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 5.6

Strumenti pratici per la sicurezza online

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 5.6

Strumenti pratici per la sicurezza online

Obiettivi:

- Fornire ai partecipanti strumenti e tecniche pratiche per identificare e mitigare le minacce online più comuni, tra cui phishing, malware e truffe.
- Acquisire competenze nell'utilizzo di risorse di sicurezza informatica, come gestori di password, VPN e browser sicuri, promuovendo al contempo la comprensione della gestione della privacy online.
- Promuovere pratiche online sicure e responsabili attraverso una valutazione critica delle piattaforme digitali, riconoscendo i segnali di allarme delle minacce informatiche e adottando abitudini di protezione come la segnalazione di attività sospette.

Messaggio/i chiave:

- Consapevolezza e preparazione sono la prima linea di difesa. Comprendere le minacce online e disporre degli strumenti giusti consente di navigare nel mondo digitale in modo sicuro.
- La tua sicurezza è nelle tue mani. Sfruttando strumenti pratici come VPN, browser sicuri e impostazioni sulla privacy puoi proteggere i tuoi dati personali e mantenere il controllo sulla tua presenza online.

TIPO DI LEZIONE:

Panoramica della lezione

La sicurezza online dipende in larga misura dalla capacità di utilizzare efficacemente strumenti progettati per proteggere le informazioni personali e prevenire le minacce digitali. Questa lezione si concentra sull'interazione pratica e concreta con i principali strumenti di sicurezza informatica, come gestori di password, VPN e impostazioni di privacy. I partecipanti esploreranno attivamente il funzionamento di questi strumenti, ne testeranno le funzionalità e apprenderanno strategie per integrarli nella routine digitale quotidiana. Attraverso attività guidate, acquisiranno sicurezza nell'applicazione di questi strumenti per salvaguardare la propria presenza online e rispondere ai rischi con soluzioni pratiche.

Il workshop è organizzato in 4 fasi:

1: Introduzione agli strumenti di sicurezza online (10 min)

2: Esplorazione pratica degli strumenti (15 min)

3: Gestione del rischio basata su scenari (10 min)

4: Riflessioni finali (5 min)

Passo 1

Introduzione agli strumenti di sicurezza online

Ti è mai capitato di imbatterti in qualcosa di sospetto online? Magari un'e-mail strana che ti chiede di reimpostare la password, un pop-up che offre un premio gratuito o un sito web che richiede troppe informazioni personali? Queste situazioni possono sembrare rischiose, e spesso lo sono.

La buona notizia è che esistono strumenti **pratici che puoi utilizzare** per proteggerti in momenti come questi. Al termine di questa attività, saprai come riconoscere questi rischi e utilizzare strumenti come gestori di password, VPN e impostazioni di privacy per rimanere al sicuro online. Approfondiamo il discorso e vediamo come questi strumenti possono aiutarti!

Passo 1

Introduzione agli strumenti di sicurezza online

Ecco tre semplici strumenti che possono rendere la tua vita online molto più sicura:

- **Gestori di password**: Ti aiutano a creare e memorizzare password complesse e univoche, così non devi ricordarle tutte.
- **VPN (Virtual Private Network)**: Proteggono la tua attività online, in particolare sulle reti Wi-Fi pubbliche, mantenendo sicura la tua connessione.
- **Impostazioni sulla privacy del browser**: Ti consentono di controllare quali informazioni i siti web possono raccogliere su di te, come la tua posizione o le tue abitudini di navigazione.

Oggi ci concentreremo su questi strumenti perché possono fare un'enorme differenza nella sicurezza online.

Pensa all'ultima volta che ti sei imbattuto in qualcosa di strano online, magari un sito web che non ti sembrava affidabile. Come l'hai gestito? L'hai ignorato, hai indagato ulteriormente o magari ci hai addirittura cliccato sopra?

Facciamo un brainstorming insieme:

- Quali tipi di minacce o rischi online hai notato in precedenza?
- Quali strumenti o strategie utilizzi già per proteggerti online?

Ci prenderemo qualche minuto per condividere idee in gruppo. Non preoccuparti se non hai vissuto questa esperienza in prima persona: le storie dei tuoi colleghi potrebbero suscitare nuove riflessioni.

Passo 2

Esplorazione pratica degli strumenti

Ora è il momento di immergerci ed esplorare come semplici strumenti possano rendere più sicura la tua presenza online. In questa attività, proverai le impostazioni di privacy del browser e metterai alla prova le tue capacità di creazione di password utilizzando *The Password Meter*. Iniziamo!

