Come riconoscere un'immagine creata dall'intelligenza artificiale

Maria Cattini | 28/07/2026 | Intelligenza Artificiale

Fino a poco tempo fa bastava osservare una fotografia con attenzione. Una mano con sei dita, un testo incomprensibile sullo sfondo, un volto leggermente deformato erano indizi sufficienti per sospettare che quell'immagine fosse stata generata dall'intelligenza artificiale.

Oggi quel metodo funziona sempre meno.

I sistemi più recenti producono immagini estremamente credibili. Riescono a riprodurre volti, animali, oggetti e ambienti con un livello di precisione che rende quasi inutile cercare piccoli errori grafici. Chi continua a basarsi solo sull'aspetto dell'immagine rischia di cadere proprio nella trappola costruita dai truffatori.

Il vero cambiamento riguarda il modo di verificare una fotografia. Non bisogna più chiedersi se "sembra vera", ma se esistono elementi che permettono di dimostrarne l'origine.

L'immagine è solo una parte della storia

Una fotografia non convince perché è perfetta.

Convince perché arriva insieme a una storia capace di suscitare emozioni.

Le campagne fraudolente costruite con immagini generate dall'intelligenza artificiale seguono quasi sempre questo schema: una situazione urgente, un invito ad agire rapidamente e la richiesta finale di denaro o informazioni personali. L'immagine serve soltanto ad aumentare la credibilità del racconto.

Questo cambia completamente il modo di affrontare il problema.

Invece di analizzare ogni singolo dettaglio grafico, conviene osservare il contesto.

Chi pubblica l'immagine?

Quando è comparsa per la prima volta?

È presente anche su altri siti?

Esistono fonti indipendenti che confermano quanto viene raccontato?

Sono domande molto più utili del classico "questa mano mi sembra strana".

Perché il nostro cervello continua a fidarsi delle immagini

Le fotografie hanno sempre avuto un enorme potere persuasivo.

© 2026 Coondivido — Tutti i diritti sono riservati

Per decenni sono state considerate una prova visiva di ciò che era realmente accaduto. Anche sapendo che oggi un'immagine può essere generata in pochi secondi, il nostro cervello continua ad attribuirle automaticamente un elevato livello di credibilità.

È proprio questo meccanismo psicologico che viene sfruttato nelle campagne fraudolente.

Quando un contenuto genera empatia, paura o senso di urgenza, molte persone interrompono il processo di verifica e reagiscono d'impulso.

L'obiettivo non è ingannare tutti.

È convincere abbastanza persone prima che qualcuno inizi a fare domande.

Cinque verifiche che richiedono meno di cinque minuti

Quando un'immagine accompagna una richiesta di denaro, una raccolta fondi o una notizia particolarmente sorprendente, vale la pena dedicare pochi minuti alla verifica.

1. Cerca l'immagine sul web

La ricerca inversa rimane uno dei controlli più efficaci.

Se la fotografia esiste da tempo, oppure è stata pubblicata con un contesto completamente diverso, è probabile che qualcuno la stia riutilizzando per costruire una narrazione ingannevole.

Naturalmente questo controllo non basta da solo. Un'immagine generata ex novo potrebbe non comparire ancora da nessuna parte.

2. Controlla chi la sta pubblicando

Un account creato da pochi giorni, con pochissimi contenuti e una storia poco coerente, merita molta più attenzione rispetto a un profilo consolidato.

L'affidabilità della fonte conta spesso più dell'immagine stessa.

3. Cerca conferme indipendenti

Se un fatto è realmente accaduto, è probabile che esistano altre testimonianze, fotografie o fonti che ne parlano.

Quando tutto ruota attorno a una sola immagine e a un solo account, la prudenza è d'obbligo.

4. Verifica la provenienza quando possibile

Alcuni sistemi consentono di individuare informazioni sulla provenienza del file o eventuali filigrane inserite durante la generazione automatica.

