CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Pratiche di educazione non formale:

Morphing e Deepfakes

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.

#13	**Padroneggiare l'enigma digitale: Contrastare i fenomeni di Morphing e Deepfake**
Minaccia/e	**Morphing e Deepfakes**
	Il morphing comporta la manipolazione di immagini digitali attraverso strumenti online, consentendo agli autori, spesso giovani ragazze e donne, di alterare le fotografie pubblicate online per scopi nefasti. Queste immagini alterate possono essere sfruttate per ricattare, creare profili online ingannevoli, fare sexting, partecipare a chat sessuali illecite e generare contenuti pornografici. Gli attacchi di morphing possono comportare l'uso di software di editing delle immagini per combinare le foto biometriche dei passaporti, producendo un'immagine che rappresenta in modo ingannevole un composito di due individui. Allo stesso modo, i deepfake rappresentano una forma sofisticata di manipolazione digitale, in cui le sembianze di una persona in un'immagine o in un video vengono sostituite con quelle di un'altra, creando contenuti altamente realistici ma completamente inventati. I deepfakes comportano rischi significativi nell'ambito delle minacce informatiche giovanili, in quanto contribuiscono alla diffusione di disinformazione, manipolano le percezioni e facilitano il cyberbullismo, amplificando così il potenziale di danno e sfruttamento nel regno digitale.
Tipologia	Analisi critica dei contenuti online
Durata	120 minuti/2 ore (può essere adattato in base all'approfondimento delle attività)
Modalità	In presenza [in aula]
Obiettivo	L'obiettivo di questa pratica è quello di fornire ai partecipanti le competenze e le conoscenze per valutare criticamente le immagini e i video digitali, applicare giudizi etici quando si tratta di contenuti morphed o deepfake, mostrare un comportamento online responsabile e proteggere la propria identità digitale personale.
Obiettivi di apprendimento	Valutare criticamente le immagini digitali: I partecipanti saranno in grado di esaminare criticamente le immagini digitali alla ricerca di segni di manipolazione, applicando la loro comprensione delle tecniche di morphing. Applicare giudizi etici: I partecipanti dimostreranno la capacità di applicare giudizi etici quando creano, condividono o incontrano immagini modificate, riconoscendo i potenziali danni e rispettando i diritti degli individui. Dimostrare un comportamento online responsabile: I partecipanti dimostreranno un comportamento online responsabile, rispettando la privacy, chiedendo il consenso prima di condividere le immagini e scoraggiando la diffusione di informazioni false attraverso immagini modificate. Proteggere l'identità digitale personale: I partecipanti metteranno in atto strategie efficaci per proteggere le immagini e le informazioni personali online, come l'utilizzo di impostazioni di privacy forti, la filigrana delle foto personali e la cautela nel condividere le immagini sui social media.
Profilo del tirocinante	Gruppo di età: 15-17 anni Background educativo: Studenti delle scuole superiori

	Prerequisiti: conoscenza di base dell'uso di Internet e delle piattaforme di social media.
n° partecipanti	15-20 (ideale per facilitare le discussioni e le attività di gruppo)
I materiali	Dispositivi connessi a Internet (laptop/tablet) Proiettore e schermo per le presentazioni Lavagna e pennarelli Dispense stampate con esempi di immagini/video morphed e deepfake Guide e risorse per la verifica dei fatti 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: Assicurarsi che tutti i dispositivi digitali siano collegati a Internet e pre-caricare i siti web e gli esempi pertinenti. Stampare le dispense e assicurarsi che tutto il materiale sia disponibile.
Attuazione	*Introduzione (10 minuti):* Dare il benvenuto ai partecipanti e introdurre l'argomento. Spiegare brevemente le minacce poste dal morphing e dai deepfake. Delineare gli obiettivi e la struttura della sessione (facoltativo). *Presentazione interattiva (30 minuti):* Presentare esempi di contenuti morphed e deepfake. Gli esempi sono riportati nell'Allegato_. Discutete le tecniche utilizzate per creare tali contenuti. Evidenziare le implicazioni del mondo reale e le considerazioni etiche. *Attività di gruppo: Analisi critica (30 minuti):* Dividete i partecipanti in piccoli gruppi (3-4 persone). Fornite a ogni gruppo una serie di immagini e video digitali. Ce ne sono molti disponibili online. Chiedete ai gruppi di identificare i segni di manipolazione e di discutere le loro scoperte. *Giudizi etici e comportamento responsabile (20 minuti):*

