# OPEN YOUR EYES

## TRAINING COURSE
## 24 sept - 02 oct

2025-1-BG01-KA153-YOU-000303719

# TABLE OF CONTENTS



FRAUD AND CYBERCRIME ARE EVERYDAY THREATS THAT EXPLOIT TRUST, VULNERABILITY, AND DIGITAL HABITS. YOUNG PEOPLE ARE OFTEN AMONG THE MOST EXPOSED, AND YOUTH WORKERS PLAY A KEY ROLE IN HELPING THEM RECOGNIZE RISKS, PREVENT HARM, AND RECOVER WHEN TARGETED.

THE OPEN YOUR EYES TRAINING COURSE, HELD IN BULGARIA FROM 23 SEPTEMBER TO 3 OCTOBER 2025, BROUGHT TOGETHER YOUTH AND SOCIAL WORKERS FROM EIGHT COUNTRIES—BULGARIA, ITALY, SPAIN, ROMANIA, SERBIA, NORTH MACEDONIA, LITHUANIA, AND HUNGARY. SUPPORTED BY ERASMUS+ (2025-1-BG01-KA153-YOU-000303719), THE COURSE STRENGTHENED THE CAPACITY OF YOUTH WORKERS TO UNDERSTAND FRAUDULENT SCHEMES, THEIR PSYCHOLOGICAL FOUNDATIONS, AND THE LEGAL TOOLS AVAILABLE TO COUNTER THEM.

THIS HANDBOOK DISTILLS THE LESSONS OF THE TRAINING INTO PRACTICAL GUIDANCE FOR DAILY WORK WITH YOUNG PEOPLE. IT COMBINES PSYCHOLOGICAL INSIGHTS, PREVENTION STRATEGIES, AND REAL-LIFE CASES, OFFERING CONCRETE TOOLS TO SUPPORT THOSE AT RISK OR ALREADY AFFECTED BY FRAUD. BEYOND SERVING YOUTH WORKERS, IT ALSO SUPPORTS AWARENESS CAMPAIGNS IN SCHOOLS AND YOUTH CENTRES, ACCOMPANIED BY AN EDUCATIONAL VIDEO CREATED WITHIN THE PROJECT.

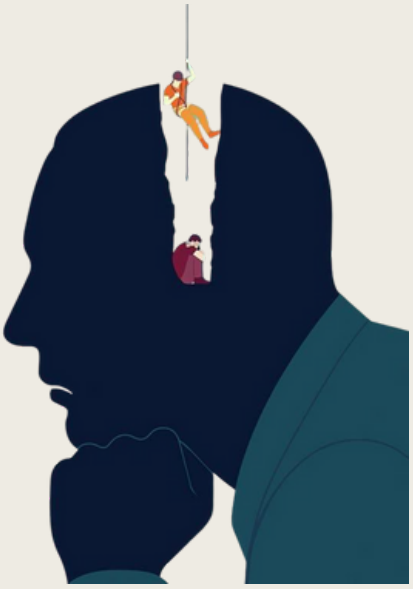
AT ITS CORE, THIS RESOURCE IS ABOUT EMPOWERMENT: BUILDING RESILIENCE, FOSTERING CRITICAL THINKING, AND GIVING YOUTH WORKERS THE CONFIDENCE TO ACT AGAINST FRAUD. WITH KNOWLEDGE AND EMPATHY, WE CAN PROTECT INDIVIDUALS AND STRENGTHEN COMMUNITIES AGAINST SCAMS OF EVERY KIND.

# HOW TO PSYCHOLOGICALLY APPROACH YOUNG PEOPLE WHO ARE (POTENTIAL) VICTIMS OF FRAUD

01

**FRAUD IS NOT ONLY A FINANCIAL ISSUE BUT ALSO A DEEPLY PSYCHOLOGICAL ONE, AND THE WAY WE RESPOND TO IT CAN MAKE THE DIFFERENCE BETWEEN HELPING SOMEONE REFLECT OR PUSHING THEM FURTHER AWAY.**

# WHY VICTIMS DENY FRAUD



ONE OF THE FIRST LESSONS IS THAT VICTIMS RARELY ADMIT THEY HAVE BEEN DECEIVED. EVEN WHEN THE EVIDENCE IS OBVIOUS TO OTHERS, THEY MAY STRONGLY RESIST ACKNOWLEDGING IT. THIS IS BECAUSE THE HUMAN BRAIN WORKS HARD TO PROTECT THE EGO. ACCEPTING THAT ONE HAS FALLEN FOR A SCAM MEANS ADMITTING THAT SOMEONE FOOLED US, WHICH FEELS LIKE ADMITTING WEAKNESS OR LACK OF INTELLIGENCE. FOR MANY, THIS IS INTOLERABLE, SO DENIAL BECOMES THE DEFAULT DEFENSE.

