

WEBTECTIVII

GHIDUL INSTRUCTORULUI

Cum folosim jocul Webtectivii
pentru noile generații
#SigurepeInternet



Cofinanțat de
Uniunea Europeană



SAVE
School Anti-Violence Ecosystem

program coordonat de

World Vision
ROMÂNIA

Proiect derulat de:



Proiect derulat de:
Alianța Pentru Mobilitate Socială

WEBTECTIVII

Educația digitală devine o aventură a siguranței!

WebTectivii este un joc educațional inovator de tip „mystery case files” care transformă lecțiile despre siguranța online într-o investigație palpitantă, punând elevii în rolul de „super detectivi” care trebuie să rezolve cazul **„Disparația Smarandei”**.

Lucrând în echipe, copiii analizează dosare fizice ce conțin probe simulate fidel după realitate — capturi de ecran din conversații, profiluri false și link-uri capcană — având misiunea de a identifica tacticile de manipulare și indiciile abuzului cibernetic. Prin acest proces de deducție logică și analiză critică, jocul înlocuiește discursurile moralizatoare cu o experiență practică, ajutând copiii să recunoască pericolele digitale și să dezvolte comportamente reale de autoprotecție.



Cofinanțat de
Uniunea Europeană



program coordonat de
World Vision
ROMÂNIA

Proiect derulat de:
Amos
Asociația Pentru Mobilitate Socială

CONTINUTUL JOCULUI

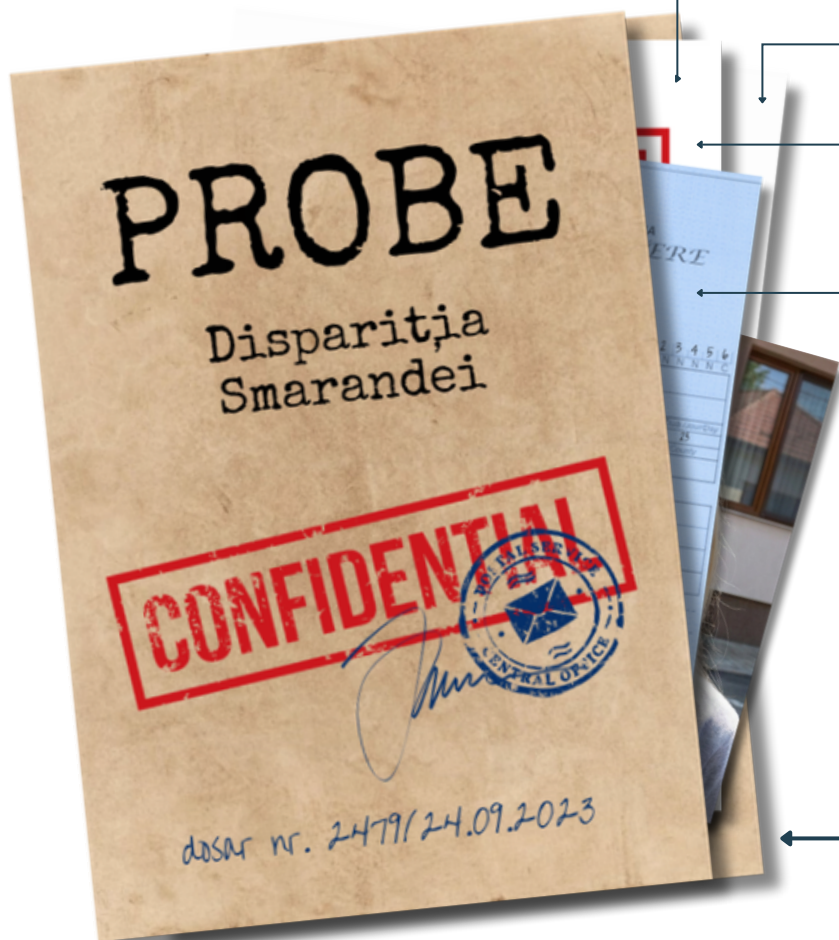
Dosarul conține replici fidele ale interacțiunilor reale din mediul online.

Fiecare probă este o lecție de siguranță deghizată într-un indiciu, antrenând gândirea critică a copiilor pentru a deosebi intențiile bune de cele periculoase.

Dosarul:

1. Coperta/Dosarul
Fizic: Trebuie să fie etichetat „CONFIDENȚIAL” și să poarte numărul de dosar nr. 2479/24.09.2023 – Titlu: „Dispariția Smarandei”.
2. Descrierea Misiunii: O scurtă introducere care prezintă scenariul (adolescentă dispărută, suspiciune de racolare online).

DOSARUL



PROBELE

Reprezentarea vizuală a riscurilor și indicii cu privire la caz (mesaje capcană, profiluri false).

Probele Digitale (Capturi de ecran printate): pentru a reconstrui cronologia și metoda de manipulare (Grooming & Phishing).

1. Conversația Instagram „New Star Dance”: Discuția inițială în care este abordată și flatată („ai foarte mult potențial”).
2. Conversația WhatsApp „New Star”:
 - a. Cererea datelor personale și confirmarea vârstei (14 ani).
 - b. Trimiterea pozelor și link-ul malițios (bit.ly) cu presiunea de timp („riști să pierzi șansa”).
3. Conversația cu „Irina” (Prietena Compromisă): Discuția în care prietena o încurajează suspect de mult să trimită numărul de telefon.
4. Conversațiile despre Bani (Mobilul): Discuțiile cu „Mircea” și „Sara” care dovedesc că Smaranda avea nevoie disperată de 200 de lei.
5. Profilul de Instagram al Victimei (Smaranda): Captură care arată că are școala („s.g. Ecaterina Teodorescu”) trecută public în bio.
6. Profilul de Instagram al Agresorului: Captura cu contul „newstardanceromania” care arată elementele de cont fals (puține postări, urmăritori boți).
7. Instagram Story (Locația): Captura cu postarea din sala de dans care dezvăluie locația în timp real („Academia de Dans Fantezia”).

Probele Documentare și Indicii Fizice: leagă activitatea online de acțiunile din lumea reală.

1. Bonul Fiscal (K-Express Dej): Dovada cumpărăturilor (apă, paste, conserve) făcute pe 21.09.2023 la ora 21:05, indicând pregătirea pentru o plecare/grup.
2. Istoricul Căutărilor Google: Foiaia care arată căutările incriminatoare: „cazare Beclean”, „model acord parental editabil”, „euro în lei”.
3. Biletul Post-it: Notița scrisă de mână „Joi 17:30 antr.” – confirmă orarul cunoscut de agresor.
4. Harta Traseului: O imagine cu ruta Dej – Beclean – Bistrița (printată de pe Google Maps).

Fotografii de la Fața Locului și Supraveghere

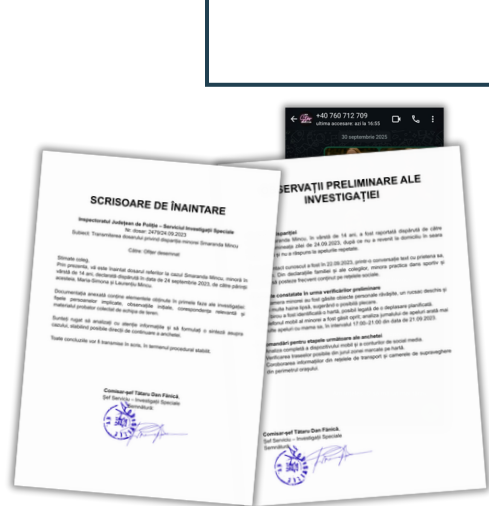
1. Camera Smarandei: Fotografie de ansamblu a dormitorului. Detaliu critic: Pe birou trebuie să se vadă o hartă fizică deschisă (elementul de planificare offline).
2. Imaginea CCTV (Supraveghere): Fotografia alb-negru care surprinde momentul urcării în mașină pe 21.09.2023 la ora 21:32:02.
3. Exteriorul Blocului: Fotografia locuinței, pentru a confirma că agresorii știau unde locuiește.
4. Portretele Persoanelor: Fotografii cu Smaranda, părinții, Irina și Ana pentru identificarea personajelor.

Simulări ale discuțiilor uzuale dintre victimă și prieteni.



Capturi de ecran cu solicitări venite de la profiluri necunoscute sau false.

Reproduceri ale adreșelor web înșelătoare, ascunse adesea în spatele unor promisiuni goale.



Rapoarte și documente oficiale care simulează realitatea.

Imagini cu locuri sau comportamente uzuale.



Pasii prin care învățăm #siguranțăpeinternet!

Pași prin care învățăm #siguranțăpeinternet!

Etapele jocului:

#PregătireaDetectivilor: Briefing realizat de instructor

Aceasta este etapa de imersiune, unde instructorul setează atmosfera și transformă sala de clasă într-o „agenție de investigații”.

