ERASMEDIAH – RAFFORZAMENTO EDUCATIVO CONTRO L'IPERCONNETTIVITÀ
DEI SOCIAL MEDIA NUMERO DI PROGETTO: 2023-1-HU01-KA220-YOU-000161173

MODULO 5

SICUREZZA INFORMATICA E SICUREZZA ONLINE

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.

Lezione 5.4

Riconoscere le minacce informatiche e strategie per prevenire l'esposizione a contenuti inappropriati

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.

Durata: 40 minuti

Lezione 5.4

Riconoscere le minacce informatiche e strategie per prevenire l'esposizione a contenuti inappropriati

Obiettivi:

- Sviluppare la consapevolezza dei rischi online più diffusi, come l'esposizione a contenuti inappropriati, il cyberbullismo e il grooming, in particolare nei confronti di utenti vulnerabili come bambini e adolescenti.
- Fornire agli studenti competenze fondamentali per riconoscere i segnali di allarme delle minacce informatiche, come link sospetti, comportamenti predatori online e contenuti manipolativi.
- Incoraggiare abitudini proattive nella gestione delle interazioni online, promuovendo il pensiero critico, identificando spazi digitali sicuri e mantenendo una comunicazione aperta sulle esperienze online.

Messaggio/i chiave:

- Le minacce online spesso si nascondono dietro piattaforme o interazioni apparentemente innocue. Riconoscere i segnali è fondamentale per la sicurezza.
- Semplici accorgimenti, come l'utilizzo di filtri per i contenuti e il mantenimento di una comunicazione efficace, possono aiutare a prevenire l'esposizione a contenuti dannosi e minacce informatiche.

TIPO DI LEZIONE:

Panoramica della lezione

Nell'attuale ambiente digitale iperconnesso, l'esposizione a contenuti inappropriati e minacce informatiche è un rischio costante. Questa lezione è progettata per fornire una comprensione completa della natura e dei rischi di queste minacce, strumenti pratici per mitigarle e strategie per promuovere interazioni online più sicure. Attraverso esercizi coinvolgenti e consigli pratici, al termine della sessione sarete meglio preparati a navigare nel mondo digitale in modo sicuro e responsabile.

Il workshop è organizzato in 4 fasi:

1: Nozioni fondamentali sulle minacce informatiche e sui contenuti inappropriati (10 min)

2: Riconoscere i segnali di allarme e i rischi (15 min)

3: Approcci per la prevenzione e la mitigazione (10 min)

4: Riflessione e applicazione (5 min)

Passo 1

Nozioni essenziali sulle minacce informatiche e sui contenuti inappropriati

Ti è mai capitato di imbatterti in qualcosa online che ti ha fatto sentire a disagio o insicuro?
Le minacce informatiche sono attività dannose che prendono di mira individui o sistemi online, con l'obiettivo di rubare informazioni, causare danni o sfruttare vulnerabilità. Alcuni esempi:

- Cyberbullismo: utilizzo di piattaforme online per molestare o intimidire.
- Phishing: invio di messaggi ingannevoli per indurre le persone a rivelare informazioni personali.
- Adescamento: instaurare una relazione con qualcuno online per poi sfruttarlo in seguito, spesso in modo inappropriato.

Cosa costituisce un **contenuto inappropriato**?
Contenuti dannosi, espliciti o inadatti a determinate fasce d'età, come:

- Immagini o video espliciti.
- Messaggi manipolativi o predatori.
- Materiale violento o incitante all'odio.

Passo 1

Nozioni essenziali sulle minacce informatiche e sui contenuti inappropriati

L'esposizione a tali contenuti può causare disagio emotivo, danneggiare le relazioni e portare a conseguenze a lungo termine come il furto di identità o lo sfruttamento.

Attività

Ora ci divideremo in piccoli gruppi. A ogni gruppo verrà assegnato uno scenario da analizzare:

Scenario 1: Ricevi un'e-mail da uno sconosciuto che ti chiede informazioni personali

Scenario 2: Vedi un collegamento sospetto in un'e-mail

Scenario 3: Ti imbatti in un commento inappropriato sui social media

Il tuo compito è rispondere alle domande del tuo gruppo:

- Cosa c'è di rischio in questa situazione?
- Come puoi rispondere in modo sicuro?

Una volta che i gruppi hanno terminato il lavoro, condividete insieme le conclusioni.

Passo 2

Riconoscere i segnali di allarme e i rischi

Dai un'occhiata agli esempi qui sotto e chiediti se hai mai visto qualcosa di simile su Internet. Durante il brainstorming, discuti in gruppo su quali di questi segnali d'allarme sono più comuni e su come puoi reagire.

1. Mittente sconosciuto o sospetto

- Ricevi un messaggio da qualcuno che non conosci, che ti chiede informazioni personali o ti invita a cliccare su un link.
- L'indirizzo email sembra insolito, ad esempio "bank123random@mail.com" invece di un indirizzo ufficiale.
- *Domanda di discussione:* "Cosa fai quando ricevi un messaggio da qualcuno che non riconosci?"

2. Errori di ortografia o grammatica

- Il messaggio è pieno di errori di ortografia o di frasi strane.
- Esempio: "Il tuo account è bloccato! Clicca qui per riattivarlo"
- *Domanda di discussione:* "Gli errori in un messaggio ti rendono sospettoso? Perché sì o perché no?"

Passo 2 Riconoscere i segnali di allarme e i rischi

3. Richieste urgenti o minacce

- Messaggi come: "Se non paghi entro 24 ore, il tuo account verrà disattivato!"
- Il contenuto cerca di spaventarti o di spingerti ad agire rapidamente.
- *Domanda di discussione:* "Come si fa a distinguere un vero avviso da una truffa?"

4. Offerte troppo belle per essere vere

- Pubblicità che promettono premi incredibili: "Hai vinto un iPhone nuovo di zecca! Clicca qui per richiedere il tuo premio"
- Siti web che offrono vantaggi irrealistici con poco sforzo.
- *Domanda di discussione:* "Perché questo tipo di offerte sono pericolose?"

Passo 2 Riconoscere i segnali di allarme e i rischi

5. Link o allegati sconosciuti

- Ricevi un link che non sembra affidabile, come "www.freegift.now".
- Allegati provenienti da mittenti sconosciuti che potrebbero contenere virus.
- *Domanda di discussione:* "Come si può verificare se un collegamento o un allegato è sicuro?"

Nel vostro gruppo, scegliete uno di questi segnali di allarme e discutete su come gestireste la situazione.
Alla fine, ogni gruppo condividerà le proprie intuizioni e idee su come evitare questi rischi nelle attività quotidiane online.

Passo 3

Approcci per la prevenzione e la mitigazione

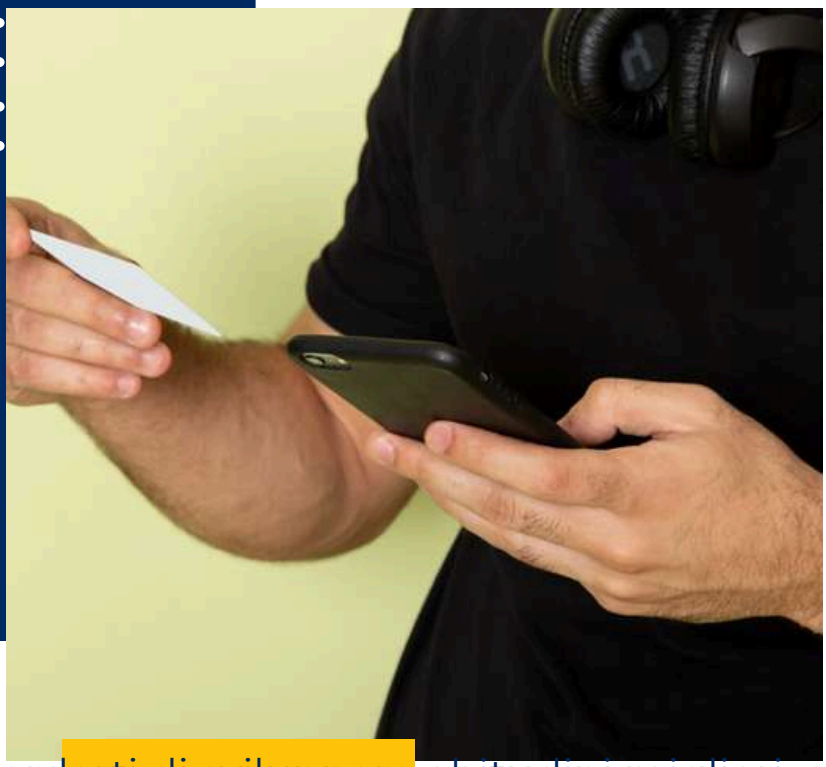
Il modo migliore per rimanere al sicuro online è adottare misure proattive che proteggano i propri dati e prevengano i rischi prima che si verifichino. Esploriamo semplici strategie che puoi iniziare a utilizzare subito.

