Episodio 5

1. **"Media Literacy 101: Media Online (bot, deep fake, shallow fake)"**

Musica di apertura

CONDUTTORE: Benvenuti a "Media Literacy 101," la serie radiofonica che mira a educare e potenziare gli ascoltatori per navigare nel panorama mediatico in modo critico e informato.

CONDUTTORE: Nell'episodio di oggi ci concentreremo sulla competenza digitale e sulla sicurezza online.

Citazione audio 1: Comprendere Internet e come funziona

CONDUTTORE: Internet è una rete globale di computer che consente alle persone di condividere informazioni e comunicare tra loro. È uno strumento potente che ha cambiato il modo in cui viviamo e lavoriamo. Tuttavia, è importante capire come funziona Internet e i potenziali rischi ad esso associati.

Citazione audio 2: Tecniche utilizzate per diffondere disinformazione

CONDUTTORE: La disinformazione viene spesso diffusa attraverso i social media, dove può essere amplificata da bot e altri account automatizzati. Può anche essere diffusa tramite e-mail, messaggi di testo, forum, chat room, foto, video e altre forme di comunicazione online.

I programmi informatici conosciuti come Intelligenza Artificiale (AI) con la capacità di sostituire video, audio o foto originali, noti come deep fake, stanno diventando una fonte di preoccupazione circa la diffusione di disinformazione e malinformazione. Basta dare un'occhiata ai profili ***deep fake*** di Tom Cruise e Keanu Reeves su Instagram per capire quanto siano convincenti. Questi programmi possono replicare persone reali mentre fanno e dicono cose che non hanno effettivamente fatto o detto. Se stai osservando un politico mentre fa e dice qualcosa in un video, è difficile dubitare della sua autenticità. Qui entra in gioco l'antica "intuizione", e la conoscenza del carattere diventa estremamente importante. Dobbiamo chiederci se ciò che vediamo si allinea con ciò che so di questa persona.

Le "***shallow fake***" sono altrettanto preoccupanti, ma sono create da qualcuno con strumenti di video editing di base. Un contenuto multimediale esistente può essere completamente modificato e manipolato per presentare una storia o un messaggio diverso. L'obiettivo sia dei deep fake che dei shallow fake è distorcere e falsificare.

I *bot* di Internet sono applicazioni software progettate e programmate per completare attività ripetitive automaticamente, e più velocemente, rispetto agli esseri umani, e lavorano 24/7. Esistono diversi tipi di bot, ad esempio Alexa e Siri sono *chatbot* che possono simulare conversazioni. Le piattaforme dei social media hanno bot sociali che influenzano le discussioni online. Se stai facendo acquisti online, i bot di shopping ti aiuteranno a trovare il miglior prezzo per il prodotto che stai cercando.
Gli Spider, noti anche come Crawlers, trovano contenuti per motori di ricerca come Google o Firefox. Tutti questi sono noti come "bot buoni" e possono essere utilizzati per sostituire gli esseri umani in aree come il servizio clienti, il business e l'intrattenimento.

In effetti, le chatbot vengono ora utilizzate nell'assistenza agli adulti anziani per combattere l'isolamento sociale e assistere nelle attività quotidiane.
I bot malevoli sono bot utilizzati per i crimini informatici, e includono gli ***spambot*** che indirizzano gli utenti ai siti web attraverso promozioni pop-up, così che gli ***hacker*** possano attaccare i siti web e raccogliere informazioni personali e sensibili.

Citazione audio 3: Come individuare i bot malevoli

CONDUTTORE: Ci sono diversi modi per sapere se il tuo sistema è stato infettato.

- La connessione Internet è più lenta del solito
- Il computer si blocca senza motivo
- Potrebbe richiedere più tempo del solito per spegnere o riavviare il pc
- Ci sono estensioni nel tuo browser che non hai installato
- Le finestre pop-up appaiono anche quando non stai usando Internet
- Ricevi avvisi che ti invitano a fare clic su un link o il tuo computer verrà infettato
- I tuoi amici ricevono e-mail o messaggi da te che non hai inviato

Citazione audio 4: Suggerimenti per creare password forti e proteggere la tua privacy online

CONDUTTORE: Proteggere la tua privacy online è importante, specialmente perché sempre più nostre informazioni personali vengono condivise online. Approfondiremo in modo più dettagliato nel nostro prossimo episodio come proteggerti online, ma ecco alcuni suggerimenti per creare password forti e proteggere la tua privacy online:

- Usa una combinazione di lettere, numeri e caratteri speciali nelle tue password
- Evita di utilizzare informazioni facilmente indovinabili come il tuo nome o la tua data di nascita
- Stai attento alle reti Wi-Fi pubbliche
- Usa le impostazioni di privacy sui tuoi account social media

Citazione audio 5: Come individuare ed evitare truffe e frodi online

CONDUTTORE: Le truffe e le frodi online possono assumere molte forme, dalle e-mail di phishing ai siti web falsi. Ecco alcuni suggerimenti per individuare ed evitare truffe e frodi online:

- Stai in guardia rispetto alle e-mail e ai messaggi di testo non richiesti
- Stai attento alle offerte che sembrano troppo belle per essere vere
- Non fornire informazioni personali a meno che tu sia certo della legittimità della richiesta
- Controlla gli errori di ortografia e grammatica su siti web o e-mail
- Usa l'autenticazione a due fattori quando disponibile

Citazione audio 6: Ospite

CONDUTTORE: Per spiegare meglio ciò di cui abbiamo discusso oggi, vorrei dare il benvenuto a …….

CONDUTTORE: Nel nostro prossimo episodio ci concentreremo ulteriormente su come proteggerti dalla disinformazione e dalla manipolazione sui social media.

CONDUTTORE: Assicurati di sintonizzarti la prossima settimana per il sesto episodio di "Media Literacy 101". E non dimenticare di visitare il nostro sito web per ulteriori informazioni e risorse sulla media literacy.

Musica di chiusura

CONDUTTORE: Grazie per esservi sintonizzati su "Media Literacy 101". Fino alla prossima volta, rimanete informati, rimanete curiosi e rimanete media literate.

Musica di chiusura