- Contextul: Instructorul anunță elevii că vor deveni „super detectivi” și vor lucra în echipe pentru a rezolva un caz complex, denumit „Misterul din Rețea” sau cazul specific „Dispariția Smarandei”.
- Organizarea: Elevii sunt împărțiți în echipe de câte **5 membri**.
- Misiunea: Se explică obiectivul clar: analizarea unui dosar confidențial pentru a descoperi indiciile manipulării și a înțelege ce s-a întâmplat cu victima, folosind logica și perspicacitatea.

#RezolvămMistere: Joacă ghidată de instructor

În această etapă, elevii interacționează direct cu dosarul fizic. Instructorul are rolul de facilitator, ghidând echipele fără a le oferi soluțiile.

- **Faza 1:** Deschiderea Dosarului și Analiza Probelor: Echipele primesc dosarul fizic care conține replici fidele ale interacțiunilor online (printscreen-uri, profiluri false, mesaje). Elevii trebuie să examineze conversații și să identifice semnele de manipulare (lingușire, presiune).
- **Faza 2:** Conectarea Indiciilor (Puzzle-ul Logic): Elevii corelează informațiile din mediul online cu cele din lumea reală. De exemplu, leagă postarea locației sălii de dans (Story) cu nevoia urgentă de bani și cu momentul dispariției surprins pe camerele CCTV.
- **Faza 3:** Identificarea Amenințării: Echipele trebuie să recunoască tacticile agresorului: promisiuni false („câștigătorii primesc premii atractive”), urgența artificială pentru apel la FOMO (fear of missing out) („riști să pierzi șansa”) și cererea de date personale sau imagini.

#LecțiiÎnvățate: Dezbateri ghidate pentru concluzii corecte

Aceasta este cea mai importantă etapă, unde experiența jocului este transformată în competențe de siguranță pe termen lung. Discuția se axează pe „**Lecțiile cheie**” identificate în raport:

- **Confidențialitatea datelor:** Discuție despre cum divulgarea școlii sau a locației în timp real (check-in) poate duce la localizarea fizică a copilului.
- **Mitul „străinului prietenos”:** Analiza faptului că profilurile online pot fi false și că nu trebuie să avem încredere în necunoscuți, indiferent cât de binevoitori par.
- **Puterea lui „NU”:** Întărirea ideii că elevii au dreptul să refuze cereri de poze sau întâlniri și că trebuie să anunțe un adult de încredere (părinte, profesor) dacă se simt amenințați sau confuzați.
- **Amprenta digitală:** Conștientizarea faptului că tot ce postează online (poze, comentarii) rămâne acolo permanent și poate fi folosit împotriva lor.

Structură de timp recomandată:

#PregătireaDetectivilot: Briefing realizat de instructor

🕒 00:00 – 00:05 (5 min)

Obiectiv: Captarea atenției și setarea contextului.

Acțiune: Instructorul anunță elevii că pentru următoarele 45 de minute nu mai sunt elevi, ci „detectivi” în cadrul unei agenții de investigații digitale.

Organizare: Împărțirea rapidă în echipe de 5 elevi.

Distribuirea materialelor: Fiecare echipă primește dosarul fizic sigilat cu eticheta „CONFIDENȚIAL – Dosar nr. 2479/24.09.2023”.

Misiunea: „O adolescentă pe nume Smaranda a dispărut. Poliția ne-a dat acces la conversațiile ei, la pozele din cameră și la imagini de pe camerele de supraveghere. Trebuie să aflați CINE a convins-o să plece, UNDE s-a dus și CE GREȘELI de securitate a făcut.”

#RezolvămMistere: Joacă ghidată de instructor

🕒 00:05 – 00:30 (25 min)

Obiectiv: Analiza probelor și conectarea indiciilor. Instructorul nu dă răspunsuri, doar ghidează.

Acțiune:

- **Min 05-15 (Faza Online): Elevii analizează capturile de ecran.**

Trebuie să identifice profilul fals „New Star Dance Competition” (semne: puține postări, urmăritori boți).

Trebuie să observe presiunea psihologică din mesajele WhatsApp („riști să pierzi șansa”) și link-ul suspect.

Identificarea „complicelui”: Irina (cont spart/compromis) care insistă nefiresc.

- **Min 15-25 (Faza Fizică & Cronologia): Elevii analizează probele fizice.**

Harta din cameră: Elevii observă harta deschisă pe birou în poza dormitorului.

Bonul și locația: Corelarea bonului de la K-Express Dej (ora 21:05) cu imaginea CCTV (ora 21:32).

Destinația: Descoperirea traseului spre Beclean/Bistrița folosind istoricul căutărilor.

Sfat pentru instructor: Dacă o echipă se blochează, instructorul poate pune o întrebare ajutătoare: „Ați verificat data și ora de pe bonul de cumpărături față de ora de pe camera de supraveghere?” sau „De ce credeți că avea nevoie de 200 de lei?”.

#Lecții învățate: Dezbateri ghidată pentru concluzii corecte

🕒 00:30 – 00:45 (15 min)

Aceasta este partea unde lecțiile sunt extrase prin „răsturnarea de situație”.

A. Revelația (Momentul „Aha!”) Instructorul dezvăluie adevărul:

„Detectivi, Smaranda este în siguranță. Aseară a fost la o petrecere cu paste („Pasta Party”) la o prietenă, profitând că părinții erau plecați. Acea mașină neagră din CCTV era un taxi sau mașina unui prieten, nu a răpitorului.”

B. Lecțiile Învățate (Reformulate pentru acest final)

- **Lecția 1:** Gândirea Critică vs. Biasul de Confirmare
 - Explicație: „Ați crezut că e răpită, așa că ați interpretat orice indiciu (harta, mașina, lipsa părinților) ca o dovadă a răpirii. În realitate, harta era poate pentru o excursie viitoare, iar mașina era transport legitim.”
 - Concluzie: Nu trageți concluzii bazate pe frică. Verificați faptele. Bonul fiscal a fost cheia: nimeni nu fuge de acasă cu 5 pungi de paste și sos de roșii, dar oricine face asta pentru o petrecere.
- **Lecția 2:** Pericolul a fost REAL, chiar dacă nu s-a concretizat
 - Explicație: „Faptul că Smaranda a mers la petrecere nu înseamnă că New Star Dance nu era o țeapă. Era! Escrocul a încercat să o manipuleze. Smaranda a fost norocoasă că a avut alte planuri (petrecerea) și a ignorat escrocul în ultima clipă.”
 - Concluzie: Ignorarea pericolului nu îl face să dispară. Data viitoare, s-ar putea să nu mai aibă o petrecere care să o distragă.
- **Lecția 3:** Vulnerabilitatea rămâne
 - Explicație: „Chiar dacă nu a fost răpită acum, Smaranda a făcut greșeli majore. A postat locația exactă a sălii de dans pe Story și are școala în bio. Dacă „New Star” era un prădător sexual real și hotărât, ar fi putut veni după ea la sală, indiferent dacă ea îi răspundea sau nu pe WhatsApp.”
 - Concluzie: Siguranța online înseamnă să nu oferi indicii agresorilor, chiar și atunci când nu interacționezi direct cu ei.

Rezumat pentru Instructor:

Scopul nu mai este „prinderea hoțului”, ci conștientizarea faptului că online, suntem expuși chiar și când nu suntem victime directe.

Sfat pentru instructor: Transformă "Greșeala" în "Momentul Aha!" - Nu le spune direct că au greșit dacă susțin scenariul răpirii. În schimb, pune-le o singură întrebare capcană înainte de a dezvălui adevărul: "Dacă a fost răpită pentru trafic sau șantaj, de ce răpitorii au lăsat-o să se oprească să cumpere 5 pungi de paste, sos de roșii și ciocolată?"

A photograph of a classroom scene. In the foreground, two young men are seated at a wooden desk. The one on the left is partially visible, looking towards the right. The one in the center is wearing a blue polo shirt and is gesturing with his right hand while speaking. On the desk in front of them are various items: a stack of papers, a blue pen, a stack of colorful sticky notes, a black bag, a pink bag, and a tablet. In the background, a teacher, a man in a grey polo shirt, is standing and smiling. Behind him is a large blackboard with some faint chalk marks.

GHIDARE DEZBATERI

Cum trecem de la
"predică" la dialog?

Filosofia educației non-formale

De la Profesor la Ghid: Cum coordonezi un joc, nu o lecție

În acest exercițiu, rolul dumneavoastră se schimbă fundamental. Nu mai sunteți profesorul care deține „răspunsul corect” și îl predă elevilor. Deveniți Investigatorul Șef care își ghidează echipa să gândească singură. Scopul nu este ca elevii să ghicească scenariul din prima, ci să își exerseze „mușchiul” gândirii critice. Chiar dacă o iau pe o pistă greșită, procesul de analiză este mai valoros decât rezultatul final.

