



Webinar on

Cybersecurity & Impact of Social Media

Date: 06th September 2025, Saturday

Organised By

Odisha School Education Programme Authority (OSEPA)
Bhubaneswar

In Collaboration with

UNICEF Odisha

Technical Partner

IDENTITY Foundation Trust



IDENTITY
FOUNDATION

About the Collaboration:

The **Odisha School Education Programme Authority (OSEPA)**, under the Department of School & Mass Education, Government of Odisha, in collaboration with **UNICEF Odisha** and its technical partners, conducts career guidance webinars for secondary school students. These sessions are designed to empower students of grade 9th & 10th with the knowledge and confidence to make informed career decisions. The initiative focuses on strengthening the transition from school to higher education and the world of work through structured, student-friendly career awareness and guidance interventions.

About the Webinar Series:

As part of the ongoing career guidance initiative, the webinar was successfully organised by the Odisha School Education Programme Authority (OSEPA) on **06th September 2025 (Saturday) at 10:30 AM**. Held at the OSEPA Rushikulya Conference Hall, the session focused on the topic **“Cybersecurity & Impact of Social Media”**. The webinar was attended by students and faculty members from Grades 9 and 10, along with key officials from OSEPA. The session began with a welcome address by Mr. Tanmay Behera (OES), Deputy Director, Vocational Education, OSEPA, who warmly greeted the resource person, moderator, students, and teachers for participating in the webinar.

About the Resource Person:

ACP Akshaya Kumar Nayak is a seasoned law enforcement professional currently serving as the Assistant Commissioner of Police (ACP) and Officer-in-Charge of the Cyber Crime and Economic Offences Police Station in Bhubaneswar, Odisha. With over 24 years of extensive experience in policing and a specialized focus on cybercrime investigation and digital forensics since 2011, ACP Nayak has established himself as a leading expert in combating cyber threats within the state.

He holds multiple academic qualifications including a Master of Arts, Bachelor of Laws (LLB), Bachelor of Education (B.Ed.), and Bachelor of Science degrees from reputed institutions such as Indira Gandhi National Open University and Utkal University. Additionally, he has completed a postgraduate certificate in Cyber Law, equipping him with a robust understanding of the legal frameworks surrounding cyber offenses.

ACP Nayak is well-regarded for his active role in training and capacity building, frequently conducting sessions on cyber laws, major criminal laws, and cybersecurity awareness for police officers and scientific personnel. His commitment to continuous professional development is reflected in his recent completion of Mastercard's Cybersecurity Program, which enhanced his insight into global cybersecurity practices, risk mitigation, and threat analysis.



His expertise spans cybercrime investigation techniques, digital forensics, penetration testing, OSINT (Open-Source Intelligence), and cyber threat intelligence. ACP Nayak has contributed as a resource person in national consultations on cyber laws related to women and has demonstrated leadership in investigating complex VoIP-related cybercrime cases.

Welcome Note by the Moderator:

Mr. Jasobant Narayan Singhlal, Founder and Director of Identity Foundation Trust, moderated the Session 3 of the Career Webinar Series by warmly welcoming students and teachers from various schools. He encouraged students to actively engage in the session by attentively listening to the resource person and thoughtfully absorbing the shared insights. Mr. Singhlal emphasised the importance of such sessions in helping students and teachers mark safe from cyber threats and frauds being in the digital world. He highlighted that gaining clarity about cybersecurity and online safety requires curiosity and active participation. To that end, he urged students to not hesitate in asking questions during the session, as open dialogue is a key part of meaningful learning. His remarks set a motivating tone for the session, aiming to inspire students to take charge of their future career choices.



We're in Digital World:

The Resource Person (RP) highlighted that we all are living in a digital world and most of us are carrying a smart phone in our hand as the first step in the digitally smart world. However, we need to think that how much we're safe with our smart gadgets like smart phones. He highlighted that, the students being in their adolescent age, have been using social media platforms like Instagram, Facebook, WhatsApp, Snapchats, etc. However, they are not concern about their security while creating their digital footprint. This has also increased digital addiction amongst the young generation. Hence, he urged to take maximum precautions and distance yourselves from digital addiction as much as possible.

Common Cyber Threats, its Consequences & Precautions:

While discussing common cyber threats, the Resource Person emphasized that a significant number of young individuals are increasingly becoming emotionally influenced by social media platforms. This vulnerability often arises when strangers compliment or comment on their photos and short videos, prompting them to share more personal content. Many young users frequently update details of their daily lives on platforms such as Instagram, Snapchat, and Facebook, inadvertently exposing sensitive

information. Cyber attackers exploit these details to create fake profiles, which are then misused for unethical or criminal activities, including fraud and online harassment.

The Resource Person cautioned that when young individuals frequently share details of their daily activities online, cyber attackers often track these patterns, leading to severe consequences. Such oversharing has resulted in heinous crimes, including kidnapping, abduction, blackmail, and the creation of deepfake profiles. He stressed the critical need for awareness and discretion in digital behaviour to safeguard against such malicious threats.

A particularly concerning trend is that children often register their accounts using their parents' personal information. Consequently, when such data is misused, unsuspecting parents may face legal or social complications despite having no direct involvement. The RP strongly advised students to exercise caution while engaging online, underscoring the importance of digital literacy and responsible social media usage.

The Resource Person further advised young participants to refrain from excessively documenting and publicizing every aspect of their personal lives on social media. He suggested that, whenever possible, students should share group photographs rather than individual images and practice minimalistic sharing to safeguard their privacy. He also drew attention to the concept of "Digital Detox," advocated by the Hon'ble Prime Minister of India, Shri Narendra Modi. Elaborating on the idea, he explained that Digital Detox involves the conscious reduction or temporary elimination of digital device and social media usage. This practice not only enhances mental and physical well-being but also nurtures stronger interpersonal relationships, sharpens concentration, and allows individuals to reconnect with the present moment in a more meaningful way.



Phishing & Spoofing Attack:

While elaborating on the various types of cyberattacks, the Resource Person explained in detail the concepts of **phishing and spoofing**. He emphasised that phishing is one of the most prevalent forms of cybercrime, wherein attackers masquerade as credible institutions such as banks, government



agencies, or reputed organisations to deceive individuals into divulging sensitive personal information. These details may include passwords, banking credentials, or credit card numbers.

Phishing attempts are typically carried out through deceptive emails, fraudulent text messages, or counterfeit websites designed to mimic legitimate portals. For instance, a victim may receive an email that appears to be from their bank, urging them to “verify their account” by clicking on a link, which then redirects to a fraudulent site engineered to capture their login credentials.

Similarly, the Resource Person highlighted that spoofing is another sophisticated form of cyberattack where adversaries impersonate trusted individuals, devices, or networks to unlawfully gain access to data or systems. Spoofing often involves falsifying email addresses, caller IDs, or IP addresses to create the illusion of authenticity.

An illustrative example is when a cybercriminal forges an email to resemble an official communication from a senior authority, such as a company’s CEO, requesting access to confidential information.

Preventive measures to escape from Cyberattack:

By including practical safeguards, students can empower themselves not just to understand the risks, but also to protect themselves in real life. Like as;

- **Use multi-factor authentication (MFA):** Always enable two-step verification for email, banking, and social media accounts.
- **Verify URLs:** Check the website address carefully before entering credentials—fraudulent links often look similar to the original.
- **Avoid clicking unknown links/attachments:** Never open attachments or links from unverified sources.
- **Use strong, unique passwords:** And change them regularly.
- **Adopt a zero-trust mindset:** Be cautious, even if a message appears to come from a familiar person or authority.

Spam Calls & Messaged and It’s Reporting to Government for Necessary Actions:

Discussing about the spam calls and messages, the Resource Person shared that Unwanted calls or messages are known as spam, or Unsolicited Commercial Communication (UCC). These are commercial or promotional messages that are sent against your registered preferences or without your consent. Spam is, for instance, when a business contacts you about loans, sales, or other offers even though you never consented to receive them. Spam can also take the form of repeated calls or a large number of messages from unknown individuals.

For reporting of these spam messages and calls, the RP recommended that;

1. Go to the Sanchar Saathi portal website (sancharsaathi.gov.in) and find the Chakshu-Report Suspected Fraud & UCC / Spam section.
2. Choose what kind of unwanted communication you got: call, SMS, or WhatsApp.
3. Enter details like:
 - a. Your mobile number (that received the message/call)
 - b. The sender’s number (if visible)
 - c. Date and time you received it
 - d. What the message/call said (briefly) or what you saw
4. Sometimes you can attach a screenshot of the message or record the content.

5. Verify your details by OTP (one-time password) to show it's your own mobile number.
6. Submit the report. If the complaint is made within 3 days of receiving spam, action may be taken quickly. If after 3 days, the report still helps authorities to track patterns.

Ensuring Your Social Media Profiles are Safe:

The Resource Person emphasized the importance of keeping social media profiles safe from attackers or hackers. He advised that users can directly approach META's Grievance Officer for concerns related to Facebook, Instagram, or WhatsApp. To do this, users should draft a formal email mentioning their issue, such as fake profiles, harassment, or account security. The complaint must include the account details, screenshots (if any), and a clear description of the problem. META's Grievance Officer then



reviews the request and takes necessary action in accordance with the Information Technology (Intermediary Guidelines) Rules, 2021.