# BUILDING TRUST INSTEAD OF CONFLICT

AS YOUTH WORKERS OR FRIENDS, WE DO HOLD INFLUENCE OVER VICTIMS, BUT DIRECT CONFRONTATION USUALLY BACKFIRES. ENTERING INTO A HEATED DEBATE OFTEN DAMAGES THE RELATIONSHIP, LEAVING THE VICTIM ISOLATED AND BEYOND OUR REACH. THE GOAL IS NOT TO WIN AN ARGUMENT BUT TO PRESERVE TRUST. A DESTROYED RELATIONSHIP MEANS LOSING THE CHANCE TO SUPPORT THEM IN RECOGNIZING THE FRAUD AND REGAINING CONTROL OVER THEIR SITUATION.

# ASKING CRITICAL QUESTIONS

THE MOST EFFECTIVE APPROACH IS GENTLE CURIOSITY. INSTEAD OF TELLING SOMEONE OUTRIGHT THAT THEY ARE BEING SCAMMED, WE CAN ASK OPEN QUESTIONS SUCH AS: “COULD YOU EXPLAIN TO ME HOW THIS BUSINESS MODEL WORKS?” OR “WHERE IS THE REVENUE REALLY COMING FROM?” SUCH QUESTIONS AVOID PRESSURE OR SUPERIORITY AND INSTEAD ENCOURAGE REFLECTION. IDEALLY, THE PERSON BEGINS TO NOTICE CONTRADICTIONS THEMSELVES AND SLOWLY REALIZES THE TRUE NATURE OF THE SCHEME.

# UNDERSTANDING PERSONAL MOTIVATIONS

This questioning approach also allows us to connect more deeply with the person. We begin to understand their ambitions, dreams, and the unmet needs that made them vulnerable in the first place. These weaknesses are not flaws but natural human desires for social approval, for wealth, for belonging, or for recognition. Fraudsters exploit exactly these needs by presenting opportunities that appear to bring dreams within reach. The closer the dream seems, the more people let down their guard, and the more vulnerable they become.

# WORKING WITH NOT AGAINST THE VICTIM

Recognizing these psychological dynamics allows youth workers to support victims with empathy rather than judgment. By strengthening the areas where unmet needs exist, we can help young people build resilience and confidence, reducing the chances of them being deceived again. The guiding principle is to work with them, not against them, always remembering that every person is full of aspirations and vulnerabilities that deserve respect and understanding.