PRINCIPII

1. **Întrebări, nu Răspunsuri:** Când un elev se blochează sau trage o concluzie greșită, nu îl corectați imediat. Întrebați: „Ce dovadă te-a făcut să crezi asta?” sau „Există vreo altă explicație posibilă pentru acest indiciu?”.
2. **Validăm logica, nu neapărat concluzia:** Chiar dacă elevii greșesc scenariul (ex: cred că Smaranda e răpită), lăudați faptul că au corelat indicii. „Îmi place cum ați legat mașina de mesajul primit, e o ipoteză validă. Hai să vedem dacă se confirmă cu restul probelor.”
3. **Tăcerea este utilă:** După ce puneți o întrebare, așteptați câteva secunde. Lăsați-i să gândească. Dacă răspundeți dumneavoastră prea repede, ei vor înceta să mai caute soluții.
4. **Atacăm Ideea, nu Persoana:** În investigație, contrazicem o teorie, nu pe colegul care a emis-o. Folosim expresii de genul: „Nu sunt de acord cu ipoteza ta pentru că...” în loc de „Nu ai dreptate/Ești fraier”.
5. **Orice ipoteză e permisă, dar trebuie probată:** Nu există idei „proaste”, există doar idei fără dovezi. Dacă cineva spune „A fugit cu extraterestrii”, întrebăm simplu: „Avem vreo probă în dosar care susține asta?”.

GESTIONAREA MOMENTULUI „AM FOST PĂCĂLIȚI”

Cum transformăm frustrarea în învățare:

- Nu spuneți: „Ați greșit, nu a fost răpită.”
- Spuneți: „Ați construit un scenariu foarte plauzibil bazat pe frică și coincidențe. Creierul nostru este programat să ne protejeze, așa că vede pericole peste tot. Astăzi am învățat diferența dintre ceea ce pare a fi (mesaje înfricoșătoare) și ceea ce este (un bon de cumpărături banal).”

MODELUL ORID

Cum transformăm o dezbatere haotică într-o lecție structurată?

O greșeală frecventă în dezbateri este să sărim direct la concluzii („A fost răpită!”) fără a analiza faptele. Pentru a evita haosul și a calma spiritele, folosim metoda ORID. Aceasta ghidează creierul elevilor prin patru etape logice: de la ce au văzut, la ce au simțit, ce au înțeles și, în final, ce vor face.

NIVELUL OBIECTIV (Faptele)

- Întrebarea cheie: „Ce ați văzut concret în dosar?” În această etapă, interziceți interpretările. Căutăm doar date, cifre, ore, obiecte. Este momentul în care „detectivii” își aliniază probele.
- Întrebări de ghidaj:
 - „Ce oră apare pe bonul fiscal? Dar pe camera de supraveghere?”
 - „Ce obiecte ați identificat pe masa din dormitorul Smarandei?”
 - „Care este lista exactă de cumpărături de pe bon? Citiți produsele.”
 - „Ce scrie în biografia de Instagram a Smarandei?”

● CAPCANĂ DE EVITAT: Dacă un elev spune: „Am văzut că e speriată”, corectați-l blând: „Asta e o interpretare. Ce ai văzut concret? Un mesaj cu multe semne de exclamare, nu frica.”

NIVELUL REFLEXIV (Emoțiile)

- Întrebarea cheie: „Cum v-ați simțit citind mesajele?” Aici validăm reacția emoțională. Este normal ca elevii să se fi speriat de mesajele agresorului. Dacă nu discutăm frica acum, ea le va bloca gândirea logică mai târziu.
- Întrebări de ghidaj:
 - „Când ați citit mesajul 'Riști să pierzi șansa', ce ați simțit? Presiune? Curiozitate?”
 - „Vi s-a părut prietenoasă sau suspectă insistența Irinei?”
 - „Câți dintre voi s-ar fi simțit flatați de mesajul 'Ai foarte mult potențial'?”

NIVELUL INTERPRETATIV (Sensul)

- Întrebarea cheie: „Ce înseamnă aceste indicii puse cap la cap?” Acesta este „motorul” dezbaterii. Aici analizăm scenariile, contrazicem ipoteze și, în final, dezvăluim adevărul (că a fost la o petrecere).
- Întrebări de ghidaj (Înainte de revelație):
 - „De ce credeți că a căutat 'cazare ieftină'? Are legătură cu fuga sau cu altceva?”
 - „De ce și-ar lua cineva 5 pungi de paste și sos de roșii dacă fuge de acasă?”
 - Întrebări de ghidaj (După revelație):
 - „Cum se schimbă povestea acum că știți că a fost la o petrecere? Mesajele de la New Star mai au vreo legătură cu plecarea ei?”
 - „Ce greșeli reale de securitate a făcut, chiar dacă nu a fost răpită?” (Ex: Locația pe Story).

● SFAT: Aici se produce marea învățare despre Bias-ul de Confirmare. Arătați-le cum au ignorat bonul cu „mâncare de petrecere” doar pentru că s-au concentrat pe mesajele alarmante („scary”) de pe WhatsApp.

NIVELUL DECIZIONAL (Acțiunea)

- Întrebarea cheie: „Ce facem noi diferit de mâine?” Fără acest pas, jocul rămâne doar o distracție. Trebuie să transferăm experiența în viața reală a elevilor.
- Întrebări de ghidaj:
 - „Dacă mâine primiți un mesaj de la un agent care caută talente („scouter”), care e primul lucru pe care îl verificați?”
 - „Câți dintre voi aveți școala trecută la profil sau dați Check-in în timp real? Cine își schimbă setările azi?”
 - „Cui îi spuneți dacă vi se pare ceva suspect, chiar dacă e doar o 'coincidență'?”

TEHNICI NON-FORMALE

Tehnicile non-formale pentru a dinamiza dezbaterea și a implica toți elevii.

Într-o investigație, fiecare voce contează. Uneori, cei mai vocali elevi pot domina discuția, impunând o teorie greșită grupului. Alteori, clasa poate cădea de acord prea repede. Folosiți aceste 3 tehnici pentru a „agita apele” și a forța o analiză mai profundă.

TEHNICA „PÂNZA DE PĂIANJEN” (Vizualizarea Coincidențelor)

Această metodă este cea mai eficientă pentru a demonta vizual scenariul fals al răpirii și a explica Bias-ul de Confirmare.

- Cum funcționează:
 - Desenați un cerc pe tablă cu numele „SMARANDA”.
 - Lipiți în jurul ei imaginile cu probele cheie (sau scrieți-le): Bonul fiscal, Mesajul de amenințare, Mașina neagră, harta.
 - Rugați un elev să tragă o linie între Mesajul de Amenințare și Mașina Neagră.
 - Momentul de analiză: Întrebați clasa: „Această linie este solidă? Avem vreo dovadă că șoferul mașinii este cel care a scris mesajul? Sau este o linie imaginară desenată de frica noastră?”

TEHNICA „AVOCATUL DIAVOLULUI” (Testarea Argumentelor)

Când toată clasa este convinsă că „Smaranda a fost răpită de New Star Dance”, intrați dumneavoastră în rolul contra-argumentului pentru a le testa logica.

- Exemplu de intervenție a profesorului:
 - „Sunt de acord că New Star pare suspect. Dar, dacă eu aș fi un răpitor periculos care vrea să o ia pe sus, de ce aș lăsa-o să se oprească la magazin să cumpere 5 pungi de paste și 3 borcane de sos?”
 - „Dacă voia să fugă fără urmă, de ce și-ar fi dat check-in public la sala de dans cu câteva ore înainte?”

ÎNTREBARE DE DEZBATERE: „Cine poate găsi o explicație nevinovată pentru harta de pe birou? Dacă nu e un plan de fugă, ce altceva ar putea fi?” (Răspuns posibil: O temă la geografie, o excursie cu școala, un vis de vacanță).

TEHNICA „CELE 4 COLȚURI” (Dezbatere prin Mișcare)

Această tehnică scoate elevii din bănci și îi obligă să ia o poziție clară. Este excelentă pentru subiectele sensibile legate de vinovăție.

- Cum funcționează:
 - Definiți colțurile clasei: Total de acord, Parțial de acord, Parțial dezacord, Total dezacord.
 - Lansați o afirmație provocatoare: „Smaranda este singura vinovată pentru situația în care a ajuns.”
 - Elevii se așază în colțul care corespunde opiniei lor.
 - Cereți argumente din fiecare colț.

TEHNICA „POST-IT STORMING” (Pentru elevii timizi)

Nu toți elevii au curajul să ridice mâna. Această metodă le dă tuturor o voce egală.

- Sarcina: „Aveți 2 minute. Scrieți pe un post-it o singură greșală de securitate pe care ați observat-o în dosar (ex: locația pe story, școala în bio, discuția cu străini).”
- Acțiunea: Lipiți toate bilețelele pe tablă.
- Rezultatul: Veți obține o „hartă a vulnerabilităților” creată de clasă. Veți observa că mulți vor identifica Locația pe Story sau Școala în Bio, validând cunoștințele grupului.

FISA DE DEZBATERE anchetă CAZUL SMARANDA

Echipa: _____

ETAPA 1: PRIMA IMPRESIE (Fără analiză profundă)

După ce ați răsfoit rapid dosarul, care este scenariul vostru? Ce credeți că s-a întâmplat cu Smaranda?

 Ipoteza noastră:

(Ex: A fost răpită / A fugit de acasă / S-a întâlnit cu traficanții)

.....

.....

.....

ETAPA 2: ANALIZA PROBELOR (Fapte vs presupuneri)

Analizați probele din dosar.