Parte 1: Impostazioni sulla privacy del browser

Il tuo browser può controllare la quantità di informazioni che i siti web raccolgono su di te. Controlliamo e modifichiamo le tue impostazioni sulla privacy:

1. Apri le impostazioni sulla privacy del tuo browser (cerca "Impostazioni" o "Preferenze", quindi vai su "Privacy" o "Sicurezza").
2. Esaminare queste aree chiave:

- **Prevenzione del tracciamento**: E attivata?
- **Cookie**: I cookie di terze parti sono bloccati?
- **Autorizzazioni**: Quali siti web possono accedere alla tua posizione, alla tua fotocamera o al tuo microfono?

Passo 2 Esplorazione pratica degli strumenti

3. Apporta modifiche: attiva tutte le impostazioni sulla privacy che ritieni possano aiutarti a proteggere i tuoi dati.

Per esempio:

- Blocca i cookie di tracciamento.
- Disattiva la condivisione della posizione per i siti web di cui non ti fidi.

Riflessione rapida: Cosa ti ha sorpreso delle tue impostazioni attuali? Hai apportato modifiche?

Parte 2: Test della sicurezza della password con *The Password Meter*

Creare una password complessa è uno dei modi più semplici per proteggere i tuoi account. Ora, vediamo quanto sono sicure le tue password:

1. Vai a The Password Meter.
2. Pensa a una nuova password (non usarne una che hai già!).

Passo 2 Esplorazione pratica degli strumenti

3. Inseriscilo in *The Password Meter* e guarda il feedback:
   - Quanto è sicura la tua password?
   - Quali suggerimenti fornisce per renderlo più forte?

4. Sperimenta modificando la tua password in base al feedback (ad esempio, aggiungi simboli, allungala o mescola lettere minuscole e maiuscole). Guarda come migliora il punteggio!

Rifletti un attimo: Quanto è stato facile o difficile creare una password sicura? C'è qualcosa che faresti diversamente quando imposterai le password in futuro?

Al termine di questa attività, avrai migliorato le impostazioni sulla privacy del tuo browser e avrai imparato a creare password più sicure!

Passo 3

Gestione del rischio basata su scenari

Dopo aver esaminato alcuni strumenti pratici, vediamo come possono essere applicati a situazioni reali. Lavorerete in piccoli gruppi per analizzare scenari, identificare i rischi e decidere come affrontarli utilizzando gli strumenti discussi.

Leggi lo scenario fornito al tuo gruppo. Ecco alcuni esempi:

1. *Ricevi un'email che ti informa di aver vinto un premio, ma il link sembra sospetto. Cosa fai?*
2. *Quando installi un'app di social media, ti viene chiesto di accedere alla tua posizione, alla tua fotocamera e al tuo microfono. Dovresti consentirlo?*
3. *Stai utilizzando una connessione Wi-Fi pubblica in un bar e ti viene chiesto di accedere a un sito web sconosciuto. Come puoi proteggerti?*

Parla con il tuo gruppo dei rischi presenti nel tuo scenario. Chiedeti:

- *Cosa potrebbe andare storto se non agisci con cautela?*
- *Perché questa situazione sembra pericolosa?*

Decidi come potresti utilizzare strumenti pratici per gestire il rischio. Ad esempio:

- *Utilizzare le impostazioni sulla privacy del browser per bloccare le autorizzazioni non necessarie.*
- *Evita di cliccare su link sospetti e controlla le email per individuare eventuali segnali di phishing.*
- *Attiva una VPN per proteggere la tua connessione alle reti Wi-Fi pubbliche.*

Passo 3

Gestione del rischio basata su scenari

Dopo alcuni minuti, ogni gruppo condividerà:

- *Quali rischi hai individuato nello scenario*
- *Quali strumenti o misure hai utilizzato per rimanere al sicuro*

Pensaci: In che modo questi strumenti potrebbero aiutarti nelle tue attività online?

Strumenti pratici come le impostazioni di privacy del browser, le VPN e il rilevamento del phishing possono trasformare situazioni rischiose in situazioni gestibili. Usarli regolarmente rende molto più facile la sicurezza online!

Passo 4

Riflessioni finali

Riflettiamo su ciò che hai imparato e su come lo utilizzerai per rimanere al sicuro online.

Fase 1: Rifletti

Rifletti su queste domande:

- Quale strumento (ad esempio, impostazioni di privacy del browser, VPN, gestori di password) ti è stato più utile? Perché?
- Come è cambiata la tua visione della sicurezza online dopo aver utilizzato questi strumenti?

