



Webinar on

Cybersecurity & Impact of Social Media

Date: 20th December 2025, Saturday

Organised By

**Directorate of Higher Secondary
Education (DHSE), Bhubaneswar**

In Collaboration with

UNICEF Odisha

Technical Partner



**IDENTITY
FOUNDATION**

About the Collaboration:

The **Directorate of Higher Secondary Education (DHSE)**, 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 grades 11 & 12th 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 **Directorate of Higher Secondary Education (DHSE)** on 20th December 2025 (Saturday) at 12:00 PM. Held at the DHSE Conference Hall, the session focused on the topic “Cybersecurity & Impact of Social Media”. The webinar was attended by students and faculty members from Grades 11 and 12, along with key officials from OSEPA. The session began with a welcome address by Ms. Niyati Pattnaik (IAS) Director, DHSE, who warmly greeted the resource person, moderator, students, and teachers for participating in the webinar.

Number of institutions attended in the webinar	117	
Number of students attended the webinar	12,526	
Number of Boys from Grade 11, attended in the webinar	2337	6933
Number of Girls from Grade 11, attended in the webinar	4496	
Number of Boys from Grade 12, attended in the webinar	2091	5693
Number of Girls from Grade 12, attended in the webinar	3602	
Number of teachers/faculties who attended the webinar	816	
Number of male teachers attended the webinar	380	
Number of female teachers attended the webinar	436	

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 specialised focus on cybercrime investigations 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 offences.

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 Session 12 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 stay safe from cyber threats and frauds 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 a Digital World:

The Resource Person (RP) highlighted that we all are living in a digital world, and most of us are carrying a smartphone in our hand as the first step in the digitally smart world. However, we need to think about how safe our smart gadgets are, like smartphones. He highlighted that the students, being in their adolescent age, have been using social media platforms like Instagram, Facebook, WhatsApp, Snapchat, etc. However, they are not concerned about their security while creating their digital footprint. Such behaviour has also increased digital addiction amongst the young generation. Hence, he urged them to take maximum precautions and distance themselves 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 publicising every aspect of their personal lives on social media. He suggested that, whenever possible, students should share group photographs rather than individual images and practise 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 reputable 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 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 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 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, and 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 like time, sender/caller number, message/call content, and 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) by providing all the details. Police ask for evidence like messages, call logs, and screenshots.
- You can also use online portals (i.e., the 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, acknowledgement, and 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 grant to apps (for example, access to camera and contacts).
- Dial 1930 to report financial cyber fraud or file complaints via the National Cyber Crime Reporting Portal (cybercrime.gov.in).

ISEA (Information Security Education and 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, it's in its third phase. Its goal is to develop human resources and to increase awareness among citizens about cyber hygiene, safe digital behaviour, 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, and 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 programmes 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 for rural students in grades 11 and 12 in Odisha, equipping them with essential knowledge to navigate the digital world safely. The session discussed common cyber threats, how to use social media safely, and how important it is to keep personal information safe online. Students also learnt about government initiatives like CyberDost, ISEA, and the Sanchar Saathi portal, which enabled them to identify and report cybercrimes effectively. The programme fosters awareness, responsibility, and confidence, enabling young learners to embrace technology while ensuring their digital safety and well-being.

Attendance Details:

Name of The District	Institutions Count	Class XI		Class XII		Faculties		Districtwise Total Students
		Boys	Girls	Boys	Girls	Male	Female	

Angul	7	95	162	94	148	14	18	499
Balasore	7	59	325	72	247	29	23	703
Baragarh	4	95	146	103	169	14	12	513
Bhadrak	6	103	195	58	134	12	13	490
Bolangir	8	337	529	340	469	36	21	1675
Cuttack	7	19	259	13	189	20	35	480
Deogarh	1	25	30	30	36	2	3	121
Dhenkanal	3	78	154	88	109	11	9	429
Gajapati	2	16	25	30	20	4	2	91
Ganjam	8	149	205	96	182	29	30	632
Jagatsinghpur	4	23	148	31	146	15	20	348
Jajpur	2	22	85	0	15	4	11	122
Jharsuguda	2	41	58	11	20	2	2	130
Kalahandi	4	101	177	84	142	23	7	504
Kandhamal	1	25	18	0	0	2	3	43
Kendrapara	4	87	143	87	86	22	13	403
Keonjhar	5	125	262	117	191	15	12	695
Khurda	7	99	262	63	176	27	70	600
Koraput	4	40	239	71	72	13	14	422
Malkangiri	1	48	82	73	41	5	3	244
Mayurbhanj	7	224	227	165	204	17	12	820
Nawarangpur	2	57	49	48	48	5	11	202
Nayagarh	1	0	65	0	100	2	8	165
Nuapada	2	47	58	32	55	5	10	192
Puri	1	34	49	29	41	2	15	153
Rayagada	2	73	77	79	83	6	3	312
Sambalpur	5	36	98	30	104	10	13	268
Sonepur	1	10	15	25	37	10	2	87
Sundargarh	9	269	354	222	338	24	41	1183
Gender-wise Total	117	2337	4496	2091	3602	380	436	12526
Class-wise Total		6,833		5,693		816		

Photos from the Ground:

