CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Pratiche di educazione non formale:

Doxing

R2 CYBER TOOLKIT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

#15	**Tattiche anti-doxing: Mantenere la propria vita privata**
Minaccia/e	**Doxing**
	Il doxing, nel contesto delle minacce informatiche giovanili, è la pratica malevola di raccogliere e pubblicare informazioni private o identificative su un individuo senza il suo consenso, in genere attraverso Internet. Questo atto è spesso finalizzato a intimidire, minacciare, molestare, svergognare o esercitare potere sulla vittima. Il doxing può portare a gravi conseguenze per i giovani, tra cui disagio psicologico, perdita della privacy e, in alcuni casi, danni fisici. Sfrutta l'accessibilità delle informazioni personali nell'era digitale, violando il diritto alla privacy e alla sicurezza online.
Tipologia	Esercizi di simulazione
Durata	110 minuti/1 ora e 50 minuti (può essere adattato in base alla profondità delle attività)
Modalità	In presenza [in aula]
Obiettivo	L'obiettivo di questa pratica è quello di fornire ai partecipanti le conoscenze e le competenze necessarie per proteggere la propria privacy online, comprendere il comportamento etico online e rispondere efficacemente al doxing e alle relative minacce informatiche.
Obiettivi di apprendimento	Strategie di protezione della privacy: In grado di utilizzare strategie per proteggere la propria privacy e le informazioni sensibili online, riducendo il rischio di diventare vittima di doxing. Condotta etica online: Dimostrare una comprensione del comportamento etico negli spazi online, impegnandosi a rispettare la privacy e la dignità degli altri. Risposta critica al cyberbullismo: Sviluppare le competenze per rispondere in modo appropriato al cyberbullismo e alle molestie, comprese le azioni da intraprendere se loro o qualcuno che conoscono è vittima di doxing. Mitigazione del rischio di furto d'identità: Applicare le conoscenze su come salvaguardare le informazioni personali e finanziarie per prevenire il furto di identità e le frodi. Alfabetizzazione legale sul doxing: Comprendere i propri diritti legali e le potenziali azioni legali che possono essere intraprese contro gli autori del doxing, nonché le implicazioni legali del doxing.
Profilo del tirocinante	Gruppo di età: 15-17 anni Background educativo: Studenti delle scuole superiori s Prerequisiti: conoscenza di base dell'uso di Internet e delle piattaforme di social media.
n° partecipanti	20-25
I materiali	Dispositivi connessi a Internet (laptop/tablet)

	Proiettore e schermo per le presentazioni Lavagna e pennarelli Dispense stampate sulle strategie di protezione della privacy e sui diritti legali Schede di scenario per esercizi di simulazione Quaderni e penne per i partecipanti
Preparazione	Allestimento della sede: Disporre i posti a sedere in aula in modo da facilitare le discussioni di gruppo e la visione dello schermo del proiettore. Preparare i materiali: Preparare i computer/tablet con il software necessario e l'accesso a Internet. Stampare e organizzare le dispense e le schede di scenario.
Attuazione	*Introduzione (10 minuti):* Dare il benvenuto ai partecipanti e introdurre il tema del doxing. Spiegare lo scopo della sessione e gli obiettivi di apprendimento. *Panoramica sul Doxing (10 minuti):* Presentare una breve panoramica sul doxing, compresi esempi di vita reale e potenziali impatti. Discutere perché è una minaccia significativa, soprattutto per i giovani. *Strategie di protezione della privacy (15 minuti):* Distribuire le dispense e spiegare le varie strategie per proteggere le informazioni personali online (facoltativo). Coinvolgere i partecipanti in una discussione sull'importanza delle impostazioni della privacy sulle piattaforme dei social media. *Esercizio di simulazione: Identificazione delle vulnerabilità (20 minuti):* Dividete i partecipanti in piccoli gruppi. Fornire a ciascun gruppo uno scenario immaginario (vedi allegato) in cui devono identificare le potenziali vulnerabilità della privacy e suggerire misure di protezione. I gruppi presentano i loro risultati e suggerimenti. *Condotta etica online (10 minuti):*

