



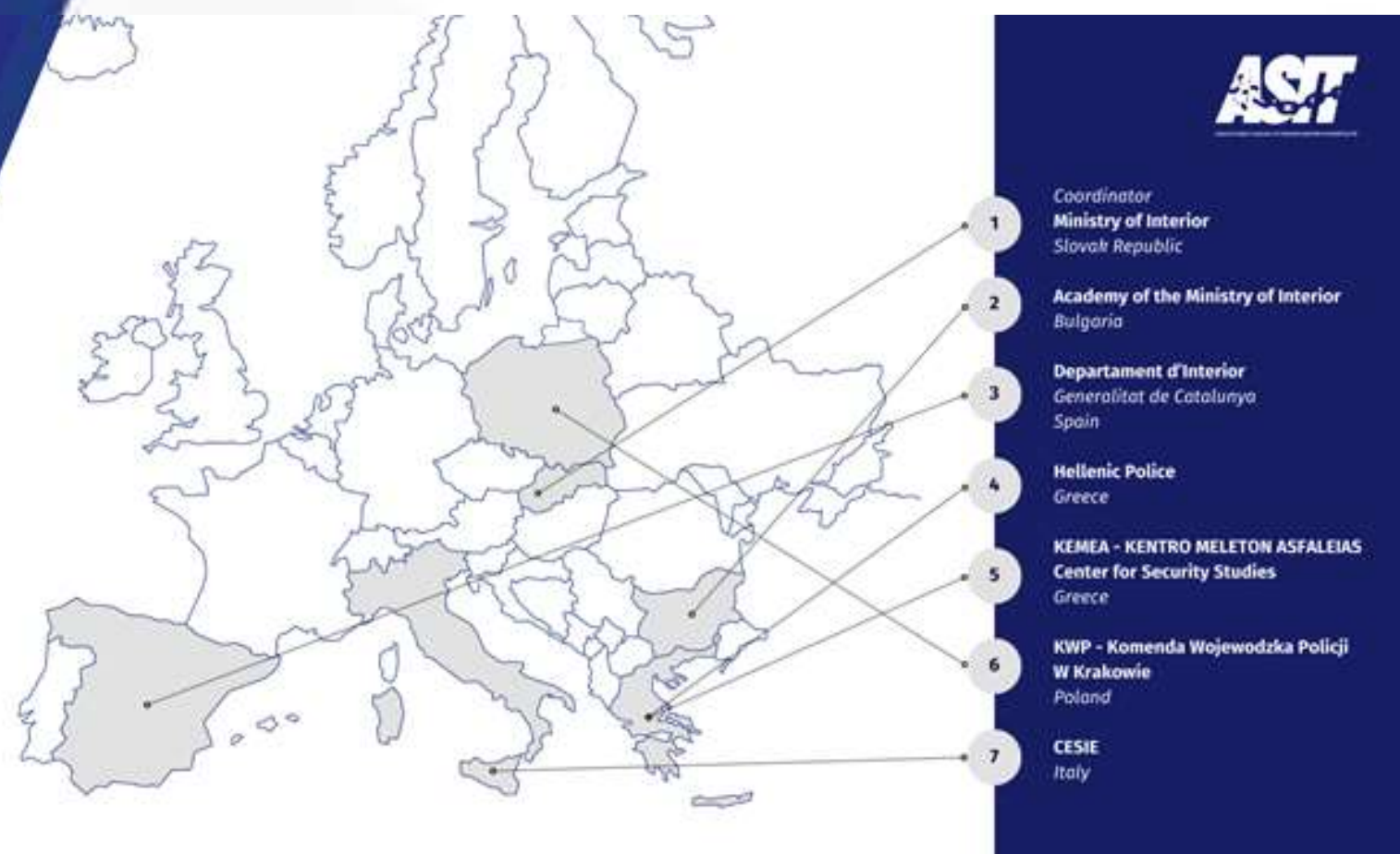
Algorithms Support Measures and Improved Capacity in Countering Trafficking



Co-funded by
the European Union

TRAFFICKING IN HUMAN BEINGS SELF-LEARNING COURSE

A module about technology-facilitated trafficking and how to identify digital footprints



ASIT Initiative

- The self-learning module is part of an inter-agency project and is available in various languages. Each language version also reflects on the national specifics.
- The international initiative ASIT aims to tackle new forms of human trafficking by promoting the ability to identify victims and uncover the modus operandi of perpetrators across a wide range of stakeholders.
- The seven European partners collaborate to create a network of collaborative intervention teams that share data and information supported by technological tools.
- The international actions support the improvement of identification and protection of victims of trafficking in human beings by networking frontline workers and LEA and **building professional capacities**, making available methodologies and digital tools to mitigate the risks of trafficking and protecting vulnerable groups by raising awareness and cooperation.

Practical information



- ✓ This self-learning course is designed to enhance abilities and knowledge about the technologies used by traffickers and how technologies could help preventing from the attempts and/or crimes of trafficking in human beings.
The course is for everybody.

If you are technology firm, online service provider and data manager, take advantage of this course and contribute to our joint efforts in combating human trafficking facilitated in the digital world.

- ✓ Return to the course is available repeatedly.

