students from classes 9th to 12th with the aim of educating them about common cyber threats and safe online practices. A total of 28 students participated in the session. The event began with an interactive introduction session where both the organizers and students introduced themselves. Participants were then asked about their familiarity with emails, social media platforms, spam messages, cyberattacks, and online scams in order to understand their existing awareness levels.

The session continued with discussions on important cybersecurity topics including phishing attacks, hacking, spam emails, OTP fraud, and social engineering techniques. Students were educated about how scammers manipulate victims through fake calls, messages, links, and social media accounts. Special emphasis was placed on the importance of never sharing OTPs, passwords, or personal information with unknown individuals.

Participants were also informed about the National Cyber Crime Helpline Number – 1930 – and were encouraged to share the helpline information with their family members and friends so that cyber fraud incidents could be reported quickly.

To make the session interactive and engaging, students were provided with various real-life scam scenarios and were divided into teams of 4–5 members to enact short roleplays based on the situations given. Some of the scenarios included were:

- OTP Loan Scam – where scammers offer fake instant loans and trick victims into sharing OTPs.

• Fake Delivery Scam – where victims are asked to pay small delivery charges for unknown parcels.
• Social Media Fake Friend Scam – where fake accounts impersonate friends and request urgent moneytransfers.
• Gaming Scam – where children are lured using promises of free game rewards, skins, or diamonds through malicious links.

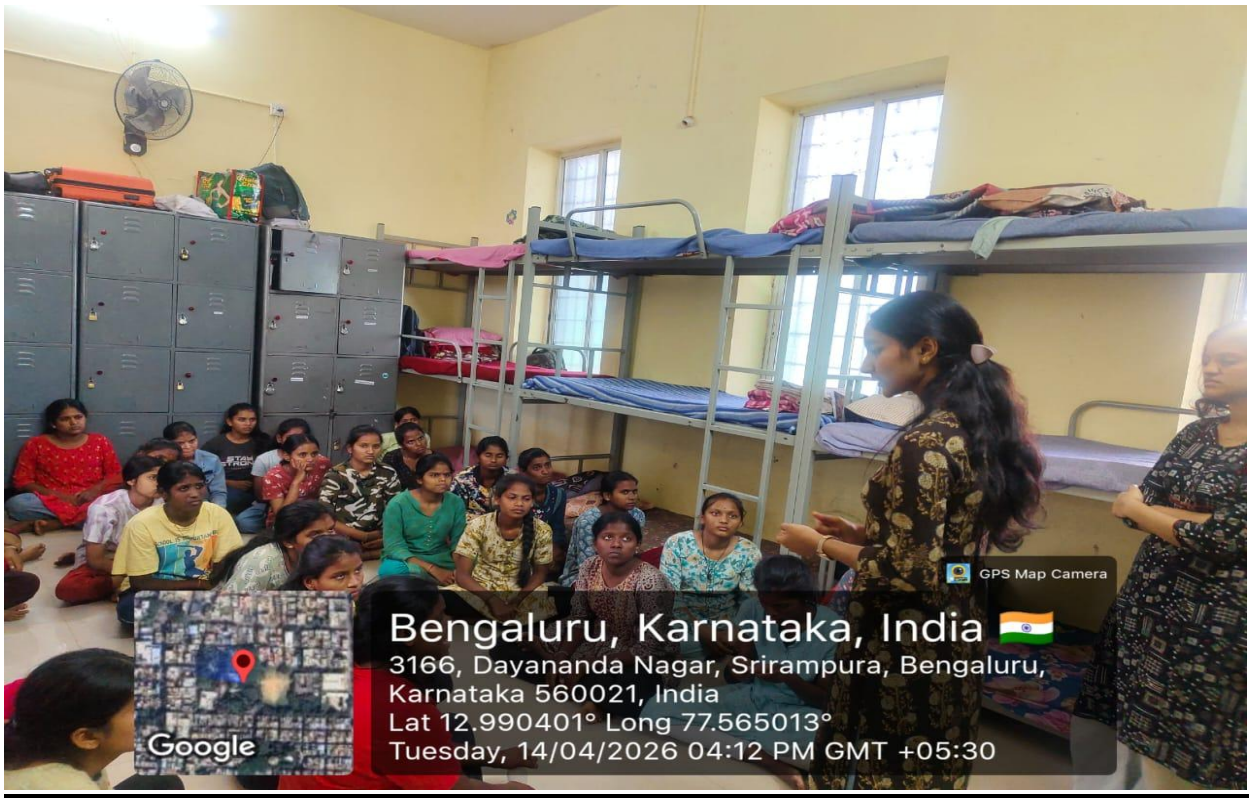
Each activity highlighted important warning signs and taught students how to respond safely in such situations. The roleplay format encouraged active participation, teamwork, and practical understanding of cybersecurity concepts among the students.

The event concluded with a quick revision of all the important points discussed during the session, including recognizing scams, avoiding suspicious links, protecting OTPs, and reporting cybercrime incidents. Chocolates were distributed to all participants at the end of the event as a token of appreciation and encouragement.