Government Initiatives to Address Cybercrime in Odisha:

Highlighting about the initiatives taken by the government of Odisha to address

and tackle cybercrime and economic offences, the government has introduced 35 cybercrime branches across the state where sufficient numbers of uniformed staff are deployed. In addition to that, experts including IT experts, finance & accounts analysts, and cyber forensic experts have been appointed, all ranks of police personnel (from constables to DSPs) are to receive training in cybercrime investigation, digital forensics, call detail record/IP analysis, etc. In case if you face any cybercrime or economic offence;

- **Note down details:** time, sender/caller number, message/call content, screenshots if possible.
- **Visit nearest Cybercrime or Economic Offences Police Station (CEPS)** in your district. If there is none, go to your district SP office or the cybercrime cell.
- **File an FIR (First Information Report):** give all the details. Police ask for evidence like messages, call logs, screenshots.
- **You can also use online portals:** National Cybercrime Reporting Portal or call helplines (e.g. 1930). If available, use Odisha state's cybercrime unit or online complaint mechanisms through the state police website.
- Keep copies of the complaint, acknowledgment, reference numbers. Follow up by visiting the station or via phone if needed.

Awareness against Cybercrime & Economic Offences:

While explaining the government's social media campaigns aimed at spreading awareness on cybercrime and economic offences, the Resource Person highlighted the initiatives **CyberDost** and **ISEA**. He strongly encouraged all students and teachers to actively follow these official Instagram pages to stay informed and practice safe digital habits.

Cyber Dost:

- **CyberDost** is an awareness campaign run by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs (MHA), Government of India.
- It uses social media platforms like Twitter, Facebook, Instagram, and Telegram to share simple tips, short videos, images, creatives, and advice on how people can stay safe online.
- Examples of advice from CyberDost include:
 - Avoid clicking suspicious links or installing unknown apps.
 - Be careful about permissions you give to apps (for example, access to camera, contacts).
 - Dial **1930** to report financial cyber fraud or file complaints via **National Cyber Crime Reporting Portal (cybercrime.gov.in)**.



ISEA - for Information Security Education & Awareness

- ISEA stands for Information Security Education & Awareness. It is a Government of India initiative under the Ministry of Electronics & Information Technology (MeitY).
- It began in 2005, and as of October 2023 is in its third phase. Its goal is to develop human resources and to increase awareness among citizens about cyber hygiene, safe digital behavior, and information security.
- ISEA has four major verticals (or focus areas):
 - Training and certifying roles like CISOs (Chief Information Security Officers) and other cybersecurity professionals.
 - Grooming students and encouraging innovation (ideas, products, solutions in cybersecurity).
 - Strengthening research and academic education in emerging areas of information security (e.g. cryptography, AI, network security).
 - Creating Cyber-aware “Digital Naagriks” (citizens) through mass awareness — teaching people about safe practices online, protecting privacy, avoiding phishing etc.
- ISEA also offers programs such as Cyber Shakti (for women), Cyber Shikshak (for teachers), and various role-based awareness and progression pathways.

Conclusion:

The webinar on Cybersecurity and the Impact of social media provided valuable insights to rural students of Grade 9 and 10 in Odisha, equipping them with essential knowledge to navigate the digital world safely. The session highlighted common cyber threats, responsible use of social media, and the importance of protecting personal information online. Students also learned about government initiatives like CyberDost, ISEA, and the Sanchar Saathi portal, empowering them to identify and report cybercrimes effectively. The program fostered awareness, responsibility, and confidence, enabling young learners to embrace technology while ensuring their digital safety and well-being.

Queries Answered During the Session:

If I want to be a social media content creator, then how can I ensure that my profile on Instagram is not in the radar of cyber attackers?	To protect your Instagram profile as a social media content creator from cyber attackers, consider the following key measures: ● Use a strong, unique password combining letters, numbers, and symbols. ● Enable two-factor authentication (2FA) for an extra layer of security, requiring a verification code alongside your password. ● Set your account to private to control who can see your posts and stories. ● Regularly review followers and block any suspicious or unknown accounts. ● Carefully manage permissions for third-party apps connected to your account. ● Avoid logging in from public or shared Wi-Fi networks; always use protected, trusted internet connections. ● Keep your device's operating system and Instagram app updated to fix security vulnerabilities. ● Use trusted antivirus and anti-malware software. ● Be cautious of phishing attempts via direct messages or emails asking for login info. ● Avoid clicking on suspicious links or sharing personal details publicly. ● Regularly check login activity in Instagram settings for unfamiliar devices or locations. ● Enable contact recovery options via phone number and email, and keep them up to date. ● Regularly backup content to prevent data loss. By combining strong security practices with cautious online behaviour, you can significantly reduce the risk of cyber threats targeting your Instagram account.
How can we ensure that our parents are not getting trapped in any cyber threats?	To protect parents from falling victim to cyber threats, several proactive steps can be taken: ● Regularly educate parents about common cyber threats like phishing, scams, malware, and identity theft. ● Teach them to recognize suspicious emails, messages, and links and avoid sharing personal or financial information online. ● Help them set strong, unique passwords for all online accounts, ideally using a password manager. ● Enable two-factor authentication (2FA) on critical accounts, such as email and banking. ● Ensure their devices have updated antivirus software and the latest security patches installed. ● Guide parents to adjust privacy settings on social media and communication apps to limit data exposure. ● Discourage clicking on unknown links or attachments in emails or messages. ● Encourage the use of secured Wi-Fi networks over public networks.

