ALVA'S INSTITUTE OF ENGINEERING & TECHNOLOGY
(A Unit of Alva's Education Foundation(R), Moodubidire) Affilliated to Visvesvaraya Technological University, Belagavi,
Approved by AICTE, New Delhi, Recognized by Govt. of Karnataka.
Accredited by NAAC with A+ & NBA (ECE & CSE)
Shobhavana Campus, MIJAR-574225, Moodubidire, D. K., Karnataka

ALVA'S
Education Foundation®

CYBER SECURITY CLUB

REPORT ON:

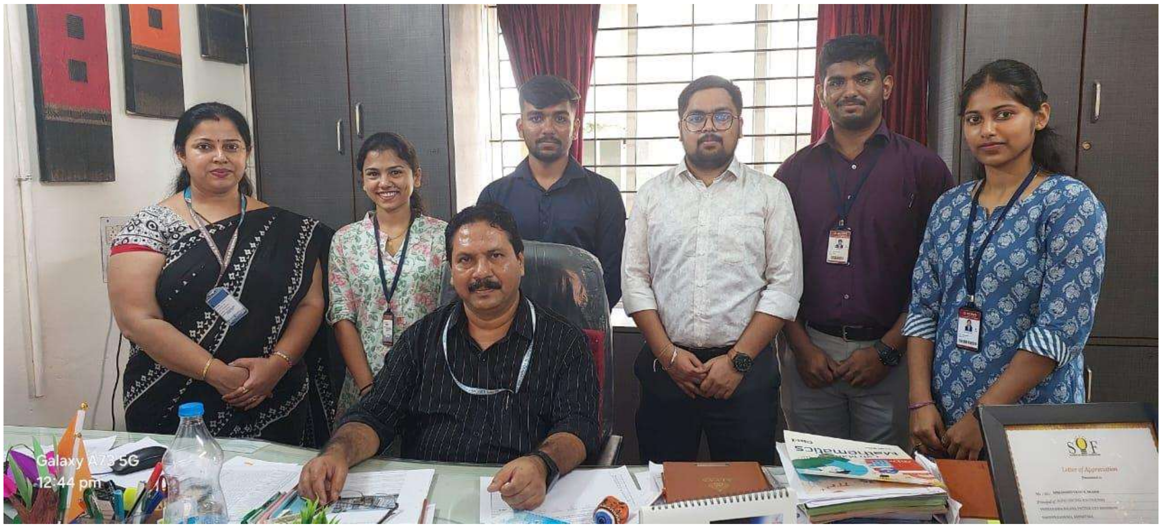
“Cyber Ethics Awareness Program by Alva's Cyber Security Club”

Students:

1. Sujaykumar B Adoor	4AL21CG057
2. Manoj M	4AL21CG036
3. Sharvari M S	4AL21CG049
4. Chandana N M	4AL21IS064
5. Vinith Kalikar	4AL21CG062

Reported to:

Mrs. Deepika Kamath
Club Co-ordinator
Cyber Security Club,
AIET, Mijar-574225



Introduction

Alva’s Cyber Security Club recently conducted a vital awareness program on **Cyber Ethics** for the students of Alva’s CBSE School. This session was designed to educate children about the dangers and safety measures of navigating the online world. The session was highly engaging and left a lasting impression on the children, who learned about various online threats such as cyberbullying, online predators, mobile phone security, and more. Through real-life examples and interactive discussions, the club members aimed to arm the students with knowledge about safe and responsible internet usage.

1. Online Predators

In today's world, children and teens are increasingly vulnerable to online predators who use social media, chat rooms, and gaming platforms to exploit them. The session highlighted Rita's story, but online predators can use various sophisticated techniques to manipulate children. **Grooming** is one such tactic where the predator gradually builds trust over time.

Predators may pose as other children or teens to make the victim feel comfortable. In some cases, they use psychological manipulation, offering emotional support, compliments, and gifts. Once they gain the victim's trust, they push boundaries by requesting personal information or photos. This situation can quickly escalate into **blackmail** or **extortion**, as in Rita's case.

The club emphasized the importance of **parental supervision** and using privacy settings on social media. Monitoring tools and regular conversations between parents and children can help reduce these risks. Various software programs allow parents to track their children’s online activities, limiting exposure to harmful individuals.

More Online Safety Tips:

- Use monitoring software to track internet usage.
- Regularly check privacy settings on social media platforms.
- Discuss online activities openly with family members.

2. Cyberbullying

Cyberbullying can take many forms, from sending hurtful messages to spreading rumors and even sharing embarrassing photos or videos without consent. Chintu's story is just one example, but the scope of cyberbullying is much broader. Victims of cyberbullying often experience **depression, anxiety**, and **low self-esteem**. The harmful effects of cyberbullying can also lead to severe consequences such as withdrawal from school, loss of interest in activities, and in extreme cases, suicidal thoughts.

The session highlighted the importance of bystanders in cyberbullying cases. When children witness cyberbullying, they should not remain silent. Reporting the bully to a teacher, parent, or platform administrator can help stop the abuse. Platforms like Facebook and Instagram have built-in tools for reporting harassment and bullying, which children should be encouraged to use.

The club also stressed the legal consequences of cyberbullying. In some cases, cyberbullying can lead to criminal charges, especially if it involves threats, harassment, or the dissemination of private materials without consent.

Legal Implications of Cyberbullying:

- Cyberbullying can be prosecuted under the **IT Act, 2000**.
- Victims can file complaints with **cyber police**.
- Social media platforms have reporting tools for harassment.