Questi controlli non forniscono una risposta definitiva, ma rappresentano un ulteriore elemento da aggiungere alla valutazione complessiva. Il materiale di riferimento ricorda che anche questi strumenti hanno limiti: l'assenza di una filigrana non dimostra che l'immagine sia autentica e la presenza di credenziali descrive l'origine del file, non la veridicità della scena rappresentata.

5. Chiediti sempre chi trae vantaggio dalla tua reazione

Questa domanda vale più di qualsiasi software.

Se qualcuno ti chiede di inviare soldi, dati personali o credenziali basandosi quasi esclusivamente su una fotografia, fermati.

© 2026 Coondivido — Tutti i diritti sono riservati

L'urgenza è uno degli strumenti più efficaci nelle campagne di truffa.

Quando la fotografia diventa un'esca

Le immagini create con l'intelligenza artificiale raramente circolano da sole. Quasi sempre accompagnano una storia costruita per ottenere qualcosa: denaro, fiducia, dati personali o visibilità.

Il documento di riferimento richiama alcuni degli scenari più frequenti.

Raccolte fondi emotive

Una fotografia mostra una persona in difficoltà, un bambino, un animale ferito o una famiglia colpita da una tragedia. Il testo invita a donare immediatamente perché "ogni minuto conta".

L'immagine può essere completamente artificiale oppure rappresentare una scena che non ha alcun legame con la storia raccontata.

Prima di effettuare una donazione conviene verificare chi organizza la raccolta, se esiste un sito ufficiale, se altre fonti parlano della stessa iniziativa e se l'ente indicato risulta realmente coinvolto.

Annunci di animali smarriti

Le fotografie di cani e gatti suscitano una forte reazione emotiva. Per questo vengono spesso condivise migliaia di volte in poche ore.

Anche in questo caso il controllo non dovrebbe fermarsi all'immagine. È utile verificare dove è stato pubblicato l'annuncio, se il profilo che lo diffonde ha una storia coerente e se le informazioni coincidono con quelle presenti nei canali locali dedicati agli animali smarriti.

Falsi profili sentimentali

Le piattaforme di incontri e i social network rappresentano un altro contesto delicato. Un volto realistico non garantisce che dietro quell'account esista davvero la persona mostrata nella fotografia.

L'immagine può essere stata generata appositamente per creare un'identità credibile, difficile da rintracciare tramite le normali ricerche online.

Finti artisti e opere inesistenti

Le immagini generate dall'IA consentono anche di creare portfolio convincenti, opere mai realizzate o presunti autori che non esistono.

Quando un artista compare improvvisamente con decine di lavori perfetti ma senza alcuna presenza documentata nel tempo, vale la pena approfondire la verifica prima di acquistare un'opera o promuoverne il lavoro.

Gli errori che favoriscono la disinformazione

Molti controlli falliscono non perché manchino gli strumenti, ma perché vengono usati nel modo sbagliato.

L'errore più comune consiste nel cercare un unico elemento che dimostri se un'immagine è autentica oppure no.

Nella pratica funziona raramente.

Una ricerca inversa potrebbe non trovare nulla semplicemente perché l'immagine è stata pubblicata

© 2026 Coondivido — Tutti i diritti sono riservati

da pochi minuti. Allo stesso modo, la presenza di credenziali o filigrane descrive il percorso del file, non certifica che ciò che vediamo corrisponda a un fatto realmente accaduto. Il documento insiste proprio su questo aspetto: nessun indicatore, preso isolatamente, basta per arrivare a una conclusione.

Un secondo errore è lasciarsi guidare dall'emotività. Più una fotografia suscita indignazione, paura o compassione, maggiore dovrebbe essere l'attenzione dedicata alla verifica.

Un caso pratico

Immagina di ricevere sui social una fotografia di un cucciolo apparentemente abbandonato.

Il post racconta che l'animale ha bisogno di cure urgenti e invita a inviare un contributo economico tramite un link.

In pochi minuti puoi eseguire una verifica ragionata:

1. Controlli quando è stato creato il profilo che pubblica l'appello.
2. Cerchi la stessa storia su siti o pagine locali.
3. Effettui una ricerca inversa dell'immagine.
4. Verifichi se l'associazione indicata esiste davvero e utilizza quel canale ufficiale.
5. Valuti se il messaggio insiste soprattutto sull'urgenza oppure fornisce elementi verificabili.