Fase 2: Pianifica il tuo prossimo passo

Scrivi un'azione che intraprenderai per migliorare la tua sicurezza online.

- Cosa farai? (ad esempio, "Userò un gestore di password per creare password complesse").
- Quando lo farai? (ad esempio, "Entro la fine della settimana").

Il primo passo è usare strumenti pratici: sii coerente per mantenere alta la tua sicurezza online!

Riepilogo dei punti chiave

- **Le impostazioni sulla privacy del browser, i gestori di password e le VPN sono strumenti semplici ma potenti per migliorare la tua sicurezza online.**
- **Gestisci attivamente le informazioni che condividi online modificando le impostazioni sulla privacy e limitando le autorizzazioni non necessarie.**
- **Aggiorna regolarmente le impostazioni sulla privacy, crea password sicure e controlla le autorizzazioni delle app per fare della sicurezza online una parte integrante della tua vita digitale.**
- **Sii proattivo: combinando strumenti con pensiero critico e rimanendo informati, sarai preparato ad affrontare le minacce online in continua evoluzione.**
- **Prova a testare anche altri strumenti pratici online per comprendere e migliorare la tua sicurezza digitale: più strumenti saprai usare, più aumenterai la tua sicurezza!**

Istruzioni per operatori giovanili, educatori e insegnanti

Obiettivo:
Questa lezione si concentra sul fornire ai partecipanti le competenze pratiche per utilizzare gli strumenti di base per la sicurezza online. Attraverso esercizi e discussioni individuali e di gruppo, acquisiranno la capacità di identificare e gestire le minacce online più comuni, rafforzare la propria protezione digitale con risorse come gestori di password, VPN e impostazioni di privacy, e integrare abitudini più sicure nelle loro attività online quotidiane.

Materiali necessari:

- Accesso a Internet per strumenti di test (ad esempio, VPN, gestori di password)
- Computer portatili, tablet o smartphone per esercizi pratici
- Lavagna bianca o lavagna a fogli mobili per il brainstorming e la sintesi delle discussioni
- Fogli di carta bianchi per prendere appunti
- Penne, matite o pennarelli colorati

Fase 1: Introduzione agli strumenti di sicurezza online (10 min)

1. Inizia coinvolgendo i partecipanti con una domanda pertinente: "Ti è mai capitato di imbatterti in qualcosa online che ti è sembrato sospetto, come un'e-mail strana, un pop-up che offriva un premio o un sito web che chiedeva troppe informazioni personali?". Spiega brevemente che queste situazioni possono sembrare rischiose e spesso lo sono, ma esistono strumenti pratici per affrontarle.
2. Suscita l'attenzione per la sessione su tre strumenti essenziali: gestori di password, VPN e impostazioni di privacy del browser. Sottolinearne l'importanza spiegando che i gestori di password aiutano a creare e memorizzare password complesse e univoche, le VPN proteggono l'attività online su reti Wi-Fi pubbliche e le impostazioni di privacy del browser controllano quali informazioni i siti web possono raccogliere, come la posizione o le abitudini di navigazione.
3. Incoraggia i partecipanti a riflettere sulle proprie esperienze con i rischi online, chiedendo: "Ripensa all'ultima volta che ti sei imbattuto in qualcosa di sospetto online. Come l'hai gestito?"
4. Avvia una breve discussione con domande come: "Quali tipi di minacce online hai notato?" e "Quali strumenti o strategie utilizzi già per proteggerti?". Invita i partecipanti a condividere le loro storie o idee, sottolineando che imparare gli uni dagli altri può dare origine a nuove intuizioni.
5. Concludi sottolineando l'importanza di questi strumenti nella gestione dei rischi online, affermando: "Utilizzando strumenti come gestori di password, VPN e impostazioni sulla privacy, è possibile navigare con sicurezza nel mondo digitale proteggendo al contempo le proprie informazioni personali". Mantenere la discussione interattiva e di supporto, assicurandosi che i partecipanti si sentano incoraggiati a condividere i propri pensieri e ad apprendere dal gruppo.

Fase 2: Esplorazione pratica degli strumenti (15 min)

1. Inizia spiegando l'obiettivo di questa attività: esplorare strumenti pratici che migliorano la sicurezza online attraverso le impostazioni della privacy del browser e i test di sicurezza della password.
2. Dividi l'attività in due parti per garantire un approccio strutturato.