Restiamo negli stessi gruppi. Leggi il seguente elenco di semplici azioni che puoi intraprendere per ridurre i rischi online:

- **Utilizza password complesse** e uniche e aggiornale regolarmente.
- **Abilita l'autenticazione a più fattori (MFA)** per gli account importanti.
- **Evita link e allegati sospetti:** verifica sempre la fonte.
- **Controlla le impostazioni sulla privacy** sui social media e sulle app per controllare chi può vedere le tue informazioni.
- **Mantenere aggiornato il software** per correggere le vulnerabilità di sicurezza.

Nel vostro gruppo, discutete quali di queste azioni mettete già in pratica e quali potreste trovare difficili da implementare.
Rispondete insieme a queste domande:

- "Quale strategia ritieni sia la più efficace per rimanere al sicuro online?"



Passo 3

Approcci per la prevenzione e la mitigazione

"Come puoi ricordarti di sviluppare abitudini migliori, come controllare le impostazioni sulla privacy o evitare link rischiosi?" Dopo il brainstorming, ogni gruppo condivide una **nuova** strategia che intende adottare e spiega in poche parole perché è importante.

Come riflessione finale, prenditi un momento per pensare a un'abitudine o a uno strumento specifico che ti impegnerai a utilizzare immediatamente per migliorare la tua sicurezza online. Scrivilo su un post-it e pensa a come puoi aiutare gli altri ad adottare le stesse abitudini. Condividendo le tue conoscenze, puoi creare un ambiente online più sicuro non solo per te stesso, ma anche per i tuoi amici, la tua famiglia e la tua comunità.

Passo 4

Riflessione e applicazione

Ora che abbiamo esplorato i rischi online e le strategie di prevenzione, è il momento di riflettere su ciò che abbiamo imparato e pensare a come applicarlo alla nostra vita digitale quotidiana.

Prenditi un momento per rispondere silenziosamente alla domanda:

- "Qual è un'abitudine che hai attualmente e che potrebbe metterti a rischio online?"

Scrivi la tua risposta su un post-it.

Come passo successivo, formatevi una coppia e condividete le vostre riflessioni:

- Spiega l'abitudine rischiosa che hai individuato e perché potrebbe rappresentare un problema.
- Condividi l'azione o lo strumento che intendi adottare per mitigare questo rischio.
- Scambiatevi feedback o idee aggiuntive per rafforzare i vostri piani.
- Discutere come queste strategie possono essere applicate in diverse situazioni, ad esempio utilizzando una rete Wi-Fi pubblica, condividendo informazioni personali o evitando adescamenti e phishing.

Riepilogo dei punti chiave

- La consapevolezza è il primo passo per proteggersi.
- I segnali di allarme sono ovunque, ma una volta che impari a riconoscerli e a reagire in modo appropriato, puoi migliorare notevolmente la tua sicurezza online!
- Conoscere le minacce informatiche e i contenuti inappropriati ti consente di identificare i potenziali rischi e di reagire con sicurezza.
- Riconoscere i rischi nelle situazioni quotidiane online consente di agire rapidamente ed evitare i pericoli.
- Diffondendo la consapevolezza, contribuisci a creare una comunità online più sicura per tutti.

