



WP2 - PR.I.S.C.I.LLA PROGRAM EDUCAȚIONAL PENTRU TINERII CU DIZABILITĂȚI INTELECTUALE

Modulul 3: Riscuri potențiale în utilizarea rețelelor sociale

Document creat de: EDRA

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



PR.I.S.C.I.LLA PROGRAM EDUCAȚIONAL PENTRU TINERII CU DIZABILITĂȚI INTELECTUALE

Modulul 3: Riscurile potențiale în utilizarea rețelelor sociale

Rezumatul modulului	În acest modul veți învăța despre riscurile care pot apărea atunci când utilizați rețelele de socializare. Aceste riscuri includ hărțuirea online (când oamenii sunt răi cu tine online), „grooming” (când un adult pretinde că este cineva de vârsta ta și te păcălește să împărtășești fotografii sau să te implici în activități intime) și “phishing” (când cineva încearcă să vă fure identitatea sau parolele). Veți învăța, de asemenea, cum să identificați aceste riscuri și cum să rămâneți în siguranță atunci când utilizați rețelele de socializare.
Rezultatele învățării din cadrul modulului	Până la sfârșitul acestui modul, veți putea să: 1. Înțelegeți ce este hărțuirea online, ademenirea și pescuitul. 2. Recunoașteți situațiile în care pot apărea aceste riscuri. 3. Aflați sfaturi și măsuri pentru a vă proteja de aceste riscuri.
Principiile educaționale adoptate	Acest modul este conceput pentru a te ajuta: • Să vă asumați riscuri pozitive prin folosirea rețelelor sociale în siguranță. • Să simțiți că dețineți controlul acțiunilor dumneavoastră online. • Să vă construiți independența în utilizarea rețelelor sociale. • Să faceți alegeri corecte cu încredere.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Conținutul modului

În modulele anterioare am învățat că rețeaua socială este un spațiu plin de posibilități. Este un loc unde putem descoperi informații interesante, să ne împărtășim gândurile și sentimentele pe diferite teme și să interacționăm cu oameni care ne împărtășesc interesele.

Cu toate acestea, este important să ne amintim că mediul online are și riscuri. Pentru a ne bucura de rețelele de socializare în siguranță, trebuie să înțelegem aceste riscuri și să învățăm cum să ne protejăm de ele. În acest fel, putem profita la maximum de experiențele noastre online, rămânând în siguranță.

Acum vă vom prezenta unele dintre cele mai des întâlnite riscuri: hărțuirea online, grooming și phishing.

Ce este hărțuirea online?

Hărțuirea online se întâmplă atunci când oamenii folosesc rețele de socializare sau platforme online pentru a trimite mesaje răutăcioase, pentru a posta comentarii jignitoare, sau pentru a răspândi zvonuri.

Exemple de hărțuire online:

- Atunci când cineva vă comentează la poza: „Arăți atât de ciudat! Nimeni nu te place.”
- Un grup de persoane care trimit mesaje răutăcioase într-o conversație de grup, făcându-vă să vă simțiți exclus sau trist, de exemplu “Haideți să o ignorăm și să nu o mai lăsăm să facă parte din grup.”
- Cineva vă trimite un mesaj în privat spunând: “Ești atât de naiv! Încetează să mai faci postări.”

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Sfaturi practice de evitat

1. **Nu răspundeți.** Dacă cineva vă trimite mesaje răutăcioase, nu răspundeți.
2. **Salvați dovada.** Faceți capturi de ecran mesajelor sau comentariilor răutăcioase pentru a le arăta unei persoane de încredere.
3. **Blocați și raportați.** Utilizați instrumentele platformei pentru a bloca hărțuitorul și a-i raporta comportamentul.
4. **Discutați cu cineva de încredere.** Împărtășiți-vă sentimentele cu un părinte, profesor sau prieten.
5. **Fiți bun în mediul online.** Tratați-i pe ceilalți cu respect pentru a contribui la crearea unui mediu online pozitiv.

Ce este „Grooming-ul”?