Parte 1: Impostazioni sulla privacy del browser (8 minuti)

1. Guida i partecipanti ad aprire le impostazioni sulla privacy del proprio browser (andare su "Impostazioni" o "Preferenze", quindi trovare "Privacy" o "Sicurezza"). Chiedere loro di rivedere le aree chiave:
   - Prevenzione Del tracciamento: assicurarsi che sia abilitata.
   - Cookie: Controlla se i cookie di terze parti sono bloccati.
   - Autorizzazioni: Controlla quali siti web possono accedere alla loro posizione, alla loro fotocamera o al loro microfono.
2. Incoraggia i partecipanti ad apportare modifiche, ad esempio bloccando i cookie di tracciamento o disabilitando la condivisione della posizione non necessaria.
3. Successivamente, stimola una rapida riflessione: "Cosa ti ha sorpreso delle tue impostazioni attuali? Hai apportato modifiche?". Questo aiuta i partecipanti a collegare le loro scoperte al valore di questi strumenti.

Parte 2: Test di sicurezza della password (5 minuti)

1. Chiedi ai partecipanti di accedere al Password Meter. Chiedere loro di creare una nuova password (non una che usano già) e di testarne la sicurezza.
2. Incoraggiali ad analizzare il feedback e a sperimentare modifiche, come l'aggiunta di simboli, la combinazione di maiuscole e minuscole o l'aumento della lunghezza, per vedere come migliora il punteggio.
3. Concludi con una riflessione: "Quanto è stato facile o difficile creare una password sicura? C'è una cosa che faresti diversamente quando imposterai le password in futuro?"
4. Concludere l'attività sottolineandone il valore pratico.
5. Mantenere la sessione pratica e coinvolgente, offrendo indicazioni secondo necessità mentre i partecipanti esplorano e applicano questi strumenti.

Fase 3: Gestione del rischio basata su scenari (10 min)

1. Questa attività aiuta i partecipanti ad applicare gli strumenti di sicurezza online a scenari di vita reale. Dividete i partecipanti in piccoli gruppi e assegnate a ciascun gruppo uno scenario, ad esempio:
   - Un'e-mail sospetta con un link a un premio.
   - Un'app di social media che richiede autorizzazioni eccessive.
   - Utilizzo di una rete Wi-Fi pubblica e mi viene visualizzata una richiesta di accesso non familiare.
2. Chiedi ai gruppi di discutere i rischi, tenendo conto di:
   - "Cosa potrebbe andare storto se non agisci con cautela?"
   - "Perché questa situazione sembra pericolosa?"
3. Chiedi loro di identificare come gestire il rischio utilizzando strumenti come le impostazioni sulla privacy del browser, evitando link di phishing o abilitando una VPN.
4. Successivamente, ogni gruppo condivide i rischi identificati e gli strumenti utilizzati per affrontarli.
5. Concludi sottolineando: "Strumenti come le impostazioni sulla privacy, le VPN e il rilevamento del phishing semplificano la gestione dei rischi online. L'uso regolare di questi strumenti rafforza la sicurezza online". Mantenere la sessione focalizzata e incoraggiare spunti pratici e attuabili.

Fase 4: Riflessioni finali (5 min)

1. Concludi la sessione guidando i partecipanti attraverso un esercizio di riflessione per consolidare quanto appreso. Iniziare chiedendo loro di considerare:
   - "Quale strumento (ad esempio, impostazioni di privacy del browser, VPN, gestori di password) ti è stato più utile? Perché?"
   - "Come è cambiata la tua visione della sicurezza online dopo aver utilizzato questi strumenti?"
2. Incoraggia i partecipanti a condividere brevemente i propri pensieri, favorendo un ambiente favorevole alla discussione.
3. Successivamente, incoraggiali a pianificare un'azione concreta per migliorare la loro sicurezza online, ad esempio:
   - "Cosa farai?" (ad esempio, "Userò un gestore di password per creare password complesse.")
   - "Quando lo farai?" (ad esempio, "Entro la fine della settimana").
4. Concludi sottolineando l'importanza della coerenza, ricordando ai partecipanti: "Gli strumenti pratici sono il primo passo: sii coerente per mantenere forte la tua sicurezza online!" Mantieni un tono motivante e focalizzato sull'applicazione delle lezioni apprese alle pratiche online quotidiane.