Deosebiți ce vedeți (Fapte) de ce credeți (Presupunere).

PROBA:	FAPTE:	PRESUPUNERI
Mesajele WhatsApp	Scrie: „Riști să pierzi șansa”. Link bit.ly.	Smaranda a dat click
Harta din cameră		
		
Mașina Neagră (CCTV)		
		
Bonul Fiscal		
		
.....		
		
.....		
		
.....		
		
.....		
		

ETAPA 3: VERDICTUL ȘI VULNERABILITĂȚILE

Indiferent dacă a fost răpită sau nu, Smaranda a făcut greșeli care i-au pus siguranța în pericol.

● **Locația: (Unde a greșit?)**

Indiciu: Verificați Story-ul de pe Instagram.

● **Profilul: (Ce informație privată e publică?)**

Indiciu: Verificați Bio-ul profilului ei

● **Încrederea: (Cum a reacționat la mesaje?)**

Indiciu: Discuția cu New Star.

● **Urgența artificială: (Cum au forțat-o să acționeze rapid?)**

Indiciu: Citiți ultimele mesaje de pe WhatsApp. Ce condiție de timp i-au pus?

● **Link-urile suspecte: (Pe ce a dat click fără să verifice?)**

Indiciu: Căutați textul albastru din conversație.

● **Validarea Socială: (Cine a împins-o de la spate?)**

Indiciu: Recitiți discuția cu Irina. Vi se pare normal cât de mult insistă?



SIGURANȚA PE INTERNET

Concepte cheie abordate
în joc.

1 AMPRENTA DIGITALĂ FIZICĂ

Concept: Cum devine profilul tău o hartă pentru străini

 **DEFINIȚIE DE DETECTIV:** Majoritatea oamenilor cred că „date personale” înseamnă doar CNP-ul sau adresa de acasă. În realitate, Amprenta Digitală Fizică este formată din micile detalii pe care le presăram voluntar pe internet: școala, parcul preferat, clubul de sport. Puse cap la cap, aceste firimituri de informație creează o hartă exactă a mișcărilor tale zilnice. Se numește Doxing Involuntar – când te expui singur fără să îți dai seama.

PROBA DIN DOSAR:

Să analizăm biografia de Instagram a Smarandei:

@smaranda.08 "Scenele sunt lumea mea. Ritmul e limbajul meu."  s.g. Ecaterina Teodoroiu 

Smaranda a scris numele școlii gimnaziale direct în profilul public. Oricine intră pe profilul ei știe acum:

1. În ce oraș locuiește (căutând școala pe Google).
2. Unde poate fi găsită fizic între orele 08:00 și 14:00.
3. Ce vârstă aproximativă are.

RED FLAG (SEMNALUL DE ALARMĂ):

Când vezi următoarele detalii în Bio sau în descrierile pozelor publice:

Numele complet al școlii sau liceului.

Numele clubului de sport unde te antrenezi.

Cartierul sau zona în care stai (ex: "Mănăstur Life").

Poze repetate din fața scării blocului unde se vede numărul străzii.

SFATUL WEBTECTIVULUI:

"Fii un mister, nu o țintă!" Informațiile din BIO sunt publice!

1. Șterge școala: Nu te ajută cu nimic să știe străinii unde înveți. Prietenii tăi știu deja.
2. Fii vag: În loc de "Locuiesc în cartierul X, strada Y", folosește doar orașul sau o descriere creativă.
3. Testul Străinului: Roagă pe cineva care nu te cunoaște să se uite la profilul tău timp de 1 minut. Dacă poate ghici unde vei fi mâine dimineață la 8, ai o problemă de securitate!

ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:

"Dacă un străin ar vrea să îți facă o 'surpriză' neplăcută Smarandei, cât de greu i-ar fi să o găsească știind doar numele școlii din bio?"

2 GEOTAGGING ȘI TRACKING

Concept: Pericolul de a posta locația în timp real

 **DEFINIȚIE DE DETECTIV:** Funcția de „Location” (Locație) sau „Check-in” este un instrument cu două tăișuri. Când postezi o poză cu eticheta locului în timp ce încă ești acolo, le oferi urmăritorilor (și posibililor agresori) coordonatele tale GPS exacte. Aceasta transformă profilul tău dintr-un album foto într-un sistem de urmărire în timp real.

 **PROBA DIN DOSAR:**

Să analizăm Story-ul postat de Smaranda:

O poză din interiorul sălii de antrenament cu tag-ul locației:

 ACADEMIA DE DANS FANTEZIA.

Fotografia are câteva elemente care indică informații:

1. Eticheta Locației: Indică exact clădirea în care se află.
2. Timpul: Scribe „1m” (acum un minut). Asta înseamnă că Smaranda este ACUM în acea clădire.
3. Contextul: Sala pare goală, ceea ce sugerează că este singură sau a ajuns prima, crescând vulnerabilitatea.

 **RED FLAG (SEMNALUL DE ALARMĂ):**

Când vezi aceste detalii în Story:

- Textul „Just Now” sau „1m ago” combinat cu o locație specifică.
- Poze cu fundaluri ușor de recunoscut (nume de străzi, stații de autobuz, magazine unice) postate instantaneu.
- Check-in la școală sau acasă.

 **SFATUL WEBTECTIVULUI: „Regula LATERGRAM”**

Nu posta niciodată UNDE ești, CÂND ești acolo!

1. Postează cu întârziere: Fă poza acum, postează-o după ce ai plecat de la locație (Later-gram = Later Instagram).
2. Fii general: Folosește tag-ul orașului („Cluj-Napoca”), nu al străzii sau al clădirii specifice.
3. Close Friends: Dacă vrei neapărat să pui locația în timp real, fă-o doar pentru lista de „Prieteni Aproiați”, nu Public.

 **ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:**

Dacă 'New Star' ar fi fost un agresor care pândește în zonă și ar fi văzut Story-ul cu '1m ago', de cât timp ar fi avut nevoie să ajungă la sală? "Cine mai poate folosi în moduri nepotrivite astfel de informații?"

3 ANATOMIA UNUI PROFIL FALS

Concept: Cum deosebești un cont real de o „fantomă”

 **DEFINIȚIE DE DETECTIV:** Un „Cont Fantomă” (Shell Account) este un profil creat rapid, adesea folosind boți sau imagini furate, cu scopul de a părea legitim pentru a înșela victimele. Escrocii știu că ne uităm la numărul de urmăritori (Followers) pentru a decide dacă avem încredere, așa că adesea cumpără urmăritori falși pentru a crea o iluzie de popularitate.

 **PROBA DIN DOSAR:**

Să analizăm profilul @newstardanceromania:

Urmărind acest profil putem observa că există mai multe informații care ridică semne de întrebare cu privire la autenticitatea contului. Acestea pot fi folosite pentru a evalua orice alte conturi.

1. Raportul Suspect: Are 852 Followers (Urmăritori) dar doar 4 Postări. Un cont real cu atâția fani ar avea mult mai mult conținut.
2. Following: Urmărește doar 23 de persoane (de obicei țintele).
3. Bio-ul Vag: „DM pentru colaborări” – o competiție națională serioasă ar avea un site oficial (.ro), nu ar discuta afaceri prin mesaje private.

 **RED FLAG (SEMNALUL DE ALARMĂ):**

Semne că vorbești cu un bot sau un escroc:

- Mii de urmăritori, dar foarte puține Like-uri/Comentarii la poze.
- Poze generice, furate de pe Pinterest sau cu text mult (grafică ieftină), fără fețe umane reale etichetate.
- Gramatică stricată sau traduceri automate în descriere.
- Contul este creat foarte recent (poți verifica la „About this account”).

 **SFATUL WEBTECTIVULUI:**

"Investighează Influencerul" Nu te lăsa impresionat de cifre!

1. Verifică etichetările: Mergi la secțiunea „Tagged Photos”. Un cont real (mai ales o competiție) va fi etichetat de participanți reali.
2. Caută pe Google: Caută numele concursului. Dacă nu există știri, site oficial sau mențiuni pe alte site-uri, nu există.
3. Reverse Image Search: Dacă poza de profil pare prea perfectă, caut-o pe Google Images. S-ar putea să fie a unui model din altă țară.

 **ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:**

"De ce credeți că escrocii cheltuie bani să cumpere 800 de urmăritori falși? Cum ne influențează acel număr decizia de a răspunde la mesaj?"

4 METODA „VÂNĂRII DE TALENTE”

(Concept: Ingineria socială prin validare și lingușire)

 **DEFINIȚIE DE DETECTIV:** „Grooming-ul” nu începe cu amenințări, ci cu laude. Metoda „Talent Scout” (Vânătorul de Talente) exploatează nevoia naturală a tinerilor de a fi apreciați și validați. Agresorul se prezintă ca o autoritate (manager, scout, fotograf) și folosește complimente exagerate pentru a crea o conexiune emoțională rapidă. Odată ce victima se simte „specială” și „aleasă”, va face orice pentru a nu pierde acea validare.