„Grooming-ul” Este atunci când un adult folosește internetul pentru a manipula și a păcăli o persoană tânără să împărtășească informații personale, să trimită fotografii private sau să se implice în comportamente nesigure. Groomerii pretind adesea că sunt prieteni, persoane de vârstă ta sau persoane care te înțeleg pentru a-ți câștiga încrederea.

Exemple de Grooming

- O persoană din mediul online vă trimite mesaje și complimente prietenoase, punându-vă întrebări personale precum „Unde locuiești?” sau „Poți să îmi trimiți o fotografie cu tine?”
- Cineva spune: „Chiar îmi place cum arăți. Ești foarte frumoasă. Unchiul meu deține o agenție de modeling și te poate face celebră dacă îmi trimiți câteva fotografii cu tine.”

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Sfaturi practice pentru a evita grooming-ul

1. **Nu împărtășiți informații personale.** Nu divulgați niciodată adresa, numărul de telefon, numele școlii sau parolele.
2. **Aveți grijă cu fotografiile.** Nu trimiteți fotografiile dumneavoastră persoanelor pe care nu le cunoașteți.
3. **Ai încredere în sentimentele tale.** Dacă cineva din mediul online vă face să vă simțiți inconfortabil, nu mai vorbiți cu persoana respectivă.
4. **Discută cu o persoană de încredere.** Dacă vă simțiți nesigur/ă în legătură cu cineva din mediul online, spuneți-i unui părinte, profesor sau îngrijitor.
5. **Blocați și raportați.** Utilizați setările platformei pentru a bloca persoana și a-i raporta comportamentul.

Ce este "Phishing"?

„Phishing-ul” este atunci când cineva pretinde că este o persoană sau o companie de încredere pentru a vă fura informații precum: parolele, detaliile contului sau banii. Aceste persoane folosesc adesea adrese de e-mailuri, mesaje sau site-uri web false pentru a vă păcăli.

Exemple de Phishing

- Primiți un e-mail care pare a fi de la banca dumneavoastră și care spune: „Există o problemă cu contul dumneavoastră bancar. Vă rugăm să faceți clic aici pentru a vă conecta.”
- Primiți un mesaj care spune: „Ați câștigat un premiu! Faceți clic pe acest link pentru a-l revendica.”

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Sfaturi practice pentru a evita phishing-ul

1. **Nu dați clic pe link-uri necunoscute.** Dacă primiți un mesaj sau un email de la cineva în care nu aveți încredere, ignorați-l și nu dați clic pe nici un link din mesaj.
2. **Verificați expeditorul.** Uitați-vă cu atenție la adresa de e-mail sau la numele de utilizator al expeditorului. Mesajele false au adesea mici greșeli de ortografie.
3. **Păstrați-vă parolele în siguranță.** Nu vă împărtășiți niciodată parolele cu nimeni.
4. **Atenție la premii.** Dacă cineva vă spune că ați câștigat ceva uimitor, dar vi se pare ciudat sau prea ușor, probabil că nu este real.
5. **Utilizați site-uri web securizate.** Asigurați-vă că numele unui site web începe cu „https://” și prezintă simbolul unui lacăt.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Scenariul de caz Introducere	Explică participanților că vor auzi/citi 3 povești diferite, fiecare prezentând o situație care are loc în mediul online. Aceste povești sunt concepute pentru a-i ajuta să înțeleagă unele riscuri care îi înconjoară în timp ce folosesc rețelele de socializare și internetul. După citirea fiecărei povestiri, ghidați participanții într-o dezbatere, punându-le întrebări specifice. Încurajați-i să reflecteze asupra situației, să identifice riscurile implicate și să se gândească la cele mai bune modalități de a reacționa în siguranță. Scopul acestei activități este de a ajuta participanții să recunoască pericolele online și să dezvolte strategii pentru a se proteja.
Scenariul de caz 1	Cazul lui Lucia Lucia are 19 ani și îi place să deseneze. Adesea își distribuie lucrările de artă pe rețelele de socializare. Într-o zi, cineva îi trimite un mesaj în care îi spune: „Bună! Îmi plac desenele tale. Ești atât de talentată! Putem fi prietene?” Lucia se simte fericită și răspunde: „Mulțumesc! Sigur!” După câteva zile, persoana respectivă începe să-i pună Luciei întrebări personale precum: „Unde locuiești?” și „Poți să-mi trimiți o poză cu tine?” De asemenea, îi spune Luciei: „Nu spune nimănui despre convorbirea noastră - este secretul nostru.” 1. Ce s-ar putea întâmpla dacă Lucia împărtășește online informații personale cu o persoană pe care nu o cunoaște?