Nessuno di questi controlli, da solo, dimostra che il post sia autentico o falso. Insieme permettono però di raccogliere indizi sufficienti per decidere se fidarsi oppure attendere ulteriori conferme.

È questo il passaggio che distingue una verifica da un'impressione.

Il metodo conta più dell'occhio

L'evoluzione dell'intelligenza artificiale rende sempre più difficile riconoscere un'immagine osservandola soltanto.

Di conseguenza cambia anche il modo di difendersi.

Non serve allenarsi a trovare il pixel fuori posto o la mano con un dito in più. Questi dettagli possono ancora comparire, ma non rappresentano più il criterio principale.

La verifica diventa un processo composto da più elementi: origine del contenuto, autore, cronologia della pubblicazione, conferme indipendenti e contesto.

Quando questi tasselli raccontano la stessa storia, la fiducia aumenta.

Quando si contraddicono, la prudenza rimane la scelta migliore.

Un'immagine convincente non costituisce una prova. È soltanto uno degli elementi da valutare. Ed è proprio questa consapevolezza che oggi rappresenta la difesa più efficace contro fotografie artificiali usate per manipolare, truffare o diffondere informazioni fuorvianti.

Cosa fare se sospetti che un'immagine sia falsa

Se una fotografia ti convince al punto da spingerti ad agire subito, è proprio quello il momento in cui dovresti rallentare.

Il documento da cui prende spunto questo articolo suggerisce una serie di azioni semplici ma efficaci quando si sospetta una truffa costruita con immagini generate dall'intelligenza artificiale.

© 2026 Coondivido — Tutti i diritti sono riservati

Conserva le prove

Prima di segnalare un profilo o cancellare una conversazione, salva gli elementi disponibili.

Uno screenshot dell'immagine, del profilo e dei messaggi può rivelarsi utile se la pagina viene eliminata poche ore dopo.

Interrompi ogni pagamento

Molte campagne fraudolente puntano a ottenere un primo versamento di piccola entità. Successivamente arriva una nuova richiesta con una motivazione diversa.

Se iniziano a emergere dubbi sull'autenticità della storia, interrompi immediatamente qualsiasi trasferimento di denaro.

Proteggi i tuoi dati

Se hai condiviso password, coordinate bancarie o altre informazioni sensibili, il problema non riguarda più soltanto l'immagine.

In questo caso è opportuno modificare le credenziali coinvolte e contattare rapidamente il proprio istituto bancario quando sono stati comunicati dati finanziari.

Segnala il profilo

Ogni piattaforma mette a disposizione procedure per segnalare account fraudolenti.

Una singola segnalazione potrebbe non produrre effetti immediati, ma contribuisce ad alimentare i sistemi di controllo automatici e le verifiche manuali.

L'intelligenza artificiale non è il problema

Sarebbe facile attribuire ogni responsabilità all'IA.

La realtà è più complessa.

L'intelligenza artificiale genera immagini. Sono le persone a decidere come impiegarle.

Lo stesso sistema che consente di creare illustrazioni, ricostruzioni storiche o materiale didattico può essere sfruttato anche per inventare identità inesistenti, costruire campagne di disinformazione o rendere più credibili tentativi di truffa.

Per questo motivo la risposta non consiste nel diffidare di qualsiasi immagine.

Consiste nel cambiare metodo. Per oltre un secolo abbiamo attribuito alla fotografia un valore quasi documentale. Oggi quel presupposto non basta più.

Una fotografia può continuare a rappresentare un fatto reale, ma non possiamo considerarla una prova soltanto perché appare convincente.

La verifica richiede qualcosa di diverso: confrontare fonti, ricostruire il contesto, individuare chi ha pubblicato il contenuto e capire quale interesse potrebbe avere.

È un processo leggermente più lungo rispetto a osservare una fotografia per pochi secondi.