Punti chiave:
Al termine della lezione, i partecipanti acquisiranno una chiara comprensione di come utilizzare strumenti di base come gestori di password, VPN e impostazioni di privacy del browser per migliorare la propria sicurezza online. Impareranno a identificare le minacce più comuni, come il tracciamento dei dati, e ad adottare misure proattive per proteggere le proprie informazioni personali. Integrando questi strumenti e strategie nella loro routine quotidiana, saranno in grado di navigare nel mondo digitale con sicurezza, riducendo al minimo le potenziali minacce. Per comunicare efficacemente questi concetti, è consigliabile utilizzare scenari pertinenti ed esempi chiari per dimostrare l'impatto concreto di questi strumenti sulla sicurezza online quotidiana.

Attività di follow-up e da svolgere a casa:

Incoraggia i partecipanti a esaminare più attentamente le loro attuali pratiche online, rivedendo e modificando le impostazioni di privacy del browser, testando la sicurezza delle loro password con strumenti come *The Password Meter* ed esplorando le funzionalità VPN. Incaricateli di valutare le autorizzazioni delle applicazioni utilizzate di frequente, individuando i potenziali rischi e implementando alternative più sicure. Infine, chiedete ai partecipanti di condividere un consiglio di sicurezza appena appreso con un amico o un familiare, rafforzando le loro conoscenze e diffondendo la consapevolezza sulla sicurezza digitale.

Suggerimenti per gli insegnanti:

È possibile utilizzare esempi pratici e reali e altri esercizi interattivi per dimostrare come strumenti come gestori di password, VPN e impostazioni di privacy possano essere utilizzati efficacemente per migliorare la sicurezza online. Mostra ai partecipanti passo dopo passo come navigare e configurare questi strumenti, rendendo la sessione pratica e fruibile. Crea un ambiente aperto e collaborativo in cui i partecipanti si sentano a proprio agio nel discutere le proprie esperienze con le minacce online e nel porre domande. Sottolinea l'importanza di utilizzare regolarmente questi strumenti e di integrarli nelle routine online quotidiane per garantire una protezione digitale coerente e proattiva.

Strumenti

Get Safe Online

Un sito web completo che offre consigli gratuiti e semplici su un'ampia gamma di argomenti relativi alla sicurezza online. Include guide pratiche su come proteggere le informazioni personali, evitare le truffe e comunicare online in modo sicuro. I contenuti sono intuitivi e pensati per utenti con conoscenze tecniche minime.

www.getsafeonline.org

The Password Meter

Uno strumento gratuito che valuta la sicurezza delle password e fornisce suggerimenti per migliorarle. Gli studenti possono sperimentare la creazione di password e ricevere feedback immediati sul loro livello di sicurezza, rendendolo un modo interattivo per comprendere l'importanza di password complesse.

passwordmeter.com

Riferimenti

- Alice. (3 ottobre 2022). 5 strumenti per la sicurezza online. Ryadel. Tratto da https://www.ryadel.com/en/5-privacy-data-protection-security-tools
- Naviga in sicurezza online. (n.d.). Tratto da https://www.getsafeonline.org
- Team Goodwall. (24 marzo 2022). I 7 migliori strumenti di sicurezza online e impostazioni di privacy per proteggerti. Tratto da https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings
- Lakhwani, S. (19 giugno 2024). Fondamenti di sicurezza informatica [Guida per principianti 2024]. Blog di upGrad KnowledgeHut. Tratto da https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- Il misuratore di password. (n.d.). Recuperato da https://passwordmeter.com
- Vodafone. (n.d.). Utilizzo di strumenti per la sicurezza e il benessere online. Tratto da https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools

QUIZ

1. Qual è la funzione principale di una rete privata virtuale (VPN)?
A. Fornire protezione antivirus automatica
B. Aumentare la velocità di Internet
C. Prevenire gli annunci pop-up su tutti i siti Web
D. Crittografare l'attività online, in particolare sulle reti Wi-Fi pubbliche

2. Quale comportamento potrebbe mettere a rischio la tua sicurezza online?
A. Utilizzare password complesse e univoche per ogni account
B. Modificare regolarmente le impostazioni sulla privacy nel browser
C. Utilizzare un gestore di password per memorizzare le credenziali di accesso
D. Fare clic su ogni collegamento in e-mail indesiderate

3. Qual è un passaggio consigliato per migliorare le impostazioni sulla privacy del browser?
A. Utilizzo delle impostazioni predefinite senza modifiche
B. Blocco dei cookie di tracciamento e disattivazione delle autorizzazioni non necessarie
C. Disattivazione dei cookie per tutti i siti web
D. Consentire a tutti i siti web di accedere alla tua posizione