PROBA DIN DOSAR:

Să analizăm mesajul de abordare de pe Instagram:

„Echipa noastră ți-a urmărit performanțele și credem că ai foarte mult potențial în dans 🕺. Ai vrea să participi la concursul pe care îl organizăm?”

Mai multe elemente descriu metoda:

1. Ego-ul: Mesajul începe direct cu un compliment puternic („foarte mult potențial”).
2. Vague Authority: „Echipa noastră” – nu specifică cine sunt, dar sună oficial.
3. Exclusivitatea: Sugerează că au urmărit-o de mult timp (ceea ce e fals, e un mesaj copy-paste), făcând-o să se simtă unică.

RED FLAG (SEMNALUL DE ALARMĂ):

Când vezi aceste tipare în mesaje:

- Străini care te laudă excesiv încă din primul mesaj.
- Expresii vagi precum „Am văzut profilul tău și ne place”, fără detalii specifice.
- Oportunități de carieră (modeling, dans, ambasador de brand) oferite pe Instagram, nu pe canale oficiale.

SFATUL WEBTECTIVULUI:

"Regula: Prea frumos să fie adevărat"

1. Verifică sursa: Cere un link către site-ul oficial al agenției sau concursului.
2. Google it: Caută textul mesajului pe Google. De multe ori e un script folosit la mii de victime.
3. Nu plăti: Dacă ți se cere să plătești o taxă de înscriere sau un „kit de start”, e 100% țeapă.

ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:

De ce credeți că escrocii folosesc complimente? Cum ne afectează laudele capacitatea de a gândi critic? De ce îi cred oamenii?”

5 CONTURILE COMPROMISE

Concept: Când prietenul tău nu e de fapt prietenul tău

 **DEFINIȚIE DE DETECTIV:** Cea mai periculoasă capcană este cea care vine de la o persoană de încredere. Atacatorii sparg conturile utilizatorilor (prin phishing) și le folosesc pentru a trimite mesaje listei de prieteni. Aceasta se numește „Transfer de încredere”: ai încredere în Irina, deci ai încredere în link-ul trimis de ea. Contul Irinei a devenit un „Zombie” – arată ca ea, dar nu e.

 **PROBA DIN DOSAR:**
Să analizăm insistența Irinei:

Smaranda e sceptică: „hmm, nu știu, e puțin ciudat că scriu direct...” Irina insistă: „Atunci dă-le numărul! E clar că e ceva serios, altfel nu ți-ar fi scris.”

Mai multe elemente descriu metoda:

1. Schimbarea de rol: Irina, care de obicei e o prietenă egală, devine brusc o „agentă de vânzări” pentru concurs.
2. Presiunea: Ea împinge acțiunea („Dă-le numărul!”) în loc să fie precaută.
3. Logica circulară: „E serios pentru că ți-au scris” – un argument fals menit să elimine dubiile Smarandei.

 **RED FLAG (SEMNALUL DE ALARMĂ):**
Semne că un prieten a fost hack-uit:

- Îți cere bani, voturi la un concurs, sau numărul de telefon brusc.
- Îți trimite link-uri fără context („Uite ce am găsit, ești tu în video?”).
- Folosește un limbaj diferit de cel uzual (prea formal sau cu greșeli de traducere).

 **SFATUL WEBTECTIVULUI:**

"Verificarea pe al doilea canal" Dacă mesajul e dubios, schimbă aplicația!

1. Sună: Dacă Irina îți scrie pe Insta să dai click undeva, sun-o pe telefon (voce).
2. Întrebarea capcană: Întreabă ceva ce doar voi doi știți („Cum a fost la testul de la mate de azi?”). Un hacker nu va ști să răspundă. (Smaranda putea să o întrebe de "gluma zilei" cu nivelul B-minus).

 **ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:**

Smaranda a avut un instinct bun inițial ('e puțin ciudat'). De ce credeți că a renunțat la el după mesajul Irinei?"

6 PHISHING ȘI LINK-URI MALIȚIOĂSE

(Concept: Capcanele ascunse în spatele textului albastru)

 **DEFINIȚIE DE DETECTIV:** „Phishing-ul” (pescuitul de date) este încercarea de a te păcăli să îți dai singur cheile de la casă. Agresorii știu că nu le vei da parola dacă ți-o cer direct. Așa că îți trimit un link către un site fals care arată exact ca Instagram, Google sau o pagină de concurs. Când te loghezi acolo, parola ta ajunge direct la ei. Pentru a ascunde adresa site-ului fals.

 **PROBA DIN DOSAR:**

Să analizăm link-ul primit de Smaranda pe WhatsApp:

<http://bit.ly/inscriere-dans2025>

Mai multe elemente descriu metoda:

1. Masca: Link-ul începe cu bit.ly. Acesta este un serviciu legitim, dar este folosit de hackeri pentru a ascunde destinația reală.
2. Insecuritatea: Începe cu http://, nu cu https://. Litera „s” vine de la Secure (Securizat). Site-urile serioase folosesc întotdeauna HTTPS.
3. Contextul: I se cere să completeze o „fișă de înscriere”. Cel mai probabil, acel link ducea la un formular care cerea date personale.

 **RED FLAG (SEMNALUL DE ALARMĂ):**

Nu da click dacă:

- Link-ul este prescurtat (bit.ly, tinyurl, is.gd) și vine de la un necunoscut.
- Domeniul conține greșeli de scriere intenționate (ex: Instagram.com cu L mic în loc de I mare, sau facebok.com).
- Ți se cere să te „re-loghezi” pentru a vedea conținutul.

 **SFATUL WEBTECTIVULUI:**

"Verifică înainte de Click" Fii suspicios cu orice text albastru!

1. Link Decoders: Dacă primești un link scurt, copiază-l (fără să-l deschizi) și lipește-l într-un site de tip „URL Expander” (caută pe Google).
2. Nu te loga din link-uri: Dacă primești un mesaj „Ți-a fost spart contul, intră aici să-l recuperezi”, ignoră link-ul. Intră tu direct în aplicație/site.
3. Antivirus: Instalează o soluție de securitate pe telefon.

 **ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:**

"Dacă Smaranda ar fi accesat link-ul și ar fi apărut o pagină care îi cerea 'Loghează-te cu Instagram pentru a confirma înscrierea', ce s-ar fi întâmplat în secunda următoare?"

7 URGENȚA ARTIFICIALĂ (FOMO)

Concept: Cum blochează frica gândirea critică

 **DEFINIȚIE DE DETECTIV:** Escrocii știu un secret despre creierul uman: nu putem fi speriați și logici în același timp. Când suntem sub presiune, partea rațională a creierului se oprește, și preia controlul partea instinctuală. Pentru a activa acest mecanism, ei creează o criză de timp. Se numește „Urgență Artificială” sau exploatarea FOMO (Fear Of Missing Out - Frica de a rata ocazia).

PROBA DIN DOSAR:

Să analizăm schimbarea de ton a agresorului

„E important să intri azi... durează doar 2 minute.” „Dacă nu te înscrii imediat, riști să pierzi șansa. Nu vrem să rămâi pe dinafară!”

La început a fost politicos, dar când Smaranda a zis „O să mă uit mai târziu”, a devenit agresiv:

1. Ultimatumul: Impune un termen limită nerealist (acum, imediat, azi) pentru ceva ce ar trebui să dureze săptămâni (înscrierea la un concurs).
2. Minimizarea Efortului: „Durează doar 2 minute” – o tehnică de manipulare pentru a te face să acționezi fără să gândești („eh, e rapid, hai să o fac”).
3. Amenințarea Pierderii: „Riști să pierzi șansa”. Oamenii sunt mai motivați de frica de a pierde ceva decât de dorința de a câștiga ceva.

RED FLAG (SEMNALUL DE ALARMĂ):

- „Trebuie să acționezi ACUM/IMEDIAT.”
- „Oferta expiră în 10 minute.”

SFATUL WEBTECTIVULUI:

"Regula celor 5 minute" Urgența este inamicul siguranței.

1. Pune pauză: Când cineva te grăbește online, oprește-te. Pune telefonul jos. Numără până la 10.
2. Întreabă-te: „O instituție serioasă (bancă, școală, concurs) m-ar amenința pe WhatsApp că pierde locul dacă nu dau click în 2 minute?” Răspunsul e NU.
3. Verifică: Dacă ești stresat că pierzi o șansă, caută contactul oficial al organizatorului și întreabă-i pe ei, nu pe persoana din chat.

ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:

"De ce credeți că agresorul a devenit nervos când Smaranda a spus 'O să mă uit mai târziu'? Ce se întâmplă dacă victima are timp să se gândească?"

8 VULNERABILITATE FINANCIARĂ

Concept: Când lipsa banilor te face să iei decizii proaste

 **DEFINIȚIE DE DETECTIV:** Escrocii caută întotdeauna un „punct slab” la victime. De cele mai multe ori, acesta este nevoia de bani. Fenomenul se numește „Financial Grooming” sau „Money Muling”. Agresorul îți promite câștiguri rapide, premii în bani sau un job bine plătit, dar îți cere o mică sumă la început (taxă de înscriere, taxă de transport, garanție).