Istruzioni per operatori giovanili, educatori e insegnanti

Obiettivo:
Questa lezione è progettata per sensibilizzare sui rischi online, tra cui minacce informatiche e contenuti inappropriati, e fornire ai partecipanti strategie pratiche per promuovere interazioni online più sicure. Analizzando scenari reali, i partecipanti impareranno a identificare i rischi, riconoscere i segnali di allarme e adottare misure preventive.

Materiali necessari:

- Lavagna a fogli mobili o strumento di presentazione digitale per delineare i concetti chiave
- Penne e pennarelli
- Fogli di carta bianchi per prendere appunti o completare attività
- Accesso a strumenti come *CyberWise* o *Malwarebytes Browser Guard* (nel caso in cui vengano presentati ai partecipanti)
- Post-it colorati per il brainstorming

Fase 1: Nozioni fondamentali sulle minacce informatiche e sui contenuti inappropriati (10 min)

1. Inizia chiedendo ai partecipanti: "Avete mai incontrato qualcosa online che vi è sembrato pericoloso o sospetto?". Incoraggiatene alcuni a condividere le loro esperienze o a fornire un breve esempio, come aver ricevuto un'e-mail sospetta o aver visto un commento offensivo. Usate questo esempio per sottolineare l'importanza di comprendere e affrontare i rischi online.
2. Mini lezione: spiegare le principali minacce informatiche: phishing, adescamento, ecc. Definire i contenuti inappropriati, tra cui:
   - Materiale esplicito: immagini e video dannosi o espliciti.
   - Messaggi predatori: comunicazione manipolativa o dannosa.
   - Contenuti non adatti all'età - Materiale non adatto a determinate fasce d'età.
3. Attività: dividere i partecipanti in gruppi da 3-5 persone e assegnare a ciascun gruppo uno dei tre scenari diversi.

Istruzioni per i gruppi:

1. Analizzre il rischio: analizza cosa rende rischioso lo scenario (ad esempio, mittente sconosciuto, tono urgente o collegamento sospetto).
2. Suggerire azioni sicure, brainstorming su risposte pratiche:
   - email: evitare di cliccare sui link, verificare il mittente tramite canali ufficiali o segnalalo come spam.
   - commenti inappropriati: bloccare l'utente, segnalare il commento ed evitare di rispondere.
   - link sospetti: passare il mouse sopra per controllare l'URL, non cliccare se non si è sicuri e consultare una fonte attendibile.
3. Condivisione dei risultati: i gruppi riassumono la loro analisi e la condividono con la classe. Evidenziano le strategie comuni e ne discutono l'efficacia.
4. Concludere rafforzando i punti chiave, collegando l'attività a strategie più ampie per la sicurezza online da esplorare nei passaggi successivi.

Fase 2: Riconoscere i segnali di allarme e i rischi (15 min)

1. Presentare ai partecipanti i segnali di allarme più comuni delle minacce informatiche utilizzando esempi chiari:

- Link sospetti o mittenti sconosciuti: messaggi provenienti da contatti sconosciuti con link o allegati (ad esempio, "www.freeprizes.xyz").
- Errori di ortografia o richieste urgenti: messaggi come "Il tuo account è bloccato! Riattivalo subito", spesso scritti male per creare urgenza.
- Offerte troppo belle per essere vere: promesse di premi o offerte, come "Hai vinto un iPhone gratis!"

È anche possibile utilizzare elementi visivi, come screenshot di tentativi di phishing, e incoraggiare i partecipanti a condividere esempi per un maggiore coinvolgimento.

2. Il passo successivo è condurre un esercizio di gruppo. Dividete i partecipanti in piccoli gruppi e assegnate a ciascun gruppo un segnale di allarme specifico da analizzare (ad esempio, messaggi urgenti o link sospetti). Fornite i seguenti passaggi:

a. Analizzare l'avvertimento: discuti cosa rende la minaccia convincente (ad esempio, urgenza o inganno).
b. Proporre soluzioni: fai brainstorming sulle risposte, ad esempio verificando le fonti, evitando link sospetti o segnalando truffe.
c. Riassumere i risultati: prepara suggerimenti pratici per evitare la minaccia.