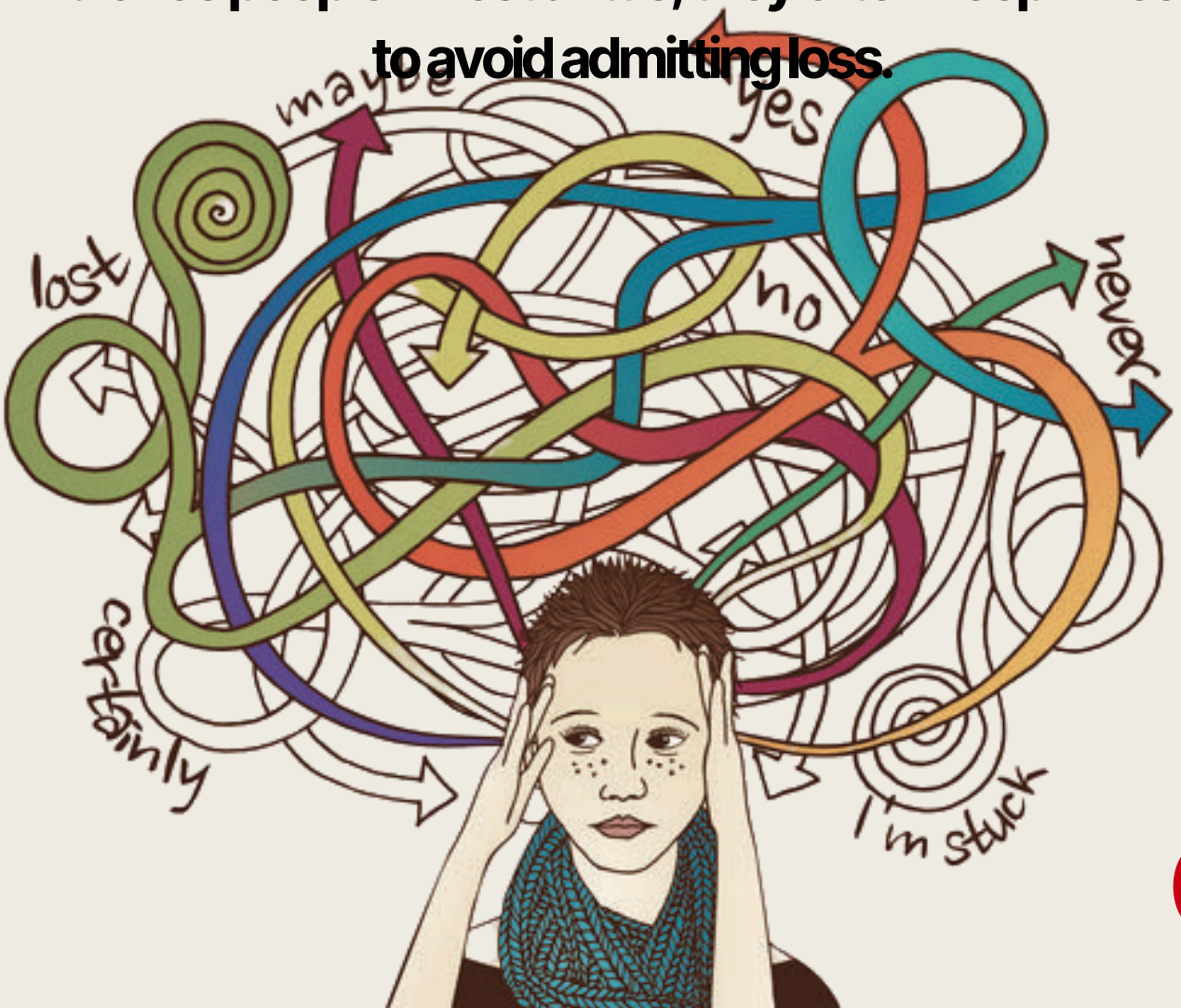
(01]

# ASSESSING VULNERABILITIES AND WEAK SPOTS (02)

Fraud succeeds because it preys on human behavior as much as on technology. Scammers press psychological buttons, exploit stressful situations, and take advantage of our digital habits. At the same time, new technologies make scams more realistic than ever. By understanding these weak spots, we can build awareness and strengthen our defenses.

# HUMAN PSYCHOLOGY

Scammers know how to trigger predictable reactions. Urgent warnings like “your account is blocked” push people to act without checking. Authority symbols such as bank logos or official seals create false trust. Scarcity tactics—“last ticket, price ends today”—pressure quick decisions, while friendliness or romance lowers defenses. Social proof, through fake testimonials or profit screenshots, makes schemes seem legitimate. And once people invest a little, they often keep investing to avoid admitting loss.



# SITUATIONAL CONTEXT

Circumstances also shape vulnerability. On small screens or in mobile apps, it is easy to miss suspicious URLs. Multitasking and time pressure reduce careful thinking, and many breaches begin with a single click or share. Financial stress creates fertile ground for rental scams, marketplace cons, and “too good to be true” offers. Shame is another factor: many victims do not report fraud, which hides its scale and makes others easier to target.

# DIGITAL HABITS

OUR EVERYDAY ONLINE BEHAVIOR OFTEN OPENS THE DOOR. REUSING PASSWORDS OR RELYING ONLY ON SMS CODES WEAKENS ACCOUNT SECURITY. CLICKING REFLEXIVELY ON LINKS OR SCANNING QR CODES WITHOUT CHECKING THEIR SOURCE EXPOSES PEOPLE TO PHISHING OR "QUISHING." OVERSHARING ON SOCIAL MEDIA GIVES SCAMMERS PERSONAL DETAILS THAT MAKE THEIR LURES MORE CONVINCING.