	Facilitare una discussione di gruppo sulle implicazioni etiche del morphing e dei deepfakes. Incoraggiare i partecipanti a condividere i loro pensieri sul comportamento responsabile online. Presentare casi reali in cui morphing e deepfakes hanno causato danni. *Protezione dell'identità digitale personale (20 minuti):* Condividere strategie per proteggere le immagini e le informazioni personali online. Dimostrare come utilizzare le impostazioni di privacy e gli strumenti di watermarking. Discutere le migliori pratiche per la condivisione di immagini sui social media. *Domande e risposte e conclusione (10 minuti):* Aprire la discussione per domande e risposte. Riassumete i punti chiave della sessione. Fornire risorse aggiuntive per l'ulteriore apprendimento (facoltativo).
Suggerimenti e consigli	Incoraggiate la partecipazione attiva ponendo domande aperte e stimolando le discussioni. Utilizzate in modo efficace i supporti visivi per illustrare i punti e tenere i partecipanti impegnati. Utilizzate una varietà di esempi, tra cui casi semplici e complessi di morphing e deepfake, per soddisfare diversi livelli di comprensione.
Misure di sicurezza	Garantire la sicurezza di Internet durante le attività online. Creare uno spazio rispettoso e non giudicante per le discussioni.
Valore aggiunto	I partecipanti acquisiranno la capacità di identificare i contenuti manipolati, di comprendere le implicazioni etiche della creazione e della condivisione di contenuti manipolati, di adottare un comportamento online più responsabile, di ridurre il rischio di abusi e di migliorare la propria privacy online, e svilupperanno pensiero critico.
Feedback e valutazione	Incoraggiare i partecipanti a fornire un feedback alla fine della sessione per migliorare le pratiche future.
Conclusione	Questa pratica affronta efficacemente le crescenti minacce poste dal morphing e dai deepfakes, fornendo ai partecipanti competenze e conoscenze essenziali. La pratica non solo migliora l'alfabetizzazione digitale, ma promuove anche un comportamento responsabile e un pensiero critico, allineandosi perfettamente agli obiettivi dichiarati. I partecipanti escono con una maggiore consapevolezza della

	manipolazione digitale e degli strumenti per combatterla, rendendo questa pratica estremamente rilevante e d'impatto nell'odierna era digitale.

Allegato. Stampa di esempi popolari di Morphing e Deepfake

Esempio popolare di morphing
FaceApp e Snapchat Filters: Queste popolari applicazioni consentono agli utenti di scambiare il proprio volto con quello di celebrità o di altre persone. Gli utenti possono scattare una foto e utilizzare gli strumenti dell'app per sovrapporre il volto di una celebrità al proprio, creando immagini divertenti o inquietanti. Ad esempio, le persone spesso scambiano il proprio volto con quello di attori come Leonardo DiCaprio o cantanti come Beyoncé per vedere come apparirebbero come personaggi famosi.
Esempi popolari di deepfake
Il Mandaloriano (serie di Star Wars): Il personaggio di Luke Skywalker, così come era apparso negli anni '80, è stato ricreato utilizzando la tecnologia deepfake nella serie di Star Wars "The Mandalorian". Questo ha permesso al personaggio di apparire molto più giovane dell'età attuale dell'attore.

Figura 1: Il Mandaloriano (serie Star Wars): Il personaggio di Luke Skywalker Deepfake (Fonte: https://nypost.com/2022/02/03/fans-suspect-youtuber-behind-awesome-book-of-boba-fett-cgi/)

Mark Zuckerberg Deepfake: Un video dell'amministratore delegato di Facebook Mark Zuckerberg in cui sembra discutere del controllo dei dati rubati di miliardi di persone. Questo deepfake è stato creato come progetto artistico per evidenziare i problemi di privacy e il potenziale uso improprio della tecnologia deepfake.

Allegato. Tecniche utilizzate per la creazione di contenuti morphing e deepfake

Durante il segmento di presentazione interattiva, il facilitatore deve illustrare le seguenti tecniche utilizzate per creare contenuti morphed e deepfake:

Morphing dell'immagine:

Modifica manuale: Utilizzo di un software come Adobe Photoshop per modificare manualmente le immagini, fondendo le caratteristiche di più foto. Questo include tecniche come la stratificazione, la mascheratura e le modalità di fusione.

Scambio di volti: Utilizzo di strumenti e applicazioni per lo scambio di volti che sostituiscono automaticamente il volto di una persona con quello di un'altra in una foto o in un video.

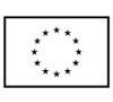
Strumenti AI: Impiego di strumenti di intelligenza artificiale in grado di modificare i volti comprendendo le strutture facciali e apportando modifiche realistiche.

Creazione di deepfake: **Reti avversarie generative (GAN):** Capire come funzionano le GAN, con una rete neurale che genera immagini false e un'altra che cerca di rilevarle, affinando i falsi nel tempo. **Autoencoder:** Utilizzo di autoencoder, reti neurali addestrate per comprimere le immagini e poi ricostruirle, per alterare i volti nei video mappandoli su un volto diverso. **Algoritmi di apprendimento profondo:** Applicazione di algoritmi di deep learning per creare video falsi altamente realistici mediante l'addestramento su grandi set di immagini e video della persona target. **Sintesi vocale:** Utilizza tecnologie text-to-speech e modelli di deep learning per clonare la voce di una persona, rendendo il deepfake ancora più convincente grazie alla sincronizzazione della voce con il video.
Montaggio video: **Montaggio fotogramma per fotogramma:** Modifica manuale dei fotogrammi del video per cambiare le apparenze o le azioni, che richiede molto tempo ma può produrre manipolazioni molto dettagliate. **Motion Tracking:** Utilizzo di un software per tracciare e manipolare il movimento delle caratteristiche in un video, assicurando che i cambiamenti appaiano naturali quando il soggetto si muove. **Lip Syncing:** Impiego di tecnologie di sincronizzazione labiale per far corrispondere i movimenti della bocca di una persona nel video con una traccia audio diversa, spesso utilizzata insieme alla sintesi vocale.

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.