3. Alla fine, ogni gruppo presenta le proprie intuizioni e strategie. Sintetizza in un elenco unico su una lavagna o una lavagna a fogli mobili le buone pratiche. Concludi sottolineando l'importanza della cautela, della verifica e del pensiero critico per rimanere al sicuro online.

Fase 3: Approcci per la prevenzione e la mitigazione (10 min)

1. Inizia sottolineando l'importanza di adottare misure proattive per proteggere i dati personali e ridurre i rischi online. Presenta un elenco di semplici azioni che i partecipanti possono adottare immediatamente, come:

- Utilizzare password complesse e uniche e aggiornarle regolarmente.
- Abilitare autenticazione a più fattori (MFA) per gli account critici.
- Evitare link e allegati sospetti verificandone le fonti.
- Revisione delle impostazioni sulla privacy sui social media e sulle app.
- Mantenere aggiornato il software per risolvere le vulnerabilità della sicurezza.

Spiega come queste azioni possono mitigare efficacemente i rischi online più comuni.

2. Mantenere i partecipanti nei loro gruppi esistenti e fornire l'elenco delle azioni. Chiedere loro di discutere e completare i seguenti compiti:

1. Discussione di gruppo:

- Identifica quali azioni mettono già in pratica e quali trovano difficili.
- Discutere perché alcune strategie potrebbero essere più difficili da implementare e fare brainstorming su come superare queste sfide.

2. Rispondi alle domande chiave:

- "Quale strategia ritieni sia la più efficace per rimanere al sicuro online?"
- "Come puoi ricordarti di sviluppare abitudini migliori, come controllare regolarmente le impostazioni sulla privacy o evitare link rischiosi?"

3. Condividi nuove strategie:

- Ogni gruppo seleziona una nuova strategia che intende adottare, spiega perché è importante e la condivide con gli altri.

Fase 3: Approcci per la prevenzione e la mitigazione (10 min)

3. Concludete l'attività chiedendo a ciascun partecipante di riflettere individualmente su un'abitudine o uno strumento che si impegnerà a utilizzare immediatamente per migliorare la propria sicurezza online. Chiedete loro di scriverlo su un post-it. Incoraggiate i partecipanti a pensare a come condividere questa abitudine con amici, familiari o colleghi per promuovere collettivamente un ambiente online più sicuro.

Fase 4: Riflessione e applicazione (5 min)

1. Riflessione individuale:
   - Chiedi agli studenti: "Qual è un'abitudine online che puoi cambiare per migliorare la sicurezza?"
   - I partecipanti scrivono le loro risposte su post-it.
2. Discussione tra pari:
   - Dividere i partecipanti in coppie per condividere i propri obiettivi e suggerire misure concrete.
3. Conclusione:
   - Concludi con un messaggio motivazionale. Potrebbe essere, ad esempio: "Piccoli cambiamenti nel tuo comportamento online possono fare una grande differenza per la tua sicurezza e quella della tua comunità".

Punti chiave:
I partecipanti dovrebbero concludere la sessione con una chiara comprensione di come identificare minacce informatiche e contenuti inappropriati, come tentativi di phishing, messaggi manipolativi o link sospetti. Sottolineare l'importanza di strategie di sicurezza pratiche, come l'utilizzo di password complesse, l'abilitazione dell'autenticazione a più fattori e la personalizzazione delle impostazioni sulla privacy per proteggere le informazioni personali.
Invitare i partecipanti ad adottare una mentalità proattiva, promuovendo il pensiero critico e mantenendo discussioni aperte sui rischi online. Rafforzare questi principi attraverso la pratica regolare e la condivisione delle conoscenze con gli altri, creando un effetto domino che promuova abitudini online più sicure all'interno delle proprie comunità.

Attività di follow-up e da svolgere a casa:
Chiedere ai partecipanti di:

- Rivedere le impostazioni personali dei social media.
- Strumenti di test come Malwarebytes Browser Guard o filtri di contenuto.
- Condividere una strategia appresa con un amico o un familiare.