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



	a) Ar putea folosi informațiile ca să o păcălească sau pentru a-i face rău. b) Ar putea deveni cele mai bune prietene. c) Nimic; împărtășirea informațiilor personale este întotdeauna sigură. 2. Ce ar trebui să facă Lucia atunci când cineva îi cere o fotografie cu ea? a) Să o trimită rapid pentru a fi politicoasă. b) Să spună “nu” și să blocheze persoana respectivă. c) Să întrebe persoana respectivă de ce are nevoie de poză. 3. Dacă Lucia se simte nesigură în legătură cu această situație, care este cel mai bun pas de urmat? a) Să discute cu un adult de încredere despre mesaj. b) Să își ignore sentimentele și să continue discuția. c) Să își întrebe prietenii dacă ei cred că este în regulă.
Scenariul de caz 2	Cazul lui Luca Luca distribuie o poză amuzantă cu el pe rețelele de socializare. Cineva comentează „Arăți atât de prost!” , iar celelalte persoane încep să râdă și să scrie lucruri răutăcioase despre el. Luca se întristează și nu știe ce să facă. Se întreabă dacă ar trebui să își șteargă contul sau să răspundă cu furie la comentarii.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271





	1. Care este primul lucru pe care Luca ar trebui să îl facă în legătură cu comentariile răutăcioase? a) Să ignore comentariile și să facă captură de ecran ca dovezi. b) Să posteze un răspuns în care să scrie lucruri răutăcioase. c) Să își șteargă contul imediat. 2. Cu cine ar trebui să vorbească Luca dacă se simte rănit în legătură cu acele comentarii? a) Un adult de încredere, cum ar fi un profesor, un părinte sau îngrijitor. b) Persoana care a postat comentariile. c) Cu nimeni; ar trebui să țină asta pentru el. 3. Care este modalitatea bună prin care Luca ar putea face față hărțuirii online pe viitor? a) Să evite să mai distribuie ceva online. b) Să blocheze și să raporteze persoanele care sunt răutăcioase. c) Să scrie o postare lungă în care să explice cât de rănit se simte.
Scenariul de caz 3	Cazul lui Ana Ana primește un e-mail care pare să fie de la magazinul său online preferat. E-mailul spune "Felicitări! Ați câștigat un card cadou în valoarea de 50 €! Faceți clic aici pentru a obține premiul." Ana foarte încântată, deși nu este sigură dacă este adevărat. Ea observă că adresa de

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



	e-mail este ciudată, iar link-ul nu se potrivește cu site-ul web magazinului. 1. Ce ar trebui să facă Ana înainte de a accesa link-ul? a) Să verifice dacă adresa de e-mail și link-ul par reale și se potrivesc cu site-ul web al magazinului. b) Să facă clic repede, înainte ca premiul să dispară. c) Să răspundă la e-mail pentru a cere mai multe detalii. 2. Care este un semn de avertizare cum că acest e-mail ar putea fi fals? a) E-mailul cere informații personale. b) E-mailul este scris într-un mod prietenos. c) E-mailul include numele magazinului. 3. Dacă Ana consideră că acest e-mail este suspicios, ce ar trebui să facă? a) Să raporteze e-mailul ca phishing și să îl șteargă. b) Să redirectioneze e-mailul prietenilor ei pentru a verifica dacă este real. c) Să ignore e-mailul, dar să îl păstreze în căsuța poștală.
Materiale adiționale	
Resurse	