 **PROBA DIN DOSAR:**

Să analizăm disperarea Smarandei:

„Mircea, te rog mult... ai cum să mă ajuti cu ăia 200 de lei? Îți dau înapoi săptămâna viitoare, promit.”, „Sara, mai ai banii ăia? Îmi trebuie neapărat azi.”

Ea trimite mesaje repetate prietenilor cerând bani, aparent fără motiv:

1. Vulnerabilitatea: Smaranda avea nevoie urgentă de 200 de lei (pentru petrecere, cum am aflat ulterior).
2. Riscul: Dacă „New Star Dance” i-ar fi cerut o taxă de înscriere de 150 de lei promițându-i un premiu de 1000 de euro, ea ar fi fost victima perfectă.
3. Secretomania: Nu le spune prietenilor pentru ce îi trebuie banii, doar că îi trebuie „neapărat”.

 **RED FLAG (SEMNALUL DE ALARMĂ):**

- „Câștigă 500 lei pe zi lucrând de acasă / dând like-uri.”
- „Ai câștigat un iPhone/Premiu, dar trebuie să plătești transportul.”
- Orice agenție de modeling/casting care îți cere bani pentru „book foto”.

 **SFATUL WEBTECTIVULUI:**

Nu plăti ca să fii plătit! Banii nu cad din cer pe internet.

1. Regula de Aur: Dacă cineva îți cere bani ca să îți dea bani, e o țeapă. Punct.
2. Nu fi curier de bani: Dacă cineva îți propune să treacă bani prin contul tău și să păstrezi un comision, refuză! Ești folosit pentru spălare de bani (Money Mule) și poți avea dosar penal.
3. Vorbește: Dacă ai o problemă financiară reală, vorbește cu părinții. O greșeală recunoscută e mai ieftină decât o datorie la cămătari sau escroci.

 **ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:**

""Credeți că Smaranda ar fi acceptat să plătească o taxă de înscriere la concurs? Cum ne schimbă lipsa banilor deciziile?"

9 CONTURILE PUBLICE

Concept: Cine te privește din întuneric fără să știi?

 **DEFINIȚIE DE DETECTIV:** Pe internet, nu vorbești într-o cameră cu prietenii, ci pe un stadion cu luminile stinse. Tu nu vezi publicul, dar publicul te vede pe tine. Acesta este conceptul de Monitorizare Pasivă. Prădătorii nu atacă imediat. Mai întâi privesc, analizează și adună informații din umbră, profitând de conturile setate pe „Public” sau de utilizatorii care acceptă orice cerere.

 **PROBA DIN DOSAR:**

Să analizăm prima propoziție a agresorului:

„Echipa noastră ți-a urmărit performanțele și credem că ai potențial...”

Agresorul a avut acces la conținutul Smarandei (video-uri cu dans) înainte de a o contacta.:

1. Contul ei era Public.
2. Sau a acceptat cererea de urmărire a unui necunoscut („fan”) care a stat la pândă.

 **RED FLAG (SEMNALUL DE ALARMĂ):**

Semne că ai „porțile deschise”:

- Ai contul pe „Public” deși ești minor (sub pretextul „vreau să fiu influencer” sau „nu am nimic de ascuns”).
- Numărul tău de Followers este mult mai mare decât numărul persoanelor pe care le cunoști în viața reală.
- Primești like-uri sau vizualizări la Story de la conturi pe care nu le cunoști.

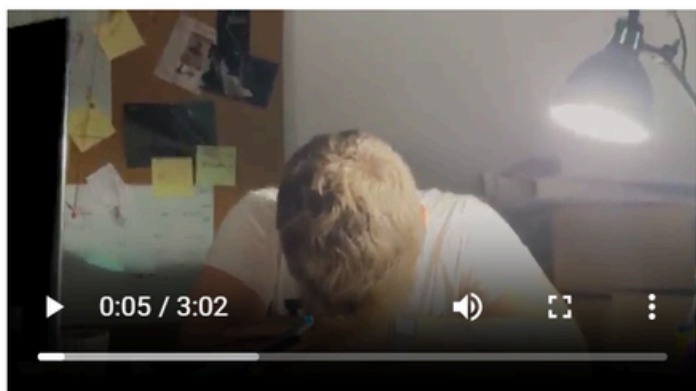
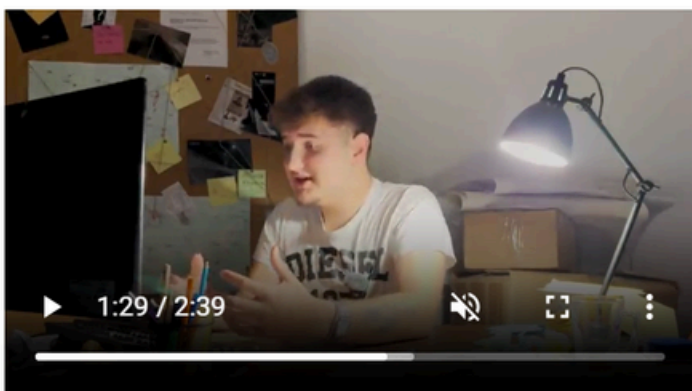
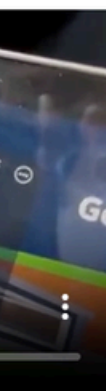
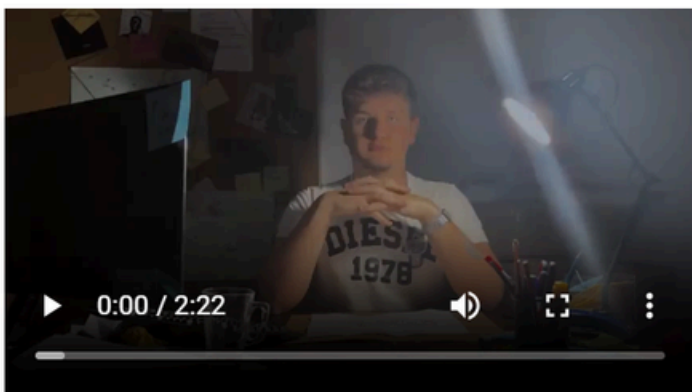
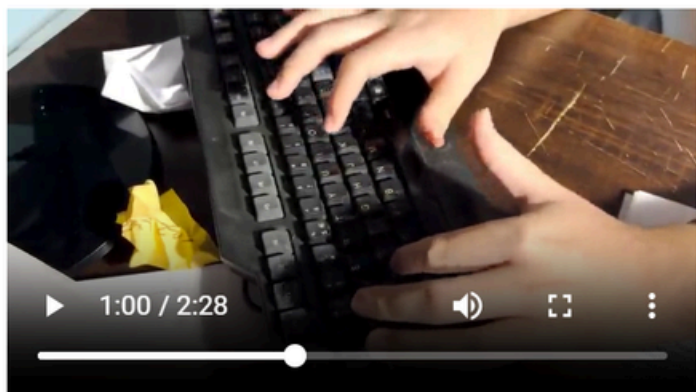
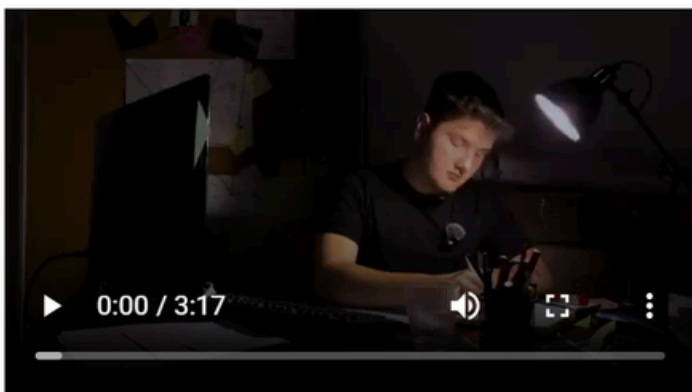
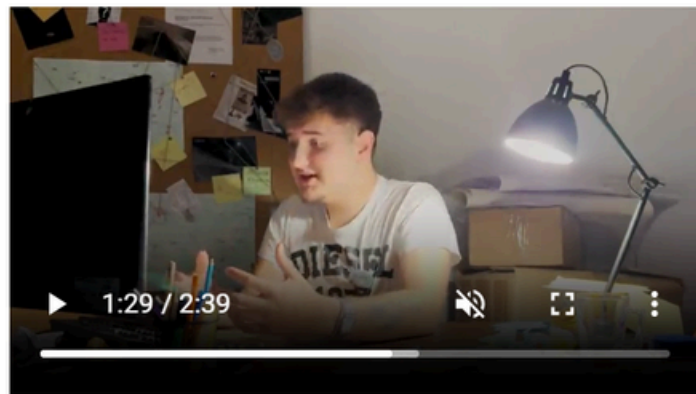
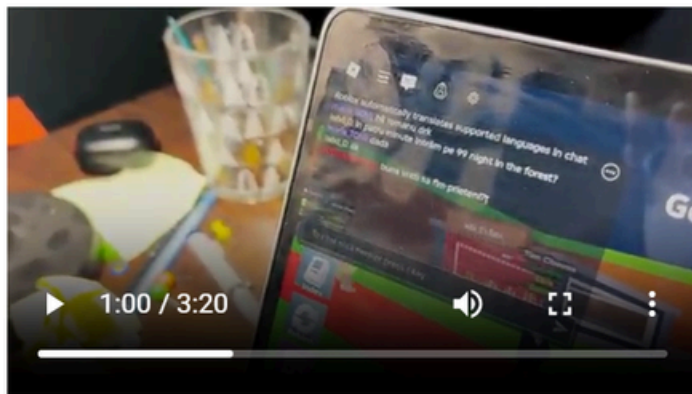
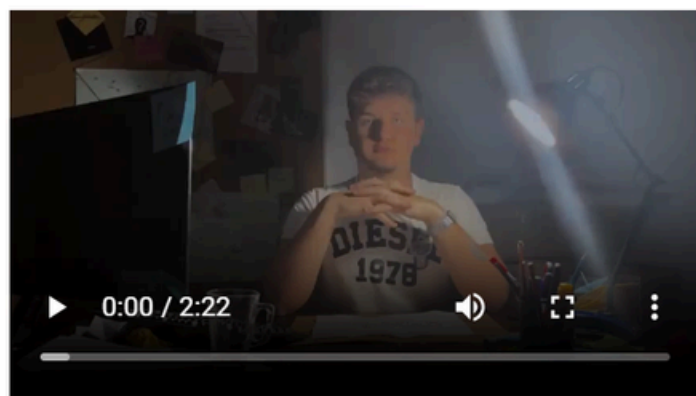
 **SFATUL WEBTECTIVULUI:**