Ma è anche molto più affidabile.
Fino a poco tempo fa bastava osservare una fotografia con attenzione. Una mano con sei dita, un testo incomprensibile sullo sfondo, un volto leggermente deformato erano indizi sufficienti per

© 2026 Coondivido — Tutti i diritti sono riservati

sospettare che quell'immagine fosse stata generata dall'intelligenza artificiale.

Oggi quel metodo funziona sempre meno.

I sistemi più recenti producono immagini estremamente credibili. Riescono a riprodurre volti, animali, oggetti e ambienti con un livello di precisione che rende quasi inutile cercare piccoli errori grafici. Chi continua a basarsi solo sull'aspetto dell'immagine rischia di cadere proprio nella trappola costruita dai truffatori.

Il vero cambiamento riguarda il modo di verificare una fotografia. Non bisogna più chiedersi se "sembra vera", ma se esistono elementi che permettono di dimostrarne l'origine.

L'immagine è solo una parte della storia

Una fotografia non convince perché è perfetta.

Convince perché arriva insieme a una storia capace di suscitare emozioni.

Le campagne fraudolente costruite con immagini generate dall'intelligenza artificiale seguono quasi sempre questo schema: una situazione urgente, un invito ad agire rapidamente e la richiesta finale di denaro o informazioni personali. L'immagine serve soltanto ad aumentare la credibilità del racconto.

Questo cambia completamente il modo di affrontare il problema.

Invece di analizzare ogni singolo dettaglio grafico, conviene osservare il contesto.

Chi pubblica l'immagine?

Quando è comparsa per la prima volta?

È presente anche su altri siti?

Esistono fonti indipendenti che confermano quanto viene raccontato?

Sono domande molto più utili del classico "questa mano mi sembra strana".

Perché il nostro cervello continua a fidarsi delle immagini

Le fotografie hanno sempre avuto un enorme potere persuasivo.

Per decenni sono state considerate una prova visiva di ciò che era realmente accaduto. Anche sapendo che oggi un'immagine può essere generata in pochi secondi, il nostro cervello continua ad attribuirle automaticamente un elevato livello di credibilità.

È proprio questo meccanismo psicologico che viene sfruttato nelle campagne fraudolente.

Quando un contenuto genera empatia, paura o senso di urgenza, molte persone interrompono il processo di verifica e reagiscono d'impulso.

L'obiettivo non è ingannare tutti.

È convincere abbastanza persone prima che qualcuno inizi a fare domande.

Cinque verifiche che richiedono meno di cinque minuti

Quando un'immagine accompagna una richiesta di denaro, una raccolta fondi o una notizia particolarmente sorprendente, vale la pena dedicare pochi minuti alla verifica.

© 2026 Coondivido — Tutti i diritti sono riservati

1. Cerca l'immagine sul web

La ricerca inversa rimane uno dei controlli più efficaci.

Se la fotografia esiste da tempo, oppure è stata pubblicata con un contesto completamente diverso, è probabile che qualcuno la stia riutilizzando per costruire una narrazione ingannevole.

Naturalmente questo controllo non basta da solo. Un'immagine generata ex novo potrebbe non comparire ancora da nessuna parte.

2. Controlla chi la sta pubblicando

Un account creato da pochi giorni, con pochissimi contenuti e una storia poco coerente, merita molta più attenzione rispetto a un profilo consolidato.

L'affidabilità della fonte conta spesso più dell'immagine stessa.

3. Cerca conferme indipendenti

Se un fatto è realmente accaduto, è probabile che esistano altre testimonianze, fotografie o fonti che ne parlano.

Quando tutto ruota attorno a una sola immagine e a un solo account, la prudenza è d'obbligo.

4. Verifica la provenienza quando possibile

Alcuni sistemi consentono di individuare informazioni sulla provenienza del file o eventuali filigrane inserite durante la generazione automatica.

Questi controlli non forniscono una risposta definitiva, ma rappresentano un ulteriore elemento da aggiungere alla valutazione complessiva. Il materiale di riferimento ricorda che anche questi strumenti hanno limiti: l'assenza di una filigrana non dimostra che l'immagine sia autentica e la presenza di credenziali descrive l'origine del file, non la veridicità della scena rappresentata.