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



Activitatea modulului	
Denumirea activității	Identificarea riscurilor
Obiective	Veți exersa identificarea riscurilor potențiale în diferite scenarii online și veți discuta acțiunile adecvate pe care ar trebui să le luăm pentru a rămâne în siguranță.
Metodologii de învățare	Învățarea prin practică, exerciții practice și activități interactive
Timp alocat pentru activitate	30 de minute
Resurse necesare	Cartonașe cu scenarii Hârtie și pix, dacă doriți să scrieți răspunsurile.
Instrucțiuni	În această activitate veți vedea imagini sau veți auzi scurte povestiri despre lucruri care se pot întâmpla în mediu online. Sarcina dumneavoastră este să: 1. Decideți dacă situația este riscantă sau sigură. 2. Spuneți de ce credeți că este riscantă. 3. Explicați ce ați face pentru a fi în siguranță. Exemplu: Haideți să începem cu un exemplu simplu pentru a vă ajuta să înțelegeți cum funcționează această activitate: Un necunoscut vă trimite un mesaj în care vă spune “Ești atât de tare! Ne putem întâlni?” Întrebați-vă:

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



- Este riscant?
- De ce ar putea fi riscant?
- Ce ar trebui să faceți într-o astfel de situație?

Răspuns:

Da, este riscant pentru că nu cunoașteți persoana respectivă. S-ar putea să nu fie cine pretind că sunt. Ar trebui să ignorați mesajul, să o blocați și să îi spuneți ce se întâmplă unei persoane de încredere.

Acum, veți vedea diferite scenarii online. Pentru fiecare dintre ele, gândiți-vă bine și răspundeți la următoarele întrebări:

- Este riscant sau sigur?
- De ce credeți că este riscant sau sigur?
- Ce ați face pentru a rămâne în siguranță?

Scenariul 1:

Cineva din mediul online spune: Te pot ajuta să obții mulți urmăritori dacă îmi trimiți parola ta.

Scenariul 2:

Un prieten postează o fotografie amuzantă cu dumneavoastră fără să vă ceară permisiunea.

Scenariul 3:

Cineva comentează la postarea dumneavoastră "Ești atât de urât/ă, toată lumea te urăște"

Scenariul 4:

Primești un e-mail care spune "Felicitări! Ați câștigat 1.000 €! Faceți clic aici pentru a vă revendica premiul."

Scenariul 5:

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271





Sunteți într-un grup de chat online despre jocul dumneavoastră video preferat. Cineva din chat întreabă: „Care este ziua ta de naștere? Vrem să o sărbătorim cu tine!”

Scenariul 6:

Primiți un mesaj de la cineva care spune “Căutăm persoane care să lucreze de acasă. Doar trimiteți numele, adresa și detaliile bancare pentru a începe!”

Scenariul 7:

Faceți o fotografie de grup cu prietenii într-un parc și doriți să o postați pe rețelele de socializare. Unul dintre prietenii dumneavoastră spune că nu vrea ca poza sa să apară pe internet.

Scenariul 8:

Un străin vă trimite un mesaj în care vă spune: „Ești atât de cool și de drăguță! Mi-ar plăcea să vorbim mai mult. Poți să-mi spui mai multe despre tine?”

Exemple de răspunsuri

Exemplu de răspuns scenariul 1

- Acest lucru este riscant deoarece ar putea utiliza parola dumneavoastră pentru a vă prelua contul.
- Nu ar trebui să spuneți nimănui parolele dumneavoastră.

Exemplu de răspuns scenariul 2

- Acest lucru ar putea fi riscant deoarece fotografia v-ar putea face de râs sau ar putea împărtăși informații private.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



- Ar trebui să îi cereți prietenului dumneavoastră să șteargă poza și să îi explicați de ce este important să vă ceară permisiunea.

Exemplu de răspuns scenariul 3

- Aceasta este hărțuire online deoarece comentariul este răutăcios și v-ar putea răni sentimentele.
- Ar trebui să faceți o captură de ecran comentariului, să blocați acea persoană și să îi spuneți unei persoane de încredere.

Exemplu de răspuns scenariul 4

- Acest lucru este riscant deoarece este probabil o înșelătorie de phishing pentru a vă fura informațiile personale.
- Ar trebui să ștergeți e-mailul sau să îl raportați ca spam. Nu dați niciodată clic pe linkuri din e-mailuri de acest tip.