3. Mobile Phone Security

With the increasing use of mobile phones among children, their security risks have also grown. Children are quick to explore new apps and features, but many apps are designed with vulnerabilities that can compromise personal data.

Bunny's story is a good example of how downloading unverified apps can lead to problems like **location tracking**. Another concern is **malware**—apps that are seemingly harmless but can collect data such as contacts, messages, and even passwords.

During the session, the importance of **regular updates** and **mobile security software** was discussed. Children should be encouraged to download security apps that scan for viruses and protect their data. Furthermore, features like **two-factor authentication** (2FA) can be employed to add an extra layer of security.

Children should also be made aware of the **phishing scams** that can occur through text messages (SMS phishing). These scams often trick users into clicking malicious links, downloading harmful files, or sharing sensitive information.

More Security Tips:

- Avoid using public Wi-Fi without a VPN (Virtual Private Network).
- Enable **remote wipe** options in case the phone is lost or stolen.
- Use strong and unique passwords for different accounts.
- Turn off location services unless necessary.

4. Mobile Phone Addiction

Mobile phone addiction is becoming a global issue, particularly among children and teenagers. The overuse of mobile devices can lead to a range of problems, including **sleep disorders**, **academic decline**, and even **social isolation**. In Sunny’s case, his excessive phone use affected his family relationships and school performance.

The session also introduced the concept of **nomophobia**, or the fear of being without a mobile phone. This can cause constant anxiety and the compulsive need to check one's phone, even in inappropriate situations, like during class or family gatherings.

Parents and educators should collaborate to set healthy limits on screen time. Simple strategies like **turning off notifications**, using **screen-time management apps**, and setting specific times for mobile usage can significantly reduce the risk of addiction.

Consequences of Mobile Addiction:

- Impaired concentration and academic performance.
- Increased **risk of accidents** due to distracted walking or driving.
- Psychological issues like **depression** and **anxiety**.

Solutions:

- ▪ Introduce digital detox periods where no electronic devices are used.
- ▪ Encourage children to engage in physical activities or hobbies.
- ▪ Educate children on the value of **face-to-face communication** over texting.

5. Meeting Strangers Online

The dangers of meeting strangers online are multifaceted. The session discussed how Raju was tempted to meet his online friend without telling his parents. This situation is common, as children can be lured by strangers offering **gifts**, promises of friendship, or even opportunities in gaming or online communities.

In more dangerous scenarios, children can fall victim to **human trafficking** or **sexual exploitation** when they meet people they only know from online interactions. The club reiterated that while the internet is a great way to connect with new people, it is crucial to be cautious. Children were advised to never meet someone they don't know in real life without a trusted adult accompanying them.

Detailed Advice for Meeting Online Friends:

- Always meet in **public places** and inform multiple people about the meeting.
- Do not share real-time location with online friends.
- Block or report individuals who pressure for a meeting without parental consent.

6. Online Gaming Addiction

Online gaming is a popular pastime, but excessive gaming can lead to addiction, particularly in children. **Vijay's** case demonstrated how gaming addiction can disrupt sleep patterns and academic performance.

Online games often use **reward systems** to keep players engaged, encouraging long periods of play to achieve higher ranks, unlock features, or receive virtual rewards. This mechanism can lead to neglecting schoolwork, social isolation, and even **health problems** like obesity due to inactivity.

The session also touched on the **financial risks** of online gaming, particularly when games have **in-app purchases** or **loot boxes** that require real money. Children may unknowingly spend large amounts on virtual items, which can result in financial stress for their families.

Solutions for Online Gaming Addiction:

- Set time limits on gaming, allowing no more than one hour a day.
- Encourage outdoor play or other hobbies to balance screen time.
- Use parental controls to manage in-game purchases and screen time.

7. Picture Morphing and Online Harassment

Picture morphing is becoming a common method for online harassment, where personal images are altered to create explicit or inappropriate content. This was highlighted through **Raveena's** story, where her images were morphed and shared online without her consent.

The club discussed how morphed images are used to **blackmail** individuals or damage their reputation. Victims of morphing often face severe emotional trauma and may feel helpless in the face of online abuse. Children were advised to be cautious about the images they upload and to avoid oversharing on social media platforms.

Additionally, the session touched on the legal aspects of picture morphing, which is considered a serious crime under **cyber laws**. Children were encouraged to report such activities immediately.

Legal Action and Protection:

- Victims can file a complaint with the **Cyber Crime Cell**.
- Social media platforms can be asked to remove morphed images.
- Laws like the **IT Act, 2000** offer protection against image misuse.

Conclusion

The **Cyber Ethics Awareness Program** conducted by Alva's Cyber Security Club was a resounding success, providing valuable insights into safe internet usage. With the rapid growth of the internet and mobile technologies, children face unprecedented online threats. This session empowered them with the knowledge and tools needed to navigate these challenges safely.

From learning about online predators and cyberbullying to mobile security and the dangers of online gaming, the program covered all aspects of online safety. The stories and real-life examples used during the session made these issues relatable and impactful for the students.

Moving forward, it is essential to continue educating children on cyber safety, making them aware of the evolving risks in the digital world. Schools, parents, and communities must collaborate to ensure that the younger generation grows up with a responsible and ethical approach to technology.

Galaxy A73 5G
12:59 pm

09/12/23

Head of the Department
Dept. of Computer Science & Engineering
Alva's Institute of Engineering and Technology
Mijar, Moodubidire - 574 225, D.K. Karnataka, India