5. Chiediti sempre chi trae vantaggio dalla tua reazione

Questa domanda vale più di qualsiasi software.

Se qualcuno ti chiede di inviare soldi, dati personali o credenziali basandosi quasi esclusivamente su una fotografia, fermati.

L'urgenza è uno degli strumenti più efficaci nelle campagne di truffa.

Quando la fotografia diventa un'esca

Le immagini create con l'intelligenza artificiale raramente circolano da sole. Quasi sempre accompagnano una storia costruita per ottenere qualcosa: denaro, fiducia, dati personali o visibilità.

Il documento di riferimento richiama alcuni degli scenari più frequenti.

Raccolte fondi emotive

Una fotografia mostra una persona in difficoltà, un bambino, un animale ferito o una famiglia colpita da una tragedia. Il testo invita a donare immediatamente perché "ogni minuto conta".

L'immagine può essere completamente artificiale oppure rappresentare una scena che non ha alcun legame con la storia raccontata.

© 2026 Coondivido — Tutti i diritti sono riservati

Prima di effettuare una donazione conviene verificare chi organizza la raccolta, se esiste un sito ufficiale, se altre fonti parlano della stessa iniziativa e se l'ente indicato risulta realmente coinvolto.

Annunci di animali smarriti

Le fotografie di cani e gatti suscitano una forte reazione emotiva. Per questo vengono spesso condivise migliaia di volte in poche ore.

Anche in questo caso il controllo non dovrebbe fermarsi all'immagine. È utile verificare dove è stato pubblicato l'annuncio, se il profilo che lo diffonde ha una storia coerente e se le informazioni coincidono con quelle presenti nei canali locali dedicati agli animali smarriti.

Falsi profili sentimentali

Le piattaforme di incontri e i social network rappresentano un altro contesto delicato. Un volto realistico non garantisce che dietro quell'account esista davvero la persona mostrata nella fotografia.

L'immagine può essere stata generata appositamente per creare un'identità credibile, difficile da rintracciare tramite le normali ricerche online.

Finti artisti e opere inesistenti

Le immagini generate dall'IA consentono anche di creare portfolio convincenti, opere mai realizzate o presunti autori che non esistono.

Quando un artista compare improvvisamente con decine di lavori perfetti ma senza alcuna presenza documentata nel tempo, vale la pena approfondire la verifica prima di acquistare un'opera o promuoverne il lavoro.

Gli errori che favoriscono la disinformazione

Molti controlli falliscono non perché manchino gli strumenti, ma perché vengono usati nel modo sbagliato.

L'errore più comune consiste nel cercare un unico elemento che dimostri se un'immagine è autentica oppure no.

Nella pratica funziona raramente.

Una ricerca inversa potrebbe non trovare nulla semplicemente perché l'immagine è stata pubblicata da pochi minuti. Allo stesso modo, la presenza di credenziali o filigrane descrive il percorso del file, non certifica che ciò che vediamo corrisponda a un fatto realmente accaduto. Il documento insiste proprio su questo aspetto: nessun indicatore, preso isolatamente, basta per arrivare a una conclusione.

Un secondo errore è lasciarsi guidare dall'emotività. Più una fotografia suscita indignazione, paura o compassione, maggiore dovrebbe essere l'attenzione dedicata alla verifica.

Un caso pratico

Immagina di ricevere sui social una fotografia di un cucciolo apparentemente abbandonato.

Il post racconta che l'animale ha bisogno di cure urgenti e invita a inviare un contributo economico tramite un link.

In pochi minuti puoi eseguire una verifica ragionata:

© 2026 Coondivido — Tutti i diritti sono riservati

1. Controlli quando è stato creato il profilo che pubblica l'appello.
2. Cerchi la stessa storia su siti o pagine locali.
3. Effettui una ricerca inversa dell'immagine.
4. Verifichi se l'associazione indicata esiste davvero e utilizza quel canale ufficiale.
5. Valuti se il messaggio insiste soprattutto sull'urgenza oppure fornisce elementi verificabili.

Nessuno di questi controlli, da solo, dimostra che il post sia autentico o falso. Insieme permettono però di raccogliere indizi sufficienti per decidere se fidarsi oppure attendere ulteriori conferme.

È questo il passaggio che distingue una verifica da un'impressione.

Il metodo conta più dell'occhio

L'evoluzione dell'intelligenza artificiale rende sempre più difficile riconoscere un'immagine osservandola soltanto.

Di conseguenza cambia anche il modo di difendersi.

Non serve allenarsi a trovare il pixel fuori posto o la mano con un dito in più. Questi dettagli possono ancora comparire, ma non rappresentano più il criterio principale.

La verifica diventa un processo composto da più elementi: origine del contenuto, autore, cronologia della pubblicazione, conferme indipendenti e contesto.

Quando questi tasselli raccontano la stessa storia, la fiducia aumenta.

Quando si contraddicono, la prudenza rimane la scelta migliore.

Un'immagine convincente non costituisce una prova. È soltanto uno degli elementi da valutare. Ed è proprio questa consapevolezza che oggi rappresenta la difesa più efficace contro fotografie artificiali usate per manipolare, truffare o diffondere informazioni fuorvianti.

Cosa fare se sospetti che un'immagine sia falsa

Se una fotografia ti convince al punto da spingerti ad agire subito, è proprio quello il momento in cui dovresti rallentare.

Il documento da cui prende spunto questo articolo suggerisce una serie di azioni semplici ma efficaci quando si sospetta una truffa costruita con immagini generate dall'intelligenza artificiale.

Conserva le prove

Prima di segnalare un profilo o cancellare una conversazione, salva gli elementi disponibili.

Uno screenshot dell'immagine, del profilo e dei messaggi può rivelarsi utile se la pagina viene eliminata poche ore dopo.

Interrompi ogni pagamento

Molte campagne fraudolente puntano a ottenere un primo versamento di piccola entità. Successivamente arriva una nuova richiesta con una motivazione diversa.

Se iniziano a emergere dubbi sull'autenticità della storia, interrompi immediatamente qualsiasi trasferimento di denaro.

Proteggi i tuoi dati

© 2026 Coondivido — Tutti i diritti sono riservati

Se hai condiviso password, coordinate bancarie o altre informazioni sensibili, il problema non riguarda più soltanto l'immagine.

In questo caso è opportuno modificare le credenziali coinvolte e contattare rapidamente il proprio istituto bancario quando sono stati comunicati dati finanziari.

Segnala il profilo

Ogni piattaforma mette a disposizione procedure per segnalare account fraudolenti.

Una singola segnalazione potrebbe non produrre effetti immediati, ma contribuisce ad alimentare i sistemi di controllo automatici e le verifiche manuali.

L'intelligenza artificiale non è il problema

Sarebbe facile attribuire ogni responsabilità all'IA.

La realtà è più complessa.

L'intelligenza artificiale genera immagini. Sono le persone a decidere come impiegarle.

Lo stesso sistema che consente di creare illustrazioni, ricostruzioni storiche o materiale didattico può essere sfruttato anche per inventare identità inesistenti, costruire campagne di disinformazione o rendere più credibili tentativi di truffa.

Per questo motivo la risposta non consiste nel diffidare di qualsiasi immagine.

Consiste nel cambiare metodo. Per oltre un secolo abbiamo attribuito alla fotografia un valore quasi documentale. Oggi quel presupposto non basta più.

Una fotografia può continuare a rappresentare un fatto reale, ma non possiamo considerarla una prova soltanto perché appare convincente.

La verifica richiede qualcosa di diverso: confrontare fonti, ricostruire il contesto, individuare chi ha pubblicato il contenuto e capire quale interesse potrebbe avere.

È un processo leggermente più lungo rispetto a osservare una fotografia per pochi secondi.

Ma è anche molto più affidabile.

© 2026 Coondivido — Tutti i diritti sono riservati