Exemplu de răspuns scenariul 5

- Acest lucru este riscant, deoarece împărtășirea zilei dumneavoastră de naștere într-o conversație

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271





	publică poate duce la furtul identității sau la contacte nedorite. ● Trebuie să evitați să dați detalii personale, cum ar fi ziua dumneavoastră de naștere completă, în spații publice. Dacă cineva vă întreabă, spuneți politicos că nu împărtășiți informații personale online. Exemplu de răspuns scenariul 6 ● Acest lucru este riscant deoarece este probabil o înșelătorie menită să vă fure informațiile personale sau financiare. ● Ar trebui să ștergeți mesajul imediat și să raportați expeditorul. Nu împărtășiți niciodată informații importante, cum ar fi adresa sau detaliile bancare, cu persoane pe care nu le cunoașteți. Exemplu de răspuns scenariul 7 ● Acest lucru este sigur numai dacă respectați dorința prietenului dumneavoastră și nu postați imaginea. Ignorarea solicitării lor nu ar fi nici sigură și nici amabilă. ● Trebuie să vă asigurați că cereți permisiunea tuturor persoanelor din fotografie înainte de a o posta online. Dacă cineva spune nu, alegeți o altă fotografie sau nu o postați deloc. Exemplu de răspuns scenariul 8
--	---

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



- Acest lucru este riscant deoarece străinii care fac complimente ar putea încerca să vă manipuleze sau să câștige încrederea dumneavoastră din motive nesigure.
- Nu ar trebui să răspundeți mesajului. Blocați acea persoană imediat și spuneți-i unei persoane de încredere ce s-a întâmplat.

Reflectare

După terminarea scenariilor, gândiți-vă puțin la ceea ce ați învățat.

Întrebați-vă:

- Care risc v-a surprins cel mai mult?
- Cum v-ați simțit când ați decis ce să faceți în fiecare situație?
- Ce veți face diferit data viitoare când veți fi online?

Discutați cu grupul sau profesorul despre răspunsurile dumneavoastră. Împărtășirea gândurilor vă poate ajuta să vă simțiți mai încrezători cu privire la siguranța online.

Concluzie

Ați făcut o treabă excelentă identificând riscurile și gândindu-vă cum să fiți în siguranță în mediul online. Nu uitați:

- ✓ Dacă ceva vi se pare în neregulă online, aveți încredere în sentimentele voastre.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



	✓ Nu împărtășiți informații personale sau parole cu persoanele pe care nu le cunoașteți. ✓ Vorbiți întotdeauna cu cineva de încredere dacă nu sunteți sigur/ă de o situație.
--	---

Activitatea modului	
Denumirea activității	Joc de rol
Obiective	Veți exersa cum să răspundeți la diferite riscuri online, jucând situații în grupuri mici. Această activitate vă va ajuta să vă simțiți mai încrezători cu privire la ce să faceți dacă vă confrunțați cu aceste riscuri în viața reală. Veți învăța: ✓ Cum să răspundeți la riscurile online comune. ✓ Cum să faceți alegeri inteligente și sigure atunci când ceva nu este în regulă. ✓ Cum să cereți ajutor atunci când e nevoie.
Metodologii de învățare	Joc de rol
Timp alocat pentru activitate	30-40 de minute

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Resurse necesare	• Cartonașe cu scenariul sau foi tipărite cu scenariul. • Un spațiu sigur pentru jocuri de rol în grupuri mici.
Instrucțiuni	Veți lucra în grupuri mici pentru a pune în scenă diferite situații. Fiecare grup va primi un scenariu despre un risc online. O persoană va juca rolul persoanei care se confruntă cu problema, iar ceilalți vor juca diferite roluri, cum ar fi un prieten, persoana periculoasă sau un adult de încredere. După ce vom juca scenariul, vom vorbi despre ce s-a întâmplat și cum să gestionăm situația. Scenariul 1 • Poveste: Cineva din mediul online spune: „Ești atât de talentat! Pot să văd mai multe poze cu tine? Îți promit că nu le voi împărtăși cu nimeni.” • Roluri: ○ Persoana căreia i se cer fotografii ○ Necunoscutul. ○ O persoană de încredere sau un prieten alături de care își exprimă opiniile și caută sfaturi. • Etape de acțiune: ○ Refuză să trimită fotografii. ○ Blochează necunoscutul.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