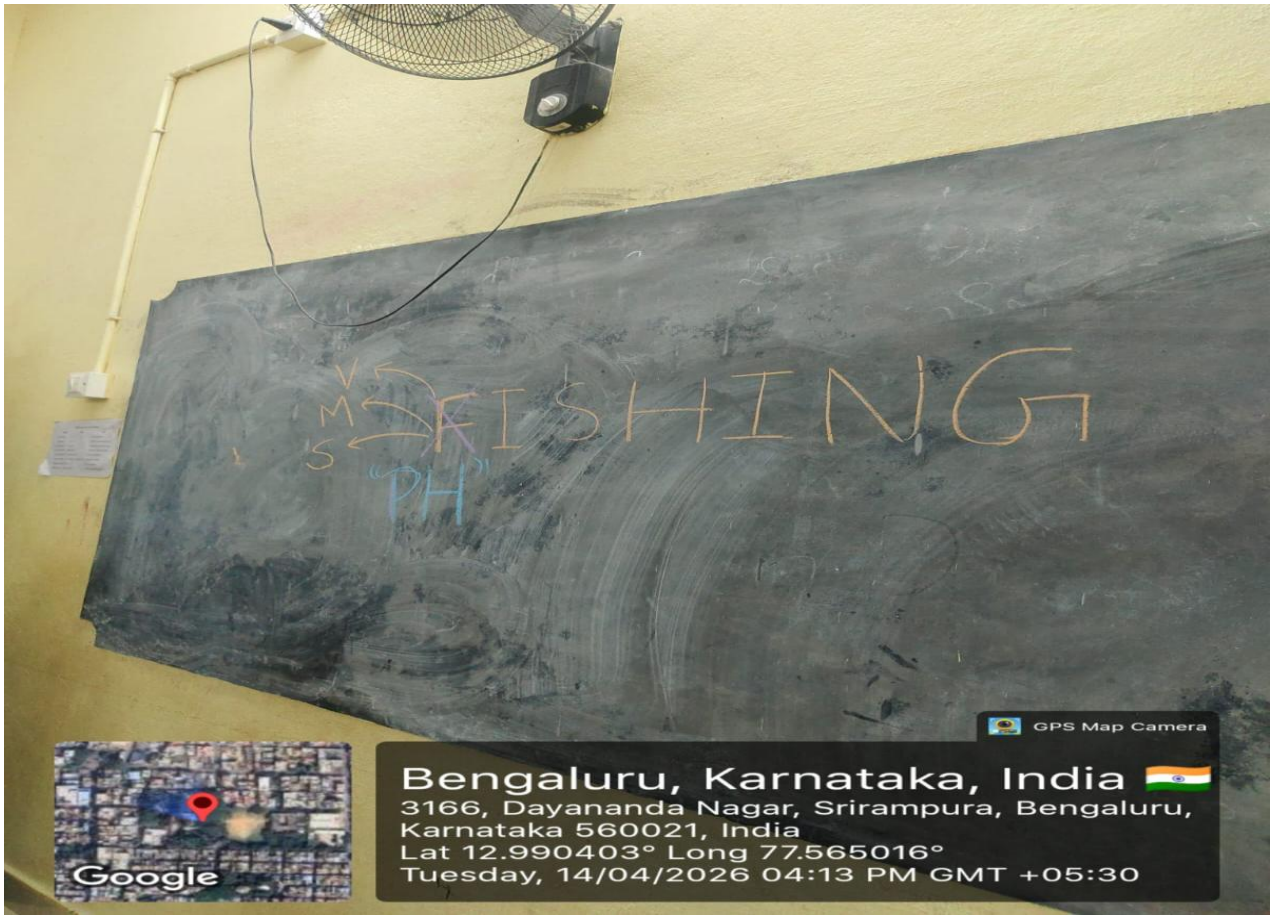
OUTCOMES:

- Participants gained awareness about common cyber threats such as phishing, OTP fraud, fake delivery scams, social media scams, and gaming-related scams.
- Students developed the ability to identify suspicious messages, calls, links, and online activities using real-life examples and scenarios.
- Participants understood the importance of protecting personal information, passwords, and OTPs from cybercriminals.
- Students learned safe online practices and responsible digital behaviour while using mobile phones, social media, and gaming platforms.
- The interactive roleplay activities improved student participation, engagement, teamwork, and practical understanding of cybersecurity concepts.
- Participants became aware of the Cyber Crime Helpline Number (1930) and the importance of reporting cyber fraud incidents immediately.
- The session successfully created interest and awareness among students regarding cybersecurity and online safety.

PHOTOS:


GPS Map Camera
Bengaluru, Karnataka, India
3166, Dayananda Nagar, Srirampura, Bengaluru, Karnataka 560021, India
Lat 12.990401° Long 77.565013°
Tuesday, 14/04/2026 04:12 PM GMT +05:30
Google


GPS Map Camera
Bengaluru, Karnataka, India
47, Police Station Rd, Dayananda Nagar, Srirampura, Bengaluru, Karnataka 560021, India
Lat 12.990332° Long 77.564829°
Tuesday, 14/04/2026 03:56 PM GMT +05:30
Google


FISHING
"PH"
GPS Map Camera
Bengaluru, Karnataka, India
3166, Dayananda Nagar, Srirampura, Bengaluru, Karnataka 560021, India
Lat 12.990403° Long 77.565016°
Tuesday, 14/04/2026 04:13 PM GMT +05:30
Google


GPS Map Camera
Bengaluru, Karnataka, India
3166, Dayananda Nagar, Srirampura, Bengaluru, Karnataka 560021, India
Lat 12.99034° Long 77.564881°
Tuesday, 14/04/2026 05:57 PM GMT +05:30
Google