- ✓ By completing this module, the participant will learn about the THB and its digital footprints. The knowledge can be applied in daily work and private life. Thus, he/she will help raise awareness in identifying signs of human trafficking and refer the victim to authorities that can provide protection and help.

- ✓ The estimated duration of the self-learning is approximately 60 minutes, but we recommend that each participant complete it at an individual pace and in suitable conditions for adequate information acquisition.

Course outline

The self-learning modules is divided into four blocks.
Introduction to main learning objectives.

- ✓ The introduction part examines how traffickers systematically use digital tools to identify, manipulate, and control victims, creating a web of dependency that can be difficult to escape.
- ✓ The definition of human trafficking has evolved significantly in the digital age, with perpetrators leveraging technology throughout the exploitation cycle.
- ✓ The identification section will bring knowledge that will help correctly identify the online perpetrator's activities;
- ✓ The last part is to encourage greater technology development and use for decreasing the risk of trafficking in human beings.

1 INTRODUCTION

2 DEFINITION

3 IDENTIFICATION

4 SUPPORT & PROTECTION

Human trafficking as a global problem



latent, hidden criminal activity of the perpetrators

to illustrate the dimension of human trafficking, the vast majority of publications and reports only provide estimates of the number of victims, or estimates of the profits of illegal groups of human traffickers



the most profitable illegal activities

human trafficking ranks among the top three most profitable illegal activities, along with drug and arms trafficking



49,6 milion victims worldwide

according to data published by the International Labour Organization (ILO), the International Organization for Migration (IOM) and the Walk Free organization, there are an estimated 49.6 million victims of human trafficking worldwide



236 billion US dollars

according to estimates by the International Labour Organization (ILO) from 2024, the annual profits of human traffickers represent volumes of illegally acquired funds amounting to 236 billion US dollars

PART 1

ASST

INTRODUCTION

Adequate Support measures and Improved capacities in countering THB

Learning objectives

By completing this self-learning modul participant will gain an overview

- ✔ On how to identify technology-based approaches of perpetrators to get in contact with a victim of human trafficking and control them.
- ✔ About the red flags for identifying the misleading recruitment and digital gaps and better understanding additional “invisible” vulnerabilities of victims
- ✔ Technology developers and facilitators of online marketplaces gain valuable insights into how to enforce the functionalities of their products to decrease the risk of misuse and technology-facilitated trafficking in human beings.

Course benefits

- 1 raising awareness**
Education increases general knowledge of human trafficking and its forms in the technology-supported world.
- 2 early identification**
Knowing about the dark side of the technologies enables the implementation of early identification tactics against perpetrators' attempts.
- 3 ensuring timely intervention**
Mastering principles of identification and knowing about the possibilities of help and support for victims of human trafficking.
- 4 improvement of monitoring and protection**
Learning how to improve equipment and solutions for monitoring, following and investigating traffickers and protecting victims.

Course overview



Introduction

Scope

The course is divided into **four parts** (introduction, definition, identification and referral mechanism/reporting). The education module is available **online**, which can be completed in approximately one hour. Alternatively, the learning content is **downloadable** and can be used as a **support tool in the operational and daily work of anybody who might encounter a victim of trafficking. It can also contribute to awareness of vulnerable groups or produce information materials or SW, apps, plug-ins, or tools to decrease or prevent** potential criminal activities.

Content

Provided minimum required knowledge to watch for the signs of a trafficked person, the possibilities of assistance for a victim of human trafficking and forms of reporting to the relevant entities.

Target group

Information Technology Companies/Platforms, e-business providers and all front-line workers, everyone who want to know more about hidden technological gaps making the trafficking of human beings possible.

Training output

Knowledge about technology misused by perpetrators and how technology can help to prevent from trafficking in human beings.

Online service providers - responsibilities

- Control of job advertisements,
- Job advertisement validations plug-ins/tools,
- Tools to scrape job advertisement sites and apply markers for preventing the misuse of platforms for victimising persons in trafficking,
- Online confidential reporting allows anonymous reporting of THB cases to identify trafficking in human beings instances,
- Accessible mechanism for clients to flag up suspicious advertisements/activities,
- Raising awareness of technology-related risks

Does human trafficking happen only in physical space?

No, human trafficking is happening also in virtual world.

Yes, human trafficking is happening just and only in the physical space.

Adequate Support measures and Improved capacities in countering THB

PART 2

The background features the letters 'ASST' in a large, bold, dark blue font. A chain graphic, also in dark blue, is overlaid across the letters, with links connecting the 'S' and 'T' characters.

DEFINITION

Adequate Support measures and Improved capacities in countering THB



Definition

DEFINITION of human trafficking

Directive 2011/36 /EU (supplemented by Directive 2024/1712) expanded the definition of human trafficking given by the Palermo Protocol for other purposes as follows

ACT

recruitment, transportation, transfer, harbouring or reception of persons, **including the exchange or transfer of control over those persons**

MEANS

the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person

PURPOSE

as a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, **including begging**, slavery or practices similar to slavery, servitude, **the exploitation of surrogacy, of forced marriage, of illegal adoption or the exploitation of criminal activities**, or the removal of organs.

Please use self-learning modules no. 5 to gain complete information about international legislation and the legislation of the selected 6 EU MS.

PART 2

Technology against technology in trafficking in human beings

Adequate Support measures and Improved capacities in countering THB



Definition

Essentials

Online Recruitment

Traffickers often use social media platforms, job posting sites, and dating apps to lure victims: fake job offers or misleading advertisements promising lucrative opportunities.

Anonymous Communication

Encrypted messaging apps and other communication tools allow traffickers to operate covertly.

Financial Transactions

Digital payments, including cryptocurrencies and e-wallets, can facilitate anonymous payments for trafficking services, making it difficult to trace the money flow back to the traffickers.

Digital Platforms and Trafficking

The rise of digital platforms has, unfortunately, provided traffickers with new avenues to exploit vulnerable individuals. Online advertisements and social media can lure victims or promote illegal services.

PART 3

IDENTIFICATION

Adequate Support measures and Improved capacities in countering THB



Misuse of technology

Traffickers use technology for "trapping and exploiting a person using deception, violence, or coercion."

Usual activities of perpetrators assisted by technology of apps, websites and mobile phones:

- to recruit, control, market, and exploit vulnerable individuals
- to advertise false jobs, sell victims online, and transfer cryptocurrency
- to communicate and control the (potential) victims

Most used technologies

- Smartphone texting features – sometimes traffickers provide the victims with smartphones with embedded IT tools to control, monitor and manipulate the victims remotely,
- Private messaging apps
- Voice Over IP (VoIP) to communicate with buyers
- Tracking the victim's movements to display dominance and control
- Digital manipulation through a job offer scam
- Social media sites are used for recruiting potential victims
- Internet became the top recruitment location for all trafficking forms



Recruitment: Digital traps (examples)

Technology provides traffickers with abilities to:

- Craft online strategies, utilising social media platforms and employment websites to cast wider nets for potential victims,
- Access to vulnerable individuals while maintaining anonymity and distance.
- Create elaborate digital personas and false opportunities tailored to target specific vulnerabilities.
- Advertise high-paying jobs with minimal qualifications, modelling opportunities, or romantic relationships.
- Appeal to individuals facing economic hardship, seeking better opportunities, or longing for connection—making the recruitment process both targeted and efficient.
- Conduct extensive research on potential victims by analysing their social media profiles and identifying insecurities, financial difficulties, or family problems that can be exploited.
- Craft personalised approaches that increase their success rate when making initial contact.
- Operate across multiple platforms and jurisdictions, quickly shutting down accounts when detected and establishing new digital identities to continue their operations with minimal disruption.

Understanding the Technology Enabled Cycle of Exploitation



Identification

Identification & Targeting

Traffickers use social media platforms and online forums to identify vulnerable individuals, looking for signs of emotional distress, financial hardship, or isolation. They analyse public profiles to craft personalised approaches based on victims' interests, needs, and vulnerabilities.

Trust Building & Grooming

Using messaging apps and dating platforms, traffickers establish seemingly genuine relationships, offering emotional support, romantic interest, or promising opportunities. They maintain constant communication to create emotional dependency and slowly normalise inappropriate behaviours.

Isolation & Control

As the relationship deepens, traffickers use technology to separate victims from support networks, monitor communications through spyware, demand constant availability online, and create digital evidence for blackmail through compromising photos or videos.

Exploitation & Coercion

Victims are coerced into exploitation through digital means - advertising services on specialised websites, arranging "appointments" through encrypted messaging, monitoring location through GPS tracking, and using digital payment systems that leave victims financially dependent.



Identification

Understanding the Technology Communication and Control

Smartphone Communication

Traffickers exploit standard texting features and messaging apps to maintain continuous contact with victims, issue instructions, and exert psychological pressure through constant monitoring.

Secure Messaging Apps

End-to-end encrypted applications provide traffickers with secure communication channels that are challenging for authorities to intercept or monitor.

VoIP Services

Voice Over IP services enable traffickers to communicate with clients and victims using disposable numbers that are difficult to trace back to their true identities.

GPS Tracking

Location tracking features facilitate real-time surveillance of victims' movements, creating an atmosphere of complete control and hindering escape attempts.



Understanding the Technology

Powerful tool for dominance (examples)

Modern smartphones create unprecedented opportunities for constant surveillance and psychological manipulation.

- Victims are often required to answer calls or messages immediately, send photo verification of their whereabouts, or keep location services enabled at all times.
- Victims experience a sense of inescapable monitoring that erodes any sense of privacy or autonomy.
- Even when not physically present, traffickers maintain a virtual presence in victims' lives through technology, making the control feel absolute and escape seem impossible.
- Additionally, digital means are used to isolate victims from supportive networks.
- These include monitoring social media accounts,
- Intercepting communications with family or friends, and
- Gradually cutting off legitimate social connections.
- Digital isolation diminishes opportunities for intervention or escape.



Identification

Understanding the Technology

Technology-driven financial exploitation examples

Cryptocurrency Transactions

Anonymous digital currency transfers that are difficult to trace or block

Identity Concealment

Tools that hide traffickers' identities during financial operations

Digital Wallets

Secure online accounts for storing illegal proceeds outside traditional banking systems

Money Transfer Services

Online platforms that facilitate quick cross-border transactions with minimal verification

The financial aspects of human trafficking have been revolutionised by digital technologies, creating unprecedented opportunities for traffickers to monetise their criminal activities while avoiding detection.



Understanding the Technology

Cryptocurrencies and traffickers (examples)

Cryptocurrency is a particularly valuable tool due to its pseudonymous nature and challenges for law enforcement tracking.

Cryptocurrencies:

- Allow traffickers to receive payments without revealing their identities or locations,
- Can be transferred between traffickers across international borders instantly, without traditional banking systems' oversight or reporting requirements,
- Creates additional hurdles for investigators attempting to follow the money trail,
- Leverage various digital payment platforms that offer varying degrees of anonymity,
- Allow clients to pay for services or exploitation using methods that appear legitimate on the surface but are difficult to connect to criminal activities,
- Elaborate digital money laundering schemes, moving funds through multiple platforms and jurisdictions to further obscure their origins.

Understanding the Technology

Digital marketplace (examples)



Identification

- Creating efficient systems for connecting with potential clients while maintaining operational security.
- Authorised posting tools simultaneously place hundreds of advertisements across multiple websites.
- Search engine optimisation techniques ensure false advertisements appear prominently in relevant searches.

Content management has evolved significantly with cloud storage technologies:

- Exploitative images and videos can be stored securely online, accessible only to paying customers through password-protected portals or encrypted communication channels.
- This approach reduces the risk of physically possessing incriminating material while maintaining the ability to monetise it repeatedly.

The permanent nature of digital content creates an ongoing challenge for survivors:

- Once exploitative material is uploaded to the internet, it can be endlessly copied, redistributed, and reposted, creating a form of perpetual victimisation.
- Removed content from one platform reappears elsewhere, creating a devastating cycle for survivors attempting to reclaim their lives.

PART 3

Case study

No. 1

Adequate Support measures and Improved capacities in countering THB



Identification

Maria, a 19-year-old student struggling financially, received a message on Instagram about a modelling opportunity. The account appeared legitimate, with professional photos and testimonials. After weeks of friendly conversation and professional assurances, she agreed to travel for a photoshoot. Upon arrival, her documents were confiscated, and she was forced into sexual exploitation, with threats that compromising photos would be sent to her family if she didn't comply.

The traffickers used messaging apps with disappearing content to communicate with clients, GPS tracking to monitor her movements and withheld earnings through a digital payment system they controlled. Maria's story illustrates how traffickers seamlessly blend legitimate online recruitment with progressive manipulation, ultimately transitioning from digital grooming to physical exploitation.

Does the case study describe a human trafficking?

No. The story describes a case of sexual abuse, but not human trafficking.

Yes, Maria was a victim of human trafficking.

Could we qualify the establishment of rapid emotional relation?

No.

Yes, unusual expressions of deep feelings or offers of opportunities that seem too good to be true within short timeframes of online interaction.

Was is suspicious to be asked about her bank account number?

No, a completely normal procedure was used without any suspicious activity.

Yes, early requests for bank account details, money transfers, or personal identification documents under seemingly legitimate pretexts.

Was technology used for isolation and pressure?

The case study clearly shows that the technologies were not misused.

Encouraging secrecy about the relationship or opportunity, discouraging discussion with friends or family, or creating urgency to travel without proper planning.

What is the form of trafficking in human beings in the case study?

The case study does not describe a case of human trafficking, therefore exploitation cannot be found there.

Maria was a victim of trafficking for sexual exploitation.

What indicators can the online platform operator notice?

There are no indicators, no human trafficking.

User nickname - creation, wording, intensity of use since creation, added photos, suspicion of a child's profile.

What steps should the online platform operator take?

Nothing, just let the users using the platform.

Contact the Police.

PART 3

Case study No. 2

Adequate Support measures and Improved capacities in countering THB



Identification

Michael is a 32-year-old man facing financial difficulties after losing his job during an economic downturn.

While searching online job boards, he discovered what appeared to be a legitimate opportunity for well-paid work abroad in the hospitality industry. The recruiter established contact through a professional-looking email address and conducted several video interviews, presenting convincing documentation and contracts.

After Michael accepted the position, the recruiter arranged and paid for his travel documents and transportation. Upon arrival in the destination country, the situation rapidly deteriorated. His passport was confiscated "for processing," and the promised job never materialised. Instead, he was forced to work in a restaurant under exploitative conditions, with his wages withheld to "repay" his travel costs and accommodation.

The traffickers installed tracking apps on the smartphone they provided for "work communication," monitored his limited internet access, and threatened to release embarrassing manufactured photos to his family if he attempted to seek help. They also controlled his digital identity by maintaining possession of his documents and limiting his access to communication platforms.

Is this a case of human trafficking?

Yes, the case study describes a trafficking in human beings case.

No, the case does describe any human trafficking.

Did Michael get contracted by official job placement company?

He used the official website of a job placement agency.

He was not contracted by a legally authorised agency.

What forms of coercion did you notice in the case study?

None of form of coercion was in the case study.

For example threat of violence, monitoring and control, debt bondage.

Was a dept bondage in place?

No, Michael did not borrow money from the perpetrator.

Yes, the recruiter arranged and paid for his travel documents and transportation to make Michael financially dependent on him.

Did the trafficker maintain control through the use of technologies?

No, the person was not monitored at all.

Yes, a tracking map was installed in the smartphone.

Could Michael travel?

No, he was confined to the place of work cause his travel documents were “confiscated”.

Yes, he could.

Were threatening methods in place?

Yes, the perpetrator threatened to release embarrassing manufactured photos to his family if he attempted to seek help.

No, Michael was not physically abused.

PART 3

Signs and Digital footprints of THB

Adequate Support measures and Improved capacities in countering THB

Indicators

Anybody can identify a potential /assumed victim of trafficking based on a list of indicators and their compliance with the knowledge about the criminal phenomenon of trafficking in human beings.

It is necessary to define **what an indicator actually is.**

✔ An indicator is a signal that alerts an observer to the possibility that an individual may be a potential victim of human trafficking.

✔ The indicators serve as guidelines or markers to help identify a victim's appearance or behaviour.

For instance, instead of appearing withdrawn and closed off, a victim may display signs of aggression

✔ or erratic behaviour. In some cases, the individual might appear overly cheerful or even hysterical.



Different digital platforms present unique trafficking indicators based on their features and user interactions.

Understanding these platform-specific warning signs is essential for effective detection and intervention.

Each online environment creates distinct opportunities for traffickers, resulting in specialized techniques tailored to platform architecture and user behaviour patterns.

General signs in virtual world

Identification



Age-Inconsistent Online Activity

Online behaviours do not align with a person's stated age: minors with profiles suggesting adult-oriented services, individuals with knowledge of adult venues that are inappropriate for their age, or discussions of travel patterns and locations that are inconsistent with their education or employment status.

Unusual Digital Location Patterns

Frequent and unexplained location changes, visible through check-ins, geotagged posts, or dating app locations, can indicate movement typical of trafficking circuits, such as posts from hotels or locations known for their involvement in trafficking activities.

Suspicious Timing Patterns

Posts or online activity concentrated during late-night hours, particularly when combined with signs of sleep deprivation in images, can suggest controlled working conditions. Similarly, patterns showing 24/7 online availability or responses at unusual hours may indicate exploitation.

Digital isolation represents another critical indicator

Victims often show signs of reduced contact with previous connections, declining or unwillingness to video chat with family or friends.

Physical indicators in digital content provide important clues, such as images of bruising, malnourishment, brands or tattoos marking ownership, or inappropriate attire for the weather conditions.



Perpetrators can be disguised by

Recruitment Language Patterns

- Traffickers often use specific linguistic patterns, including promises of fast money, modelling or entertainment opportunities that seem too good to be true.
- Job descriptions lack details, but emphasising high compensation should raise immediate concerns.

Romantic recruiters frequently use "love bombing" techniques

- Overwhelming attention and affection, followed by isolation tactics and requests for compromising images that can later be used for blackmail.

Coded Language and Symbolic Communication

- Common patterns include references to "roses," "donations," or "gifts" as euphemisms for payment; transportation offers such as "in-call" and "out-call"; and age indicators disguised as measurements or non-standard numerical references.

Network Analysis Indicators

- Perpetrator profiles often reveal connections to multiple potential victims who fit similar demographic patterns. These connections may appear as friend lists with numerous young people from vulnerable populations, particularly those expressing financial difficulties or emotional distress.



Perpetrators digital footprints

Traffickers typically **employ a recognisable progression in their communications**

- they identify vulnerabilities, offer solutions to problems, promise relationships or opportunities, and gradually introduce control mechanisms.

Trafficking networks are **characterised by coordinated posting across multiple accounts with identical or nearly identical text, images, or contact information; accounts that exhibit** geographic movement patterns consistent with trafficking circuits; and rapid profile regeneration following account shutdowns.

Financial patterns visible through **cryptocurrency transactions**, mobile payment apps, or online marketplaces can further confirm suspicions when they reveal unusual transaction frequencies or amounts that are inconsistent with stated business purposes.

Perpetrators often **display a high degree of operational security awareness**. This includes frequent platform switching to avoid detection, the use of Virtual Private Networks (VPNs) to mask locations, the utilisation of temporary phone numbers or email addresses, and the employment of encrypted communication channels.



Misleading Platform-Specific Indicators

Identification

Advertising and Classifieds Websites

- These include excessive emphasis on youth, newcomer status, or exotic ethnicity; multiple ads with different names but identical contact information; professionally photographed images inconsistent with amateur advertisements; and inconsistencies between the text and metadata regarding location.
- Price structures that indicate unusually short appointments or services described through thinly veiled euphemisms are additional warning signs.

Social Media Platforms

- Trafficking indicators include profiles with minimal personal history but extensive activity.
- accounts that appear to be operated by someone other than the person featured in images, inconsistent posting locations that align with known trafficking circuits, and
- profiles with unusually segmented audience groups.
- Features like rapid friend/follower acceptance from specific demographics, restricted commenting access on posts, and evidence of someone else controlling account access are particularly concerning when observed together.

Other Indicators of Tech Supporting THB



Identification

Encrypted Messaging Applications

- Warning signs include conversations that rapidly shift from public platforms to encrypted channels, messages containing standardised language that appears scripted rather than conversational,
- unusual timing patterns suggesting controlled access and
- conversations that quickly progress from casual introductions to requests for compromising images or in-person meetings.

Gaming Platforms and Virtual Worlds

- Gaming environments have emerged as recruitment grounds where traffickers exploit primarily young users.
- Indicators include unusually generous in-game gifts from strangers, conversations that quickly turn to personal problems, offers of real-world assistance, attempts to establish communication channels outside the gaming platform, and in-game meetups that lead to requests for personal information or offline contact.

Dating applications present particularly complex environments for human trafficking.

- red flags include profiles that emphasise the financial benefits of relationships,
- rapid attempts to move conversations off-platform,
- inconsistent location information, and
- profiles that disappear and reappear in different cities following predictable circuits.

PART 4

REPORT & PROTECTION

Adequate Support measures and Improved capacities in countering THB

PART 4

Reporting

Adequate Support measures and Improved capacities in countering THB



Protect

Can individuals report suspected human trafficking anonymously?



Yes, individuals can often report suspected human trafficking anonymously.

Various channels facilitate anonymity, including hotlines, online tip forms, and direct contact with law enforcement agencies.

Discretion is essential for whistleblowers or those who fear retaliation regarding their reports.



- **Immediate Response:** Prioritise the safety of potential victims and other guests. Contact law enforcement without delay. Refrain from confronting suspected traffickers directly to avoid escalating the situation and compromising safety.
- **Document and Report:** Keep meticulous records of all relevant details, including dates, times, physical descriptions of individuals involved, and actions taken.
- **Cooperate with Authorities:** Provide law enforcement with all pertinent information, including guest records, security footage, and any observations or suspicions you have gathered.
- **When human trafficking is suspected or detected on business premises, swift and decisive action is of the utmost importance.**

What to do if a presumed victim is at the workplace?

If the victim is detected at the workplace, it is necessary to find out sensitively what happened.

- Make sure that there are no people from the victim's working environment present with the victim and you at the interview. Make sure that people from the victim's working environment do not see you having interview with the victim.
- Tell the victim who you are and try to reassure them that they do not need to be afraid because you want to help them.
- Listen and ask questions, but avoid questions that start with the word "why".
- Identify whether they may be a victim of human trafficking based on basic indicators. Act on suspicion of human trafficking, as it is a serious crime.
- Be mindful of ethical standards, i.e. respect the fundamental human rights, freedoms and dignity of the victim, be aware that the person did not become a victim voluntarily, do not judge the victim for their appearance, nationality, health status and the activity they were forced to perform.



When communicating with the victim, it is most important to realise:

- **the person in front of you is a victim** of a crime and not a perpetrator of the crime of human trafficking
- the crime of human trafficking **violates the basic rights and freedoms** of the victim, which is also reflected in the victim's behavior and appearance
- a victim of human trafficking is a particularly vulnerable victim and requires **special protection and assistance**
- there are many reasons why trafficked persons are not considered victims of trafficking or do not ask for help. Victims of trafficking are psychologically and physically abused and constantly controlled, they fear retribution, revenge against themselves and their families or they feel responsible for their situation. They also don't even know that different forms of help are available.

How to help a victim



Reporting

You may encounter a victim of human trafficking in a public place or in the community, where you work.

They may be running away from their perpetrator and in poor physical and mental condition. To determine if he/she is a victim of human trafficking, you need to sensitively find out what happened.

- Ask your colleagues for assistance to ensure that the victim's basic needs are met. This includes making sure the situation is safe and reporting the incident to the police.
- Depending on your abilities and available resources, contact the police or any national helpline to obtain contact information for organisations that provide shelter, food, drinks, rest, or access to other basic needs. - **Contact the police immediately or call existing national helplines to report any suspicion of a criminal act.**
- Given the current mood and situation, the victim may be reluctant to engage with the support and assistance system or the police.
- If the victim does not wish to contact a human trafficking support organisation, respect their decision. Please provide them with the **National Human Trafficking Helpline number and the police.**
- In cases where there is an imminent threat to the victim's life or health, you must contact the police immediately.
- Remember that it is ultimately the victim's decision to report the incident to the police.
- Be mindful that various forms of assistance are available in each country without requiring the victim to report or cooperate with the police.

When contacting the police is obligatory

However, there are situations when it is necessary to contact the Police:

- in case of threat to the life and health of the victim,
- if the victim and you are in any danger (at the same time, try to leave the place where such danger exists),
- if there is reason to believe that the person in question is a child. Ensure that it is not a child, as there are specific procedures in place for children. Some young people under 18 may pretend to be of legal age.



**Referral
mechanism**

Not to forget

Try to preserve as many materials and traces as possible that could lead to the identification of the perpetrators and/or victims, and hand them over to the Police immediately if:

- during your work, you come across web content showing non-standard situations affecting the integrity of persons, which you consider authentic and shows obvious signs of involuntary action by the actor or actors or
- you identify children in such situations in the content.