QUIZ

4. Qual è lo scopo delle impostazioni sulla privacy del browser?
A. Velocizzare l'esperienza di navigazione dell'utente
B. Memorizzare le password dell'utente in modo sicuro
C. Controllare quali informazioni i siti Web possono raccogliere sull'utente
D. Impedire la visualizzazione di annunci pop-up su tutti i siti Web

5. Come puoi migliorare la sicurezza della tua password?
A. Includendo simboli, mescolando maiuscole e minuscole e aumentando la lunghezza
B. Utilizzando frasi comuni facili da ricordare
C. Evitando l'uso di numeri e caratteri speciali
D. Testando ripetutamente la stessa password

Soluzioni

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

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

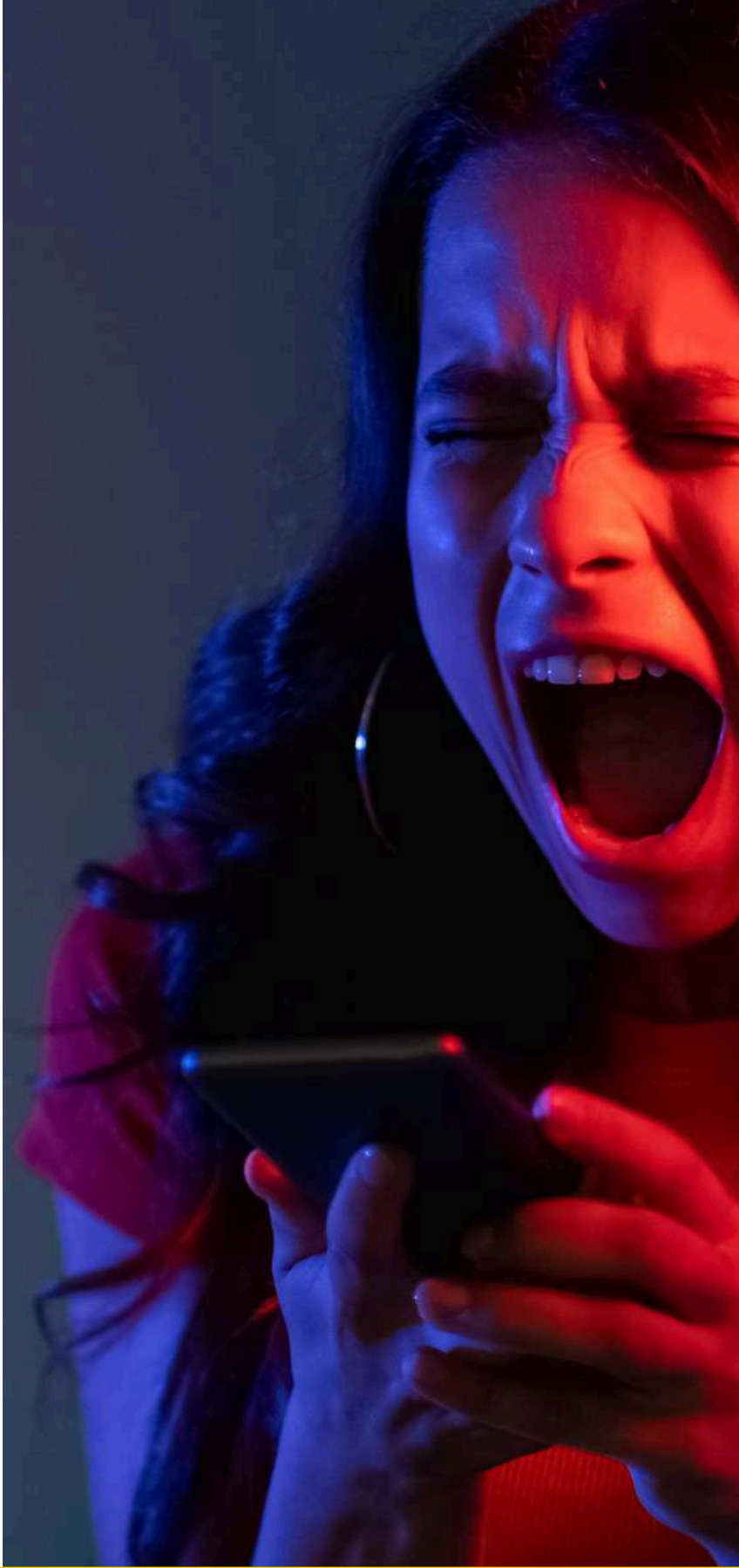
LABC

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.