Suggerimenti per gli insegnanti:
Rendi le lezioni coinvolgenti utilizzando esempi concreti e immagini chiare per spiegare i rischi online e le strategie pratiche di sicurezza. Incoraggia discussioni interattive per aiutare i partecipanti a entrare in sintonia con il materiale. Attività pratiche, come la creazione di guide sulla sicurezza, aiutano a consolidare i concetti. Mantieni un ambiente aperto e collaborativo in cui le domande sono ben accette e sottolinea i benefici a lungo termine di abitudini online sicure. Rafforza le lezioni chiave attraverso attività di follow-up o riflessioni di gruppo per garantire che i partecipanti memorizzino e applichino ciò che hanno imparato.

Strumenti

CyberWise

CyberWise è una piattaforma educativa che offre strumenti, risorse e guide per aiutare le persone, in particolare genitori, educatori e studenti, a comprendere la sicurezza online. Offre moduli su come riconoscere le minacce informatiche come phishing, cyberbullismo e contenuti inappropriati, oltre a strategie per mitigare i rischi.

www.cyberwise.org

Malwarebytes Browser Guard

Si tratta di un'estensione gratuita per browser che protegge gli utenti da phishing, truffe, malware e contenuti inappropriati. Blocca attivamente siti web e annunci dannosi, garantendo una navigazione più sicura per tutti gli utenti, non solo per i bambini.

www.malwarebytes.com

Riferimenti

- CyberWise. (n.d.). Recuperato da https://www.cyberwise.org
- Dalby, J. (15 gennaio 2021). Come evitare contenuti inappropriati. Gabb Now. Tratto da https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (25 settembre 2023). Evoluzione della minaccia alla sicurezza informatica: una panoramica della portata della minaccia informatica. Tratto da https://figshare.com/ndownloader/files/42443952
- Lynch, M. (5 aprile 2024). 19 semplici modi per bloccare contenuti inappropriati. The Tech Edvocate. Tratto da https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (21 febbraio 2024). Navigating the Cyber Security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. Tratto da https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (n.d.). Recuperato da https://www.malwarebytes.com/browserguard
- Roy, R. (23 agosto 2021). Cos'è una minaccia informatica? Definizione, tipologie, ricerca, best practice ed esempi. Tratto da https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (n.d.). 10 tipi di minacce alla sicurezza informatica e soluzioni. Tratto da https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

QUIZ

1. Qual è il segnale chiave di un tentativo di phishing?

A. Ricevere un messaggio da un account precedentemente sconosciuto ma verificato

B. Un'e-mail senza link, immagini o allegati

C. Un'e-mail che ti esorta ad agire immediatamente, spesso con una grammatica scadente

D. Un messaggio da un mittente noto che richiede informazioni di routine

2. Quale comportamento potrebbe aumentare il rischio di minacce informatiche?

A. Aggiornare regolarmente i dispositivi e le app

B. Fare clic sui link nelle e-mail senza verificare il mittente

C. Utilizzare l'autenticazione a due fattori per gli account online

D. Rivedere le impostazioni sulla privacy sui social media una volta al mese

3. Quale abitudine aiuta a non cadere vittima delle minacce informatiche?

A. Utilizzare un gestore di password per creare e memorizzare password univoche

B. Accettare tutte le autorizzazioni durante l'installazione di app per comodità

C. Condividere le password con amici fidati o familiari per avere un ripiego nel caso in cui le si dimentichi

D. Ignorare gli avvisi di sicurezza del browser

QUIZ

4. Cosa rende un collegamento sospetto e potenzialmente dannoso?
A. Utilizza la crittografia HTTPS
B. Reindirizza a un altro sito web
C. Contiene caratteri o domini insoliti
D. È condiviso da un amico in un messaggio diretto

5. Qual è la strategia più efficace per prevenire l'esposizione a contenuti inappropriati?
A. Ridurre al minimo le interazioni online
B. Disattivare tutte le notifiche sui dispositivi
C. Affidarsi esclusivamente al software antivirus
D. Utilizzo dei filtri dei contenuti e regolazione delle impostazioni sulla privacy