PART 4

Legal and governmental assistance and protection of victims

Adequate Support measures and Improved capacities in countering THB

Who is acting in the coordinated approach to protection of victims



**Protection
mechanism**

- Governmental institutions and agencies dealing with (potential) victims of THB
- Non-governmental organisations ensuring hotlines, protected and safe accommodation and/or integration, trauma-related, stabilisation, financial and/or social, and/ health activities/services.
- The mechanism ensures proper, coordinated, and accountable governance of preventive, protection, and assistance-driven actions, including annual funds for protection incentives.
- The parties provide information and data for analyses and information products such as reports, promotional materials, educational and dissemination deliverables.
- The parties of the national referral mechanism monitor, propose and empower legal amendments, action plans, strategies and policies to ensure justice for the victims and adequate penalisation of perpetrators, accomplices and businesses involved in the process of trafficking and exploitation.

Type of assistance



Protection

Member States shall take the necessary measures to ensure that assistance and support for a victim are not made conditional on the victim's willingness to cooperate in the criminal investigation, prosecution or trial, without prejudice to Directive 2004/81/EC or similar national rules.

The following protection path ensured greater support to any victim of “modern slavery”:

Initial Contact:

National hotlines, police, NGOs, or hospitals

Needs Assessment:

Evaluation of immediate and long-term needs



Official Identification:

Formal recognition as a trafficking victim

Coordinated Support:

Referral to appropriate service providers

What kind of protection are victims of trafficking entitled to?:



Protection

Victim Status Recognition: providing legal residence permits during proceedings

Recovery Period Support: 30-90 days reflection time for victims

Protection Tools: Witness protection programs and anonymous testimony

Crisis Accommodation:

- **Immediate safe housing** for 3-6 months
- **Transition Housing:** Longer-term subsidised accommodation
- **Specialised Shelters:** Gender-specific and family-friendly facilities
- **Security Measures:** 24/7 staff, restricted access, confidential locations

Immediate relief: Emergency cash assistance, Basic needs allowance, Transportation vouchers

Compensation scheme: state-funded victim compensation, civil claims against traffickers, lost earnings recovery

Long-term support: Education grants. Vocational training funding, Microloans for entrepreneurs

Healthcare services: emergency and ongoing treatment without charge, trauma-informed therapy and counselling, substance abuse treatment programs, Sexual health services and reproductive care

Social integration support: Language training and vocational courses, Job placement and career development

Country-Specific Programs

Bulgaria	ANIMUS Association, Crisis Centre Sofia
Spain	APRAMP, Red Cross trafficking program
Poland	La Strada Poland, National Intervention Centre
Slovakia	Greek- Catholic Charity, Catholic Charity
Italy	Article 18 program, On the Road NGO
Greece	A21 Campaign, National Referral Mechanism
Austria	LEFÖ-IBF, MEN VIA for male victims



-  BULGARIA
-  SPAIN POLAND
-  GREECE GERMANY



Protection

Add information about protection incentives in your country, conditions, rules and etc.

Possible alternative PART 4

protection and

prevention:

accountable use of

technology
Adequate Support measures and Improved capacities in countering THB

Technology must also provide alternative mechanisms in support of the official public incentives for protection and reintegration of the victims of trafficking in human beings.



Technological firms, as well as e-based service and product providers, or online job facilitators, can significantly contribute to protecting against illegal content and related information on the Internet in cases of illegal activity committed through a computer system, computer networks, or computer data.

In the case of human trafficking, focus on the persons who are the subject of offers, whether they are children or adults, how they behave and therefore their appearance indicators.



PROTECTION

The IT sector is crucial in combating human trafficking through enhanced cybersecurity measures.

- Protecting databases that contain sensitive information about trafficking victims and ensuring law enforcement can effectively access this data are critical to building a comprehensive response.

Technological Solutions for Prevention

- Innovations like machine learning and data analytics can help identify trafficking patterns and empower organisations to act promptly.
- Technology can assist in raising awareness and educating communities about the signs of trafficking.

Collaboration for Action

- Partnerships between tech companies, governments, and nongovernmental organisations are essential in addressing the complex challenges posed by human trafficking.
- Through collaborative efforts, data sharing, and advancing technology, we can make significant strides in preventing trafficking and supporting victims.

How to facilitate counter trafficking in human beings in the cyber world?

- Develop support protocols for cooperation with social networks and gig-economy companies
- Promote social advertising to prevent victimisation
- Develop an early warning response mechanism

What type of Software development can contribute to the prevention of trafficking in human beings?

- solution to collect, store and process electronic evidence using SW, Big Data Analytics, AI, machine learning,
- web scraping tools, open source intelligence OSINT for monitoring the dark net,
- social network analysis,
- automatic searching tool,
- cyber-patrolling,
- the covert online investigation,
- equipment for detection, tapping, etc.

Tools and Strategies to Prevent from THB Attempts



PROTECTION

Effectively identifying technology-facilitated trafficking requires sophisticated technical approaches combined with human expertise and institutional coordination.

- **Machine learning models** for spotting trafficking patterns
- Machine learning models have emerged as powerful tools for detecting trafficking patterns across massive datasets that would overwhelm human analysts.
- Systems that identify subtle correlations between seemingly unrelated digital activities **recognise linguistic patterns** associated with trafficking and flag suspicious network behaviours across platforms.
- Advanced models may incorporate natural language processing to detect coded communications, image analysis to identify potentially exploitative content, and anomaly detection to flag unusual behavioural or financial patterns.