# TECHNOLOGY AND PLATFORMS

Recent advances make scams harder to spot. AI-generated voices and videos allow criminals to impersonate family members, colleagues, or officials with unsettling realism. Cloned websites look almost identical to legitimate ones. Phishing attacks continue to rise, especially against financial services and online payments. Yet despite these new tools, the majority of breaches still come down to human error—mis-clicks, misplaced trust, or rushed responses.

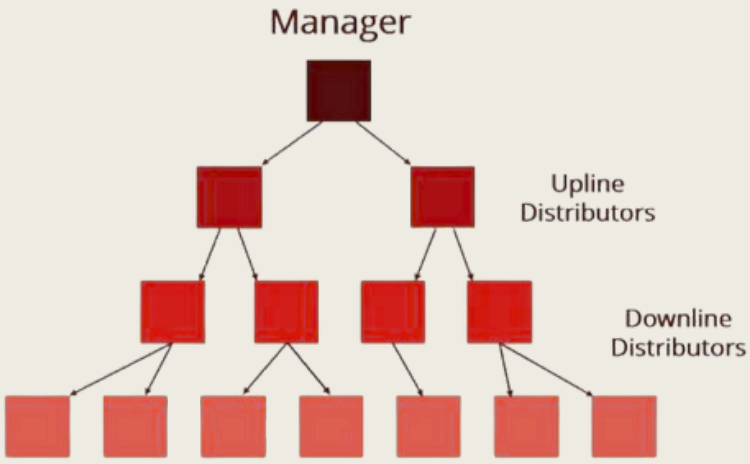
# MLM VS PYRAMID SCHEMES (03)

NOT ALL BUSINESS OPPORTUNITIES THAT INVOLVE SELLING PRODUCTS OR RECRUITING OTHERS ARE THE SAME. SOME ARE LEGAL AND SUSTAINABLE, WHILE OTHERS ARE ILLEGAL SCAMS DESIGNED TO COLLAPSE. UNDERSTANDING THE DIFFERENCE BETWEEN MULTI-LEVEL MARKETING (MLM) AND PYRAMID SCHEMES IS KEY TO PROTECTING YOURSELF FROM FINANCIAL LOSS.


# PYRAMID SCHEMES

A pyramid scheme is an illegal money-making plan that depends almost entirely on constant recruitment. New participants are usually asked to pay a fee or make an "investment," and their money is used to pay earlier members rather than to support the sale of real products or services. Because the model requires an endless supply of new recruits, it is mathematically destined to fail, leaving those at the bottom with heavy losses. Well-known examples include La Bella Vida, BurnLounge, and the investment fraud orchestrated by Bernard Madoff.

# MULTI-LEVEL MARKETING (MLM)




**Multi-Level Marketing, or MLM, is a legal type of direct sales. Individuals sell genuine products or services—such as cosmetics, kitchenware, or health supplements—and may also earn small commissions when they recruit others who sell. The critical distinction from a pyramid scheme is that income in MLM should come mainly from product sales to real customers rather than from joining fees or recruitment. Established companies like Tupperware, Herbalife, and Avon operate as MLMs, but they are required to follow consumer-protection laws and provide transparent information about earning potential.**

# IN-PERSON SOCIAL ENGINEERING

## (04)

Social engineering happens when someone tries to manipulate you into giving away information or doing something you normally would not, simply by acting confident, friendly, or persuasive. It can occur anywhere—online, at school, or in social groups—and it often works because people do not stop to question what is being asked of them. The most important principle is to think before you share. If someone asks for your password, money, or personal details, it is always worth pausing to reflect. Asking questions, checking with someone you trust, and noticing red flags such as secrecy, pressure, or unrealistic promises are simple but powerful ways to stay safe.