	● Periodically review their devices for any unusual activity or unfamiliar apps. ● Assist with setting up alerts for financial transactions to detect fraud early. ● Maintain open communication so they feel comfortable reporting any suspicious online activity. By combining education, robust security measures, and supportive monitoring, parents can be safeguarded effectively against cyber threats.
How can we report to the government if we face any cybercrime?	If you encounter a cybercrime in India, you can report it to the government through the following official channels: ● Visit the National Cyber Crime Reporting Portal at www.cybercrime.gov.in to file complaints related to cybercrimes such as hacking, identity theft, online fraud, or cyberbullying. ● The portal allows direct reporting and provides assistance with complaint status tracking. ● You can also report cybercrime to your local police station, which may forward the case to the specialized Cyber Crime Cell. ● Locate your nearest cybercrime police unit via state government websites. ● Contact the Ministry of Home Affairs helpline for cybercrime-related grievances. ● For child-related cybercrime, report to www.cybercrimehelpline.gov.in or cybercrime helpline (1093) the Childline helpline (1098). ● Provide detailed information including screenshots, URLs, dates, and descriptions. ● Keep copies of all communication or evidence related to the cyber incident.
What is the best way to practice digital detox?	The best way to practice a digital detox involves a combination of mindful planning, setting boundaries, and creating healthy habits: ● Define the purpose of your digital detox (reduce stress, improve focus, better sleep). ● Choose a specific period for detoxification, such as a few hours daily, a full day weekly, or a weekend. ● Designate areas at home (e.g., bedroom, dining table) where digital devices are not allowed. ● Establish specific times, like during meals or one hour before bedtime, to stay offline. ● Turn off non-essential notifications to minimize distractions. ● Use apps that track screen time and set limits on social media or entertainment apps. ● Engage in hobbies such as reading, walking, exercising, or spending quality time with family and friends. ● Practice mindfulness or meditation to reconnect with self-awareness. ● Start by reducing usage gradually rather than abruptly. ● Inform close contacts about your digital detox to gain their support and understanding.

By consistently implementing these strategies, a digital detox can improve mental well-being, productivity, and real-world connections.

YouTube Engagement Analytics:

Total views during YouTube Live	5,389
Average view duration	14:52 minutes
Peak concurrent viewers	1,550

Attendees Details:

Districts	No. of Schools	No. of Attendees for Class IX		No. of Attendees for Class X	
		Boys	Girls	Boys	Girls
Angul	110	2733	2831	2712	2796
Balasore	52	1234	1236	1084	1144
Bargarh	6	197	135	183	143
Bhadrak	82	1975	1881	1808	1748
Bolangir	42	812	1063	694	978
Boudh	23	475	610	412	561
Cuttack	21	631	460	573	408
Deogarh	23	441	358	437	356
Dhenkanal	54	1305	1286	1131	1142
Gajapati	3	5	51	16	67
Ganjam	167	4268	4252	3901	3960
Jagatsinghpur	106	1845	1857	1748	1806
Jajpur	27	622	616	520	515
Jharsuguda	59	943	1108	947	1083
Kalahandi	44	752	804	820	813
Kandhamal	69	1106	1873	1083	1834
Kendrapara	85	1719	1812	1657	1647
Keonjhar	5	95	157	86	123
Khordha	2	94	95	65	71
Koraput	49	1338	1651	1304	1549
Malkangiri	10	242	267	264	243
Mayurbhanj	78	1570	1677	1420	1571
Nabarangapur	1	89	15	105	25
Nayagarh	6	109	137	103	129
Nuapada	35	846	955	773	871
Puri	16	288	369	287	360
Rayagada	30	533	1088	418	924
Sambalpur	32	644	841	556	714
Sonepur	17	181	278	224	248
Sundargarh	7	167	169	142	185
Total		27,259	29,932	25,473	28,014
Grand Total		57,191		53,487	
		1,10,678			

Photos from the Ground:

