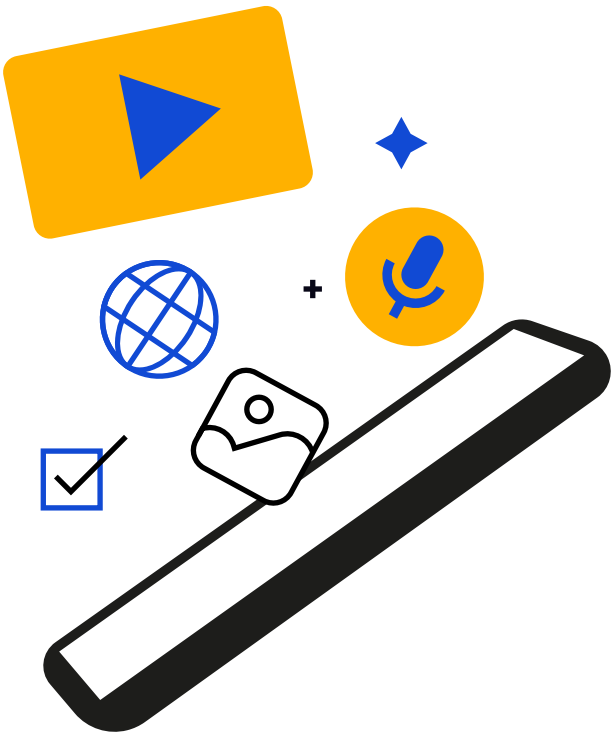
MIM
Ministero dell'Istruzione
e del Merito

SICURNAUTI
LA TUA GUIDA NELLA GALASSIA DIGITALE

L'UTILIZZO SICURO DEI CONTENUTI MULTIMEDIALI

www.unica.istruzione.gov.it

INDICE DEI CONTENUTI

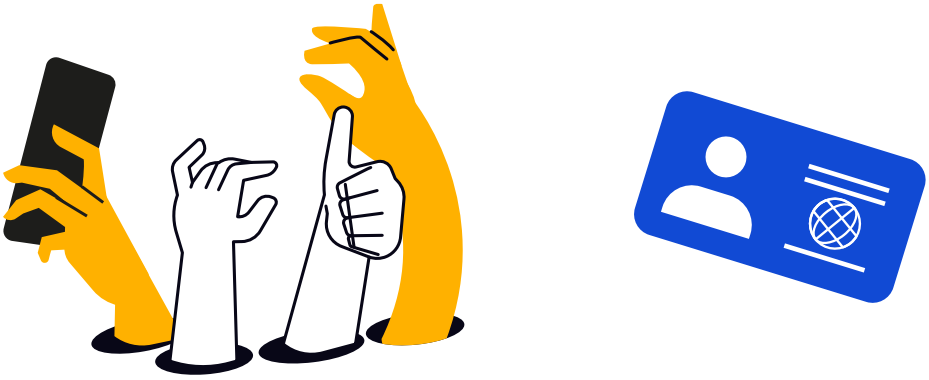


1 INTRODUZIONE: LA SICUREZZA DEI CONTENUTI MULTIMEDIALI NELL'ECOSISTEMA DIGITALE

Ogni giorno milioni di utenti condividono foto, video, registrazioni e messaggi su piattaforme *social*, canali di *streaming* e sistemi di messaggistica, rendendo i contenuti multimediali una **componente centrale** della **comunicazione digitale odierna**.

La rapidità con cui questi contenuti possono essere prodotti e diffusi rende indispensabile sviluppare una **piena consapevolezza** sulle modalità corrette di creazione, gestione e distribuzione di tali materiali.
Non si tratta solo di evitare la sovraesposizione personale, ma anche di comprendere l'impatto che immagini, video e audio possono avere sulla **protezione dei dati personali**, sulla salvaguardia dell'**identità digitale** e sulla conformità a normative come **GDPR** e **diritto d'autore**.

In un contesto in cui i contenuti diventano facilmente riutilizzabili, alterabili (anche tramite sistemi di Intelligenza Artificiale) e conservati *online* nel tempo, la cura nella scelta di cosa pubblicare, con chi condividerlo e per quanto tempo renderlo accessibile rappresenta un elemento chiave per la sicurezza digitale.



2 I PRINCIPALI RISCHI NELL'USO QUOTIDIANO DEI CONTENUTI MULTIMEDIALI

Conoscere i principali rischi e adottare adeguate **misure di sicurezza** è **fondamentale** per un **utilizzo corretto e consapevole dei contenuti** multimediali nella vita quotidiana.
Di seguito vengono illustrati i principali rischi legati alla loro gestione.

Violazione della *privacy*

La condivisione di un'immagine, un video o un audio, può **esporre involontariamente informazioni importanti** della propria vita privata o di quella di altre persone.

Dettagli **apparentemente innocui**, come la posizione geografica, ambienti facilmente riconoscibili, volti, targhe o oggetti sullo sfondo, possono rivelare abitudini, relazioni o dati personali. Una diffusione non consapevole di questi contenuti può favorire usi impropri, furti di identità o altre forme di abuso, **compromettendo** la **riservatezza** e la **sicurezza** degli utenti.

Perdita di controllo sui contenuti

Una volta pubblicato *online*, un **contenuto può essere scaricato**, **ricondiviso** o **manipolato** senza che l'autore abbia più la possibilità di controllarne la destinazione o limitarne la diffusione. La **viralità** e la **difficoltà di tracciamento** aumentano il rischio che informazioni sensibili o materiali personali vengano manipolati o strumentalizzati, con effetti potenzialmente duraturi sulla vita privata, sulla sicurezza digitale e sulla reputazione dell'autore originale.

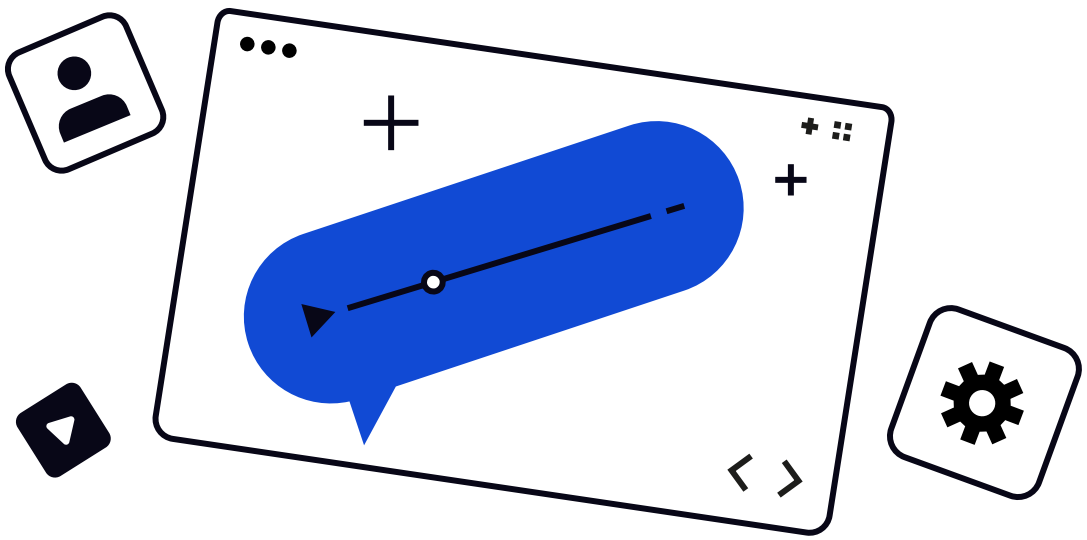
Manipolazione dei contenuti

Le tecnologie di *editing* avanzato e gli strumenti basati sull'Intelligenza Artificiale consentono di modificare immagini, audio e video con un realismo sempre maggiore. I **contenuti alterati** possono far apparire persone o situazioni in contesti mai avvenuti, **diffondere informazioni fuorvianti** o danneggiare la reputazione degli individui coinvolti. Queste manipolazioni, note anche come ***deepfake*** (*Rif. Brochure #5, L'Intelligenza Artificiale in sicurezza*), possono generare confusione, perdita di fiducia e danni d'immagine.

Furto dell'identità digitale

Immagini del volto, documenti o altre informazioni personali possono essere sfruttate dai cybercriminali per **impersonare un altro utente *online***. Con questa pratica, un attaccante può creare profili falsi, inviare messaggi o compiere azioni a nome della vittima, accedendo a servizi digitali o tentando di ingannare terzi. L'impersonificazione digitale non riguarda soltanto la diffusione di immagini, ma **può tradursi in vere e proprie frodi**, come l'accesso non autorizzato a dati personali o finanziari dell'utente.

Inoltre, il furto dell'identità digitale può avere effetti a lungo termine: le informazioni sottratte possono essere conservate e riutilizzate per ulteriori attacchi, come *phishing* mirato, truffe finanziarie o campagne di disinformazione. Le vittime rischiano non solo danni economici, ma anche la compromissione della reputazione personale e professionale. La difficoltà di rimuovere completamente i dati rubati *online* rende questo rischio particolarmente insidioso e persistente.



3 BUONE PRATICHE DI SICUREZZA: CONSIGLI PER UN USO RESPONSABILE DEI CONTENUTI DIGITALI

Per ridurre i rischi legati all'uso e alla diffusione dei contenuti multimediali è necessario adottare **precauzioni concrete e sistematiche**.

Gestione corretta delle impostazioni della *privacy*

Condividi i contenuti solo **con persone di fiducia** e **configura** correttamente le **impostazioni di *privacy*** offerte dalle piattaforme digitali, evitando di rendere pubblici materiali sensibili o non strettamente necessari.

Verifica dei contenuti e approccio prudente

Prima di inoltrare o condividere immagini, video o registrazioni audio create da altri **accertane la provenienza e valutane l'attendibilità**. Alcuni contenuti possono essere manipolati per diffondere informazioni false o generare allarmismi. Prestando attenzione a elementi sospetti e verificando le fonti, è possibile **ridurre il rischio** di contribuire involontariamente alla **diffusione di materiali ingannevoli**.

Protezione dei dispositivi digitali

Per evitare che i contenuti multimediali vengano sottratti o utilizzati in modo improprio, **mantieni i dispositivi aggiornati e protetti**. L'adozione di ***password* robuste**, l'attivazione della **verifica a più fattori** e l'uso di ***software* di sicurezza affidabili** sono misure semplici ma efficaci per ridurre il rischio di accessi non autorizzati e salvaguardare le informazioni presenti sui dispositivi (*Rif. Brochure #7, La sicurezza dei dispositivi mobili*). È inoltre consigliabile **evitare reti Wi-Fi pubbliche non protette**, eseguire ***backup* regolari dei dati** e **utilizzare crittografia locale o in *cloud*** per contenuti sensibili.

Condivisione consapevole dei contenuti

Non pubblicare foto, video o *post* sui *social* che contengano informazioni private, come quelle relative all'attività professionale. Anche **contenuti apparentemente innocui possono rivelare dati sensibili** o documenti riservati, mettendo a rischio la *privacy*, l'incolumità digitale e la reputazione personale o professionale. Valuta sempre il contesto, limita la visibilità dei *post* e utilizza piattaforme sicure per la condivisione di contenuti.

4 CASI REALI DI INCIDENTI

Furto d'identità digitale

Nel settembre del 2025 un uomo residente in provincia di Fermo è stato condannato per aver creato **numerosi profili falsi** sui *social network*, **utilizzando foto e dati personali di terzi** senza il loro consenso.
Attraverso questi profili falsi, **l'autore si spacciava per le vittime** contattando conoscenti, amici o parenti per richiedere ricariche telefoniche, carte prepagate o *voucher* in situazioni di emergenza apparentemente credibili.

Le indagini hanno evidenziato come l'**attività** del truffatore fosse **meticolosamente organizzata**, sfruttando strumenti digitali e *social network* **per rendere i profili quasi indistinguibili da quelli reali**. Ogni profilo creato veniva associato a immagini autentiche e informazioni personali reperite *online*, rendendo più difficile per i destinatari riconoscerne la falsità. L'obiettivo dell'autore non era solo ingannare singoli utenti, ma realizzare uno **schema di frode continuativo**, sfruttando la fiducia delle vittime per ottenere vantaggi economici e materiali.

Manipolazione di contenuti digitali e rischio di frodi *online*

Nel mese di giugno 2025 è stata segnalata una truffa *online* in cui il **volto di un noto giornalista italiano** è stato **utilizzato senza consenso in *post* e annunci sui *social network***, al fine di promuovere presunte piattaforme di investimento.
L'**immagine** del giornalista è stata **manipolata e affiancata a messaggi ingannevoli** che promettevano guadagni rapidi e sicuri, conferendo un'apparente autorevolezza e credibilità ai contenuti fraudolenti.

I messaggi contenevano *link* verso **siti *web*** disegnati per **simulare piattaforme di *trading* e servizi finanziari affidabili**. Gli utenti che cliccavano venivano quindi invitati a fornire dati personali o finanziari, esponendosi così a furti di informazioni e perdite economiche. Le autorità hanno poi scoperto che la campagna fraudolenta era coordinata da un gruppo criminale organizzato che operava sia in Italia che all'estero.

Intervento realizzato dal Ministero dell'Istruzione e del Merito e finanziato a valere sul Fondo per la gestione della cybersicurezza nell'ambito della misura 71 e 73 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 dell'Agenzia per la Cybersicurezza Nazionale

www.unica.istruzione.gov.it