# WARNING SIGNS OF A PYRAMID SCHEME

BEFORE JOINING ANY OPPORTUNITY, IT IS IMPORTANT TO ASK THE RIGHT QUESTIONS. IF PARTICIPATION REQUIRES PAYING A LARGE START-UP FEE, IF RECRUITING IS EMPHASIZED MORE THAN SELLING, OR IF YOU ARE PROMISED QUICK PROFITS WITH LITTLE EFFORT, CAUTION IS WARRANTED. OTHER RED FLAGS INCLUDE OVERPRICED OR LOW-QUALITY PRODUCTS AND HIGH-PRESSURE SALES TACTICS URGING YOU TO “SIGN NOW” BEFORE LOSING A SUPPOSED OPPORTUNITY.

# CORE PRINCIPLES

THE KEY IDEA IS TO PAUSE BEFORE ACTING. INFORMATION OR ACCESS SHOULD NEVER BE HANDED OVER IMPULSIVELY. CURIOSITY AND CAUTION SHOULD BE VALUED EQUALLY, SINCE ASKING QUESTIONS IS A SIGN OF INTELLIGENCE RATHER THAN RUDENESS. PROTECTING YOURSELF ALSO MEANS PROTECTING OTHERS, BECAUSE YOUR VIGILANCE HELPS KEEP YOUR FRIENDS AND COMMUNITY SAFE. ETHICAL BEHAVIOR IS JUST AS IMPORTANT: SOCIAL ENGINEERING SHOULD BE STUDIED BY OBSERVING EXAMPLES AND LEARNING WARNING SIGNS, NOT BY DECEIVING OTHERS.

# WARNING SIGNS

CERTAIN PATTERNS APPEAR AGAIN AND AGAIN IN SOCIAL ENGINEERING. SCAMMERS OFTEN PRESSURE PEOPLE TO ACT QUICKLY OR INSIST ON SECRECY BY SAYING “DON’T TELL ANYONE.” THEY MIGHT ASK FOR PERSONAL INFORMATION, PASSWORDS, OR MONEY, OR PRESENT OFFERS THAT SEEM TOO GOOD TO BE TRUE. SOMETIMES THEY RELY ON EXAGGERATED CONFIDENCE TO PUSH YOU INTO COMPLYING. RECOGNIZING THESE BEHAVIORS MAKES IT EASIER TO RESIST MANIPULATION.

# VERIFICATION HABITS

A STRONG DEFENSE IS TO CREATE A PERSONAL VERIFICATION ROUTINE. WHENEVER YOU RECEIVE A REQUEST, PAUSE AND ASK WHO IS MAKING IT, WHY THEY ARE ASKING, AND HOW THE INFORMATION WILL BE USED. THEN CONFIRM THE DETAILS WITH A TRUSTED ADULT, TEACHER, OR PEER BEFORE YOU ACT. A SIMPLE MENTAL CHECKLIST—REQUEST, PAUSE, ASK, CONFIRM, ACT—CAN BE APPLIED IN ALMOST ANY SITUATION. ENCOURAGING FRIENDS OR CLASSMATES TO ADOPT THE SAME APPROACH STRENGTHENS GROUP AWARENESS AND MAKES EVERYONE SAFER.

# TRAINING AND PRACTICE

PRACTICAL TRAINING HELPS THESE PRINCIPLES BECOME SECOND NATURE. ROLE-PLAYING SHORT SCENARIOS IS A SAFE WAY TO PRACTICE SAYING NO OR ASKING CLARIFYING QUESTIONS. SPOT-THE-WARNING GAMES, WHERE PARTICIPANTS IDENTIFY SIGNS OF PRESSURE OR SECRECY IN STORIES AND ONLINE POSTS, SHARPEN AWARENESS. REFLECTION SESSIONS ALLOW PEOPLE TO DISCUSS WHAT FELT EASY, WHAT WAS DIFFICULT, AND WHAT STRATEGIES WORKED BEST. REPEATING THESE EXERCISES REGULARLY IN A LOW-PRESSURE, EVEN PLAYFUL ENVIRONMENT MAKES THE LESSONS STICK.

# DISTANCE AND ONLINE SCHEMES PREVENTION

60% OF BUYERS PRIORITIZE AUTHENTIC CONTENT.