Soluzioni

Domanda 1: C
Domanda 2: B
Domanda 3: A
Domanda 4: C
Domanda 5: D

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

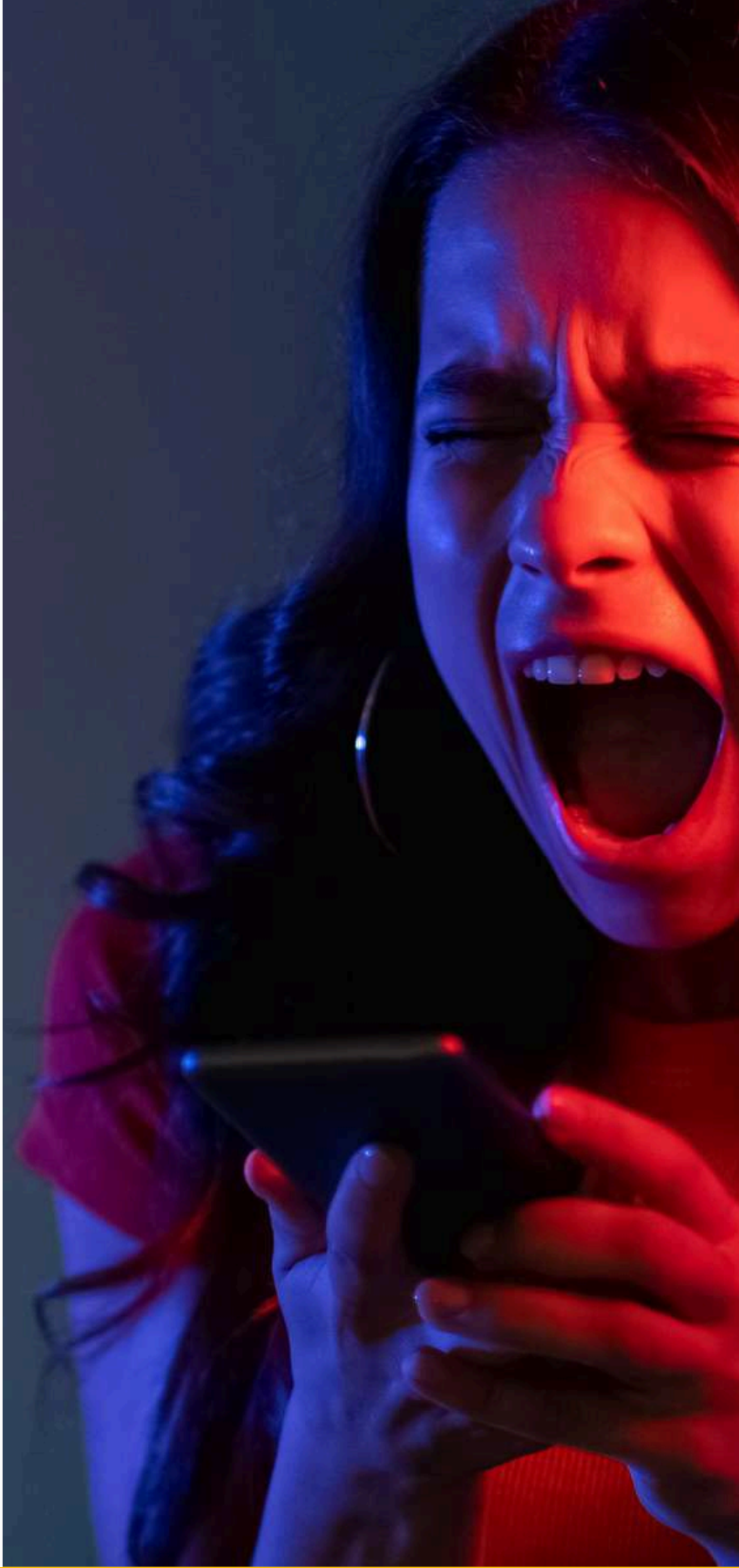
LABC

Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



Co-funded by the European Union

Finanziato dall'Unione Europea. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione Europea né l'EACEA possono essere ritenute responsabili per essi.