	○ Vorbește cu persoana de încredere despre ce s-a întâmplat.
	Scenariul 2 ● Poveste: Cineva comentează la postarea dumneavoastră: „Asta e atât de prostesc. De ce te mai obosești?” Alți oameni încep să dea aprecieri comentariului și să scrie lucruri răutăcioase. ● Roluri: ○ Persoana hărțuită. ○ Hărțuitorul. ○ O persoană de încredere sau un prieten alături de care discută despre acest lucru. ● Etape de acțiune: ○ Nu răspundeți comentariilor răutăcioase. ○ Faceți captură de ecran ca dovadă. ○ Blocați și raportați hărțuitorul.
	Scenariul 3 ● Poveste: Primiți un e-mail care spune: „Felicitări! Ați câștigat un telefon nou! Faceți clic pe acest link pentru a vă revendica premiul.”

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



	• Roluri: ○ Persoana care primește e-mailul. ○ Impostorul care a trimis acel e-mail. ○ Un prieten sau o persoană de încredere care oferă sfaturi. • Etape de acțiune: ○ Nu dați clic pe link. ○ Ștergeți e-mailul și raportați-l ca spam. ○ Discutați cu o persoană de încredere dacă sunteți nesigur/ă. Dezbatare După ce fiecare grup și-a interpretat scenariul, adunați-vă într-un grup mare pentru a discuta: • Ce a făcut ca situația să fie riscantă? • Ce a făcut persoana pentru a rămâne în siguranță? • Cum v-ați simțit să practicați această situație? • Ce ați face dacă vi s-ar întâmpla acest lucru în viața reală? Concluzie Ați făcut o treabă excelentă exersând cum să gestionați riscurile online! Nu uitați:
--	--

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



	• Întotdeauna ai încredere în instinctele tale – dacă simțiți că ceva nu este în regulă, probabil chiar nu este. • Blocați și raportați persoanele care vă fac să vă simțiți inconfortabil. • Discutați cu o persoană de încredere dacă nu sunteți sigur/ă ce să faceți.
--	--

Activitatea modului	
Denumirea activității	Joc de sortare a riscurilor
Obiective	Veți exersa identificarea comportamentelor online sigure și riscante prin sortarea exemplelor în categoriile „Sigur” sau „Riscant”.
Metodologii de învățare	Exerciții practice și activități interactive
Timp alocat pentru activitate	20 de minute
Resurse necesare	• Cartonașe cu acțiuni din mediul online. • Două zone etichetate: "Sigur" și "Riscant" (pe o tablă sau masă).
Instrucțiuni	Haideți să testăm ceea ce ați învățat despre riscurile online! În această activitate, veți vedea exemple de lucruri pe care oamenii le pot face online. Sarcina voastră este să decideți dacă fiecare exemplu este „sigur” sau „riscant”.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



Veți lucra în perechi sau în grupuri mici. Fiecare grup va primi cartonașe cu exemple de acțiuni online. Sarcina voastră este să plasați fiecare cartonaș în categoria „Sigur” sau „Riscant” pe tablă sau pe masă. După sortarea cartonașelor, vom discuta în grup despre alegerile voastre.

Să încercăm împreună un exemplu:

Exemplu de card:

"Afișarea numelui complet și a adresei pe profilul dumneavoastră."

Este sigur sau riscant?

Răspuns: Riscant. Distribuirea informațiilor personale vă poate face vulnerabil.

Acum este rândul dumneavoastră! Iată cartonașele pe care trebuie să le sortezi:

- „Acceptarea unei cereri de prietenie de la cineva pe care nu îl cunoști.”
- „Publicarea unei fotografii cu hobby-ul tău preferat.”
- „Faceți clic pe un link dintr-un e-mail care vă anunță că ați câștigat un premiu.”
- „Blocarea cuiva care îți trimite mesaje răutăcioase.”
- „Distribuirea numărului de telefon personal într-o postare publică.”
- „Primiți o cerere de prietenie de la cineva care nu are nicio poză de profil și nicio postare pe contul său.”