## INTRODUCTION

THE GROWTH OF DIGITAL PLATFORMS AND REMOTE SERVICES HAS CREATED ENORMOUS OPPORTUNITIES FOR EDUCATION, WORK, AND EVERYDAY LIFE, BUT IT HAS ALSO EXPANDED THE SPACE FOR FRAUD, SCAMS, AND ACADEMIC DISHONESTY. PREVENTING THESE RISKS REQUIRES A BALANCED STRATEGY THAT COMBINES TECHNOLOGY, CLEAR INSTITUTIONAL RULES, AND USER AWARENESS. TECHNICAL SAFEGUARDS SUCH AS MULTI-FACTOR AUTHENTICATION, ENCRYPTION, AND FRAUD DETECTION SYSTEMS PROTECT DATA AND TRANSACTIONS, WHILE ORGANIZATIONAL MEASURES LIKE AUDITS, SECURE ACCESS CONTROLS, AND REPORTING CHANNELS STRENGTHEN ACCOUNTABILITY. EQUALLY IMPORTANT IS EDUCATION: BY TRAINING PEOPLE TO RECOGNIZE PHISHING ATTEMPTS, SUSPICIOUS BEHAVIOR, OR FRAUDULENT OFFERS, INSTITUTIONS BUILD RESILIENCE AND TRUST IN ONLINE ENVIRONMENTS. IN DISTANCE LEARNING, TOOLS SUCH AS IDENTITY VERIFICATION, PROCTORING, AND PLAGIARISM DETECTION FURTHER REDUCE RISKS, WHILE IN WORKPLACES AND PUBLIC SERVICES STRONG REPORTING MECHANISMS ARE VITAL.

# PHISHING WEBSITE


A PARTICULARLY WIDESPREAD THREAT IS THE PHISHING WEBSITE. THESE SITES IMITATE BANKS, DELIVERY SERVICES, OR SOCIAL MEDIA PLATFORMS TO TRICK USERS INTO REVEALING SENSITIVE DETAILS SUCH AS PASSWORDS OR CREDIT CARD NUMBERS. THEY OFTEN RELY ON LOOK-ALIKE WEB ADDRESSES OR FAKE MESSAGES ABOUT PROBLEMS WITH PAYMENTS AND DELIVERIES. WARNING SIGNS INCLUDE UNUSUAL URLS, SPELLING MISTAKES, OR POOR DESIGN. THE SAFEST APPROACH IS TO AVOID CLICKING ON LINKS IN UNSOLICITED MESSAGES, TO TYPE IN ADDRESSES MANUALLY, AND TO RELY ON BOOKMARKS TO ACCESS IMPORTANT SERVICES. IF PERSONAL INFORMATION IS MISTAKENLY ENTERED ON A PHISHING SITE, PASSWORDS SHOULD BE CHANGED IMMEDIATELY, MULTI-FACTOR AUTHENTICATION ACTIVATED, AND BANKS NOTIFIED WITHOUT DELAY.