	Discutere i comportamenti etici online e l'importanza di rispettare la privacy degli altri. Evidenziare le conseguenze di comportamenti non etici come il doxing. *Risposta critica al cyberbullismo (15 minuti):* Presentare brevemente le strategie di risposta al cyberbullismo e al doxing. Condurre un'esercitazione di ruolo in cui i partecipanti si esercitano a rispondere a un incidente di doxing. *Mitigazione del rischio di furto d'identità (10 minuti):* Spiegare come salvaguardare le informazioni personali e finanziarie. Fornire suggerimenti ed esempi pratici. *Alfabetizzazione legale in materia di Doxing (10 minuti):* Discutere gli aspetti legali del doxing, comprese le potenziali azioni legali e i diritti delle vittime. Rispondere alle domande dei partecipanti sulle implicazioni legali. *Domande e risposte e conclusione (10 minuti):* Apre la discussione per eventuali altre domande. Riassumere i punti chiave e distribuire i moduli di valutazione per il feedback (facoltativo).
Suggerimenti e consigli	Incoraggiate la discussione aperta e assicuratevi che ogni partecipante abbia la possibilità di contribuire. Monitorare le attività del gruppo per fornire una guida e mantenere le discussioni sul filo del rasoio. Utilizzate esempi di vita reale per rendere la sessione più relazionabile e d'impatto.
Misure di sicurezza	Garantire la sicurezza di Internet durante le attività online. Mantenere un ambiente di supporto in cui i partecipanti si sentano sicuri di condividere e discutere. Siate pronti a gestire qualsiasi disagio o malessere dei partecipanti a causa della natura delicata dell'argomento.
Valore aggiunto	Conoscenze pratiche: Strategie e tecniche concrete per proteggere la propria privacy online e le proprie informazioni sensibili.

	Consapevolezza etica: Una comprensione più approfondita del comportamento etico online e dell'importanza di rispettare la privacy degli altri. Abilità di risposta: Miglioramento della capacità di rispondere efficacemente agli episodi di cyberbullismo e doxing, compresa la conoscenza delle azioni da intraprendere e di chi contattare per ottenere aiuto. Mitigazione del rischio: Migliori competenze nella salvaguardia delle informazioni personali e finanziarie per prevenire furti di identità e frodi. Comprensione legale: Una più chiara comprensione dei loro diritti legali in materia di doxing e delle potenziali azioni legali contro gli autori.
Feedback e valutazione	Incoraggiare i partecipanti a fornire un feedback alla fine della sessione per migliorare le pratiche future.
Conclusione	Questa pratica educa efficacemente i giovani agli aspetti critici della privacy online, della condotta etica e della risposta al cyberbullismo. La pratica non solo migliora la loro conoscenza dei diritti e delle responsabilità legali, ma favorisce anche un ambiente online rispettoso e sicuro. In definitiva, questa pratica consente ai giovani di navigare nel mondo digitale con fiducia, riducendo i rischi associati al doxing e ad altre minacce informatiche e rafforzando l'importanza di mantenere la privacy e un comportamento etico online.

Allegato. Esercitazione di ruolo: Risposta a un incidente di Doxing

Obiettivo: Consentire ai partecipanti di esercitarsi a rispondere efficacemente a un incidente di doxing, dotandoli delle competenze necessarie per gestire tali situazioni nella vita reale.
Durata: 15 minuti
Passi: **Introduzione all'esercizio:** Spiegate lo scopo dell'esercizio di gioco di ruolo. Sottolineare l'importanza di esercitarsi nelle risposte per essere meglio preparati nelle situazioni reali. **Distribuzione delle carte scenario:** Dividete i partecipanti in piccoli gruppi di 4-5 persone. Distribuite una scheda di scenario a ciascun gruppo. **Preparazione del gruppo:** Lasciate che ogni gruppo abbia il tempo di leggere il proprio scenario e di discutere su come reagire. Incoraggiate i partecipanti a consultare le loro dispense sulle strategie di risposta e sui diritti legali. **Gioco di ruolo:**

Ogni gruppo recita il proprio scenario, con i membri del gruppo che assumono ruoli diversi (ad esempio, la vittima, l'amico, il doxer, uno spettatore).

I facilitatori osservano e forniscono indicazioni se necessario.

Presentazioni di gruppo:

Ogni gruppo presenta il proprio scenario e dimostra la propria risposta.

Dopo ogni presentazione, lasciate un po' di tempo per il feedback dei facilitatori e dei colleghi.

Discussione e resoconto:

Condurre una breve discussione su ciò che è stato appreso dall'esercizio.

Evidenziare le strategie efficaci e affrontare eventuali aree di miglioramento.

Allegato. Esempi di schede di scenario

Scheda di scenario 1: Informazioni personali esposte

Descrizione: Un partecipante scopre che le sue informazioni personali (indirizzo di casa, numero di telefono) sono state pubblicate online da un utente anonimo.

Compito: Determinare le misure immediate per proteggere i propri account, segnalare l'incidente e informare gli adulti di fiducia o le autorità.

Scheda di scenario 2: Amico in difficoltà

Descrizione: Un amico di un partecipante è stato oggetto di doxing dopo un'accesa discussione on-line. L'amico è angosciato e non sa cosa fare.

Compito: Fornire sostegno emotivo all'amico, aiutarlo a denunciare l'incidente e consigliarlo su come proteggere le sue informazioni.

Scheda scenario 3: Compagno di classe sotto attacco

Descrizione: Un partecipante assiste al doxing di un compagno di classe in una chat di gruppo. Il doxer è una persona che conosce.

Compito: Decidere se affrontare il doxer, segnalare l'incidente all'amministratore del gruppo e alle autorità e sostenere la vittima.

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.