„Vrei Fani sau vrei Siguranță?” Faima online vine cu un cost.

1. Cercul de Încredere: Treci contul pe Privat. Astfel, tu decizi cine intră în „camera” ta.
2. Curățenia de Primăvară: Intră la lista de Followers. Elimină (Remove Follower) orice cont care nu are față, nu are nume real.
3. Testul Billboard: Chiar și pe Privat, postează doar ce ai fi confortabil să fie afișat pe un panou publicitar în centrul orașului.

 **ÎNTREBARE DE DEZBATERE PENTRU CLASĂ:**

„Smaranda s-a simțit flatată că cineva i-a urmărit dansurile. Dar cum v-ați simți dacă ați afla că un străin se uită la pozele voastre de vacanță în fiecare zi, fără să dea like, doar privindu-vă?”



Videogaleria

Intrați linkul galeriei pentru a folosi materialele video dezvoltate pentru a completa activitatea cu jocul fizic:

<https://www.webtectivii.thedavincisystem.ro/galerie-video/>

Acest modul extinde investigația din cazul „Smaranda” către situații uzuale din viața digitală a elevilor. Utilizând o serie de 10 materiale video (PSA - Public Service Announcements), instructorul va facilita sesiuni de tip Debunking (Demontare de mituri), menite să corecteze percepțiile eronate ale elevilor și părinților despre siguranța online.

Obiectivele educaționale

1. Dezvoltarea gândirii critice prin contrastarea percepției comune („Mitul”) cu realitatea tehnică („Proba Video”).
2. Identificarea riscurilor pasive (metadata, algoritmi, inginerie socială).
3. Aplicarea imediată a setărilor de securitate pe dispozitivele personale ale elevilor.

Mecanica Activității: „Tribunalul adevărului” Instructorul va modera activitatea urmând patru pași standardizați pentru fiecare videoclip:

1. Lansarea ipotezei (Alibiul): Instructorul enunță mitul (ex: „Un profil privat asigură protecție totală”).
2. Sondajul de opinie: Se solicită elevilor să voteze prin ridicare de mână valoarea de adevăr a afirmației (Adevărat/Fals).
3. Administrarea probei: Se rulează videoclipul corespunzător din Galeria WebTectivii.
4. Deliberarea și acțiunea: Se analizează argumentele prezentate în video și se implementează măsura de securitate recomandată (ex: modificarea setărilor).

VIDEO 1: APLICAȚII MONITORIZARE

Temă: Limitele Tehnologiei de Control

Descriere: Videoclipul analizează eficacitatea aplicațiilor de control parental și necesitatea completării acestora cu educație digitală.

Mitul abordat: „Dacă am instalat o aplicație de monitorizare, copilul este în siguranță.”

Realitatea (Debunking): Aplicațiile sunt utile, dar nu pot bloca riscurile sociale (bullying, manipulare) sau ingineria socială. Siguranța reală vine din dialog și educație constantă, nu doar din software.

Întrebări de Dezbateri la Clasă:

- „Vă simțiți mai protejați sau mai controlați dacă părinții folosesc aplicații de monitorizare?”

VIDEO 2: ILUZIA PROFILULUI PRIVAT

Temă: Setările de Confidențialitate și Limitele Lor

Descriere: Materialul explorează diferența dintre setările tehnice de confidențialitate și comportamentul utilizatorului, demonstrând vulnerabilitățile care persistă chiar și pe conturile restricționate.

Mitul abordat: „Dacă profilul copilului e privat, atunci e în siguranță online.”

Realitatea (Debunking): Un profil privat reduce vizibilitatea publică, dar nu elimină riscurile. În interiorul unui cont privat există chat-uri și grupuri unde pot apărea necunoscuți. Mai mult, orice conținut poate fi capturat prin screenshot și redistribuit, anulând protecția inițială. Studiile arată că utilizatorii au frecvent „sharing violations” (informații scăpate public din greșeală).

Întrebări de Dezbateri la Clasă:

- „Câți dintre voi ați acceptat cereri de urmărire de la persoane pe care nu le cunoașteți în viața reală, doar pentru a avea mai mulți urmăritori?”

VIDEO 3: RISCURILE PLATFORMELOR

Temă: Dincolo de TikTok - Siguranța pe Alte Platforme

Descriere: Videoclipul combate ideea că riscurile sunt izolate pe o singură platformă populară, demonstrând omniprezența pericolelor digitale.

Mitul abordat: „Dacă copilul meu nu are TikTok, nu are riscuri în mediul online.”

Realitatea (Debunking): Riscurile există pe orice platformă. Discord, Reddit, Instagram sau YouTube prezintă aceleași vulnerabilități: mesaje directe de la necunoscuți, conținut nefiltrat și grupuri toxice. 62% dintre adolescenți au întâlnit conținut dăunător pe platforme considerate „mai sigure”.

Întrebări de Dezbateri la Clasă:

- „Considerați că Discord sau Instagram sunt mai sigure decât TikTok? Argumentați.”

VIDEO 4: UNGHIURILE MOARTE

Temă: Monitorizarea Parentală vs. Realitatea Social Media

Descriere: Materialul analizează limitele supravegherii părintești pe rețelele sociale, evidențiind funcțiile care permit ascunderea conținutului.

Mitul abordat: „Dacă îl am pe copil la follow pe rețelele de socializare, știu tot ce face online.”

Realitatea (Debunking): Există zone invizibile pentru urmăritori, cum ar fi funcția „Close Friends” (Instagram), mesajele directe (DM) sau conturile secundare de tip „Finsta” (Friends Instagram). Statisticile arată că 42% dintre adolescenți folosesc conturi ascunse față de părinți.

Întrebări de Dezbateri la Clasă:

- „De ce simt tinerii nevoia să aibă conturi secundare (Finsta)? Este vorba de intimitate sau de ascunderea unor comportamente riscante?”

VIDEO 5: MITUL ȘTERGERII DEFINITIVE

Temă: Amprenta Digitală și Ștergerea Datelor

Descriere: Videoclipul demontează ideea că butonul „Delete” oferă o soluție definitivă la problemele online, explicând conceptul de persistență a datelor.

Mitul abordat: „Dacă copilul meu a șters ceva ce a postat, atunci a dispărut de pe internet.”

Realitatea (Debunking): Ștergerea este adesea o iluzie, deoarece „urmele digitale” persistă pe servere sau în capturile altor utilizatori. Mai grav, în cazurile de cyberbullying, victimele șterg mesajele de rușine sau frică, ceea ce elimină dovezile necesare pentru identificarea agresorilor și intervenția autorităților.

Întrebări de Dezbateri la Clasă:

- „De ce credeți că o victimă a bullying-ului ar fi tentată să șteargă mesajele primite?”
- „Ce ar trebui să facem dacă primim un mesaj de amenințare? Îl ștergem sau îl păstrăm? De ce?”

VIDEO 6: ÎNCREDEREA ÎN BRANDURI

Temă: Siguranța Site-urilor Legitime

Descriere: Materialul explică fenomenul de Malvertising (publicitate malițioasă) și de ce reputația unui site nu garantează securitatea utilizatorului.

Mitul abordat: „Atâta timp cât accesează site-uri de branduri cunoscute, copilul meu e în siguranță.”

Realitatea (Debunking): Niciun site nu este imun. Platforme precum New York Times, BBC sau Spotify au fost victime ale campaniilor de publicitate malițioasă care distribuiau malware. Siguranța depinde de vigilența la click-uri și utilizarea unor unelte de protecție (AdBlocker).