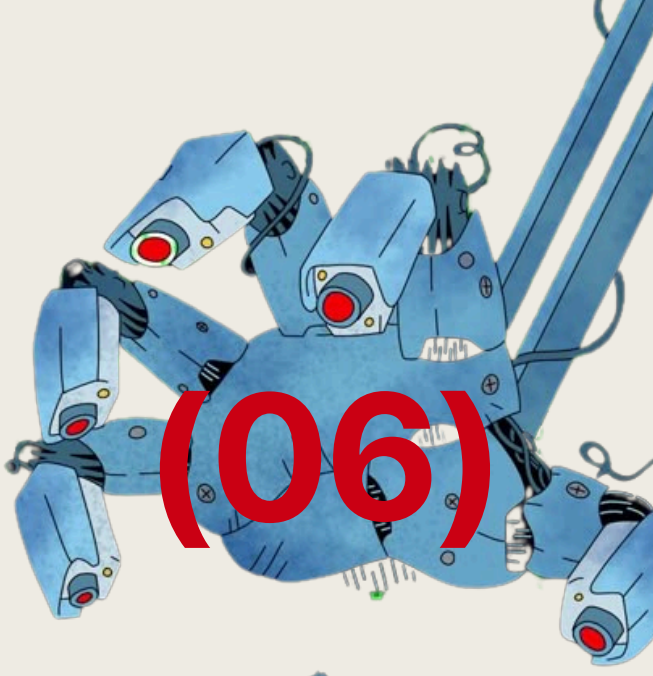
# THE SCALE OF THE PROBLEM

THE SCALE OF THE PROBLEM IS EVIDENT IN LITHUANIA, WHERE LOSSES FROM PHONE FRAUD EXCEEDED €20 MILLION IN 2025 ,AN INCREASE OF NEARLY 40 PERCENT FROM THE PREVIOUS YEAR. SCAMMERS USE A RANGE OF TECHNIQUES: POSING AS BANK OR POLICE OFFICIALS AND URGING TRANSFERS TO “SAFE ACCOUNTS”, PROMISING HIGH RETURNS FROM FRAUDULENT INVESTMENTS, SENDING SMS MESSAGES WITH MALICIOUS LINKS, OR PRETENDING TO BE RELATIVES IN URGENT NEED OF HELP. CALLER ID SPOOFING AND EVEN VOICE SYNTHESIS TECHNOLOGIES MAKE THESE SCAMS INCREASINGLY CONVINCING.

# HOW TO STAY PROTECTED

Protection ultimately depends on vigilance. Personal details, PINs, and verification codes should never be shared over the phone, even if the caller appears official. Incoming calls should always be verified by contacting the institution directly through official numbers, and suspicious messages or calls should be reported immediately. By combining technical defenses with everyday caution, individuals and institutions can significantly reduce their vulnerability and ensure that online and distance services remain safe and reliable.

# LEGAL SUPPORT OF FRAUD VICTIMS (06)



LEGAL SUPPORT ENSURES THAT FRAUD VICTIMS CAN PURSUE JUSTICE, RECOVER LOSSES, AND SAFEGUARD THEIR RIGHTS. ACCESS TO PROPER GUIDANCE AND FORMAL PROCEDURES IS ESSENTIAL, SINCE WITHOUT IT MANY CASES REMAIN UNREPORTED OR UNRESOLVED.

# LEGAL PATHWAYS FOR VICTIMS

The first step is often legal counselling. Consulting a specialized criminal or consumer lawyer helps ensure that complaints are drafted correctly, evidence is presented effectively, and victims' rights are respected throughout the process.

Equally important is filing a formal complaint. In many jurisdictions, authorities will not pursue fraud cases unless victims take the initiative by reporting at the nearest police station or online portal.

When fraud involves stolen personal data, victims must also act quickly to contain identity theft. Reporting the incident to consumer-protection agencies or financial authorities can prevent criminals from misusing stolen credentials to open accounts, place fraudulent orders, or take out loans.

## Red Flags: Recognizing a Scam

- Pressure to pay upfront.
- Missing or unclear documentation
- "Invest now or miss out" promise
- Urgent requests to make immedia payments.

## Smart Questions to Ask

- Can I see the property in person before sending money?
- Can you provide official ownership documents or utility bills in your name?
- Can we use a secure rental platform or an escrow service for payment?
- What is your company name and registration number, and where can I verify it?
- Can you share your official wallet address with past transaction records I can check?
- Are you willing to use a trusted third-party escrow service?