Tools and Strategies to Prevent from THB



PROTECTION

Data Collection and Integration

- comprehensive data collection from diverse sources, including social media platforms, advertising websites, financial transaction records, and reported cases,
- data must be integrated into unified systems that can identify cross-platform patterns while maintaining privacy protections and chain of custody for potential evidence,
- strict access controls and anonymisation where appropriate.

Pattern Analysis and Alert Generation

- temporal analysis to identify suspicious timing patterns,
- geospatial mapping to detect movement along known trafficking routes,
- network analysis to reveal connections between potential perpetrators and victims and
- sentiment analysis to identify linguistic patterns associated with coercion or control.

Human Verification and Intervention

While technological tools can identify potential trafficking situations, human expertise remains essential for verification and appropriate intervention.

Technology for protection



PROTECTION

Technology can be used to:

- Prevent human trafficking
- Protect victims
- Prosecute traffickers

Collaboration with tech firms can generate:

- specialised application programming Interface that allows secure information sharing between platforms while protecting user privacy,
- hash-matching technologies that identify known exploitative content across platforms and
- shared typologies of trafficking indicators customised to different digital environments.

Positive developments(examples):

- Tools like Spotlight have identified over 17,000 trafficking victims
- Over 300 technology tools now combat human trafficking
- Over the last decade, domestic minor sex trafficking (DMST) has evolved to become increasingly sophisticated, with traffickers leveraging technology to accelerate the spread of exploitation. In response, Spotlight, a non-profit organisation, has been at the forefront of combating DMST, utilising artificial intelligence-powered technology to aid investigations and identify juvenile victims.(Reuters, Jan/2025)

PART 4

Promote important contacts online

Adequate Support measures and Improved capacities in countering THB



**Important
contacts**

**Be accountable for countering THB supported by online services
and technology,**

**Promote on your website, social network, app, e-service, hub,
cloud and related available contacts for rapid response, help
and timely reaction.**

It can save a victim of trafficking











Reporting

The European Commission has a dedicated web page with information on how each EU country addresses, prevents and identifies human trafficking. This page also includes contact details for national authorities and relevant organisations, such as civil society groups, that work in the field of human trafficking at the national level.

In case of suspected human trafficking, call to the European emergency number: **112**. 

All helplines are free of charge

Important contacts at national level in BULGARIA

-  National Helpline for Combating Trafficking in Human Beings (for calls within Bulgaria)
0800 20 100
-  Helpline for victims of violence (for calls within Bulgaria)
0800 1 86 76
-  National Commission for Combating Trafficking in Human Beings
+359 2 807 80 50
-  National Helpline for Children
116 111
-  International Organisation for Migration
+359 2 939 47 74
-  Platform for prevention of trafficking in human beings and support to the victims
<https://nrm.bg/en/home/>

Important contacts at national level in GREECE

 Resource Line for Human Trafficking
1109

 SOS Hotline on Violence Against Women
159 00

 Emergency Social Helpline
197

 Hellenic Police
100



Reporting

Important contacts at national level in ITALY

National Anti-Trafficking Helpline

 **800 290 290**

Important contacts at national level in POLAND

National Information and Consultation Centre hotline



+48 22 628 01 20

National Information and Consultation Centre hotline



+48 47 72 56 502

Anti-Human Trafficking Department of the Criminal Office of the National Police Headquarters
hotline



+48 664 974 934

Office for Foreigners hotline



+48 47 721 7575

Important contacts at national level in SLOVAKIA

National anti-trafficking units across the country – 24/7 immediate contact via email ool@minv.sk



National helpline of Assistance to Trafficking in Human Beings Victims **0800 800 818**

National Police Force



158

Missing Children Helpline (nonstop)



116 000

National helpline for women experiencing violence



0800 212 212

Child Safety Helpline



116 111

Human Trafficking and Safe Travel Helpline (IOM Helpline)



0907 787 374

[Information Centre for Combating trafficking in Human Beings and for Crime Prevention](#), Ministry of the Interior, Pribinova 2, 812 72 Bratislava, Slovakia – responsible also for the management of the specialised

Program of Support and Assistance to Victims of HT and policy making. Email: icosl@minv.sk



Important contacts at national level in SPAIN

The National Police Force

 Contact telephone
900 10 50 90

 Email
trata@policia.es

Social media

 Twitter
@policia

 Hashtag:
#contralatrata

Partners

Coordinator

Ministry of Interior / Slovak Republic

www.minv.sk/?ministry-of-interior

Academy of the Ministry of Interior / Bulgaria

studyinbulgaria.bg/academy-of-the-ministry-of-interior-sofia.html

Departament d'Interior - Generalitat de Catalunya / Spain

web.gencat.cat/en/inici

Hellenic Police / Greece

www.astynomia.gr

KEMEA - KENTRO MELETON ASFALIAS - Center for Security Studies / Greece

kemea.gr/en

KWP - Komenda Wojewodzka Policji W Krakowie / Poland

mopol.ska.policja.gov.pl

CESIE / Italy

www.cesie.org



mossos d'esquadra

Generalitat
de Catalunya



ASIT: Digital tools and capacity building to challenges new forms of human trafficking

Internal Security Fund - ISF-2002-TF1-AG-THE (Call for proposals on actions against trafficking in human beings)

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Project Number: 101101942 - ASIT



Co-funded by
the European Union