Întrebări de Dezbateri la Clasă:

- „Ați dat vreodată click pe o reclamă care promitea un premiu ireal (iPhone gratuit), chiar dacă era pe un site cunoscut?”
- „Ce este un AdBlocker și cum ne poate proteja?”

VIDEO 7: EXPUNEREA TIMPURIE

Temă: Riscurile pentru Copiii Mici

Descriere: Materialul demontează mitul conform căruia copiii de vârstă mică sunt protejați de natura lor "neinteresantă" pentru agresori.

Mitul abordat: „Copilul meu e prea mic să întâlnească pericole online.”

Realitatea (Debunking): Riscurile apar devreme (6-8 ani) prin algoritmi (YouTube Kids) sau chat-uri în jocuri (Roblox, Minecraft). Datele arată că peste 30% dintre copiii sub 10 ani au experimentat deja forme de bullying digital.

Întrebări de Dezbateri la Clasă:

- „La ce vârstă ați avut primul cont pe o rețea socială sau într-un joc online?”

VIDEO 8: CAPCANA PRIETENULUI

Temă: Ingineria Socială și Conturile Sparte

Descriere: Videoclipul explică mecanismul prin care atacatorii cibernetici folosesc conturile de încredere pentru a răspândi malware sau tentative de phishing.

Mitul abordat: „Dacă vorbește doar cu prieteni, copilul meu e în siguranță online.”

Realitatea (Debunking): Conturile prietenilor pot fi compromise („sparte”). Hackerii preferă să trimită link-uri malițioase de pe conturi cunoscute, deoarece rata de succes este mult mai mare când mesajul vine de la o persoană de încredere. Aproximativ 40% din campaniile de phishing au loc acum pe social media și chat.

Întrebări de Dezbateri la Clasă:

- „Ați primit vreodată un mesaj ciudat (un link fără context) de la un prieten bun? Ce ați făcut?”

VIDEO 9: IGIENA PAROLELOR

Temă: Securitatea Conturilor și Partajarea Parolelor

Descriere: Materialul abordează greșelile frecvente în gestionarea parolelor și riscurile sociale asociate partajării acestora.

Mitul abordat: „Orice parolă e sigură, important e să o țină copilul minte.”

Realitatea (Debunking): Parolele simple (nume, date de naștere) sunt extrem de vulnerabile. Un risc major este social: 43% dintre adolescenți și-au împărtășit parola cu prietenii ca semn de încredere. Când relațiile se strică, aceste conturi pot fi folosite abuziv.

Întrebări de Dezbateri la Clasă:

- Este partajarea parolei o dovadă de prietenie adevărată sau un risc inutil?”
- „Cine are activată autentificarea în doi pași (2FA)? De ce credeți că este importantă?”

VIDEO 10: PERICOLUL PASIV

Temă: Metadatele și Urmărirea Pasivă

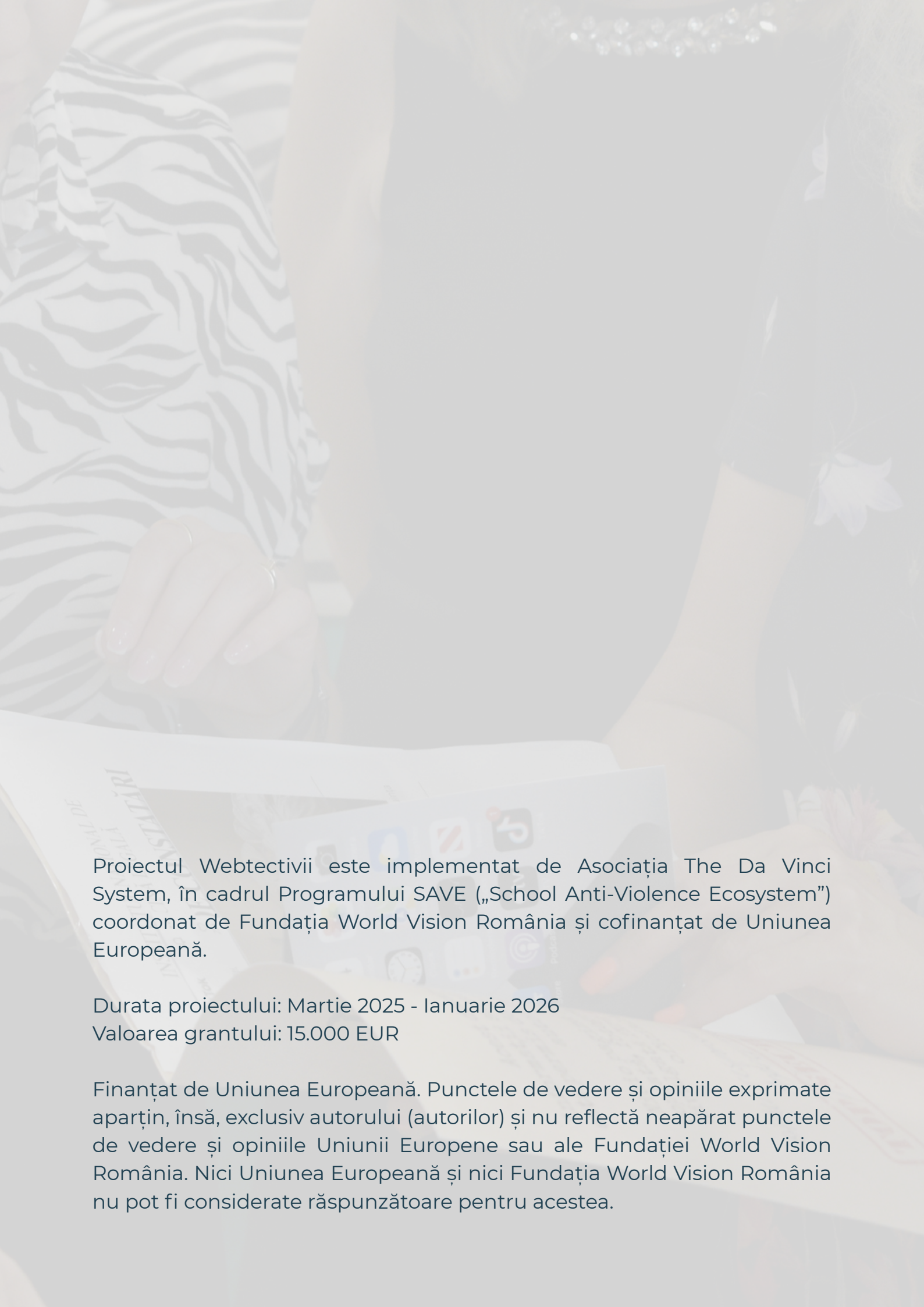
Descriere: Videoclipul evidențiază riscurile care nu implică interacțiune directă, concentrându-se pe expunerea involuntară a locației.

Mitul abordat: „Dacă nu-i scrie nimeni dubios, copilul meu e în siguranță.”

Realitatea (Debunking): Riscul poate fi pasiv. Informațiile despre locație (prin Geotagging, Insta Map, Snap Map) pot fi accesate fără contact direct. 28% dintre copiii din România au experimentat situații neplăcute din cauza partajării locației.

Întrebări de Dezbateri la Clasă:

- „Când postați o poză 'Acum', vă gândiți că oricine poate vedea exact unde sunteți?”
- „Verificați ce se vede în fundalul pozelor voastre (nume de străzi, școala) înainte de a posta?”



Proiectul Webtectivii este implementat de Asociația The Da Vinci System, în cadrul Programului SAVE („School Anti-Violence Ecosystem”) coordonat de Fundația World Vision România și cofinanțat de Uniunea Europeană.

Durata proiectului: Martie 2025 - Ianuarie 2026
Valoarea grantului: 15.000 EUR

Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Fundației World Vision România. Nici Uniunea Europeană și nici Fundația World Vision România nu pot fi considerate răspunzătoare pentru acestea.

Nu există nicio datorie
mai importantă pentru o
societate decât aceea de
a-și proteja copiii.
Siguranța lor nu este un
privilegiu pe care îl
acordăm, ci un drept pe
care suntem obligați
prin lege să îl garantăm.

Proiectul Webtectivii este implementat de Asociația The Da Vinci System, în cadrul Programului SAVE („School Anti-Violence Ecosystem”) coordonat de Fundația World Vision România și cofinanțat de Uniunea Europeană.

Durata proiectului: Martie 2025 - Ianuarie 2026
Valoarea grantului: 15.000 EUR

Finanțat de Uniunea Europeană. Punctele de vedere și opiniile exprimate aparțin, însă, exclusiv autorului (autorilor) și nu reflectă neapărat punctele de vedere și opiniile Uniunii Europene sau ale Fundației World Vision România. Nici Uniunea Europeană și nici Fundația World Vision România nu pot fi considerate răspunzătoare pentru acestea.



Cofinanțat de
Uniunea Europeană



program coordonat de
World Vision
ROMÂNIA

Proiect derulat de:

Proiect coordonat de Asociația The Da Vinci System
ROMÂNIA
ALIANȚA PENTRU MOBILITATE SOCIALĂ