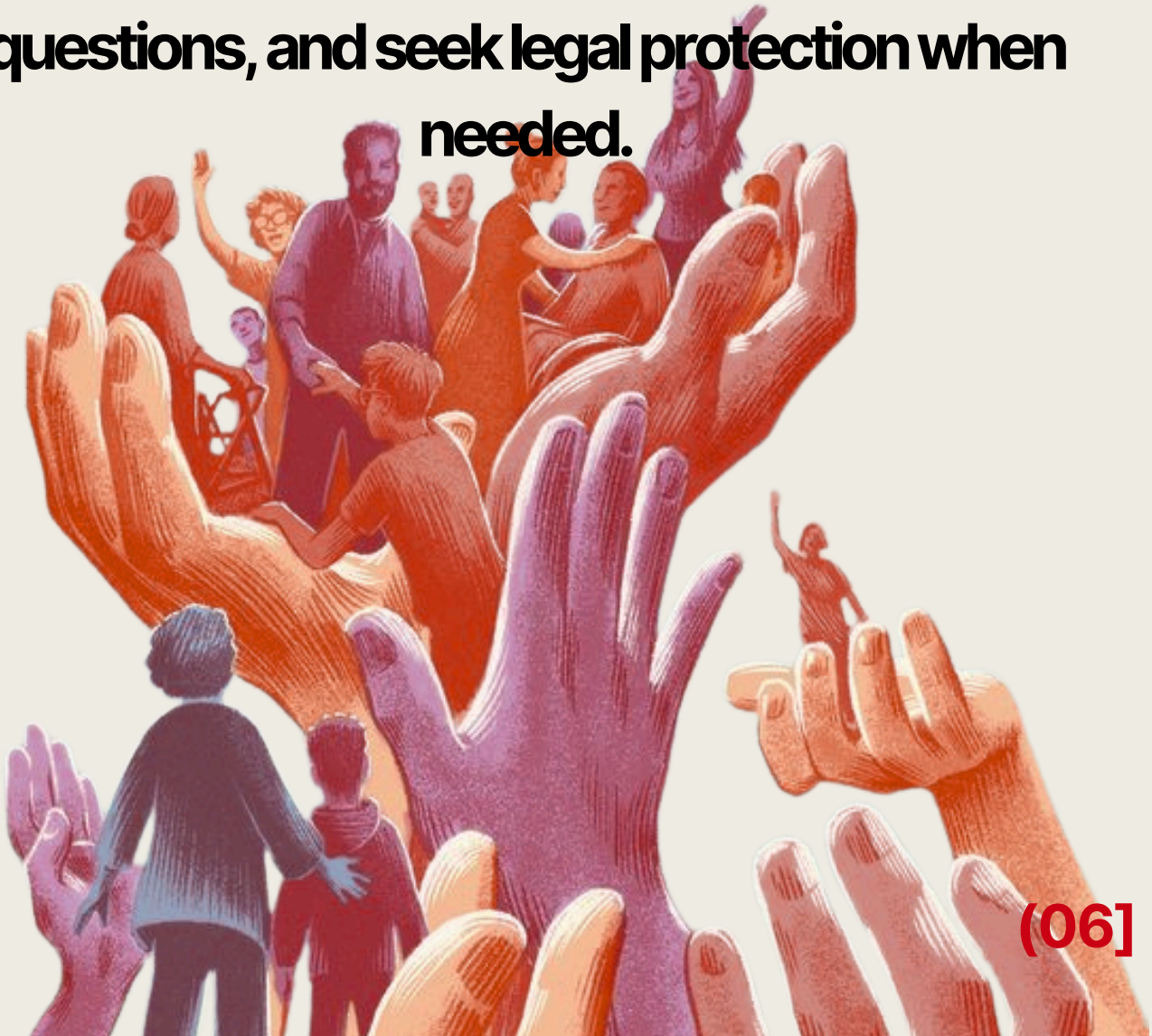
# REAL-LIFE CASES

Bulgarian authorities have recently warned about romance scams targeting men on dating platforms. Fraudsters create fake profiles, build emotional connections, and then invent emergencies to extract money. In one case, a young woman was told by her foreign partner that he had purchased expensive jewelry for her, but that customs required thousands of euros in "import taxes." She paid, only to discover she had been deceived.

Bulgaria was also the starting point of one of the world's largest financial frauds: the OneCoin Ponzi scheme, founded by Bulgarian-German entrepreneur Ruja Ignatova. Marketed as a revolutionary cryptocurrency, it defrauded investors worldwide of an estimated $4.4 billion before collapsing. Ignatova disappeared in 2017 and remains on the FBI's Most Wanted list with a $5 million reward for information leading to her arrest.

# AWARENESS AND EDUCATION

**Raising awareness is one of the most powerful tools against fraud. Our group's awareness program highlights common scams across Europe, from romance schemes to large-scale investment frauds, and equips people with the knowledge to recognize red flags, ask critical questions, and seek legal protection when needed.**



REACH OUT TO US AT
@REALLYGREATSITE

VISIT OUR WEBSITE AT
WWW.REALLYGREATSITE.COM

PRESENTED BY
OLIVIA WILSON

# LET'S CREATE SOMETHING AMAZING TOGETHER


This handbook was created by the participants of the 2025-1-BG01-KA153-YOU-000303719 **“Open Your Eyes”** project, co-funded by the Erasmus+ program of the European Union. It is to be shared and used freely and respectfully. Please rate its contents **HERE**, and check out our educational video **HERE**.

СДРУЖЕНИЕ "НИЕ"
ASSOCIATION "NIE"
ЦЕНТЪР ЗА РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ
Erasmus+