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



- „Distribuiți o fotografie a cărții dumneavoastră preferate fără alte detalii personale.”
- „Primești un mesaj care spune: „Trimite-mi locația ta ca să putem ieși împreună!” de la o persoană pe care nu o cunoști.”
- „Postezi o fotografie cu numele școlii tale pe rețelele de socializare.”
- „Prietenul tău îți spune că este hărțuit online și tu îl încurajezi să vorbească cu un adult de încredere.”

Exemple de răspunsuri:

1. „Acceptarea unei cereri de prietenie de la cineva pe care nu îl cunoști.”

Răspuns: Riscant. Acceptarea cererilor de la persoane pe care nu le cunoașteți poate fi nesigură, deoarece acestea ar putea să nu fie cine spun că sunt. Asigurați-vă întotdeauna că vă conectați doar cu persoane în care aveți încredere.

2. „Publicarea unei fotografii cu hobby-ul tău preferat.”

Răspuns: În siguranță. Împărtășirea intereselor tale, cum ar fi o fotografie cu hobby-ul tău preferat, este în regulă atâta timp cât nu include detalii private precum locația sau numele școlii tale.

3. „Faceți clic pe un link dintr-un e-mail care spune că ați câștigat un premiu.”

Răspuns: Riscant. Aceasta este probabil o înșelătorie de phishing. Dacă faceți clic pe link, impostorii ar putea avea

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union



	acces la informațiile dumneavoastră sau v-ar putea afecta dispozitivul. Ștergeți e-mailul și nu faceți clic pe link. 4. „Blocarea cuiva care îți trimite mesaje răutăcioase.” Răspuns: În siguranță. Blocarea cuiva care este rău cu tine online este o modalitate inteligentă de a opri negativitatea. De asemenea, este important să raportați comportamentul lor și să spuneți asta unui adult de încredere. 5. „Distribuirea numărului de telefon personal într-o postare publică.” Răspuns: Riscant. Partajarea numărului dumneavoastră de telefon într-o postare publică este nesigură, deoarece oricine îl poate folosi pentru a vă contacta sau pentru a afla detalii personale. Păstrați-vă numărul de telefon privat și împărtășiți-l doar cu persoanele în care aveți încredere directă. 6. „Primiți o cerere de prietenie de la cineva care nu are nicio poză de profil și nicio postare pe contul său.” Răspuns: Riscant. Acceptarea cererilor de la conturi necunoscute sau suspecte poate duce la interacțiuni nesigure. 7. „Distribuiți o fotografie a cărții dumneavoastră preferate fără alte detalii personale.”
--	---

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



	Răspuns: În siguranță. Împărtășirea intereselor generale fără dezvăluirea informațiilor private este în regulă. 8. „Primești un mesaj care spune: „Trimite-mi locația ta ca să putem ieși împreună!” de la o persoană pe care nu o cunoști.” Răspuns: Riscant. Împărtășirea locației dumneavoastră cu străinii poate fi periculoasă. 9. „Postezi o fotografie cu numele școlii tale pe rețelele de socializare.” Răspuns: Riscant. Împărtășirea numelui școlii tale poate ajuta străinii să afle unde să te găsească. 10. „Prietenul tău îți spune că este hărțuit online, iar tu îl încurajezi să vorbească cu un adult de încredere.” Răspuns: Siguranță. Sprijinirea unui prieten și ajutorarea acestuia în căutarea de ajutor este o acțiune corectă. Dezbattere După sortarea cartonașelor, discutați răspunsurile cu grupul. • Toată lumea a fost de acord cu privire la acțiunile care au fost riscante? • Ce a făcut ca unele acțiuni să fie mai sigure decât altele?
--	---

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



**Co-funded by
the European Union**



- Cum puteți să vă amintiți să rămâneți în siguranță în situații similare?

Concluzie

Bună treabă cu sortarea riscurilor! Acum știi cum să identifici comportamentele online sigure și riscante. Nu uitați, când aveți îndoieli, întrebați întotdeauna un adult de încredere.

Numărul proiectului: 2023-2-RO01-KA220-YOU-000174271

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 Agenției Executive Europene pentru Educație și Cultură (EACEA). Nici Uniunea Europeană și nici EACEA nu pot fi considerate răspunzătoare pentru acestea.



Co-funded by
the European Union